

*IBM Spectrum Protect Knowledge Center Version 8.1.2*



---

# Tabla de contenido

<b>Bienvenido</b>	1
<b>Accesibilidad</b>	1
<b>Suites de producto y productos relacionados</b>	2
<b>Archivos PDF</b>	4
<b>Actualizaciones en este release</b>	4
<b>Conceptos de IBM Spectrum Protect</b>	5
Visión general de IBM Spectrum Protect	5
Componentes de protección de datos	5
Servicios de protección de datos	6
Procesos de gestión de protección de datos	8
Interfaces de usuario	10
Conceptos de almacenamiento de datos	11
Dispositivos de almacenamiento de datos	12
Agrupaciones de almacenamiento	15
Transporte de datos a almacenar	19
Estrategias de protección de datos	22
Minimización del espacio de almacenamiento de copias de seguridad	22
Estrategias de protección ante desastres	23
Conceptos de la recuperación tras desastre	26
<b>Soluciones de protección de datos</b>	28
Selección de una solución de protección de datos	28
Solución de disco de sitio único	28
Solución de disco multisitio	29
Solución de dispositivo multisitio	30
Solución de cinta	31
Comparación de soluciones	32
Hoja de ruta de la solución	34
Solución de disco de sitio único	34
Planificación	35
Selección de un tamaño del sistema	36
Requisitos del sistema para una solución de disco de sitio único	36
Requisitos de hardware	36
Requisitos de software	38
Planificación de hojas de trabajo	39
Planificación de almacenamiento	48
Planificación de la seguridad	49
Planificación de los roles de administración	49
Planificación para comunicaciones seguras	49
Planificación de almacenamiento de datos cifrados	50
Planificación del acceso de cortafuegos	50
Implementación	51
Configuración del sistema	52
Configuración del hardware de almacenamiento	52
Instalación del sistema operativo del servidor	52
Instalación en sistemas AIX	53
Instalación en sistemas Linux	54

Instalación en sistemas Windows	57
Configuración de E/S de la multivía de acceso	58
Sistemas AIX	58
Sistemas Linux	59
Sistemas Windows	60
Creación del ID de usuario para el servidor	61
Preparación de sistemas de archivos para el servidor	61
Sistemas AIX	62
Sistemas Linux	63
sistemas Windows	63
Instalación del servidor y Centro de operaciones	64
Instalación en sistemas AIX y Linux	64
Instalación en sistemas Windows	65
Configuración del servidor y el Centro de operaciones	66
Configuración de la instancia de servidor	66
Instalación del cliente de archivado y copia de seguridad	67
Configuración de opciones para el servidor	67
Configuración de comunicaciones seguras con Seguridad de la capa de transporte	68
Configuración de Centro de operaciones	69
Registro de la licencia de producto	69
Configuración de la optimización de almacenamiento de datos	70
Definición de las reglas de retención de datos para su empresa	70
Definición de planificaciones para actividades de mantenimiento del servidor	71
Definición de planificaciones de cliente	73
Instalación y configuración de clientes de archivado y copia de seguridad	73
Registro y asignación de clientes a planificaciones	73
Instalación del servicio de gestión de cliente	74
Verificación de que el servicio de gestión de clientes está instalado correctamente	74
Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente	75
Finalización de la implementación	76
Supervisión	76
Lista de comprobación diaria	77
Lista de comprobación periódica	81
Verificación de la conformidad de licencia	87
Seguimiento del estado del sistema mediante informes de correo electrónico	88
Gestión	89
Gestión del Centro de operaciones	90
Adición y eliminación de servidores spoke	90
Adición de un servidor de radio	90
Eliminación de un servidor spoke	91
Inicio y detención del servidor web	91
Reinicio del asistente de configuración inicial	92
Cambio del servidor concentrador	92
Restauración de la configuración a un estado de preconfiguración	93
Protección de aplicaciones, máquinas virtuales y sistemas	94
Adición de clientes	94
Selección del software de cliente y planificación de la instalación	95
Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	96
Visualización de políticas	97
Edición de políticas	97
Planificación de copia de seguridad y operaciones de archivado	99
Registro de clientes	99
Instalación y configuración de clientes	100
Configuración del cliente para ejecutar las operaciones planificadas	101
Configuración de comunicaciones a través de un cortafuegos	103
Gestión de operaciones de cliente	104
Evaluación de errores en registros de errores de cliente	104
Detención y reinicio del aceptador de cliente	105

Restablecimiento de contraseñas	106
Modificación del ámbito de una copia de seguridad de cliente	106
Gestión de actualizaciones del cliente	107
Poner fuera de servicio un nodo cliente	108
Desactivación de datos para liberar espacio de almacenamiento	109
Gestión del almacenamiento de datos	110
Auditoría de un contenedor de la agrupación de almacenamiento	110
Gestión de la capacidad de inventario	111
Gestión del uso de la memoria y del procesador	112
Ajuste de actividades planificadas	113
Protección del servidor	113
Conceptos sobre la seguridad	114
Gestión de administradores	116
Cambio de los requisitos de contraseña	116
Protección del servidor en el sistema	117
Restricción del acceso de usuario al servidor	118
Limitación de acceso a través de restricciones de puerto	118
Detención e inicio del servidor	119
Detención del servidor	119
Inicio del servidor para tareas de mantenimiento o reconfiguración	120
Planificación para actualizar el servidor	120
Preparación para una parada	121
Implementación de un plan de recuperación tras desastre	121
Recuperación de paradas del sistema	122
Solución de disco multisitio	122
Planificación	123
Selección de un tamaño del sistema	124
Planificación de los sitios	125
Requisitos del sistema para una solución de disco multisitio	126
Requisitos de hardware	126
Requisitos de software	127
Planificación de hojas de trabajo	129
Planificación de almacenamiento	138
Planificación de la seguridad	139
Planificación de los roles de administración	139
Planificación para comunicaciones seguras	139
Planificación de almacenamiento de datos cifrados	140
Planificación del acceso de cortafuegos	140
Implementación	141
Configuración del sistema	142
Configuración del hardware de almacenamiento	142
Instalación del sistema operativo del servidor	142
Instalación en sistemas AIX	143
Instalación en sistemas Linux	144
Instalación en sistemas Windows	147
Configuración de E/S de la multivía de acceso	148
Sistemas AIX	148
Sistemas Linux	149
Sistemas Windows	150
Creación del ID de usuario para el servidor	151
Preparación de sistemas de archivos para el servidor	151
Sistemas AIX	152
Sistemas Linux	153
sistemas Windows	153
Instalación del servidor y Centro de operaciones	154
Instalación en sistemas AIX y Linux	154
Instalación en sistemas Windows	155
Configuración del servidor y el Centro de operaciones	156

Configuración de la instancia de servidor	156
Instalación del cliente de archivado y copia de seguridad	157
Configuración de opciones para el servidor	157
Configuración de comunicaciones seguras con Seguridad de la capa de transporte	158
Configuración de Centro de operaciones	159
Registro de la licencia de producto	160
Configuración de la optimización de almacenamiento de datos	160
Definición de las reglas de retención de datos para su empresa	161
Definición de planificaciones para actividades de mantenimiento del servidor	161
Definición de planificaciones de cliente	163
Instalación y configuración de clientes de archivado y copia de seguridad	163
Registro y asignación de clientes a planificaciones	164
Instalación del servicio de gestión de cliente	164
Verificación de que el servicio de gestión de clientes está instalado correctamente	165
Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente	166
Configuración del segundo servidor	166
Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke	167
Añadir un segundo servidor como servidor spoke	168
Habilitación de réplica	168
Finalización de la implementación	168
Supervisión	169
Lista de comprobación diaria	169
Lista de comprobación periódica	174
Verificación de la conformidad de licencia	180
Seguimiento del estado del sistema mediante informes de correo electrónico	181
Gestión	182
Gestión del Centro de operaciones	183
Adición y eliminación de servidores spoke	183
Adición de un servidor de radio	183
Eliminación de un servidor spoke	184
Inicio y detención del servidor web	184
Reinicio del asistente de configuración inicial	185
Cambio del servidor concentrador	185
Restauración de la configuración a un estado de preconfiguración	186
Protección de aplicaciones, máquinas virtuales y sistemas	187
Adición de clientes	187
Selección del software de cliente y planificación de la instalación	188
Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	190
Visualización de políticas	190
Edición de políticas	191
Planificación de copia de seguridad y operaciones de archivado	192
Registro de clientes	192
Instalación y configuración de clientes	193
Configuración del cliente para ejecutar las operaciones planificadas	194
Configuración de comunicaciones a través de un cortafuegos	196
Gestión de operaciones de cliente	197
Evaluación de errores en registros de errores de cliente	197
Detención y reinicio del aceptador de cliente	198
Restablecimiento de contraseñas	199
Modificación del ámbito de una copia de seguridad de cliente	199
Gestión de actualizaciones del cliente	200
Poner fuera de servicio un nodo cliente	201
Desactivación de datos para liberar espacio de almacenamiento	203
Gestión del almacenamiento de datos	203
Auditoría de un contenedor de la agrupación de almacenamiento	204
Gestión de la capacidad de inventario	204
Gestión del uso de la memoria y del procesador	206
Ajuste de actividades planificadas	206

Gestión de la réplica	207
Compatibilidad de réplica	207
Habilitación de la réplica de nodo	208
Protección de datos en agrupaciones de almacenamiento de contenedor de directorios	208
Modificación de los valores de réplica	210
Establecimiento de distintas políticas de retención	210
Protección del servidor	211
Conceptos sobre la seguridad	211
Gestión de administradores	213
Cambio de los requisitos de contraseña	214
Protección de IBM Spectrum Protect en el sistema	215
Restricción del acceso de usuario al servidor	215
Limitación de acceso a través de restricciones de puerto	216
Detención e inicio del servidor	216
Detención del servidor	216
Inicio del servidor para tareas de mantenimiento o reconfiguración	217
Planificación para actualizar el servidor	218
Preparación para una parada	219
Implementación de un plan de recuperación tras desastre	219
Recuperación de pérdida de datos o de paradas del sistema	219
Restauración de la base de datos	222
Recuperación de datos dañados	223
Reparación de agrupaciones de almacenamiento	224
Solución de cinta	224
Planificación	225
Requisitos de planificación de cinta	226
Requisitos del sistema para una solución basada en cinta	226
Requisitos de hardware	226
Requisitos de software	229
Planificación de hojas de trabajo	230
Planificación del almacenamiento en disco	234
Planificación del almacenamiento en cinta	234
Dispositivos de cinta y bibliotecas soportados	235
Configuraciones de dispositivos de cinta soportadas	236
Movimiento de datos entre dispositivos de almacenamiento	236
Compartición de bibliotecas	237
Movimiento de datos sin LAN	237
Mezcla de tipos de dispositivos en una biblioteca	237
Diferentes generaciones de medios en una biblioteca	238
Mezcla de medios y agrupaciones de almacenamiento	239
Definiciones necesarias para dispositivos de almacenamiento en cinta	239
Planificación de la jerarquía de agrupaciones de almacenamiento	240
Almacenamiento de datos fuera del local	242
Planificación de la seguridad	242
Planificación de los roles de administración	243
Planificación para comunicaciones seguras	243
Planificación de almacenamiento de datos cifrados	244
Planificación del acceso de cortafuegos	244
Implementación	245
Configuración del sistema	246
Configuración del hardware de almacenamiento	247
Instalación del sistema operativo del servidor	247
Instalación en sistemas AIX	247
Instalación en sistemas Linux	249
Instalación en sistemas Windows	252
Configuración de E/S de la multivía de acceso	253
Sistemas AIX	253
Sistemas Linux	254

Sistemas Windows	255
Creación del ID de usuario para el servidor	255
Preparación de sistemas de archivos para el servidor	256
Sistemas AIX	256
Sistemas Linux	257
sistemas Windows	258
Instalación del servidor y Centro de operaciones	259
Instalación en sistemas AIX y Linux	259
Instalación en sistemas Windows	260
Configuración del servidor y el Centro de operaciones	260
Configuración de la instancia de servidor	261
Instalación del cliente de archivado y copia de seguridad	262
Configuración de opciones para el servidor	262
Conceptos sobre la seguridad	263
Configuración de Centro de operaciones	265
Registro de la licencia de producto	266
Definición de las reglas de retención de datos para su empresa	266
Definición de planificaciones para actividades de mantenimiento del servidor	266
Definición de planificaciones de cliente	270
Conexión de dispositivos de cinta para el servidor	271
Conectar un dispositivo de biblioteca automática a su dispositivo	271
Seleccionar un controlador de dispositivo de cinta	271
Controladores de dispositivos de cinta de IBM	272
Controladores de dispositivos de cinta de IBM Spectrum Protect	272
Nombres de archivo especiales para dispositivos de cinta	273
Instalación y configuración de controladores de dispositivos de cinta	274
Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM	274
Sistemas AIX	275
Dispositivos SCSI y de canal de fibra	276
Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores	277
Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta	277
Configuración de dispositivos conectados a SAN de canal de fibra	278
Sistemas Linux	278
Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas	278
Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfcP)	279
Información sobre los dispositivos SCSI del sistema	280
Impedir que las etiquetas de cinta se sobrescriban	280
sistemas Windows	281
Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta	281
Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta	282
Configuración de bibliotecas para su uso por parte de un servidor	282
Definición de dispositivos de cinta	284
Definición de bibliotecas y unidades	284
Definición de bibliotecas	284
Definición de unidades	285
Definición de las clases de dispositivo de cinta	286
Definición de las clases de dispositivo LTO	287
Combinación de unidades y medios LTO en una biblioteca	287
Límites de montaje en entornos de medios mixtos LTO	288
Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior	289
Definición de clases de dispositivo 3592	289
Combinación de generaciones de unidades y medios 3592 en una sola biblioteca	290
Control de las velocidades de acceso a datos en volúmenes 3592	291
Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior	292
Configuración de la compartición de bibliotecas	292
Ejemplo: Compartir biblioteca para servidores AIX y Linux	293
Ejemplo: compartición de bibliotecas para servidores Windows	295
Configuración del servidor gestor de bibliotecas	295

Configuración de los servidores cliente de biblioteca	296
Configuración de una jerarquía de agrupaciones de almacenamiento	297
Protección de aplicaciones, máquinas virtuales y sistemas	298
Configuración del movimiento de datos sin LAN	298
Métodos de cifrado	299
Control de las operaciones de control de cintas	301
Cómo rellena volúmenes IBM Spectrum Protect	301
Especificar la capacidad estimada de los volúmenes de cinta	302
Especificación de formatos de grabación para soportes de cinta	302
Asociar objetos de biblioteca con clases de dispositivo	302
Control de las operaciones de montaje de medios para dispositivos de cinta	303
Control del número de volúmenes montados simultáneamente	303
Control de la cantidad de tiempo que un volumen permanece montado	304
Control de la cantidad de tiempo que un servidor espera una unidad	304
Operaciones de preferencia	305
Preferencia del punto de montaje	305
Preferencia de acceso a un volumen	305
Influencia de los cambios de dispositivo en la SAN	306
Visualización de la información de dispositivos	307
Medios de cinta Grabar una vez leer varias	307
Unidades preparadas para WORM	308
Incorporación de medios WORM	308
Restricciones en los medios WORM	308
Errores de montaje con medios WORM	309
Volver a etiquetar soportes WORM	309
Eliminar volúmenes WORM privados de una biblioteca	309
Creación de volúmenes DLT WORM	309
Soporte para cintas 3592 WORM cortas y normales	309
Consultar a una clase de dispositivo el valor del parámetro WORM	309
Resolución de problemas con dispositivos	309
Finalización de la implementación	310
Supervisión	311
Lista de comprobación diaria	311
Lista de comprobación periódica	316
Supervisión de los mensajes de alerta de cinta sobre errores de hardware	323
Prevenir errores causados por la incompatibilidad de los medios	323
Operaciones con cartuchos limpiadores	323
Verificación de la conformidad de licencia	324
Seguimiento del estado del sistema mediante informes de correo electrónico	325
Gestión	326
Gestión del Centro de operaciones	326
Gestión de operaciones de cliente	327
Evaluación de errores en registros de errores de cliente	327
Detención y reinicio del aceptador de cliente	328
Restablecimiento de contraseñas	329
Gestión de actualizaciones del cliente	329
Poner fuera de servicio un nodo cliente	330
Desactivación de datos para liberar espacio de almacenamiento	332
Gestión del almacenamiento de datos	332
Gestión de la capacidad de inventario	333
Ajuste de actividades planificadas	334
Optimización de operaciones habilitando la función de proximidad de los archivos de cliente	335
Efectos de la proximidad en las operaciones	336
Selección de volúmenes con proximidad habilitada	338
Selección de volúmenes con proximidad inhabilitada	339
Valores de proximidad	339
Proximidad de agrupaciones de almacenamiento de copias	340
Planificación y activación de la función de proximidad	340



Gestión de dispositivos de cinta	342
Preparación de medios extraíbles	342
Etiquetado de volúmenes de cinta	343
Dar de alta volúmenes de almacenamiento en una biblioteca	343
Incorporar un volumen en una biblioteca SCSI	344
Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca	345
Incorporación de volúmenes de almacenamiento desde los puertos de entrada/salida de la biblioteca	345
Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas	346
Incorporación de volúmenes	346
Comprobación de volúmenes en una biblioteca completa con intercambio	346
Volúmenes privados y volúmenes reutilizables	347
Direcciones de elementos para las ranuras de almacenamiento de biblioteca	347
Gestión del inventario de volúmenes	348
Control de acceso a volúmenes	348
Reutilización de cintas	349
Mantenimiento de un suministro de volúmenes reutilizables	350
Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM	350
Gestión del inventario de volumen en bibliotecas automatizadas	351
Cambiar el estado de un volumen de una biblioteca automatizada	352
Eliminación de volúmenes de una biblioteca automatizada	352
Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada	353
Gestión de una ubicación de desbordamiento	353
Auditoría de inventarios de volúmenes	354
Volúmenes grabados parcialmente	354
Operaciones con bibliotecas compartidas	355
Solicitudes del servidor para los volúmenes	356
Gestión de unidades de cinta	357
Actualización de unidades	358
Validación de datos durante operaciones de lectura/escritura en cinta	358
Unidades soportadas	359
Habilitación e inhabilitación de la protección de bloques lógicos	360
Operaciones de lectura/escritura en volúmenes	361
Gestión de agrupaciones de almacenamiento en una biblioteca de cintas	361
Limpieza de unidades de cinta	362
Métodos para limpiar unidades de cinta	362
Configuración del servidor para la limpieza de unidades en una biblioteca automatizada	363
Incorporar un cartucho limpiador en una biblioteca	364
Operaciones con cartuchos limpiadores	323
Resolución de errores relacionados con la limpieza de unidades	365
Sustitución de unidades de cinta	365
Suprimir unidades de cinta	366
Sustitución de las unidades con otras del mismo tipo	366
Migración de datos a unidades actualizadas	367
Protección del servidor	367
Gestión de administradores	367
Cambio de los requisitos de contraseña	368
Protección del servidor en el sistema	369
Detención e inicio del servidor	369
Detención del servidor	370
Inicio del servidor para tareas de mantenimiento o reconfiguración	370
Planificación para actualizar el servidor	371
Preparación para una parada	372
Preparación ante desastres y recuperación tras desastres mediante DRM.	372
Archivo del plan de recuperación tras desastre	373
Recuperación de datos de cliente y servidor	375
Obtención de detalles de recuperación	376
Restauración de la base de datos	377
Archivos PDF	378

<b>Servidores</b>	<b>378</b>
Novedades	378
Actualizaciones del Centro de operaciones	380
Actualizaciones del servidor	380
Copia de seguridad de los datos en Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube	380
Cifrado de datos de cliente en una agrupación de almacenamiento de contenedores de directorio	381
Copia de seguridad de un servidor de archivos NAS en una agrupación de almacenamiento de contenedores de directorio	381
Instalación de IBM Spectrum Protect en el sistema operativo Linux en sistemas Power Systems (little endian)	381
Proteja su entorno de almacenamiento con un protocolo de seguridad mejorado	382
Optimización de la seguridad con la clave de cifrado maestra generada automáticamente	382
Configuración de un entorno de almacenamiento utilizando la Guía de soluciones de cintas	383
Planificación de actualizaciones automáticas para la copia de seguridad y restauración de clientes	383
Actualice el servidor de IBM Spectrum Protect a la V8.1.2 antes de actualizar los clientes	383
Opciones, mandatos y parámetros del servidor en desuso y sin mantenimiento	383
Notas del release V8.1	384
Servidores	384
Centro de operaciones	385
Dispositivos	387
Archivos léame V8.1 para los fixpacks	388
Instalación y actualización	389
Implementación de una solución IBM Spectrum Protect	389
Disponibilidad de las características por sistema operativo	389
Instalación y actualización del servidor	391
AIX: Instalación del servidor	391
AIX: Planificación para instalar el servidor de IBM Spectrum Protect	392
AIX: Qué debe saber primero	392
AIX: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor	393
AIX: Planificación de rendimiento óptimo	393
AIX: Planificación del hardware del servidor y el sistema operativo	394
AIX: Planificación de discos de base de datos del servidor	396
AIX: Planificación de discos de registro de recuperación del servidor	398
AIX: Planificación de agrupaciones de almacenamiento de contenedores	399
AIX: Planificación de agrupaciones de almacenamiento DISK o FILE	405
AIX: Planificación de la tecnología de almacenamiento	407
AIX: Mejores métodos de instalación	409
AIX: Requisitos de sistema mínimos para sistemas AIX	411
AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema	413
AIX: IBM Installation Manager	414
AIX: Hojas de trabajo para planificar detalles para el servidor	415
AIX: Planificación de la capacidad	415
AIX: Requisitos de espacio de la base de datos	416
AIX: Número máximo de archivos	416
AIX: Capacidad de agrupación de almacenamiento	418
AIX: El gestor de bases de datos y el espacio temporal	418
AIX: Requisitos de espacio del registro de recuperación	419
AIX: Espacio del registro activo y archivado	419
AIX: Ejemplo: Operaciones básicas de almacén del cliente	420
AIX: Ejemplo: Varias sesiones de cliente	421
AIX: Ejemplo: Operaciones de grabación simultáneas	423
AIX: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	424
AIX: Ejemplo: Condiciones de variación extrema	424
AIX: Ejemplo: Copias de seguridad de base de datos completas	424
AIX: Ejemplo: Eliminación de datos duplicados	426
AIX: Espacio del duplicado de registro activo	430
AIX: Espacio del registro de migración tras error del archivo	430
AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	430
AIX: Supresión de archivos de retroacción de instalación	431

AIX: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	432
AIX: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	432
AIX: Prácticas más adecuadas de denominación del servidor	432
AIX: Directorios de instalación para el servidor de IBM Spectrum Protect	434
AIX: Instalación de los componentes de servidor	434
AIX: Obtener el paquete de instalación	434
AIX: Utilización del asistente de instalación	435
AIX: Utilización del asistente de instalación de la consola	436
AIX: Utilización de modalidad silenciosa	437
AIX: Instalación de paquetes de idioma del servidor	438
AIX: Idiomas locales del servidor	438
AIX: Configuración de un paquete de idiomas	439
AIX: Actualización de un paquete de idiomas	439
AIX: Realización de los primeros pasos tras instalar la versión 8.1.2	439
AIX: Creación del ID de usuario y de directorios para la instancia del servidor	440
AIX: Configuración del servidor de IBM Spectrum Protect	442
AIX: Utilización del asistente de configuración	442
AIX: Utilización de los pasos de configuración manual	442
AIX: Creación de una instancia del servidor	443
AIX: Configuración de comunicaciones de servidor y cliente en sistemas UNIX	444
AIX: Establecimiento de opciones de TCP/IP	445
AIX: Establecimiento de opciones de memoria compartida	445
AIX: Configuración de las opciones de la capa de sockets seguros	446
AIX: Formateo de la base de datos y las anotaciones	446
AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	447
AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	448
AIX: Inicio de la instancia de servidor	449
AIX: Comprobación de los derechos de acceso y límites de usuario	450
AIX: Inicio del servidor con el ID de usuario de la instancia	451
AIX: Inicio automático de los servidores	451
AIX: Inicio del servidor en modalidad de mantenimiento	452
AIX: Detención del servidor	453
AIX: Registro de licencias	453
AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	454
AIX: Ejecución de varias instancias de servidor en un solo sistema	454
AIX: Supervisión del servidor	455
AIX: Instalación de un fixpack de IBM Spectrum Protect	456
AIX: Revertir de la versión 8.1.2 a un servidor anterior	457
AIX: Referencia: Mandatos de DB2 para bases de datos del servidor	459
AIX: Desinstalar IBM Spectrum Protect	462
AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	463
AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola	463
AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	463
AIX: Desinstalación e instalación de IBM Spectrum Protect	464
AIX: Desinstalación de IBM Installation Manager	465
Linux: Instalación del servidor	465
Linux: Planificación para instalar el servidor de IBM Spectrum Protect	466
Linux: Qué debe saber primero	466
Linux: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor	467
Linux: Planificación de rendimiento óptimo	467
Linux: Planificación del hardware del servidor y el sistema operativo	468
Linux: Planificación de discos de base de datos del servidor	472
Linux: Planificación de discos de registro de recuperación del servidor	474
Linux: Planificación de agrupaciones de almacenamiento de contenedores	475
Linux: Planificación de agrupaciones de almacenamiento DISK o FILE	481
Linux: Planificación de la tecnología de almacenamiento	483
Linux: Mejores métodos de instalación	485
Linux: Requisitos mínimos del sistema para sistemas Linux	487

Linux: Requisitos mínimos del servidor Linux X86_64	487
Linux: Requisitos mínimos del servidor Linux on System z	489
Linux: Requisitos mínimos de servidor Linux on Power Systems (little endian)	491
Linux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema	492
Linux: IBM Installation Manager	493
Linux: Hojas de trabajo para planificar detalles para el servidor	494
Linux: Planificación de la capacidad	494
Linux: Requisitos de espacio de la base de datos	495
Linux: Número máximo de archivos	495
Linux: Capacidad de agrupación de almacenamiento	497
Linux: El gestor de bases de datos y el espacio temporal	497
Linux: Requisitos de espacio del registro de recuperación	498
Linux: Espacio del registro activo y archivado	498
Linux: Ejemplo: Operaciones básicas de almacén del cliente	499
Linux: Ejemplo: Varias sesiones de cliente	500
Linux: Ejemplo: Operaciones de grabación simultáneas	502
Linux: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	503
Linux: Ejemplo: Condiciones de variación extrema	503
Linux: Ejemplo: Copias de seguridad de base de datos completas	503
Linux: Ejemplo: Eliminación de datos duplicados	505
Linux: Espacio del duplicado de registro activo	509
Linux: Espacio del registro de migración tras error del archivo	509
Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	509
Linux: Supresión de archivos de retrotracción de instalación	510
Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	511
Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	511
Linux: Prácticas más adecuadas de denominación del servidor	511
Linux: Directorios de instalación para el servidor de IBM Spectrum Protect	513
Linux: Instalación de los componentes de servidor	513
Linux: Obtener el paquete de instalación	513
Linux: Utilización del asistente de instalación	514
Linux: Utilización del asistente de instalación de la consola	515
Linux: Utilización de modalidad silenciosa	515
Linux: Instalación de paquetes de idioma del servidor	516
Linux: Idiomas locales del servidor	517
Linux: Configuración de un paquete de idiomas	517
Linux: Actualización de un paquete de idiomas	518
Linux: Realización de los primeros pasos tras instalar la versión 8.1.2	518
Linux: Ajuste de parámetros del kernel en sistemas Linux	519
Linux: Actualización de parámetros	519
Linux: Valores recomendados	520
Linux: Creación del ID de usuario y de directorios para la instancia del servidor	520
Linux: Configuración del servidor de IBM Spectrum Protect	521
Linux: Utilización del asistente de configuración	522
Linux: Utilización de los pasos de configuración manual	522
Linux: Creación de una instancia del servidor	523
Linux: Configuración de comunicaciones de servidor y cliente en sistemas UNIX	524
Linux: Establecimiento de opciones de TCP/IP	525
Linux: Establecimiento de opciones de memoria compartida	525
Linux: Configuración de las opciones de la capa de sockets seguros	526
Linux: Formateo de la base de datos y las anotaciones	526
Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	527
Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	528
Linux: Inicio de la instancia de servidor	529
Linux: Comprobación de los derechos de acceso y límites de usuario	530
Linux: Inicio del servidor con el ID de usuario de la instancia	531
Linux: Inicio automático de los servidores en sistemas Linux	532
Linux: Inicio del servidor en modalidad de mantenimiento	533

Linux: Detención del servidor	534
Linux: Registro de licencias	534
Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	534
Linux: Ejecución de varias instancias de servidor en un solo sistema	535
Linux: Supervisión del servidor	535
Linux: Instalación de un fixpack de IBM Spectrum Protect	536
Linux: Revertida de la versión 8.1.2 a un servidor anterior	538
Linux: Referencia: Mandatos de DB2 para bases de datos del servidor	540
Linux: Desinstalar IBM Spectrum Protect	542
Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	543
Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola	543
Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	544
Linux: Desinstalación e instalación de IBM Spectrum Protect	544
Linux: Desinstalación de IBM Installation Manager	545
Windows: Instalación del servidor	545
Windows: Planificación para instalar el servidor de IBM Spectrum Protect	546
Windows: Qué debe saber primero	546
Windows: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor	547
Windows: Planificación de rendimiento óptimo	547
Windows: Planificación del hardware del servidor y el sistema operativo	548
Windows: Planificación de discos de base de datos del servidor	550
Windows: Planificación de discos de registro de recuperación del servidor	552
Windows: Planificación de agrupaciones de almacenamiento de contenedores	553
Windows: Planificación de agrupaciones de almacenamiento DISK o FILE	559
Windows: Planificación de la tecnología de almacenamiento	561
Windows: Mejores métodos de instalación	563
Windows: Requisitos mínimos del sistema para sistemas Windows	565
Windows: IBM Installation Manager	567
Windows: Hojas de trabajo para planificar detalles para el servidor	568
Windows: Planificación de la capacidad	568
Windows: Requisitos de espacio de la base de datos	569
Windows: Número máximo de archivos	569
Windows: Capacidad de agrupación de almacenamiento	571
Windows: El gestor de bases de datos y el espacio temporal	571
Windows: Requisitos de espacio del registro de recuperación	572
Windows: Espacio del registro activo y archivado	572
Windows: Ejemplo: Operaciones básicas de almacén del cliente	573
Windows: Ejemplo: Varias sesiones de cliente	574
Windows: Ejemplo: Operaciones de grabación simultáneas	576
Windows: Ejemplo: Operaciones básicas de almacén del cliente y del servidor	577
Windows: Ejemplo: Condiciones de variación extrema	577
Windows: Ejemplo: Copias de seguridad de base de datos completas	577
Windows: Ejemplo: Eliminación de datos duplicados	579
Windows: Espacio del duplicado de registro activo	583
Windows: Espacio del registro de migración tras error del archivo	583
Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación	583
Windows: Supresión de archivos de retrotracción de instalación	584
Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico	585
Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos	585
Windows: Prácticas más adecuadas de denominación del servidor	585
Windows: Directorios de instalación para el servidor de IBM Spectrum Protect	586
Windows: Instalación de los componentes de servidor	587
Windows: Obtener el paquete de instalación	587
Windows: Utilización del asistente de instalación	588
Windows: Utilización del asistente de instalación de la consola	588
Windows: Utilización de modalidad silenciosa	589
Windows: Instalación de paquetes de idioma del servidor	590
Windows: Idiomas locales del servidor	590

Windows: Configuración de un paquete de idiomas	591
Windows: Actualización de un paquete de idiomas	591
Windows: Realización de los primeros pasos tras instalar la versión 8.1.2	591
Windows: Creación del ID de usuario y de directorios para la instancia del servidor	592
Windows: Configuración del servidor de IBM Spectrum Protect	594
Windows: Utilización del asistente de configuración	594
Windows: Utilización de los pasos de configuración manual	595
Windows: Creación de una instancia del servidor	595
Windows: Configuración de comunicaciones en sistemas Windows	596
Windows: Establecimiento de opciones de TCP/IP	597
Windows: Establecimiento de opciones de Named Pipes	597
Windows: Configuración de las opciones de la capa de sockets seguros	598
Windows: Formateo de la base de datos y las anotaciones	598
Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos	598
Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor	599
Windows: Inicio de la instancia del servidor en sistemas Windows	600
Windows: Configuración del servidor para que se inicie como un servicio de Windows	601
Windows: Inicio del servidor como un servicio de Windows	602
Windows: Creación manual y configuración de un servicio de Windows	602
Windows: Inicio del servidor en segundo plano	603
Windows: Servicios asociados al servidor en sistemas Windows	603
Windows: Inicio del servidor en modalidad de mantenimiento	604
Windows: Detención del servidor	605
Windows: Registro de licencias	605
Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos	605
Windows: Ejecución de varias instancias de servidor en un solo sistema	606
Windows: Supervisión del servidor	606
Windows: Instalación de un fixpack de IBM Spectrum Protect	607
Windows: Revertida de la versión 8.1.2 a un servidor anterior	609
Windows: Referencia: Mandatos de DB2 para bases de datos del servidor	611
Windows: Desinstalar IBM Spectrum Protect	614
Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico	615
Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola	615
Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa	615
Windows: Desinstalación e instalación de IBM Spectrum Protect	616
Windows: Desinstalación de IBM Installation Manager	617
Actualización del servidor a la versión 8.1	617
Actualización a V8.1	618
Planificación de la actualización	619
Preparación del sistema	619
Instalación del servidor y comprobación de la actualización	622
Actualización del servidor en un entorno en clúster	626
Actualización de V6.3 o V7.1 a V8.1.2 en un entorno en clúster para AIX con una instancia de base de datos compartida	627
Actualización de V6.3 a V8.1.2 en un entorno en clúster para AIX con instancias de base de datos independientes	629
Actualización de V6.1 a V8.1.2 en un entorno en clúster para AIX	631
Actualización de V8.1.2 en un entorno en clúster para Linux	633
Actualización de V6.3 o V7.1 a V8.1.2 en un entorno en clúster para Windows	633
Actualización de V6.1 a V8.1.2 en un entorno en clúster para Windows	635
Eliminación de GSKit V7 después de actualizar a IBM Spectrum Protect V8.1.2	637
Instalación y actualización del Centro de operaciones	637
Planificación para instalar el Centro de operaciones	638
Requisitos del sistema del Centro de operaciones	639
Requisitos de sistema del Centro de operaciones	640
Requisitos del servidor concentrador y spoke	640
Consejos para designar la configuración del servidor concentrador y el servidor de radio	640
Consejos para elegir un servidor concentrador	642
Requisitos de sistema operativo	642
Requisitos del navegador web	643

Requisitos de idioma	643
Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect	645
Los ID de administrador que requiere el centro de operaciones	646
IBM Installation Manager	647
Lista de comprobación de la instalación	647
Instalar el Centro de operaciones	649
Obtención del paquete de instalación de Centro de operaciones	650
Instalación de Centro de operaciones utilizando el asistente gráfico	650
Instalar el Centro de operaciones en modalidad de consola	651
Instalación de Centro de operaciones en el modo silencioso	652
Actualización del Centro de operaciones	652
Guía de inicio de la Centro de operaciones	653
Configurar el Centro de Operaciones	654
Designar el servidor central	655
Adición de un servidor de radio	656
Envío de alertas por correo electrónico a los administradores	656
Adición de texto personalizado a la pantalla de inicio de sesión	658
Habilitación de servicios REST	658
Configuración para la comunicación segura	659
Entre el Centro de operaciones y el servidor concentrador	659
Entre el servidor concentrador y un servidor de radio	661
Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones	662
Iniciar y detener el servidor web	663
Apertura del Centro de operaciones	664
Recopilación de información de diagnóstico con el servicio de gestión de clientes	664
Instalación de servicio de gestión de clientes utilizando el asistente gráfico	665
Instalación de servicio de gestión de clientes en modalidad silenciosa	666
Verificación de la instalación	666
Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes	668
Inicio y detención del servicio de gestión de clientes	668
Desinstalación de servicio de gestión de clientes	669
Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas	669
Resolución de problemas de la instalación de Centro de operaciones	670
El asistente de instalación gráfica no puede iniciarse en un sistema AIX	670
Las letras en chino, japonés o coreano se muestran incorrectamente	670
Desinstalación de Centro de operaciones	670
Desinstalación de Centro de operaciones utilizando el asistente gráfico	670
Desinstalación del Centro de operaciones en modalidad de consola	671
Desinstalar Centro de operaciones en modalidad silenciosa	671
Volver a una versión anterior de Centro de operaciones	672
Configuración de servidores	672
Protección del servidor	674
Conceptos sobre la seguridad	675
Gestión de administradores	677
Cambio de los requisitos de contraseña	677
Protección de IBM Spectrum Protect en el sistema	678
Restricción del acceso de usuario al servidor	679
Limitación de acceso a través de restricciones de puerto	679
Protección de las comunicaciones	679
Comunicación SSL y TLS	680
Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL	682
Configuración del servidor para aceptar conexiones SSL	682
Configuración de clientes para comunicarse con el servidor utilizando SSL	683
Configuración del servidor para conectarse a otro servidor utilizando SSL	684
Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL	685
Configuración de un agente de almacenamiento para utilizar SSL	685
Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL	685

Autenticación de los usuarios mediante un servidor LDAP	686
Réplica de datos de cliente en otro servidor	686
Compatibilidad de réplica	687
Habilitación de la réplica de nodo	688
Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio	688
Modificación de los valores de réplica	690
Establecimiento de distintas políticas de retención	690
Configuración de entornos en clúster	691
Visión general del entorno en clúster	692
entorno en clúster de AIX	692
Requisitos del clúster	693
Recuperación de errores y restablecimiento de PowerHA	693
Instalación y configuración de PowerHA SystemMirror para AIX	694
Instalación y configuración del clúster	694
Configuración del nodo primario	695
Configuración de un nodo secundario con una instancia de DB2 compartida	695
Configuración de un nodo secundario con una instancia de DB2 independiente	696
Instalación del servidor en un nodo de producción	697
Instalación del cliente en un nodo de producción	697
Verificación de la configuración del servidor	698
Configurar el nodo de espera	699
Definición de los dispositivos de almacenamiento de medios extraíbles	699
Configuración del gestor de clúster	699
Resolución de problemas del entorno en clúster de PowerHA	700
entorno en clúster de Linux	700
Descripción de un entorno en clúster de dos nodos	701
Topología de disco compartido de dos nodos	703
Grupos de recursos de Tivoli System Automation	704
Configuración de un clúster	705
Requisitos previos para la configuración de un entorno en clúster	706
Instalación y configuración de componentes	706
Instalación de componentes de servidor	706
Configuración del nodo primario	706
Configuración del nodo secundario	707
Instalación de Tivoli System Automation	708
Creación de una etiqueta para los puntos de montaje	708
Instalación y configuración de Tivoli System Automation	709
Preparación para activar los nodos de clúster para el dominio	709
Configuración de recursos del grupo de volúmenes	709
Configuración de recursos que no están en un grupo de volúmenes	710
Activación de la política base	711
Adición de puntos de montaje a directorios	711
Configuración de recursos de almacenamiento	712
Adición de una agrupación de almacenamiento	712
Eliminar una agrupación de almacenamiento	713
Eliminación de un punto de montaje	713
Actualización del servidor que es un Tivoli System Automation configurado	714
entorno en clúster de Windows	714
Visión general del entorno de Microsoft Failover Cluster	715
Recuperación de errores de cinta para los nodos de un clúster	717
Planificación de un entorno en clúster	717
Hoja de trabajo de configuración del clúster	717
Planificación de la configuración de hardware y software del clúster	718
Configuración de IBM Spectrum Protect en Microsoft Failover Cluster	719
Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster	719
Preparación de un grupo de recursos de clúster para un servidor virtual	720
Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster	720
Inicialización del servidor en el nodo primario	721



Verificación de la configuración en un Microsoft Failover Cluster	721
Prueba de migración tras error	721
Mantenimiento del entorno en clúster	722
Migración de un servidor existente en un clúster	722
Añadir un servidor utilizando copia de seguridad y restauración	722
Gestión de un servidor virtual en un clúster	723
Gestión de la recuperación de errores de cinta	723
Resolución de problemas con las anotaciones de clúster	723
Configuración de clientes	724
Adición de clientes	724
Selección del software de cliente y planificación de la instalación	725
Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente	726
Visualización de políticas	727
Edición de políticas	727
Planificación de copia de seguridad y operaciones de archivado	728
Registro de clientes	729
Instalación y configuración de clientes	730
Configuración del cliente para ejecutar las operaciones planificadas	731
Configuración de comunicaciones a través de un cortafuegos	733
Personalización de políticas	734
Conceptos de políticas	734
Retención y caducidad de las versiones de copia de seguridad	735
Caducidad de archivos y procesamiento de la caducidad	736
Ejemplo: Retención cuando una política utiliza solo controles temporales	736
Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión	737
Interacciones entre configuraciones de política	739
Activación de las políticas después de las actualizaciones	740
Personalización de una política	742
Creación de una política copiando una política existente	743
Creación de un dominio de políticas	744
Control de las operaciones de cliente mediante conjuntos de opciones de cliente	745
Configuración del almacenamiento	746
Tipos de agrupaciones de almacenamiento	746
Opciones de eliminación de datos duplicados	749
Configuración de dispositivos de almacenamiento	750
Configuración de una agrupación de almacenamiento de contenedores de directorios	751
Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta	752
Rotación de volúmenes de cinta fuera del local sin DRM	754
Cambiar el umbral de reclamación de volumen	754
Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor	754
Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro	756
Configuración de una agrupación de almacenamiento de contenedores en la nube	758
Preparación para Amazon con S3 (fuera del local)	759
Preparación de un dispositivo compatible con Amazon S3	760
Preparación para Microsoft Azure (fuera del local)	761
Preparación para IBM Cloud Object Storage con Swift (fuera del local)	762
Preparación para IBM Cloud Object Storage con S3 (fuera del local)	762
Preparación para IBM Cloud Object Storage con S3 (en local)	763
Preparación para OpenStack con Swift	765
Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube	765
Optimización de rendimiento para almacenamiento de objetos en la nube	765
Gestión de agrupaciones de almacenamiento de contenedores	766
Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor	768
Limpieza de los datos de una agrupación de almacenamiento de origen	769
Auditoría de un contenedor de la agrupación de almacenamiento	770
Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos	771
Supervisión de soluciones de almacenamiento	772
Lista de comprobación diaria	772

Lista de comprobación periódica	778
Verificación de la conformidad de licencia	784
Seguimiento del estado del sistema mediante informes de correo electrónico	785
Selección, configuración y uso de herramientas de supervisión	786
Gestión de operaciones	788
Gestión de operaciones del servidor	789
Detención e inicio del servidor	789
Detención del servidor	789
Inicio del servidor para tareas de mantenimiento o reconfiguración	790
Gestión de la capacidad de inventario	791
Gestión del uso de la memoria y del procesador	793
Determinación de si Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema	793
Planificación de la actualización del servidor	795
Ajuste de actividades planificadas	795
Gestión de operaciones de cliente	796
Modificación del ámbito de una copia de seguridad de cliente	796
Evaluación de errores en registros de errores de cliente	797
Detención y reinicio del aceptador de cliente	797
Restablecimiento de contraseñas	798
Poner fuera de servicio un nodo cliente	799
Desactivación de datos para liberar espacio de almacenamiento	801
Gestión de actualizaciones del cliente	801
Gestión del Centro de operaciones	802
Adición y eliminación de servidores spoke	803
Adición de un servidor de radio	803
Eliminación de un servidor spoke	803
Inicio y detención del servidor web	804
Reinicio del asistente de configuración inicial	804
Cambio del servidor concentrador	805
Restauración de la configuración a un estado de preconfiguración	805
Configuración de bibliotecas de cintas virtuales	807
Consideraciones sobre el uso de las bibliotecas de cintas virtuales	807
Capacidad de almacenamiento para las bibliotecas de cintas virtuales	807
Configuración de unidades para las bibliotecas de cintas virtuales	808
Agregar una biblioteca de cintas virtuales a su entorno	808
Definir todas las unidades y vías de acceso de una biblioteca	809
Ejemplo: biblioteca SCSI o VTL con un único tipo de dispositivo de unidad	810
Ejemplo: Biblioteca VTL o SCSI con varios tipos de dispositivos de unidad	811
Protección de servidores de archivos NAS	812
Requisitos de NDMP	814
Interfaces para operaciones NDMP	815
Formatos de datos para operaciones de copia de seguridad NDMP	815
Gestión de operaciones NDMP	815
Gestión de los nodos del servidor de archivos NAS	816
Gestión de los transportadores de datos utilizados en las operaciones NDMP	817
Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP	818
Gestión de agrupaciones de almacenamiento para operaciones NDMP	818
Gestión de tablas de contenido	819
Impedir que las conexiones NDMP inactivas se cierren	819
Habilitar el estado activo de TCP	820
Especificar tiempo de inactividad de conexión (AIX, Linux y Windows)	820
Configuración de IBM Spectrum Protect para operaciones NDMP	820
En un entorno no de clúster	820
Configuración de una política de IBM Spectrum Protect para operaciones NDMP	822
Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect	823
Políticas para copias de seguridad iniciadas con la interfaz de cliente	823
Determinación de la ubicación de copia de seguridad NAS	824
Bibliotecas y unidades de cintas para operaciones NDMP	825

Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS	826
Configuración de una biblioteca de cintas para operaciones NDMP	828
Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS	829
Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect	830
Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS	832
Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect	833
Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect	835
Registro de nodos NAS con el servidor de IBM Spectrum Protect	836
Definición de un transportador de datos para un servidor de archivos de NAS	837
Definición de vías de acceso para operaciones NDMP	837
Definición de vías de acceso a unidades	838
Unidades conectadas a un servidor de archivos y al servidor de IBM Spectrum Protect	838
Unidades conectadas únicamente a un servidor de archivos	839
Obtención de nombres para dispositivos conectados a un servidor de archivos	839
Definición de vías de acceso a bibliotecas	840
Planificación de operaciones NDMP	841
Definición de espacios de archivos virtuales	841
Copia de seguridad de datos mediante la función de cinta a cinta	842
Traslado de datos con la función de copia de cinta a cinta	842
En un entorno en clúster de NetApp	842
Configuración de copias de seguridad de clúster completo en dispositivos de cinta	844
Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect	846
Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect	847
Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster	848
Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP	851
Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único	851
Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect	852
Copia de seguridad y restauración en nivel de archivo para operaciones NDMP	853
Interfaces para las operaciones de restauración a nivel de archivos	854
Caracteres internacionales para servidores de archivos NetApp	854
Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio	855
Operaciones de copia de seguridad y restauración a nivel de directorio	855
Copia de seguridad y restauración a nivel de directorio para operaciones NDMP	855
Copia de seguridad y restauración con instantáneas	856
Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape	856
Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra	857
Réplica de los nodos NAS	857
Protección de datos con la característica NetApp SnapLock	858
Reclamación y la característica SnapLock	859
Periodos de retención	859
Configuración de la característica SnapLock para la retención basada en sucesos	861
Protección de datos continua con la característica SnapLock	862
Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect	862
Reparación y recuperación de datos	862
Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino	863
Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor	865
Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor	867
Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino	868
Recuperación después de un siniestro	869
Reparación desde volúmenes de agrupación de almacenamiento de copia de contenedor	869
Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino	870
Reparación de un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor	871
Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado	873
Mandatos, opciones y programas de utilidad del servidor	873
Gestión del servidor desde la línea de mandatos	874
Emisión de comandos del cliente de administración	875
Inicio y detención del cliente de administración	875

Supervisión de actividades del servidor desde el cliente de administración	876
Supervisión de montajes de medios extraíbles del cliente de administración	876
Proceso de mandatos individuales desde el cliente de administración	876
Proceso de una serie de comandos del cliente de administración	877
Formateo de la salida de los comandos	877
Cómo guardar la salida del comando en una ubicación especificada	877
Opciones de cliente de administración	878
Emisión de mandatos desde el Centro de operaciones	880
Emisión de comandos desde la consola del servidor	880
Especificación de comandos de administración	880
Lectura de los diagramas de sintaxis	881
Utilización de caracteres de continuación para entrar mandatos largos	884
Denominación de objetos de IBM Spectrum Protect	884
Utilización de caracteres comodín para especificar nombres de objetos	885
Especificación de descripciones en parámetros de palabra clave	886
Control del proceso de comandos	887
Proceso de comandos de servidor	887
Detener procesos en segundo plano	887
Realización de tareas simultáneamente en varios servidores	888
Clases de privilegio	890
Comandos que requieren privilegio de sistema	890
Comandos que requieren privilegio de políticas	893
Comandos que requieren privilegio de almacenamiento	893
Comandos que requieren privilegio de operador	894
Comandos que puede emitir cualquier administrador	894
Comandos de administración	895
ACCEPT DATE (aceptar la fecha del sistema actual)	899
ACTIVATE POLICYSET (Activar un nuevo juego de políticas)	900
ASSIGN DEFMGMTCLASS (asignar una clase de gestión predeterminada)	901
AUDIT commands	902
Mandatos AUDIT CONTAINER	902
Auditoría de contenedor de nubes	902
Auditoría de un contenedor de directorios	906
AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)	910
AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)	912
AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)	914
AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)	915
AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)	916
Comandos BACKUP	920
BACKUP DB (copia de seguridad de la base de datos)	920
BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)	925
BACKUP NODE (Copia de seguridad de un nodo NAS)	926
BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)	930
BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)	933
BEGIN EVENTLOGGING (Iniciar anotación de eventos)	934
Comandos CANCEL	935
CANCEL EXPIRATION (Cancelar un proceso de caducidad)	936
CANCEL EXPORT (Suprimir una operación de exportación suspendida)	936
CANCEL PROCESS (Cancelar un proceso de administración)	937
CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)	939
CANCEL REQUEST (Cancelar una o más peticiones de montaje)	939
CANCEL RESTORE (Cancelar una sesión de restauración reinicializable)	940
CANCEL SESSION (Cancelar una o más sesiones cliente)	941
CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)	941
CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)	947
CLEAN DRIVE (Limpiar una unidad)	951
COMMIT (controlar la validación de comandos en una macro)	952

CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)	953
Comandos COPY	954
COPY ACTIVATEDATA (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)	954
COPY CLOPTSET (Copiar un conjunto de opciones de cliente)	957
COPY DOMAIN (Copiar un dominio de políticas)	958
COPY MGMTCLASS (Copiar una clase de gestión)	959
COPY POLICYSET (Copiar un juego de políticas)	960
COPY PROFILE (Copiar un perfil)	961
COPY SCHEDULE (Copiar una planificación de cliente o de comando de administración)	962
COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)	962
COPY SCHEDULE (Crear una copia de una planificación para las operaciones de administración)	963
COPY SCRIPT (copiar un script de IBM Spectrum Protect)	964
COPY SERVERGROUP (Copiar un grupo de servidores)	965
DEACTIVATE DATA (Desactivar datos para un nodo de cliente)	965
Comandos DECOMMISSION	967
DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)	968
DECOMMISSION VM (Poner fuera de servicio una máquina virtual)	969
Comandos DEFINE	970
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	971
DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)	973
DEFINE BACKUPSET (Definir un juego de copias de seguridad)	974
DEFINE CLIENTACTION (Definir una acción de cliente única)	977
DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)	981
DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)	983
DEFINE COLLOGGROUP (Definir un grupo de proximidad)	984
DEFINE COLLOCMEMBER	985
DEFINE COPYGROUP (Definir un grupo de copia)	987
DEFINE COPYGROUP (Definir un grupo de copia de seguridad)	988
DEFINE COPYGROUP (Definir un grupo de copias archivadas)	991
DEFINE DATAMOVER (Definir un transportador de datos)	994
DEFINE DEVCLASS (Definir una clase de dispositivo)	996
3590	997
3592	999
4MM	1004
8MM	1007
Centera	1012
DLT	1013
Ecartridge	1017
Archivo	1022
Generictape	1024
LTO	1026
NAS	1031
Removablefile	1033
Servidor	1034
VolSafe	1036
DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS)	1039
3590, para el servidor de medios de z/OS	1040
3592, para el servidor de medios de z/OS	1043
ECARTRIDGE, para el servidor de medios de z/OS	1047
FILE, para el servidor de medios de z/OS	1052
DEFINE DOMAIN (Definir un nuevo dominio de políticas)	1054
DEFINE DRIVE (Definir una unidad en una biblioteca)	1055
DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)	1059
DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)	1060
DEFINE LIBRARY (Definir una biblioteca)	1061
349X	1062
ACSLs	1064

EXTERNAL	1066
FILE	1068
MANUAL	1069
SCSI	1070
Compartido	1073
VTL	1073
ZOSMEDIA	1076
DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)	1077
DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)	1078
DEFINE MGMTCLASS (Definir una clase de gestión)	1079
DEFINE NODEGROUP (Definir un grupo de nodos)	1081
DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)	1082
DEFINE PATH (Definir una ruta)	1083
El destino es una unidad	1083
El destino es una biblioteca	1089
El destino es una biblioteca ZOSMEDIA	1091
DEFINE POLICYSET (Definir un juego de políticas)	1092
DEFINE PROFASSOCIATION (Definir una asociación de perfil)	1093
DEFINE PROFILE (Definir un perfil)	1097
DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)	1098
DEFINE RECOVERYMEDIA (Definir medio de recuperación)	1099
DEFINE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)	1100
DEFINE SCHEDULE (Definir una planificación de cliente)	1101
DEFINE SCHEDULE (Definir una planificación para un comando de administración)	1111
DEFINE SCRATCHPADENTRY (Definir una entrada de registro)	1117
DEFINE SCRIPT (definir un script de IBM Spectrum Protect)	1118
DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)	1120
DEFINE SERVERGROUP (Definir un grupo de nodo)	1126
DEFINE SPACETRIGGER (Definir desencadenante de espacio)	1127
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	1129
DEFINE STGPOOL (Definir una agrupación de almacenamiento)	1132
Agrupación de almacenamiento de contenedores en la nube	1134
Agrupación de almacenamiento de contenedores de directorio	1138
Agrupación de almacenamiento de copia de contenedor	1142
Agrupación de acceso aleatorio primaria	1145
Agrupación de acceso secuencial primaria	1153
Agrupación de copias	1166
Agrupación de datos activos	1173
DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)	1179
DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)	1180
DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)	1181
DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)	1183
Comandos DELETE	1189
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	1190
DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)	1191
DELETE BACKUPSET (Suprimir un juego de copias de seguridad)	1192
DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)	1195
DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)	1196
DELETE COLLOGROUP (Suprimir un grupo de proximidad)	1197
DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)	1198
DELETE COPYGROUP (Suprimir un grupo de copias de seguridad o de archivado)	1200
DELETE DATAMOVER (Suprimir un transportador de datos)	1201
DELETE DEDUPSTATS (Suprimir las estadísticas de eliminación de duplicados de datos)	1202
DELETE DEVCLASS (Suprimir una clase de dispositivo)	1205
DELETE DOMAIN (Suprimir un dominio de políticas)	1205
DELETE DRIVE (Suprimir una unidad de una biblioteca)	1206
DELETE EVENT (Suprimir registros de eventos)	1207
DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)	1208

DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)	1209
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	1212
DELETE LIBRARY (Suprimir una biblioteca)	1213
DELETE MACHINE (Suprimir información de una máquina)	1214
DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)	1214
DELETE MGMTCLASS (Suprimir una clase de gestión)	1215
DELETE NODEGROUP (Suprimir un grupo de nodos)	1216
DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)	1217
DELETE PATH (Suprimir una ruta)	1218
DELETE POLICYSET (Suprimir un juego de políticas)	1219
DELETE PROFASSOCIATION (Suprimir una asociación de perfil)	1220
DELETE PROFILE (Suprimir un perfil)	1222
DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)	1223
DELETE RECOVERYMEDIA (Suprimir medio de recuperación)	1224
DELETE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)	1224
DELETE SCHEDULE (Suprimir una planificación de cliente)	1225
DELETE SCHEDULE (Suprimir una planificación de administración)	1225
DELETE SCRATCHPADENTRY (Suprimir una entrada de registro)	1226
DELETE SCRIPT (Suprimir líneas de comandos de un script o suprimir todo el script)	1226
DELETE SERVER (Suprimir una definición de servidor)	1227
DELETE SERVERGROUP (Suprimir un grupo de servidores)	1228
DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)	1229
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	1229
DELETE STGPOOL (Suprimir una agrupación de almacenamiento)	1230
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)	1231
DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)	1233
DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)	1234
DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)	1234
DELETE VOLHISTORY (Suprimir información histórica de volúmenes)	1235
DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)	1239
Comandos DISABLE	1241
DISABLE EVENTS (Desactivar eventos para anotación de eventos)	1241
DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)	1244
DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)	1245
Comandos DISMOUNT	1246
DISPLAY OBJNAME (Mostrar un nombre de objeto completo)	1246
Comandos ENABLE	1247
ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)	1247
ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)	1250
ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)	1250
ENCRYPT STGPOOL (Cifrar datos en una agrupación de almacenamiento)	1252
END EVENTLOGGING (Detener eventos de anotaciones)	1253
EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)	1254
Comandos EXPORT	1258
EXPORT ADMIN (Exportar información del administrador)	1258
EXPORT ADMIN (Exportar definiciones del administrador a medios secuenciales)	1259
EXPORT ADMIN (Exportar información del administrador directamente a otro servidor)	1262
EXPORT NODE (Exportar información de nodos cliente)	1263
EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)	1265
EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)	1272
EXPORT POLICY (Exportar información de políticas)	1279
EXPORT POLICY (Exportar información de política a medios secuenciales)	1280
EXPORT POLICY (Exportar una política directamente a otro servidor)	1282
EXPORT SERVER (Exportar información del servidor)	1284
EXPORT SERVER (Exportar un servidor a medios secuenciales)	1285
EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)	1291
EXTEND DBSPACE (Incrementar el espacio para la base de datos)	1297
Comandos GENERATE	1299

GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)	1299
GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)	1305
GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)	1307
Comandos GRANT	1309
GRANT AUTHORITY (agregar autorización de administrador)	1309
GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)	1312
HALT (Concluir el servidor)	1313
HELP (Obtener ayuda sobre comandos y mensajes de error)	1314
IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)	1316
Comandos IMPORT	1319
IMPORT ADMIN (Importar información del administrador)	1319
IMPORT NODE (Importar información de nodos clientes)	1322
IMPORT POLICY (Importar información de políticas)	1327
IMPORT SERVER (Importar información del servidor)	1330
INSERT MACHINE (Insertar información de características o instrucciones de recuperación)	1334
ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)	1335
LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)	1336
LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)	1341
Comandos LOCK	1343
LOCK ADMIN (bloquear un administrador)	1343
LOCK NODE (Bloquear un nodo cliente)	1344
LOCK PROFILE (bloquear un perfil)	1345
MACRO (Invocar una macro)	1345
MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)	1347
Comandos MOVE	1349
MOVE CONTAINER (Mover un contenedor)	1349
MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)	1350
MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)	1353
MOVE GRPMEMBER (Mover un miembro de grupo de servidores)	1366
MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)	1367
MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)	1373
Espacios de archivos para uno o más nodos o un grupo de proximidad	1374
Espacios de archivos seleccionados de un único nodo	1377
NOTIFY SUBSCRIBERS (Notificar a servidores gestionados que actualicen los perfiles)	1380
PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca)	1380
PING SERVER (Comprobar la conexión entre servidores)	1384
PREPARE (crear un archivo de plan de recuperación)	1384
PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)	1391
Comandos QUERY	1396
QUERY ACTLOG (Consultar las anotaciones de actividades)	1397
QUERY ADMIN (Visualizar información de administrador)	1402
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	1405
QUERY ALERTSTATUS (Consultar el estado de una alerta)	1407
QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)	1410
QUERY AUDITOCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)	1411
QUERY BACKUPSET (Consultar un juego de copias de seguridad)	1413
QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)	1417
QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)	1419
QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)	1420
QUERY COLLOGROUP (Consultar un grupo de proximidad)	1422
QUERY CONTAINER (Visualización de información de contenedor)	1424
QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)	1427
QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)	1433
QUERY COPYGROUP (Consultar grupos de copia)	1434
QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de nubes)	1438
QUERY DATAMOVER (visualizar definiciones de un transportador de datos)	1441
QUERY DB (Visualizar información de base de datos)	1443



QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)	1445
QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)	1446
QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)	1451
QUERY DIRSPACE (Consultar utilización de almacenamiento de directorios FILE)	1455
QUERY DOMAIN (Consultar un dominio de políticas)	1456
QUERY DRIVE (Consultar información acerca de una unidad)	1458
QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)	1461
QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)	1469
QUERY ENABLED (Consultar eventos activados)	1471
QUERY EVENT (Consultar eventos planificados y realizados)	1472
QUERY EVENT (Visualizar planificaciones de cliente)	1473
QUERY EVENT (Visualizar planificaciones de eventos de administración)	1478
QUERY EVENTRULES (Consultar reglas para eventos de servidor o de cliente)	1481
QUERY EVENTSERVER (Consultar el servidor de eventos)	1483
QUERY EXPORT (Consultar las operaciones de exportación activas o suspendidas)	1484
QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)	1488
QUERY FILESPACE (Consultar uno o más espacios de archivos)	1489
QUERY LIBRARY (Consultar una biblioteca)	1495
QUERY LIBVOLUME (Consultar un volumen de biblioteca)	1498
QUERY LICENSE (Visualizar información sobre licencias)	1499
QUERY LOG (Visualizar información sobre el registro de recuperación)	1502
QUERY MACHINE (Consultar información de máquina)	1504
QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)	1506
QUERY MGMTCLASS (Consultar una clase de gestión)	1511
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	1513
QUERY MONITORSTATUS (Consultar el estado de supervisión)	1515
QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)	1519
QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)	1520
QUERY NODE (Consultar nodos)	1524
QUERY NODEDATA (Consultar datos de cliente en volúmenes)	1533
QUERY NODEGROUP (Consultar un grupo de nodos)	1535
QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)	1537
QUERY OPTION (Consultar opciones del servidor)	1540
QUERY PATH (visualizar una definición de ruta)	1541
QUERY POLICYSET (Consultar un juego de políticas)	1544
QUERY PROCESS (Consultar uno o más procesos de servidor)	1546
QUERY PROFILE (Consultar un perfil)	1550
QUERY PROTECTSTATUS (Consultar estado de protección de una agrupación de almacenamiento)	1552
QUERY PROXYNODE (Consulta la autorización de proxy de un nodo cliente)	1554
QUERY PVUESTIMATE (Mostrar la estimación de unidades de valor de procesador)	1555
QUERY RECOVERYMEDIA (Consultar medio de recuperación)	1558
QUERY REPLICATION (Consultar los procesos de réplica de nodos)	1560
QUERY REPLNODE (Mostrar información sobre el estado de réplica de un nodo de cliente)	1568
QUERY REPLRULE (Consultar reglas de réplica)	1571
QUERY REPLSERVER (Consultar un servidor de réplica)	1572
QUERY REQUEST (Consultar una o más peticiones de montaje pendientes)	1574
QUERY RESTORE (Consultar sesiones de restauración reiniciables)	1575
QUERY RPFCONTENT (Consultar el contenido del archivo del plan de recuperación almacenado en un servidor de destino)	1577
QUERY RPFFILE (Consultar la información del archivo del plan de recuperación almacenado en un servidor de destino)	1578
QUERY SAN (Consultar los dispositivos de la SAN)	1580
QUERY SCHEDULE (Consultar planificaciones)	1582
QUERY SCHEDULE (Consultar planificaciones de cliente)	1583
QUERY SCHEDULE (Consultar una planificación de administración)	1586
QUERY SCRATCHPADENTRY (Consultar una entrada de registro)	1588
QUERY SCRIPT (Consultar scripts IBM Spectrum Protect)	1589
QUERY SERVER (Consultar un servidor)	1592
QUERY SERVERGROUP (Consultar un grupo de servidores)	1595
QUERY SESSION (Consultar sesiones de cliente)	1596

QUERY SHREDSTATUS (Consultar estado de destrucción)	1599
QUERY SPACETRIGGER (Consultar los desencadenantes de espacio)	1601
QUERY STATUS (Consultar parámetros del sistema)	1602
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	1611
QUERY STGPOOL (Consultar agrupaciones de almacenamiento)	1613
QUERY STGPOOLDIRECTORY (Consulta de un directorio de agrupaciones de almacenamiento)	1627
QUERY SUBSCRIBER (Visualizar información de suscriptor)	1629
QUERY SUBSCRIPTION (Visualizar información de inscripción)	1631
QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)	1632
QUERY TAPEALERTMSG (Visualizar estado del comando SET TAPEALERTMSG)	1633
QUERY TOC (Visualizar tabla de contenido para una imagen de copia de seguridad)	1634
QUERY VIRTUALFSMAPPING (Consultar una correlación de espacios de archivos virtuales)	1636
QUERY VOLHISTORY (Visualizar información histórica de volúmenes secuenciales)	1637
QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)	1643
QUIT (finalizar la modalidad interactiva del cliente de administración)	1649
RECLAIM STGPOOL (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)	1650
RECONCILE VOLUMES (Reconciliar diferencias en definiciones de volúmenes virtuales)	1652
Comandos REGISTER	1654
REGISTER ADMIN (Registrar un ID de administrador)	1654
REGISTER LICENSE (Registrar una nueva licencia)	1657
REGISTER NODE (Inscribir un nodo)	1658
Comandos REMOVE	1672
REMOVE ADMIN (Suprimir un ID de usuario administrador)	1673
REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)	1673
REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)	1675
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	1676
REMOVE REPLSERVER (Eliminar un servidor de réplica)	1677
Comandos RENAME	1678
RENAME ADMIN (redenominar un administrador)	1678
RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)	1679
RENAME NODE (Cambiar el nombre de un nodo)	1682
RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)	1683
RENAME SERVERGROUP (Redenominar un grupo de servidores)	1683
RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)	1684
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)	1685
REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)	1687
REPLY (Permitir una petición para continuar el proceso)	1695
RESET PASSEXP (restablecer caducidad de contraseña)	1695
RESTART EXPORT (Reiniciar una operación de exportación suspendida)	1696
Comandos RESTORE	1697
RESTORE NODE (Restaurar un nodo NAS)	1697
RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)	1701
RESTORE VOLUME (Restaurar datos de volumen primario desde una agrupación de copia o agrupación de datos activos)	1705
Comandos REVOKE	1708
REVOKE AUTHORITY (revocar autorización de administrador)	1708
REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)	1710
ROLLBACK (Retrotraer cambios no validados en una macro)	1711
RUN (ejecutar un script de IBM Spectrum Protect)	1712
SELECT (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)	1714
Comandos SET	1722
SET ACCOUNTING (activar o desactivar registros de contabilidad)	1723
SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)	1724
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	1725
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	1726
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	1726
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	1727
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	1728

SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	1729
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	1729
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	1730
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	1731
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	1732
SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)	1732
SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)	1733
SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)	1735
SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)	1736
SET CONFIGMANAGER (Especificar un gestor de configuración)	1737
SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)	1738
SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)	1739
SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)	1739
SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)	1740
SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)	1741
SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)	1743
SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)	1744
DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)	1745
SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)	1746
SET DRMCHECKLABEL (Especificar comprobación de etiquetas)	1747
SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener comandos)	1747
SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)	1748
SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)	1749
SET DRMCOURIERNAME (Especificar el nombre del transportista)	1750
SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)	1750
SET DRMFILPROCESS (Especificar el proceso de archivos)	1751
SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)	1752
SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)	1754
SET DRMPPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)	1755
SET DRMPPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)	1757
SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)	1757
SET DRMPRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)	1758
SET DRMVaultNAME (Especificar el nombre de la cámara de seguridad)	1759
SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)	1760
SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)	1761
SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)	1761
SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)	1762
SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)	1763
SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)	1764
SET MAXCMDRETRIES (Establecer el número máximo de reintentos de comando)	1765
SET MAXSCHEDULESESSIONS (Establecer número máximo de sesiones planificadas)	1765
SET MINPWLENGTH (Establecer longitud mínima de contraseña)	1766
SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)	1767
SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)	1768
SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)	1768
SET PASSEXP (Establecer fecha de caducidad de contraseña)	1770
SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)	1771
SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)	1773
SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)	1773
SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)	1774
SET REPLRETENTION (Establecer el período de retención de los registros de réplica)	1776
SET REPLSERVER (Establecer el servidor de réplica de destino)	1777
SET RETRYPERIOD (Establecer período de tiempo entre reintentos)	1778
SET SCHEDMODES (seleccionar modalidad de planificación central)	1779
SET SCRATCHPADRETENTION (Establecer hora de retención de registro)	1779

SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)	1780
SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)	1781
SET SERVERNAME (Especificar el nombre del servidor)	1781
SET SERVERPASSWORD (Establecer contraseña de servidor)	1782
SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)	1783
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	1784
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	1785
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	1786
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	1787
SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)	1788
SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)	1789
SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)	1790
SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)	1791
SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)	1791
SETOPT (Establecer una opción de servidor para actualización dinámica)	1793
SHRED DATA (destruir datos)	1794
SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)	1796
Mandatos UNLOCK	1796
UNLOCK ADMIN (Desbloquear un administrador)	1797
UNLOCK NODE (Desbloquear un nodo cliente)	1798
UNLOCK PROFILE (Desbloquear un perfil)	1798
Comandos UPDATE	1799
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	1800
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	1801
UPDATE ADMIN (Actualizar un administrador)	1803
UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)	1806
UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)	1810
UPDATE CLOPTSET (Actualizar la descripción de un conjunto de opciones de cliente)	1811
UPDATE COLLOGGROUP (Actualizar un grupo de proximidad)	1811
UPDATE COPYGROUP (Actualizar un grupo de copia)	1812
UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)	1813
UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)	1816
UPDATE DATAMOVER (Actualizar un transportador de datos)	1818
UPDATE DEVCLASS (Actualizar los atributos de una clase de dispositivo)	1819
3590	1820
3592	1823
4MM	1827
8MM	1830
Centera	1834
DLT	1836
Ecartridge	1839
Archivo	1843
Generictape	1847
LTO	1849
NAS	1854
Removablefile	1855
Servidor	1857
VolSafe	1858
UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS)	1861
3590, para el servidor de medios de z/OS	1861
3592, para el servidor de medios de z/OS	1865
ECARTRIDGE, para el servidor de medios de z/OS	1868
FILE, para el servidor de medios de z/OS	1872
UPDATE DOMAIN (Actualizar un dominio de políticas)	1874
UPDATE DRIVE (Actualizar una unidad)	1876
UPDATE FILESPACE (Actualizar reglas de réplica de nodos de espacio de archivos)	1879
UPDATE LIBRARY (Actualizar una biblioteca)	1882

349X	1883
ACSLs	1885
EXTERNAL	1887
FILE	1888
MANUAL	1888
SCSI	1889
Compartido	1892
VTL	1892
UPDATE LIBVOLUME (Cambiar el estado de un volumen de almacenamiento)	1894
UPDATE MACHINE (Actualizar información de máquina)	1895
UPDATE MGMTCLASS (Actualizar una clase de gestión)	1896
UPDATE NODE (Actualizar atributos del nodo)	1898
UPDATE NODEGROUP (Actualizar un grupo de nodos)	1912
UPDATE PATH (cambiar una ruta)	1913
El destino es una unidad	1914
El destino es una biblioteca	1918
El destino es una biblioteca ZOSMEDIA	1920
UPDATE POLICYSET (Actualizar la descripción de un juego de políticas)	1921
UPDATE PROFILE (Actualizar una descripción de perfil)	1922
UPDATE RECOVERYMEDIA (Actualizar medio de recuperación)	1922
UPDATE REPLRULE (Actualizar reglas de réplica)	1924
UPDATE SCHEDULE (Actualizar una planificación)	1925
UPDATE SCHEDULE (Actualizar una planificación de cliente)	1925
UPDATE SCHEDULE (Actualizar una planificación de administración)	1935
UPDATE SCRATCHPADENTRY (Actualizar una entrada de registro)	1942
UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)	1943
UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)	1944
UPDATE SERVERGROUP (Actualizar una descripción de grupo de servidores)	1949
UPDATE SPACETRIGGER (Actualizar los desencadenantes de espacio)	1949
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	1951
UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)	1954
Agrupación de almacenamiento de contenedores en la nube	1955
Agrupación de almacenamiento de contenedores de directorio	1958
Agrupación de almacenamiento de copia de contenedor	1962
Agrupación de acceso aleatorio primaria	1964
Agrupación de acceso secuencial primaria	1972
Agrupación de copias	1983
Agrupación de datos activos	1988
UPDATE STGPOOLDIRECTORY (Actualización de un directorio de agrupaciones de almacenamiento)	1993
UPDATE VIRTUALFSMAPPING (Actualizar una correlación de espacios de archivos virtuales)	1995
UPDATE VOLHISTORY (Actualizar información histórica de volúmenes secuenciales)	1996
UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)	1998
Comandos VALIDATE	2001
VALIDATE ASPERA (Validación de una configuración Aspera FASP)	2001
VALIDATE CLOUD (Validar credenciales de nube)	2004
VALIDATE LANFREE (Validar rutas fuera de la LAN)	2006
VALIDATE POLICYSET (Verificar un juego de políticas)	2007
VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)	2008
VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)	2012
VARY (Activar o desactivar un volumen de acceso aleatorio)	2013
Opciones de servidor	2014
Modificación de opciones del servidor	2022
Tipos de opciones del servidor	2022
Opciones de comunicación del servidor	2022
Opciones de almacenamiento del servidor	2024
Opciones de cliente/servidor	2025
Opciones de fecha, número, hora e idioma	2026
Opciones de la base de datos	2026

Opciones de transferencia de datos	2027
Opciones de mensajes	2027
Opciones de anotaciones de eventos	2027
Opciones de seguridad y del sistema de licencias	2028
Opciones varias	2028
3494SHARED	2029
ACSACCESSID	2030
ACSLOCKDRIVE	2030
ACSQUICKINIT	2030
ACSTIMEOUTX	2031
ACTIVELOGDIRECTORY	2031
ACTIVELOGSIZE	2032
ADMINCOMMTIMEOUT	2032
ADMINIDLETIMEOUT	2033
ADMINONCLIENTPORT	2033
ADSMGROUPNAME	2033
ALIASHALT	2034
ALLOWDESAUTH	2034
ALLOWREORGINDEX	2035
ALLOWREORGTABLE	2035
ARCHFAILOVERLOGDIRECTORY	2036
ARCHLOGCOMPRESS	2036
ARCHLOGDIRECTORY	2037
ARCHLOGUSEDTHRESHOLD	2037
ASSISTVCRRECOVERY	2038
AUDITSTORAGE	2038
BACKUPINITIATIONROOT	2038
CHECKTAPEPOS	2039
CLIENTDEDUPTXNLIMIT	2040
COMMMETHOD	2041
COMMTIMEOUT	2041
CONTAINERRESOURCESTIMEOUT	2042
DATEFORMAT	2042
DBDIAGLOGSIZE	2043
DBDIAGPATHFSTHRESHOLD	2044
DBMEMPERCENT	2044
DBMTCPPORT	2045
DEDUPREQUIRESBACKUP	2045
DEDUPTIER2FILESIZE	2046
DEDUPTIER3FILESIZE	2046
DEVCONFIG	2047
DISABLEREORGTABLE	2048
DISABLESCHEDS	2048
DISPLAYLFINFO	2048
DNSLOOKUP	2049
DRIVEACQUIRERETRY	2050
ENABLENASDEDUP	2050
EVENTSERVER	2051
EXPINTERVAL	2051
EXPQUIET	2052
FASPBEGPORT	2052
FASPENDPORT	2052
FASPTARGETRATE	2053
FFDCLOGLEVEL	2054
FFDCLOGNAME	2054
FFDCMAXLOGSIZE	2055
FFDCNUMLOGS	2055
FILEEXIT	2056

FILETEXTEXIT	2056
FSUSEDTHRESHOLD	2057
IDLETIMEOUT	2057
KEEPALIVE	2058
KEEPALIVETIME	2058
KEEPALIVEINTERVAL	2059
LANGUAGE	2059
LDAPCACHEDURATION	2062
LDAPURL	2062
MAXSESSIONS	2063
MESSAGEFORMAT	2063
MIRRORLOGDIRECTORY	2064
MOVEBATCHSIZE	2064
MOVESIZETHRESH	2065
MSGINTERVAL	2065
NAMEDPIPENAME	2065
NDMPCONNECTIONTIMEOUT	2066
NDMPCONTROLPORT	2066
NDMPENABLEKEEPALIVE	2066
NDMPKEEPIDLEMINUTES	2067
NDMPPORTRANGE	2067
NDMPREFDATAINTERFACE	2068
NOPREEMPT	2069
NORETRIEVEDATE	2069
NPAUDITFAILURE	2070
NPAUDITSUCCESS	2070
NPBUFFERSIZE	2071
NUMBERFORMAT	2071
NUMOPENVOLSALLOWED	2071
PUSHSTATUS	2072
QUERYAUTH	2073
RECLAIMDELAY	2073
RECLAIMPERIOD	2074
REORGBEGINTIME	2074
REORGDURATION	2075
REPORTRETRIEVE	2075
REPLBATCHSIZE	2076
REPLSIZETHRESH	2076
REQSYSAUTHOUTFILE	2077
RESOURCETIMEOUT	2077
RESTOREINTERVAL	2078
RETENTIONEXTENSION	2078
SANDISCOVERY	2079
SANDISCOVERYTIMEOUT	2079
SANREFRESHTIME	2080
SEARCHMPQUEUE	2080
SECUREPIPES	2081
SERVERDEDUPTXNLIMIT	2081
SHMPORT	2082
SHREDDING	2083
SNMPHEARTBEATINTERVAL	2083
SNMPMESSAGECATEGORY	2083
SNMPSUBAGENT	2084
SNMPSUBAGENTHOST	2085
SNMPSUBAGENTPORT	2085
SSLFIPSMODE	2085
SSLINITTIMEOUT	2086
SSLTCPADMINPORT	2086

SSLTCPPOINT	2087
TCPADMINPORT	2087
TCPBUFSIZE	2088
TCPNODELAY	2088
TCPPOINT	2089
TCPWINDOWSIZE	2089
TECBEGINEVENTLOGGING	2090
TECHOST	2090
TECPPOINT	2091
TECUTF8EVENT	2091
THROUGHPUTDATATHRESHOLD	2091
THROUGHPUTTIMETHRESHOLD	2092
TIMEFORMAT	2092
TXNGROUPMAX	2093
UNIQUEDPTECEVENTS	2094
UNIQUETECEVENTS	2094
USEREXIT	2094
VERBCHECK	2095
VOLUMEHISTORY	2096
Herramientas del servidor	2096
DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)	2097
DSMSERV (Iniciar el servidor)	2097
Script de inicio del servidor: rc.dsmserv	2099
Script de inicio del servidor: dsmserv.rc	2100
DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)	2101
DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)	2102
DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)	2103
DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)	2105
DSMSERV INSERTDB (Mover una base de datos de servidor a una base de datos vacía)	2107
DSMSERV LOADFORMAT (Formatear una base de datos)	2109
DSMSERV REMOVEDB (Eliminar una base de datos)	2110
DSMSERV RESTORE DB (Restaurar la base de datos)	2112
DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)	2112
DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)	2115
DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)	2118
DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)	2119
Programas de utilidad de dispositivo	2119
AIX: tsmdlst (Visualizar información sobre dispositivos)	2119
Linux: autoconf (dispositivos de configuración automática)	2120
Windows: tsmdlst (Visualizar información sobre dispositivos)	2122
Scripts de servidor y macros para automatización	2124
Scripts de servidor	2124
Definición de un script de servidor	2124
Ejecución de mandatos en paralelo o en serie	2125
Continuación de mandatos a través de varias líneas de mandatos	2126
Inclusión de las variables de sustitución en un script	2126
Inclusión de sentencias de flujo lógico en un script	2127
Especificación de la cláusula IF	2127
Especificación de la sentencia EXIT	2128
Especificación de la sentencia GOTO	2128
Utilización de mandatos SELECT en un script	2128
Actualización de un script	2129
Añadir un nuevo mandato	2129
Sustitución de un mandato existente	2130
Adición de un mandato y un número de línea	2130
Supresión de un mandato de un script del servidor	2130
Consulta de un script de servidor para crear otro script de servidor	2130
Ejecución de un script del servidor	2131



Macros de cliente administrativo	2131
Grabación de mandatos en una macro	2132
Grabación de comentarios en una macro	2132
Inclusión de caracteres de continuación en una macro	2132
Inclusión de las variables de sustitución en un macro	2133
Ejecución de una macro	2134
Proceso de mandatos en una macro	2134
Códigos de retorno de los scripts para IBM Spectrum Protect	2135
Archivos PDF	2137

## Cientes

Cientes	2137
Novedades	2138
Actualizaciones del cliente de archivado y copia de seguridad	2138
Notas del release V8.1	2144
Archivos léame de los fixpacks de la versión 8.1	2146
Últimas actualizaciones de la documentación	2146
Protección para estaciones de trabajo y servidores de archivos	2146
Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)	2147
Actualización del cliente de archivado y copia de seguridad	2148
Actualización de la vía de acceso para clientes y servidores	2148
Información adicional sobre la actualización	2148
Despliegue automático del cliente de copia de seguridad y archivado	2149
Requisitos del entorno del cliente	2150
Entorno del cliente AIX	2150
Componentes instalables del cliente AIX	2150
Requisitos de sistema para el cliente de AIX	2151
Métodos de comunicación del cliente AIX	2151
Funciones de cliente de archivado y copia de seguridad disponibles en AIX	2151
Entorno de la API de HP-UX Itanium 2	2151
Componente instalable de la API de HP-UX Itanium 2	2152
Requisitos del sistema para la API de HP-UX Itanium 2	2152
Métodos de comunicación de la API de HP-UX Itanium 2	2152
Entorno de clientes de Linux on Power Systems	2152
Componentes instalables de cliente de Linux on Power Systems	2152
Requisitos de sistema para clientes en Linux en Power Systems	2152
Métodos de comunicación de cliente de Linux on Power Systems	2153
Entorno de cliente Linux x86_64	2153
Componentes instalables del cliente Linux x86_64	2153
Requisitos de sistema para clientes Linux x86_64	2153
Métodos de comunicación del cliente Linux x86_64	2153
Entorno de cliente Linux on System z	2154
Componentes instalables del cliente Linux on System z	2154
Requisitos de sistema para clientes Linux on System z	2154
Métodos de comunicación del cliente Linux on System z	2154
Entorno del cliente Mac OS X	2155
Componentes instalables del cliente Mac OS X	2155
Requisitos de sistema para clientes Mac OS X	2155
Métodos de comunicación del cliente Mac OS X	2155
Entorno de cliente Oracle Solaris	2156
Componentes instalables del cliente Oracle Solaris	2156
Requisitos de sistema para clientes Oracle Solaris	2156
Métodos de comunicación del cliente Oracle Solaris	2156
Requisitos del entorno de cliente Windows	2157
Componentes instalables del cliente Windows	2157
Requisitos de sistema para clientes Windows	2157
Métodos de comunicación del cliente Windows	2157
Funciones de cliente de archivado y copia de seguridad disponibles en las plataformas de Windows	2157
Sistemas de archivos compatibles con Windows	2158

Requisitos de soporte para NDMP (sólo Extended Edition)	2158
Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack	2158
Asistente para la configuración del cliente para Tivoli Storage Manager FastBack	2159
Instalar los clientes de archivado y copia de seguridad UNIX y Linux	2159
Instalación del cliente AIX	2160
Desinstalación del cliente AIX	2162
Instalación de la API de HP-UX Itanium 2	2163
Desinstalación de la API de HP-UX Itanium 2	2164
Instalación del cliente en Linux on Power Systems (Little Endian)	2165
Desinstalación del cliente en Linux on Power (Little Endian)	2167
Instalación del cliente Ubuntu Linux on Power Systems (Little Endian)	2168
Desinstalación del cliente en Ubuntu Linux on Power Systems (Little Endian)	2169
Instalación de la API en Linux on Power Systems (Big Endian)	2170
Desinstalación de la API en Linux on Power Systems (Big Endian)	2172
Instalación del cliente Linux x86_64	2173
Desinstalación del cliente Linux x86_64	2175
Instalación del cliente Ubuntu Linux x86_64	2176
Desinstalación del cliente Ubuntu Linux x86_64	2179
Instalación del cliente Linux on System z	2180
Desinstalación del cliente Linux on System z	2182
Instalación del cliente Mac OS X	2183
Desinstalación del cliente Mac OS X	2184
Instalación del cliente de Oracle Solaris x86_64	2185
Desinstalación del cliente Oracle Solaris x86_64	2187
Instalación de la API de Oracle Solaris SPARC	2187
Desinstalación de la API de Oracle Solaris SPARC	2188
Actualizaciones de software (clientes de AIX, Linux, Mac y Solaris)	2189
Visión general de instalación de cliente de Windows	2189
Es posible que la instalación de cliente Windows necesite un rearranque	2190
Procedimientos de instalación	2190
Instalación del cliente Windows por primera vez	2191
Actualización del cliente Windows	2193
Reinstalación del cliente Windows	2195
Instalación silenciosa	2195
Modificación, reparación o desinstalación del cliente Windows	2198
Resolución de problemas durante la instalación de (Windows)	2199
Actualizaciones de software (clientes de Windows)	2199
Instalación de servicio de gestión de cliente	2200
Configuración de clientes de copia de seguridad/archivado	2200
Configurar el cliente de IBM Spectrum Protect	2200
Tareas de usuario root y autorizado del cliente de UNIX y Linux	2202
Permitir que los usuarios no root gestionen sus propios datos	2204
Descripción general del archivo de opciones de cliente	2205
Creación y modificación del archivo opciones del sistema del cliente	2207
Creación y modificación del archivo de opciones del cliente	2209
Creación de un archivo de opciones predeterminado de usuario-cliente	2210
Creación de un archivo de opciones del usuario cliente personalizado	2211
Crear un archivo de opciones de directorio compartido	2212
Creación de varios archivos de opciones de cliente	2212
Variables de entorno (Windows)	2213
Variables de entorno (AIX, Linux, Mac, Solaris)	2213
Definir variables de entorno de idioma	2214
Definir variables de entorno de proceso	2214
Definir variables de shell Bourne y Korn	2216
Definir variables de shell C	2216
Definir variables de entorno de la API	2216
Configuración del idioma para visualizar la GUI de Java	2217
Descripción general de la configuración del cliente web	2217

Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris	2218
Configuración del cliente web en sistemas Windows	2219
Configuración del planificador	2220
Comparación entre servicios gestionados por el aceptador de cliente y servicios del planificador tradicional	2220
Configuración del cliente para que utilice el servicio del aceptador de cliente para gestionar el planificador	2221
Inicie el planificador de cliente (AIX, Linux, Mac, Solaris)	2222
Inicio del planificador cliente (Windows)	2223
Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect a través de un cortafuegos	2223
Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer	2225
Creación de un enlace simbólico para acceder a la biblioteca de GSKit más reciente	2227
Certificados raíz de entidades emisoras de certificados	2228
Configuración del sistema para copia de seguridad con registro por diario	2229
Configuración del servicio de motor con registro por diario	2229
Stanza JournalSettings (Windows)	2231
Sección JournalExcludeList	2232
Sección JournaledFileSystemSettings	2233
Modificación de stanzas	2235
Configuración del daemon de registro por diario	2236
Sección JournalSettings	2237
Sección JournalExcludeList	2238
Sección JournaledFileSystemSettings	2238
Modificación de stanzas	2240
Deduplicación de datos del lado del cliente	2241
Configuración del cliente para la eliminación de duplicados de datos	2243
Excluir archivos de la eliminación de duplicados de datos	2245
Configuración y uso de la migración tras error automática del cliente	2247
Visión general de migración tras error de cliente automatizado	2247
Requisitos para la migración tras error automática del cliente	2248
Restricciones de la migración tras error automática de cliente	2248
Funciones de migración tras error de otros componentes	2249
Configuración del cliente de migración automática tras error	2250
Determinación del estado los datos replicados del cliente	2251
Prevención de la migración tras error automática del cliente	2252
Forzar al cliente a la migración tras error	2253
Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack	2253
Configuración del cliente de copia de seguridad y archivado para proteger datos del cliente FastBack	2254
Configuración y utilización del entorno en clúster	2255
Visión general de entornos en clúster	2256
Activa/Activa: Agrupación de recursos de clúster	2256
Activa/Pasiva: Tolerante a errores	2256
Acceso simultáneo	2256
Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster	2257
Habilitación del acceso al cliente web en un entorno de clúster	2261
Migración de configuraciones de AIX/IBM PowerHA SystemMirror antiguas	2263
Copias de seguridad en un entorno de servidor en clúster	2263
Protección de los datos en los clústeres de MSCS (clientes del servidor Windows)	2264
Configurar el cliente web en un entorno en clúster	2264
Preguntas frecuentes	2265
Configuración del soporte de copias de seguridad de imagen en línea	2266
Configuración del soporte de archivos abiertos	2267
Consideraciones para la configuración de AIX antes de realizar copias de seguridad y archivado basadas en instantáneas	2268
Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea	2268
Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster	2269
Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)	2272
Registrar la estación de trabajo en un servidor	2275
Inscripción cerrada	2275
Inscripción abierta	2276
Creación de una lista de inclusión/exclusión	2276

Opciones de inclusión/exclusión	2278
Exclusión de espacios de archivos y directorios	2278
Sentencias de inclusión/exclusión para sistemas de archivos en red	2280
Excluir archivos y directorios de la copia de seguridad con registro por diario	2281
Controlar proceso de sentencias de exclusión	2281
Archivos del sistema a excluir	2283
Excluir archivos con nombres UNC	2284
Incluir y excluir archivos con caracteres comodín	2285
Inclusión y exclusión de grupos de archivos con caracteres comodín	2286
Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión	2287
Proceso de enlaces simbólicos y alias	2290
Determinar el proceso de compresión y cifrado	2290
Vista previa de los archivos de la lista de inclusión-exclusión	2291
Inclusión y exclusión de proceso de opciones	2292
Reglas de proceso y utilización de nombres UNC	2295
Uso explícito de nombres UNC para unidades remotas	2295
Conversión de nombres de vía de accesos de DOS para unidades fijas y remotas	2295
Ejemplos de coincidencia de clases de caracteres	2296
Cómo empezar	2296
Configuración de los valores de seguridad del cliente para la conexión al servidor de IBM Spectrum Protect versión 8.1.2 y posterior	2297
Valores de seguridad predeterminados para el cliente (vía de acceso rápida)	2297
Configuración del cliente sin distribución de certificados automática	2299
Almacenamiento seguro de contraseñas	2301
Derechos de seguridad y operaciones del cliente de archivado y copia de seguridad	2302
Operaciones del grupo Operadores de copia de seguridad	2304
Consideraciones que deben tenerse en cuenta antes de empezar a utilizar una cuenta del grupo de operadores de copia de seguridad	2304
Permisos necesarios para restaurar archivos que utilizan la copia de seguridad adaptable de subarchivos	2304
Permisos necesarios para copias de seguridad, archivado, restauración o recuperación de archivos en recursos de clúster	2305
Autenticación del cliente de IBM Spectrum Protect	2305
Control de cuentas de usuario	2306
Inicio de una sesión en la GUI Java	2306
contraseña de IBM Spectrum Protect	2307
Asistente para la instalación	2307
Inicio de una sesión de línea de mandatos	2307
Utilización de la modalidad por lotes	2308
Emisión de una serie de mandatos mediante la modalidad interactiva	2309
Visualización de caracteres de euro en el indicador de línea de mandatos	2309
Utilizar las opciones del mandato DSMC	2309
Especificación de cadenas de entrada que contengan espacios en blanco o comillas	2310
Inicio: consideraciones adicionales	2310
Utilización del cliente web en el nuevo entorno de seguridad	2311
Iniciar automáticamente el planificador cliente	2311
Cambio de la contraseña	2312
Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado	2313
Visualización de ayuda en línea	2314
Finalización de una sesión	2314
Foros en línea	2315
Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad	2316
Copia de seguridad de los datos	2316
Planificación de las copias de seguridad(Windows)	2319
Planificación de las copias de seguridad	2320
Los archivos de los que se hace copia de seguridad	2320
Soporte de archivos abiertos para las operaciones de copia de seguridad	2320
Copia de seguridad de datos mediante la GUI	2322
Copia de seguridad de datos mediante la línea de mandatos	2323
Supresión de datos de copia de seguridad	2325

Cuándo realizar copias de seguridad y cuándo archivar copias	2325
Consideraciones previas a la copia de seguridad (Windows)	2326
traspaso de datos sin LAN	2327
Requisitos previos del soporte para fuera de la LAN	2327
Opciones de traspaso de datos fuera de la LAN	2327
Espacios de archivos Unicode (Windows)	2328
Copias de seguridad incrementales en sistemas con restricción de memoria	2328
Copias de seguridad incrementales en sistemas con un gran número de archivos	2328
Proceso de control con una lista de inclusión-exclusión	2329
Cifrado de datos durante una operación de copia de seguridad o archivado	2330
Tamaño máximo de archivo para operaciones	2330
Cómo gestiona el cliente los nombres de usuario y de grupo largos	2330
Consideraciones previas a la copia de seguridad (UNIX y Linux)	2331
traspaso de datos sin LAN	2332
Requisitos previos del soporte para fuera de la LAN	2332
Opciones de traspaso de datos fuera de la LAN	2332
Copias de seguridad incrementales en sistemas con restricción de memoria	2333
Copias de seguridad incrementales en sistemas con un gran número de archivos	2333
Opciones de inclusión/exclusión para controlar el proceso	2334
Cifrado de datos durante una operación de copia de seguridad o archivado	2334
Soporte para sistemas de archivos y ACL	2335
Tamaño máximo de archivo para operaciones	2338
Nombres de usuario y de grupo largos	2338
Nombres de volumen en Mac OS X	2339
Precauciones respecto a la asignación de nombres de volumen en Mac OS X	2339
Precauciones respecto a la asignación de nombres de volumen en Mac OS X en sistemas de arranque dual	2340
Habilitación de Unicode para Mac OS X	2340
Disco de copia de seguridad Time Machine de Mac OS X	2340
Copias de seguridad incrementales, selectivas o incrementales por fecha (Windows)	2341
Copia de seguridad incremental completa y parcial	2342
Copia de seguridad incremental por fecha	2344
Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales	2344
Copia de seguridad diferencial de instantánea con HTTPS (Windows)	2345
Copia de seguridad selectiva	2346
Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)	2347
Copia de seguridad incremental completa y parcial	2348
Copia de seguridad incremental por fecha	2350
Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales	2350
Copia de seguridad diferencial de instantánea con HTTPS (Linux)	2352
Copia de seguridad selectiva	2352
Zona global Solaris y copias de seguridad de zonas no globales	2353
Cómo guardar permisos de acceso	2353
Establecimiento de un punto de montaje virtual	2353
Copia de seguridad de datos mediante la GUI Java	2353
Copia de seguridad de datos mediante la línea de mandatos	2354
Supresión de datos de copia de seguridad	2357
Supresión de espacios de archivos	2357
Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (Windows)	2358
Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)	2358
Copia de seguridad de datos con soporte de proxy de nodo cliente (Windows)	2359
Habilitación de varias operaciones de nodos desde la GUI	2360
Configuración del cifrado	2361
Copias de seguridad de planificación con soporte de proxy de nodo cliente	2361
Copia de seguridad con soporte de proxy de nodo cliente (UNIX y Linux)	2362
Habilitación de varias operaciones de nodos desde la GUI	2360
Configuración del cifrado	2363

Copias de seguridad de planificación con soporte de proxy de nodo cliente	2364
Ejemplos de cómo planificar una copia de seguridad de un clúster de IBM PowerHA SystemMirror	2364
Planificar una copia de seguridad de un sistema de archivos de GPFS	2366
Asociar una instantánea local con un espacio de archivos del servidor (Windows)	2367
Asociar una instantánea local con un espacio de archivos del servidor (UNIX y Linux)	2367
Copia de seguridad del estado del sistema de Windows	2367
Copia de seguridad de los archivos de Recuperación automática del sistema	2368
Preparación para la recuperación automática del sistema	2369
Crear un archivo de opciones del cliente para la recuperación automática del sistema	2369
Realizar la copia de seguridad de la unidad de arranque y de la unidad del sistema para Automated System Recovery	2370
Copia de seguridad de imagen	2370
Realización de tareas de requisitos previos antes de crear una copia de seguridad de imágenes	2372
Utilización de las copias de seguridad de imagen para realizar copias de seguridad incrementales del sistema de archivos	2374
Método 1: Uso de las copias de seguridad de imagen con las copias de seguridad incrementales de sistemas de archivos	2374
Método 2: Uso de las copias de seguridad de imagen con las copias de seguridad de imagen incremental por fecha	2375
Comparación de los métodos 1 y 2	2376
Realización de una copia de seguridad de imagen mediante la GUI	2376
Realización de una copia de seguridad de imagen mediante la línea de mandatos	2378
Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea	2378
Protección de los sistemas de archivos Btrfs	2379
Realizar la copia de seguridad y la restauración de los sistemas de archivos Btrfs	2380
Copia de seguridad y restauración de los subvolumenes Btrfs	2381
Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes	2382
Copia de seguridad de los sistemas de archivos NAS con la GUI del cliente web utilizando el Protocolo de gestión de datos de redes NDMP	2383
Copia de seguridad de sistemas de archivos NAS mediante la línea de mandatos	2384
Métodos para realizar la copia de seguridad y recuperar los datos en servidores de archivos NAS a los que se accede mediante el protocolo CIFS	2385
Soporte para Persistent Storage Manager de CDP	2386
Copia de seguridad de sistemas de archivos de red	2387
Copia de seguridad de los sistemas de archivos con partición de carga de trabajo de AIX	2387
Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte	2388
Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX	2389
Copia de seguridad de los atributos ampliados de AIX JFS2	2390
Realización de copia de seguridad de máquinas virtuales VMware	2390
Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware	2393
Creación de copias de seguridad completas de máquinas virtuales VMware	2395
Copias de seguridad paralelas de máquinas virtuales	2396
Realización de copias de seguridad de máquinas virtuales en un sistema Hyper-V	2396
Copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack	2397
Copia de seguridad de las definiciones de compartición de Net Appliance CIFS	2397
Visualización del estado del proceso de copia de seguridad	2397
Copia de seguridad(Windows): Consideraciones adicionales	2401
Archivos abiertos	2401
Nombre de espacio de archivo antiguos en especificaciones de archivos	2402
Clases de gestión	2402
Sistemas de archivos suprimidos	2403
Copia de seguridad de soportes de almacenamiento extraíbles	2403
Unidades fijas	2403
Espacios de archivos NTFS y ReFS	2404
Nombres del convenio de denominación universal	2404
Ejemplos: nombres UNC en las listas de dominios	2404
Ejemplos: copia de seguridad de nombres UNC	2404
Métodos de protección de archivo Microsoft Dfs	2405
Copia de seguridad(UNIX y Linux): Consideraciones adicionales	2407
Archivos almacenados	2408
Sistemas de archivos especiales	2409
NFS o puntos de montaje virtuales	2409

Clases de gestión	2409
Copias de seguridad de enlaces simbólicos	2409
Ejemplos: copia de seguridad incremental o selectiva de enlaces simbólicos	2410
Copia de seguridad incremental de un dominio solamente	2411
Enlaces fijos	2411
Archivos esparcidos	2412
Montajes de hard y soft de NFS	2412
Sistemas de archivos suprimidos	2413
Archivos abiertos	2413
Caracteres comodín	2413
Restauración de los datos	2414
Nombres de archivos duplicados	2416
Restauración de nombres del convenio de denominación universal	2417
Restaurar copias de seguridad activas o inactivas	2417
Restauración de archivos y directorios	2418
Restauración de datos mediante la GUI	2418
Ejemplos de restauración de datos mediante la línea de mandatos	2418
Ejemplos: restauración de grandes cantidades de datos	2420
Restauración estándar de la consulta, sin restauración de la consulta y restauración reiniciable	2421
Proceso de restauración de consulta estándar	2421
Sin consulta de proceso de restauración	2421
Proceso de restauración reiniciable	2422
Restauración del estado del sistema de Windows	2423
Restauración de los archivos de Recuperación automática del sistema	2423
Restaurar el sistema operativo cuando está funcionando el sistema	2423
Recuperación de un equipo cuando el sistema operativo de Windows no funciona	2424
Crear un CD arrancable WinPE	2424
Restaurar el sistema operativo de Windows con Automated System Recovery	2424
Restauración de archivos y árboles Dfs de Microsoft	2425
Restauración de una imagen	2425
Restauración de una imagen mediante la GUI	2426
Restauración de una imagen mediante la línea de mandatos	2427
Restauración de datos desde un conjunto de copias de seguridad	2427
Restauración de conjuntos de copias de seguridad: consideraciones y restricciones	2430
Restauración del conjunto de copias de seguridad	2430
Restauración de conjuntos de copias de seguridad mediante la GUI	2431
Restauraciones de los conjuntos de copia de seguridad utilizando una interfaz de línea de mandatos	2432
Restaurar compartimientos de Net Appliance CIFS	2432
Restauración de datos desde la copia de seguridad de VMware	2433
Restauración de copias de seguridad de máquina virtual completas	2434
Casos de ejemplo para ejecutar el acceso instantáneo de máquina virtual completa y restauración de máquina virtual instantánea completa desde la línea de mandatos del cliente de archivado y copia de seguridad	2435
Casos de ejemplo de limpieza y reparación instantánea de VM completa	2438
Recuperación de condiciones de error no estándar	2439
Escenario: Restauración de copias de seguridad de máquina virtual completas	2440
Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup	2442
Restaurar objetos individuales de Active Directory en Windows	2443
Reanimar objetos tombstone o restaurar desde la copia de seguridad de estado del sistema	2444
Restauración de objetos de Active Directory mediante la GUI y la línea de mandatos	2444
Restricciones y limitaciones al restaurar objetos de Active Directory	2445
Conservación de atributos en objetos tombstone	2446
Modificación del aceptador de cliente y servicios de agente para utilizar el cliente web	2446
Restaurar o recuperar datos durante una migración tras error	2447
Cómo autorizar a otro usuario para que restaure o recupere archivos	2448
Restauración o recuperación de archivos de otro nodo cliente	2449
Restauración o recuperación de archivos en otra estación de trabajo	2449
Supresión de espacios de archivos	2450
Restaurar una imagen en archivo	2451

Gestión de datos del sistema de archivos GPFS con agrupaciones de almacenamiento	2451
Restauración de datos a un instante específico	2452
Restauración de archivos cifrados AIX	2453
Restaurar sistemas de archivos con partición de carga de trabajo de AIX	2454
Restaurar sistemas de archivos NAS	2455
Restauración de sistemas de archivos NAS utilizando el cliente web	2455
Restauración de directorios y archivos NAS mediante el cliente web	2456
Opciones y mandatos para restaurar sistemas de archivos NAS desde la línea de mandatos.	2457
Restaurar copias de seguridad activas o inactivas	2458
Restauración de datos mediante la GUI	2459
Ejemplos de restauración desde la línea de mandatos	2459
Ejemplos: restauraciones mediante la línea de mandatos para grandes cantidades de datos	2460
Restauración estándar de la consulta, sin restauración de la consulta y restauración reiniciable	2461
Proceso de restauración de consulta estándar	2461
Sin consulta de proceso de restauración	2462
Proceso de restauración reiniciable	2463
Restauración de sistemas de archivos ZFS de Solaris	2463
Tareas de restauración adicionales	2464
Cómo autorizar a otro usuario para que restaure o recupere archivos	2464
Restauración o recuperación de archivos de otro nodo cliente	2465
Restaurar o recuperar archivos en otra estación de trabajo	2466
Restauración de un disco en caso de pérdida del mismo	2466
Supresión de espacios de archivos	2467
Habilite SELinux para restaurar los archivos en el cliente de Red Hat Enterprise Linux 5	2467
Archivar y recuperar datos con clientes de archivado y copia de seguridad	2467
Archivar y recuperar datos (Windows)	2468
Copias de archivado	2468
Copia de seguridad o archivo de instantáneas con soporte de archivos abiertos	2469
Archivado de datos con la GUI	2469
Ejemplos de archivado de datos utilizando la línea de mandatos	2470
Archivado de datos mediante el proxy de nodo cliente	2471
Supresión de datos archivados	2472
Recuperar archivos	2473
Recuperación de archivos con la GUI	2473
Recupere las copias de archivado mediante la línea de mandatos	2473
Archivar y recuperar datos (UNIX y Linux)	2474
Copias de archivado	2475
Archivado de datos con la GUI	2475
Ejemplos de archivado de datos utilizando la línea de mandatos	2476
Archivado de datos mediante el proxy de nodo cliente	2477
Supresión de datos archivados	2478
Tareas de archivado avanzadas	2479
Permisos de acceso	2479
Archivar y recuperar enlaces simbólicos	2479
Enlaces fijos	2480
Recuperar archivos	2480
Recuperación de datos con la GUI	2481
Recupere los ejemplos de datos utilizando la línea de mandatos	2481
Archivar clases de gestión	2482
Planificar operaciones para clientes de archivado y copia de seguridad	2482
Visión general del planificador de IBM Spectrum Protect	2483
Ejemplos: manejo de espacios en blanco en nombres de archivos de definiciones de planificación	2484
Horas de inicio preferentes para determinados nodos	2485
Opciones de proceso de planificador	2485
Evaluar códigos de retorno de planificación en scripts de planificación	2486
Códigos de retorno de los scripts preschedulecmd y postschedulecmd	2487
Servicios del planificador de aceptación de clientes frente a los servicios del planificador tradicional	2488



Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar	2488
Ejemplos: visualización de información sobre trabajo planificado	2491
Visualizar información sobre el trabajo completado	2493
Especificar opciones de planificación	2494
Opciones del planificador para los mandatos	2494
Activar o desactivar mandatos planificados	2494
Cambiar las opciones de proceso utilizadas por el servicio del planificador	2495
Gestionar varios requisitos de planificador en un sistema	2495
Códigos de retorno del cliente	2498
Políticas de gestión de almacenamiento	2499
Dominios de políticas y juegos de políticas	2500
Clases de gestión y grupos de copia	2501
Visualizar información sobre clases de gestión y grupos de copia	2502
Atributo Nombre de grupo de copias	2503
Atributo Tipo de copia	2503
Atributo Frecuencia de copia	2503
Atributo Versiones si datos existen	2503
Atributo Versiones si datos suprimidos	2503
Atributo Retener versiones adicionales	2503
Atributo Retener única versión	2504
Atributo Serialización de copia	2504
Parámetro de modalidad de copia	2504
Atributo Destino de copia	2505
Atributo Retener versiones	2505
Atributo Eliminar duplicados de datos	2505
Seleccionar una clase de gestión para los archivos	2505
Asignar una clase de gestión a los archivos	2506
Sustituirla clase de gestión para las copias archivadas	2507
Seleccionar una clase de gestión para los directorios	2507
Vincular clases de gestión a archivos	2508
Revincular las versiones de copias de seguridad a los archivos	2508
Período de gracia de retención	2508
Protección de retención de políticas basadas en sucesos	2509
Opciones y mandatos del cliente de copia de seguridad/archivado	2509
Lectura de diagramas de sintaxis	2510
Opciones de proceso	2512
Visión general de las opciones de proceso	2512
Opciones de comunicación	2513
Opciones de TCP/IP	2514
Opción de Named Pipes	2514
Opciones de memoria compartida	2514
Opciones de servidor	2515
Opciones de proceso de copia de seguridad/archivado	2515
Opciones de proceso de restauración y recuperación	2527
Opciones de planificación	2530
Opciones de formato e idioma	2532
Opciones de proceso de mandatos	2532
Opciones de autorización	2532
Opciones de proceso de errores	2533
Opciones de proceso de transacciones	2533
Opciones de cliente Web	2534
Utilización de opciones con mandatos	2535
Especificación de opciones con un mandato	2535
Opciones que sólo son válidas en la línea de mandatos inicial	2536
Opciones del cliente que pueden establecerse con el servidor de IBM Spectrum Protect	2537
Consulta de opciones del cliente	2538
Absolute	2553

Adlocation	2554
Afmskipuncachedfiles	2554
Archmc	2555
Archsymlinkasfile	2556
Asnodename	2556
Asnodename	2557
Asrmode	2559
Auditlogging	2560
Auditlogname	2562
Autodeploy	2565
Autofsrename	2567
Automount	2569
Backmc	2570
Backupsetname	2570
Basesnapshotname	2571
Cadlistenonport	2573
Casesensitiveaware	2573
Changingretries	2574
Class	2575
Clientview	2576
Clusterdiskonly	2576
Clusternode	2578
Collocatebyfilespec	2579
Commmethod	2580
Commrestartduration	2582
Commrestartinterval	2583
Compressalways	2583
Compression	2584
Console	2586
Createnewbase	2587
Datacenter	2588
Datastore	2589
Dateformat	2589
Dedupcachepath	2593
Dedupcachesize	2593
Eliminación de duplicados	2594
Defaultserver	2595
Deletefiles	2596
Descripción	2596
Detail	2598
Diffsnapshot	2599
Diffsnapshotname	2600
Dirmc	2601
Dironly	2602
Disablenqr	2602
Diskbuffsize	2603
Diskcachelocation	2604
Domain	2605
Domain.image	2610
Domain.nas	2611
Domain.vmfull	2612
Dontload	2619
Dynamicimage	2620
Efsdecrypt	2621
Enable8dot3namesupport	2622
Enablearchiveretentionprotection	2623
Enablededupcache	2624
Enableinstrumentation	2625

Enablelanfree	2626
Encryptiontype	2627
Encryptkey	2628
Errorlogmax	2630
Errorlogname	2631
Errorlogretention	2632
Opciones exclude	2634
Control del proceso de enlaces simbólicos y alias	2638
Control del proceso de compresión	2638
Proceso de sistemas de archivos NAS	2639
Opciones exclude de la máquina virtual	2639
Fbranch	2640
Fbclientname	2640
Fbpolicyname	2642
Fbreposlocation	2643
Fbserver	2645
Fbvolumename	2646
Filelist	2648
Filename	2650
Filesonly	2651
Followsymbolic	2652
Forcefailover	2653
Fromdate	2654
Fromnode	2655
Fromowner	2656
Fromtime	2656
Groupname	2657
Grupos (obsoleto)	2658
Host	2658
Httpport	2658
Hsmreparsetag	2659
Ieobjtype	2660
Ifnewer	2661
Imagegapsize	2661
Imagetofile	2663
Inactive	2663
Incl excl	2664
Opciones include	2665
Control del proceso de enlaces simbólicos y alias	2672
Proceso de compresión y cifrado	2672
Proceso de compresión y cifrado de copia de seguridad	2672
Proceso de sistemas de archivos NAS	2673
Opciones include de la máquina virtual	2674
Include.vm	2674
Include.vmdisk	2675
INCLUDE.VMSNAPSHOTATTEMPTS	2678
INCLUDE.VMTSMVSS	2680
Incrbydate	2682
Incremental	2683
Incrthreshold	2683
Instrlogmax	2684
Instrlogname	2685
Journalpipe	2687
Lanfreecommmethod	2687
Lanfreshmport	2689
Lanfreetcpport	2689
Lanfressl	2690
Lanfreetcpserveraddress	2691

Idioma	2691
Latest	2692
Localbackupset	2693
Makesparsefile	2694
Managedservices	2695
Maxcmdretries	2697
Mbobjrefreshtresh	2697
Mbpctrefreshtresh	2698
Memoryefficientbackup	2699
Mode	2700
Monitor	2704
Myprimaryserver	2705
Myreplicationserver	2706
Namedpipename	2707
Nasnodename	2708
Nfstimeout	2709
Nodename	2710
Nojournal (Windows)	2712
Nojournal (AIX, Linux)	2712
Noprompt	2713
Nrtablepath	2713
Numberformat	2714
Optfile	2717
Contraseña	2717
Passwordaccess	2719
Passworddir	2720
Pick	2721
Pitdate	2722
Pittime	2723
Postschedulecmd/Postnschedulecmd	2724
Postsnapshotcmd	2726
Preschedulecmd/Prenschedulecmd	2727
Preservelastaccessdate	2729
Preservepath	2730
Presnapshotcmd	2734
Queryschedperiod	2736
Querysummary	2736
Quiet	2738
Quotesareliteral	2739
Removeoperandlimit	2740
Replace	2741
Replserverguid	2742
Replservername	2744
Replsslport	2746
Repltcpport	2747
Repltcpserveraddress	2749
Resetarchiveattribute	2751
Resourceutilization	2752
Regulación de las sesiones de copia de seguridad/archivado	2753
Regulación de las sesiones de restauración	2753
Consideraciones relacionadas con la utilización de varias sesiones de cliente	2754
Retryperiod	2754
Revokeremoteaccess	2755
Runasservice	2755
Schedcmddisabled	2756
Schedcmdexception	2757
Schedgroup	2758
Schedlogmax	2759

Schedlogname	2760
Schedlogretention	2761
Schedmode	2762
Schedrestretrdisabled	2764
Scrolllines	2765
Scrollprompt	2765
Servname	2766
Sessioninitiation	2767
Setwindowtitle	2769
Shmport	2770
Showmembers	2770
Skipacl	2771
Skipaclupdatecheck	2772
Skipmissingsyswfiles	2772
Skipntpermissions	2773
Skipntsecuritycrc	2774
Skipsystemexclude	2775
Snapdiff	2776
Snapdiffchangelogdir	2783
Snapdiffhttps	2785
Snapshotcachesize	2786
Snapshotproviderfs	2787
Snapshotproviderimage	2788
Snapshotroot	2789
Srvoptsetencryptiondisabled	2792
Srvprepostscheddisabled	2793
Srvprepostsnapdisabled	2794
Ssl	2795
Sslacceptcertfromserv	2796
Ssldisablelegacytls	2796
Sslfipsmode	2797
Sslrequired	2798
Stagingdirectory	2799
Subdir	2800
Systemstatebackupmethod	2802
Tapeprompt	2803
Tcpadminport	2804
Tcpbuffsize	2805
Tcpcadaddress	2806
Tcpclientaddress	2807
Tcpclientport	2807
Tcpnodelay	2808
Tcpport	2809
Tcpserveraddress	2810
Tcpwindowsize	2810
Timeformat	2812
Toc	2814
Todate	2816
Totime	2816
Txnbytelimit	2817
Type	2818
Updatectime	2819
Usedirectory	2819
Useexistingbase	2820
Usereplicationfailover	2821
Usuarios (obsoleto)	2822
V2archive	2822
Verbose	2823

Verifyimage	2824
Virtualfsname	2824
Virtualmountpoint	2825
Virtualnodename	2826
Vmautostartvm	2827
Vmbackdir	2828
Vmbackuplocation	2829
Vmbackupmailboxhistory	2830
Vmbackuptype	2831
Vmchost	2832
Vmcpw	2833
Vmctlmc	2834
Vmcuser	2835
Vmdatstorethreshold	2835
Vmdefaultdvportgroup	2837
Vmdefaultdvswitch	2838
Vmdefaultnetwork	2838
Vmdiskprovision	2839
Vmenabletemplatebackups	2840
Vmexpireprotect	2841
Vmiscsiadapter	2842
Vmiscsiserveraddress	2843
Vmlimitperdatastore	2844
Vmlimitperhost	2845
Vmlist	2846
Vmmaxbackupsessions	2846
Vmmaxparallel	2848
Vmmaxpersnapshot	2849
Vmmaxrestoresessions	2850
Vmmaxrestoreparalleldisks	2851
Vmmaxsnapshotretry	2852
Vmmaxvirtualdisks	2853
Vmmc	2854
Vmmountage	2855
Vmnoprdmdisks	2855
Vmnovrdmdisks	2856
Vmpreferdagpassive	2857
Vmprocessvmwithindependent	2858
Vmprocessvmwithphysdisks	2859
Vmprocessvmwithprdm	2860
Vmrestoretype	2861
Vmskipctlcompression	2862
Vmskipmaxvirtualdisks	2863
Vmskipmaxvmdks	2864
Vmskipphysdisks	2864
Vmstoragetype	2865
Vmtagdatamover	2866
Vmtagdefaultdatamover	2868
Vmtempdatastore	2870
Vmverifyifaction	2870
Vmverifyiflatest	2872
Vmvstortransport	2873
Vssaltstagingdir	2874
Vssusesystemprovider	2875
Vmtimeout	2876
Webports	2877
Wildcard sareliteral	2878
Utilización de los mandatos	2879

Inicio y finalización de una sesión de mandatos de cliente	2885
Proceso de mandatos en modalidad por lotes	2885
Proceso de mandatos en modalidad interactiva	2886
Especificación de los nombres, opciones y parámetros de los mandatos de cliente	2886
Nombre de mandato	2887
Opciones	2887
Parámetros	2887
Sintaxis de especificación de archivo	2888
Caracteres comodín	2890
Consulta de mandatos de cliente	2891
Archive	2891
Archivado de FastBack	2894
Copia de seguridad de FastBack	2897
Backup Group	2900
Backup Image	2902
Copia de seguridad de imagen estática, dinámica y de instantánea	2906
Copia de seguridad de imagen desactivada y activada	2906
Utilización de la copia de seguridad de imagen para realizar una copia de seguridad incremental del sistema de archivos	2907
Backup NAS	2908
Backup Systemstate	2910
Backup VM	2912
Cancel Process	2923
Cancel Restore	2923
Delete Access	2924
Delete Archive	2925
Delete Backup	2927
Delete Filespace	2930
Delete Group	2932
Expire	2933
Help	2935
Incremental	2936
Soporte de archivos abiertos	2943
Copia de seguridad con registro por diario (Windows)	2943
Copia de seguridad con registro por diario (AIX, Linux)	2944
Copia de seguridad de puntos de montaje de volúmenes NTFS o ReFS	2946
Copia de seguridad de la raíz Dfs de Microsoft	2946
Incremental por fecha	2946
Asociación de una instantánea local a un espacio de archivos del servidor	2947
Loop	2947
Macro	2948
Monitor Process	2949
Preview Archive	2950
Previsualizar copia de seguridad	2951
Query Access	2952
Query Abjects	2952
Query Archive	2954
Query Backup	2957
Query Backupset	2961
Query Filespace	2963
Query Group	2966
Query Image	2968
Query Inclexcl	2970
Query Mgmtclass	2971
Query Node	2972
Query Options	2973
Query Restore	2974
Query Schedule	2975
Query Session	2976

Query Systeminfo	2977
Query Systemstate	2979
Query VM	2980
Restart Restore	2985
Restore	2985
Restauración de puntos de montaje de volúmenes NTFS o ReFS	2991
Restauración de puntos de unión Dfs de Microsoft	2992
Restauración de archivos activos	2992
Restauraciones de Convenio de denominación universal	2992
Restauración desde espacios de archivos que no están activados para Unicode	2993
Restauración de corrientes designadas	2993
Restauración de archivos esparcidos	2993
Restore Adobjects	2994
Restore Backupset	2995
Restauración de conjuntos de copias de seguridad: consideraciones y restricciones	2430
Restauración de conjuntos de copias de seguridad en un entorno SAN	2999
restore Backupset sin el parámetro backupsetname	3000
Restore Group	3002
Restore Image	3005
Restore NAS	3008
Restore Systemstate	3010
Restore VM	3010
Retrieve	3017
Recuperación de archivos desde espacios de archivos que no están activados para Unicode	3022
Recuperación de corrientes designadas	3022
Recuperación de archivos esparcidos	3023
Schedule	3023
Selective	3025
Soporte de archivos abiertos	3029
Asociación de una instantánea local a un espacio de archivos del servidor	3030
Set Access	3030
Set Event	3033
Establecer Netappsvm	3036
Establecer contraseña	3036
Set Vmtags	3041
programa de utilidad de configuración de servicios de cliente	3043
Instalar el servicio del planificador de copia de seguridad/archivado	3043
mandato dsmcutil	3043
Mandatos dsmcutil: opciones necesarias y ejemplos	3044
Opciones válidas de dsmcutil	3052
Archivos PDF para imprimir	3054

<b>Desarrollo de soluciones con la API de</b>	<b>3054</b>
Novedades	3055
Actualizaciones de API	3055
Notas de release de la V8.1	3056
Archivos léame para los fixpacks de la V8.1	3058
Últimas actualizaciones de la documentación	3058
Instalación de la API	3058
Visión general de la API	3059
Conceptos básicos de los archivos de opciones y configuración	3059
Configuración del entorno de la API	3060
Crear y ejecutar la aplicación de API de ejemplo	3061
Archivos de origen de aplicación de ejemplo UNIX o Linux	3061
Aplicación de ejemplo de 64 bits de Windows	3062
Consideraciones para el diseño de una aplicación	3064
Determinar los límites de tamaño	3068
Mantenimiento del control de la versión de la API	3068



Utilizar varias hebras	3069
Señales y manejadores de señal	3070
Iniciar o finalizar una sesión	3070
Seguridad de sesión	3071
Control del acceso a los archivos de contraseñas	3073
Crear un usuario administrativo con autorización de propietario de cliente	3073
ID y nombres de objeto	3074
Nombre de espacio de archivo	3075
Nombres de alto y bajo rango	3075
Tipo de objeto	3075
Acceder a objetos como propietario de sesión	3076
Acceder a objetos de nodos y propietarios	3076
Gestionar espacios de archivos	3077
Asociar objetos con clases de gestión	3078
Retener y liberar la caducidad/eliminación	3079
Consultas para el sistema IBM Spectrum Protect	3080
Eficiencia del servidor	3081
Enviar datos a un servidor	3082
El modelo de transacción	3082
Agregación de archivo	3083
Transferencia de datos sin LAN	3083
Operaciones de grabación simultánea	3083
Mejora del rendimiento de la API	3083
Configuración de la API para enviar datos de rendimiento	3084
Enviar objetos al servidor	3084
Conceptos básicos sobre archivar y realizar copias de seguridad de los objetos	3085
Compresión	3085
Eliminación de copia de almacenamiento intermedio	3086
Cifrado de la API	3087
Cifrado gestionado por la aplicación	3087
Cifrado del cliente de IBM Spectrum Protect	3089
Desduplicación de datos	3089
Eliminación de datos duplicados del lado del cliente de la API	3091
Excluir archivos de la eliminación de datos duplicados	3093
Incluir archivos para la desduplicación de datos	3093
Eliminación de datos duplicados del lado del servidor	3094
Migración tras error de la aplicación	3094
Diagramas de ejemplo de copia de seguridad/archivado	3095
Agrupación de archivos	3097
Recibir datos de un servidor	3098
Restauración o recuperación de objeto parcial	3099
Restaurar o recuperar datos	3099
Realizar consultas al servidor	3100
Seleccionar y ordenar objetos por orden de restauración	3100
Iniciar la llamada dsmBeginGetData	3102
Recibir todos los objetos para restaurar o recuperar	3102
Diagramas de ejemplo de restauración y recuperación	3103
Ejemplo de código de recepción de datos de un servidor	3104
Actualizar y eliminar objetos en el servidor	3105
Registro de eventos	3106
Resumen del diagrama de estado para la API de IBM Spectrum Protect	3106
Conceptos básicos sobre la interoperatividad	3107
Interoperatividad del cliente de archivado/copia de seguridad	3108
Asignar nombres a los objetos de la API	3108
Mandatos del cliente de copia de seguridad/archivado que se pueden utilizar con la API	3109
Interoperatividad del sistema operativo	3110
Soporte de copia de seguridad de varios nodos con el proxy de nodo de cliente	3110
Utilización de la API con Unicode	3111

Cuándo se utiliza Unicode	3111
Configuración de Unicode	3112
Llamadas a función de la API	3112
dsmBeginGetData	3117
dsmBeginQuery	3118
dsmBeginTxn	3122
dsmBindMC	3123
dsmChangePW	3124
dsmCleanUp	3125
dsmDeleteAccess	3125
dsmDeleteFS	3125
dsmDeleteObj	3126
dsmEndGetData	3127
dsmEndGetDataEx	3128
dsmEndGetObj	3128
dsmEndQuery	3128
dsmEndSendObj	3129
dsmEndSendObjEx	3129
dsmEndTxn	3130
dsmEndTxnEx	3131
dsmGetData	3132
dsmGetBufferData	3133
dsmGetNextQObj	3133
dsmGetObj	3136
dsmGroupHandler	3136
dsmInit	3137
dsmInitEx	3140
dsmLogEvent	3143
dsmLogEventEx	3143
dsmQueryAccess	3144
dsmQueryApiVersion	3145
dsmQueryApiVersionEx	3145
dsmQueryCliOptions	3146
dsmQuerySessInfo	3147
dsmQuerySessOptions	3147
dsmRCMsg	3148
dsmRegisterFS	3149
dsmReleaseBuffer	3150
dsmRenameObj	3150
dsmRequestBuffer	3151
dsmRetentionEvent	3152
dsmSendBufferData	3153
dsmSendData	3154
dsmSendObj	3155
dsmSetAccess	3157
dsmSetUp	3158
dsmTerminate	3159
dsmUpdateFS	3160
dsmUpdateObj	3160
dsmUpdateObjEx	3161
Archivo de origen de códigos de retorno de la API: dsmsrc.h	3163
Archivos de origen de definiciones de tipo de API	3172
Archivo de origen de las definiciones de la función de la API	3210
Archivos PDF para imprimir	3217

<b>Rendimiento</b>	<b>3218</b>
--------------------	-------------

**Resolución de problemas** 3218

**Mensajes, códigos de retorno y códigos de error** 3218

Introducción a los mensajes	3218
Formato de los mensajes de cliente y servidor de IBM Spectrum Protect	3219
Interpretación de los mensajes de código de retorno	3220
Ejemplo uno para el mandato QUERY EVENT	3221
Ejemplo dos para el mandato DEFINE VOLUME	3221
Mensajes de ANE	3222
Mensajes de ANR	3222
Mensajes ANS 0000-9999	3222
Códigos de retorno API	3223
Formato de códigos de retorno API	3223
Códigos de retorno API	3223
-452 E	3234
-451 E	3234
-450 E	3234
-190 E	3235
-057 E	3235
-056 E	3235
-055 E	3236
-054 E	3236
-053 E	3236
-052 E	3237
-051 E	3237
-050 E	3237
0000 I	3238
0001 E	3238
0002 E	3238
0003 E	3239
0004 W	3239
0005 E	3239
0006 E	3240
0007 E	3240
0008 E	3240
0009 W	3241
0010 E	3241
0011 E	3241
0012 E	3242
0013 E	3242
0014 E	3242
0015 E	3243
0016 E	3243
0017 E	3243
0018 E	3244
0020 E	3244
0021 S	3244
0022 S	3244
0023 S	3245
0024 S	3245
0024 E	3245
0025 E	3246
0026 S	3246
0027 E	3246
0028 E	3247
0029 S	3247
0030 E	3247

0032 E	3247
0033 E	3248
0034 E	3248
0036 E	3248
0041 E	3249
0045 E	3249
0047 E	3249
0048 E	3249
0049 E	3250
0050 E	3250
0051 E	3250
0052 E	3251
0053 E	3251
0054 E	3251
0055 E	3252
0056 E	3252
0057 S	3252
0058 S	3253
0059 E	3253
0061 E	3253
0062 S	3253
0063 E	3254
0064 E	3254
0065 E	3254
0066 E	3255
0067 S	3255
0068 E	3255
0069 E	3256
0073 E	3256
0074 E	3256
0075 E	3256
0079 E	3257
0101 W	3257
0102 E	3257
0104 E	3258
0105 E	3258
0106 E	3258
0106 E	3259
0107 E	3259
0108 E	3259
0109 E	3260
0110 E	3260
0111 E	3260
0113 E	3260
0114 E	3261
0115 E	3261
0116 E	3261
0117 E	3262
0118 E	3262
0119 E	3262
0120 E	3263
0121 I	3263
0122 E	3263
0123 E	3263
0124 E	3264
0125 E	3264
0126 E	3264
0127 E	3265

0128 E	3265
0129 E	3265
0130 E	3265
0131 E	3266
0131 S	3266
0132 E	3266
0133 E	3267
0134 E	3267
0135 E	3267
0136 E	3268
0137 E	3268
0138 E	3268
0139 S	3269
0145 S	3269
0146 S	3269
0147 S	3269
0148 S	3270
0149 S	3270
0151 S	3270
0154 E	3270
0155 T	3271
0156 E	3271
0157 S	3271
0158 E	3272
0159 I	3272
0160 E	3272
0162 E	3272
0164 E	3273
0165 E	3273
0166 E	3273
0167 E	3273
0168 E	3274
0169 E	3274
0173 E	3274
0174 E	3275
0175 E	3275
0177 S	3275
0184 E	3275
0185 W	3276
0186 E	3276
0187 E	3276
0188 S	3277
0189 S	3277
0190 S	3277
0231 E	3278
0232 E	3278
0233 E	3278
0234 E	3279
0235 E	3279
0236E	3279
0237E	3279
0238E	3280
0239E	3280
0240E	3280
0241E	3281
0242E	3281
0245 E	3281
0247 E	3282

0248 E	3282
0249 E	3282
0250 E	3282
0292 E	3283
0295 E	3283
0296 E	3283
0297 E	3284
0298 E	3284
0400 E	3284
0405 E	3284
0406 S	3285
0408 E	3285
0409 E	3285
0410 E	3286
0411 S	3286
0412 S	3286
0426 E	3287
0427 E	3287
0600 E	3287
0601 E	3288
0610 E	3288
0611 E	3288
0612 E	3288
0613 E	3289
0614 E	3289
0615 E	3289
0620 E	3290
0621 E	3290
0622 E	3290
0927 E	3291
961 E	3291
963 E	3291
0996 E	3292
0997 E	3292
0998 E	3292
1376 E	3293
2000 E	3293
2001 E	3293
2002 E	3293
2004 E	3294
2006 E	3294
2007 E	3294
2008 E	3295
2009 E	3295
2010 E	3295
2011 E	3295
2012 E	3296
2014 E	3296
2015 E	3296
2016 E	3296
2017 E	3297
2018 E	3297
2019 E	3297
2020 E	3298
2021 E	3298
2022 E	3298
2023 E	3299
2024 E	3299

2025 E	3299
2026 E	3299
2027 E	3300
2028 E	3300
2029 E	3300
2030 E	3301
2031 E	3301
2032 E	3301
2033 E	3302
2034 E	3302
2035 E	3302
2041 E	3302
2042 E	3303
2043 E	3303
2044 E	3303
2045 E	3304
2046 E	3304
2047 E	3304
2048 E	3305
2049 E	3305
2050 E	3305
2051 E	3305
2052 E	3306
2053 E	3306
2060 E	3306
2061 E	3307
2062 W	3307
2063 E	3307
2064 E	3308
2065 E	3308
2070 E	3308
2080 E	3309
2081 E	3309
2082 E	3309
2090 E	3309
2100 E	3310
2101 E	3310
2102 E	3310
2103 E	3311
2104 E	3311
2105 E	3311
2106 E	3311
2107 E	3312
2110 E	3312
2111 E	3312
2112 E	3313
2113 E	3313
2114 E	3313
2120 E	3314
2200 I	3314
2210 E	3314
2228 E	3314
2229 E	3315
2230 E	3315
2231 E	3315
2300 E	3316
2301 E	3316
2302 I	3316

2400 E	3316
2401 E	3317
2402 E	3317
2403 E	3317
2404 E	3318
2405 E	3318
4580 E	3318
4582 E	3318
4584 E	3319
4600 E	3319
4601 E	3319
4602 E	3320
4603 E	3320
4604 E	3320
4605 E	3321
4606 E	3321
5200 E	3321
5702 E	3322
5705 E	3322
5710 E	3322
5717 E	3322
5722 E	3323
5746 E	3323
5748 E	3323
5749 E	3324
5801 E	3324
Descripciones de código de E/S en mensajes del servidor	3324
Visión general de descripciones de los códigos de terminación y de operación de controladores de dispositivos	3325
Valores del código de terminación comunes a todas las clases de dispositivos	3326
Valores del código de terminación para cambiadores de medios	3327
Valores de código de finalización para controladores de cinta	3328
Descripciones de códigos de ASC y ASCQ estándares	3330
Códigos de error de dispositivo en el registro de errores del sistema AIX	3333
Códigos de retorno de IBM Global Security Kit	3334

<b>Glosario</b>	3344
A	3344
B	3347
C	3347
D	3350
E	3351
F	3352
G	3352
H	3353
I	3353
J	3354
K	3354
L	3354
M	3355
N	3356
O	3356
P	3357
R	3358
S	3359
T	3361
U	3362
V	3362
W	3363



# Documentación de IBM Spectrum Protect

---

IBM Spectrum Protect proporciona capacidades automatizadas, planificadas centralmente, de copia de seguridad mediante gestión de políticas, de archivado y de gestión de espacio para los servidores de archivos, estaciones de trabajo, máquinas virtuales y aplicaciones. Utilice la documentación de IBM Spectrum Protect para ayudarle a configurar y gestionar sus soluciones de protección de datos.

## Cómo empezar

- Instalación y actualización de servidores
- Instalación y actualización del Centro de operaciones
- Instalación de clientes de copia de seguridad y archivado
- Selección e implementación de soluciones de protección de datos
- Novedades en el servidor
- Novedades para los clientes
- [📺 Vídeos de novedades](#)
- Archivos PDF

## Tareas comunes

- Tareas de supervisión diarias
- Adición de clientes
- Réplica de datos de cliente en otro servidor
- Gestión del servidor, los clientes y el Centro de operaciones
- Configuración del almacenamiento
- Configuración de clientes de copia de seguridad/archivado
- Copia de seguridad de datos
- Mandatos del servidor, opciones y programas de utilidad

## Resolución de problemas y ayuda

- Resolución de problemas
- Optimizando rendimiento
- [📺 Últimos fix packs de clientes y servidores de IBM Spectrum Protect](#)
- [📺 IBM Software Support](#)

## Más información

- [📖 Sugerencias de usuario para IBM® Knowledge Center](#)
- Suites de producto y productos relacionados
- [📺 Página de inicio de la familia de productos](#)
- [📺 Wiki de productos IBM Spectrum Protect](#)
- [📺 IBM Spectrum Protect Developer Center](#)
- [📺 Publicaciones de IBM Redbooks](#)
- [📺 Formación de IBM System](#)
- Accesibilidad
- Avisos legales del producto

© Copyright IBM Corp. 1993, 2017

# Funciones de accesibilidad para la familia de productos IBM Spectrum Protect

---

Las funciones de accesibilidad ayudan a aquellos usuarios que tienen una discapacidad, como, por ejemplo, movilidad reducida o poca visión, a utilizar productos tecnológicos de información de forma satisfactoria.

## Visión general

---

La familia de productos de IBM Spectrum Protect incluye las siguientes funciones de accesibilidad mayores:

- Funcionamiento utilizando sólo el teclado
- Operaciones que utilizan un lector de pantalla

La familia de productos de IBM Spectrum Protect utiliza el estándar W3C más reciente, WAI-ARIA 1.0, para asegurar la conformidad con US Section 508 y Web Content Accessibility Guidelines (WCAG) 2.0. Para aprovechar las características de accesibilidad, utilice el release más reciente del lector de pantalla y el navegador web más reciente soportados por el producto.

La documentación del producto en IBM Knowledge Center está habilitada para la accesibilidad. Las funciones de accesibilidad del IBM Knowledge Center se describen en la Sección de accesibilidad de la ayuda del IBM Knowledge Center .

## Navegación con el teclado

---

Este producto utiliza teclas estándar de navegación.

## Información sobre interfaces

---

Las interfaces de usuario no tienen contenido que se actualiza de 2 a 55 veces por segundo.

Las interfaces de usuarios web se basan en las hojas de estilo en cascada para representar el contenido correctamente y para proporcionar una experiencia que se pueda utilizar. La aplicación proporciona un método equivalente para usuarios con problemas de poca visión para utilizar los parámetros de visualización del sistema, incluido el modo de alto contraste. Puede controlar el tamaño de fuente utilizando los parámetros del dispositivo o del navegador web.

Las interfaces de usuarios web incluyen puntos de referencia de navegación WAI-ARIA que puede utilizar para navegar rápidamente a áreas funcionales de la aplicación.

## Software del proveedor

---

La familia de productos IBM Spectrum Protect incluye cierto software del proveedor que no está cubierto por el acuerdo de licencia de IBM. IBM no es responsable de las características de accesibilidad de estos productos. Póngase en contacto con el proveedor para obtener información sobre accesibilidad relacionada con sus productos.

## Información de accesibilidad relacionada

---

Además del centro de atención al cliente de IBM y de los sitios web de soporte estándar, IBM dispone de un servicio telefónico TTY que permite a clientes sordos o con dificultades auditivas acceder a los servicios de ventas y asistencia técnica.

Servicio TTY  
800-IBM-3383 (800-426-3383)  
(en América del Norte)

Para obtener más información acerca del compromiso que IBM tiene con la accesibilidad, consulte IBM Accessibility.

## Suites de producto y productos relacionados

---

Las suites de IBM Spectrum Protect y productos de almacenamiento relacionados permiten ampliar y expandir las características del producto base de IBM Spectrum Protect.

## Suites de producto y opciones de licencia

---

Los productos IBM Spectrum Protect y IBM Spectrum Protect Extended Edition ofrecen los componentes principales para las operaciones de copia de seguridad y restauración automatizadas y centralizadas. Los componentes de servidor y cliente de archivado y copia de seguridad proporcionan funciones básicas como operaciones de restauración y copia de seguridad, y operaciones de recuperación y archivado para archivos, directorios e imágenes de disco.

La documentación del producto incluye información sobre IBM Spectrum Protect y IBM Spectrum Protect Extended Edition.

Las suites de producto, que combinan IBM Spectrum Protect con productos relacionados, pueden constituir una forma más fácil de comprar y gestionar el software de IBM Spectrum Protect. En las suites se incluyen productos que pueden satisfacer un amplio abanico de requisitos de protección y recuperación de datos, permitiendo una gestión de licencias más sencilla. Más información sobre las suites de productos de IBM Spectrum Protect.

## Productos relacionados

---

Puede ampliar IBM Spectrum Protect con funciones y características que están disponibles en productos relacionados.

Producto	Ventajas principales	Enlaces
----------	----------------------	---------

Producto	Ventajas principales	Enlaces
IBM Spectrum Copy Data Management	Cataloga las instantáneas de NetApp y VMware para facilitar la gestión basada en roles y la recuperación de datos de seguridad.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect High Speed Data Transfer	Utilice este producto para habilitar la tecnología Fast Adaptive Secure Protocol (FASP) para mejorar la transferencia de datos en un entorno donde se detectan problemas de rendimiento de WAN.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema</li> </ul>
IBM Spectrum Protect for Data Retention	<p>Proporciona protección de retención a largo plazo cuando se archivan registros empresariales, archivos o datos.</p> <p>El archivado de datos para satisfacer los requisitos de conformidad reguladores necesita más garantías o protecciones, denominadas protección de retención de datos. Estas garantías ayudan a garantizar que los datos no sean suprimidos de forma prematura ya sea inadvertidamente o maliciosamente. Para satisfacer los requisitos de conformidad, IBM Spectrum Protect for Data Retention proporciona más protección para datos archivados por IBM Spectrum Protect.</p>	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul> <p>Consejo: La documentación para este producto se incluye en la documentación de IBM Spectrum Protect.</p>
IBM Spectrum Protect Snapshot	<p>Protege los datos con prestaciones integradas de copia de seguridad y restauración de instantánea con conocimiento de aplicaciones.</p> <p>Los datos que almacenan las aplicaciones de IBM® DB2, SAP, Oracle, Microsoft Exchange y Microsoft SQL Server se pueden proteger con el software de IBM Spectrum Protect Snapshot . Con este software, puede crear y gestionar instantáneas a nivel de volumen para sistemas de archivos y aplicaciones personalizadas. Puede elegir si desea integrar IBM Spectrum Protect Snapshot a IBM Spectrum Protect.</p>	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect for Databases	<p>Protege los datos de Oracle y los datos de Microsoft SQL mediante tareas automáticas, programas de utilidad e interfaces. Este software crea copias de seguridad en línea, coherentes y centralizadas para ayudarle a evitar tiempos de inactividad, a proteger datos empresariales vitales y a minimizar los costes operativos.</p> <p>Consejo: Los servidores de IBM Spectrum Protect admiten copias de seguridad en línea de bases de datos de IBM DB2 e IBM Informix. No es necesario instalar IBM Spectrum Protect for Databases para hacer copia de seguridad de estas bases de datos. Para obtener más información, consulte la documentación de DB2 e Informix.</p>	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>

Producto	Ventajas principales	Enlaces
IBM Spectrum Protect for Enterprise Resource Planning	Proporciona protección que se personaliza para los datos de sistema SAP.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect for Mail	Automatiza la protección de datos de forma que las copias de seguridad se completen sin cerrar los servidores de Microsoft Exchange o los servidores de IBM Domino.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect for Space Management	Producto de gestión de almacenamiento jerárquico que reduce los costes de almacenamiento para información a la que se accede con poca frecuencia, sin cambiar la forma en que los usuarios y las aplicaciones interactúan con los datos. Puede utilizar este producto en sistemas operativos AIX y Linux.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect HSM for Windows	Producto de gestión de almacenamiento jerárquico que reduce los costes de almacenamiento para información a la que se accede con poca frecuencia, sin cambiar la forma en que los usuarios y las aplicaciones interactúan con los datos. Puede utilizar este producto en sistemas operativos Windows.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Spectrum Protect for SAN	Funciona con servidores y sistemas cliente para transferir datos a través de una SAN (red de área de almacenamiento), en lugar de una LAN. Este producto es un agente de almacenamiento que habilita las operaciones de copia de seguridad y restauración fuera de la LAN.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul> <p>Product documentation version: La documentación de IBM Spectrum Protect for SAN Versión 7.1 es aplicable a la familia de productos IBM Spectrum Protect Versión 8.1.</p>
IBM Spectrum Protect for Virtual Environments	Proporciona protección adaptada para entornos virtuales de VMware e Hyper-V.	<ul style="list-style-type: none"> <li>• Más información y compras</li> <li>• Documentación del producto</li> </ul>
IBM Tivoli Storage Manager for z/OS Media	Gestiona recursos de disco y cinta de z/OS para servidores de IBM Spectrum Protect que se ejecutan en sistemas AIX o Linux en System z.	<ul style="list-style-type: none"> <li>• Documentación del producto</li> </ul>

## Archivos PDF

Puede descargar los archivos PDF predefinidos de IBM® Knowledge Center o desde un sitio de descarga FTP.

### Archivos PDF precompilados

Consulte los temas siguientes para ver los archivos PDF predefinidos disponibles para este release:

- Soluciones de protección de datos
- Servidores
- Clientes de archivado y copia de seguridad
- API

### Paquete de archivos PDF

Descargue un paquete que contenga todos los archivos PDF para este release del siguiente sitio FTP:

<ftp://public.dhe.ibm.com/software/products/ISP/current/>

## Actualizaciones en este release

Consulte información acerca de nuevas características y mejoras que estén disponibles en los productos para comprender los posibles beneficios que puede obtener para sus operaciones de gestión de almacenamiento. Las notas del release contienen vínculos a los que puede acceder para obtener información importante antes de instalar o actualizar los productos y componentes.

Componente	Actualiza el resumen	Notas del release de V8.1
Componentes de servidor	Actualizaciones	Notas de release
Cliente de copia de seguridad y archivado	Actualizaciones	Notas de release
Interfaz de programación de aplicaciones (API)	Actualizaciones	Notas de release

## Conceptos de IBM Spectrum Protect

---

IBM Spectrum Protect proporciona un entorno de protección de datos completo.

- **Visión general de IBM Spectrum Protect**  
IBM Spectrum Protect proporciona una protección de datos centralizada y automatizada que ayuda a reducir la pérdida de datos y gestionar la conformidad con retención de datos y requisitos de disponibilidad.
- **Conceptos de almacenamiento de datos en IBM Spectrum Protect**  
IBM Spectrum Protect proporciona funciones para almacenar datos en un rango de dispositivo y almacenamiento de soporte.
- **Estrategias de protección de datos con IBM Spectrum Protect**  
IBM Spectrum Protect proporciona diversas formas de implementar varias estrategias de protección de datos.

## Visión general de IBM Spectrum Protect

---

IBM Spectrum Protect proporciona una protección de datos centralizada y automatizada que ayuda a reducir la pérdida de datos y gestionar la conformidad con retención de datos y requisitos de disponibilidad.

- **Componentes de protección de datos**  
Las soluciones de protección de datos que proporciona IBM Spectrum Protect constan de un servidor, de sistemas cliente y aplicaciones y de soporte de almacenamiento. IBM Spectrum Protect proporciona interfaces de gestión para la supervisión e informe del estado de protección de datos.
- **Servicios de protección de datos**  
IBM Spectrum Protect proporciona servicios de protección de datos para almacenar y recuperar datos de varios tipos de clientes. Los servicios de protección de datos se implementan a través de políticas que se definen en el servidor. Puede utilizar la planificación de cliente para automatizar los servicios de protección de datos.
- **Procesos para gestionar la protección de datos con IBM Spectrum Protect**  
El inventario del servidor de IBM Spectrum Protect tiene un rol clave en los procesos para la protección de datos. Defina las políticas que utiliza el servidor para gestionar el almacenamiento de datos.
- **Interfaces de usuario para entornos de IBM Spectrum Protect**  
Para las tareas de configuración y supervisión, IBM Spectrum Protect proporciona varias interfaces, incluido el Centro de operaciones, una interfaz de línea de mandatos y una interfaz administrativa SQL.

## Componentes de protección de datos

---

Las soluciones de protección de datos que proporciona IBM Spectrum Protect constan de un servidor, de sistemas cliente y aplicaciones y de soporte de almacenamiento. IBM Spectrum Protect proporciona interfaces de gestión para la supervisión e informe del estado de protección de datos.

### Servidor

---

Los sistemas cliente envían datos al servidor para que se almacenen como copias de seguridad o datos archivados. El servidor incluye un *inventario*, que es un repositorio de información sobre los datos de cliente.

El inventario incluye los siguientes componentes:

#### Base de datos

La información sobre cada archivo, volumen lógico o base de datos de la que el servidor hace copia de seguridad, archiva o migra se almacena en la base de datos del servidor. La base de datos del servidor también contiene información sobre la política y las planificaciones para los servicios de protección de datos.

#### Registro de recuperación

Los registros de las transacciones de base de datos se guardan en este registro. La base de datos utiliza el registro de recuperación para garantizar la coherencia de datos en la base de datos.

## Sistemas y aplicaciones cliente

*Clients* son aplicaciones, máquinas virtuales y sistemas que deben protegerse. Los clientes envían datos al servidor, como se muestra en Figura 1.

Figura 1. Componentes de la solución de protección de datos



### Software de cliente

Para que IBM Spectrum Protect proteja los datos de cliente, se debe instalar el software apropiado en el sistema cliente y el cliente se debe registrar en el servidor.

### Nodos de cliente

Un *nodo de cliente* es equivalente de un sistema, una máquina virtual o una aplicación, como por ejemplo un cliente de archivado y copia de seguridad que se ha instalado en una estación de trabajo para las copias de seguridad de sistema de archivos. Cada nodo de cliente debe registrarse en el servidor. Se pueden registrar varios nodos en un único sistema.

## Soportes de almacenamiento

El servidor almacena datos de cliente en el soporte de almacenamiento. Se utilizan los tipos de soporte siguientes:

### Dispositivos de almacenamiento

El servidor puede grabar datos en unidades de disco duro, matrices de discos y subsistemas, unidades de cinta autónomas, bibliotecas de cintas y otros tipos de almacenamiento de acceso aleatorio y acceso secuencial. Los dispositivos de almacenamiento pueden conectarse directamente al servidor o bien conectarse por medio de una red de área local (LAN) o una red de área de almacenamiento (SAN).

### Agrupaciones de almacenamiento

Los dispositivos de almacenamiento que están conectados al servidor se agrupan en *agrupaciones de almacenamiento*. Cada agrupación de almacenamiento representa un conjunto de dispositivos de almacenamiento del mismo tipo de soporte, como un disco o unidades de cinta. IBM Spectrum Protect almacena todos los datos de cliente en las agrupaciones de almacenamiento. Puede organizar agrupaciones de almacenamiento en una *jerarquía*, así ese almacenamiento de datos puede transferirse desde el almacenamiento de disco a un almacenamiento de coste más bajo como los dispositivos de cinta.

## Servicios de protección de datos

IBM Spectrum Protect proporciona servicios de protección de datos para almacenar y recuperar datos de varios tipos de clientes. Los servicios de protección de datos se implementan a través de políticas que se definen en el servidor. Puede utilizar la planificación de cliente para automatizar los servicios de protección de datos.

## Tipos de servicios de protección de datos

IBM Spectrum Protect proporciona servicios para almacenar y recuperar datos de cliente como se muestra en Figura 1.

Figura 1. Servicios de protección de datos



IBM Spectrum Protect proporciona los siguientes tipos de servicios de protección de datos:

#### Copia de seguridad y restauración de servicios

Puede ejecutar un proceso de copia de seguridad para crear una copia de un *objeto de datos* que se puede utilizar para la recuperación si el objeto de datos original se pierde. Un objeto de datos puede ser un archivo, un directorio o un objeto de datos definido por el usuario, como por ejemplo una base de datos.

Para minimizar el uso de los recursos del sistema durante la operación de seguridad, IBM Spectrum Protect utiliza el método *copia de seguridad incremental progresiva*. Para este método de copia de seguridad, se crea una primera copia de seguridad completa de todos los objetos de datos y en operaciones de seguridad posteriores sólo se mueven los datos cambiados al almacenamiento. Comparado con los métodos de copia de seguridad incremental y diferencial que requieren realizar copias de seguridad completas periódicas, el método de copia de seguridad incremental progresiva proporciona las siguientes ventajas:

- Reduce la redundancia de datos
- Utiliza menos ancho de banda de red
- Requiere menos espacio para las agrupaciones de almacenamiento

Para reducir más los requisitos de capacidad de almacenamiento y el uso de ancho de banda de red, IBM Spectrum Protect incluye la *optimización de almacenamiento de datos* para copias de seguridad de datos. La técnica de optimización de almacenamiento de datos elimina las extensiones de datos duplicadas de las copias de seguridad.

Ejecute un proceso de restauración para copiar un objeto desde una agrupación de almacenamiento en el cliente. Puede restaurar un solo archivo, todos los archivos del directorio o todos los datos de un sistema.

#### Servicios de archivado y recuperación

Utilice el servicio de archivado para conservar los datos que deben almacenarse durante un largo periodo de tiempo, como para la conformidad con la normativa. Los servicios de archivado proporcionan las siguientes funciones:

- Cuando archive datos, especifique durante cuánto tiempo deben estar almacenados los datos.
- Puede solicitar que los archivos y directorios se copien a un almacenamiento a largo plazo en el soporte. Por ejemplo, puede elegir almacenar estos datos en un dispositivo de cinta, que puede reducir el coste de almacenamiento.
- Puede especificar que se borren los archivos originales del cliente después de que se han archivado.

El servicio de recuperación proporciona las siguientes funciones:

- Cuando recupera datos, los datos se copian desde la agrupación de almacenamiento a un nodo cliente.
- La operación de recuperación no afecta a la copia archivada en la agrupación de almacenamiento.

#### Migrar y recuperar servicios

Puede migrar y recuperar servicios para gestionar espacio en los sistemas cliente. El objetivo de la gestión de espacio es maximizar la capacidad disponible de los soportes para los datos nuevos y minimizar el tiempo de acceso a los datos. Puede migrar datos a un almacenamiento del servidor para mantener suficiente espacio de almacenamiento libre en un sistema de archivos local. Puede almacenar datos migrados de las maneras siguientes:

- En almacenamiento de disco para almacenamiento a largo plazo
- En una *biblioteca virtual de cintas* (VTL) para una recuperación rápida de los archivos

Los archivos pueden recuperarse en el nodo de cliente a solicitud, ya sea de forma automática o selectiva.

## Tipos de datos de cliente que se pueden proteger

Puede proteger datos para los siguientes tipos de clientes con IBM Spectrum Protect:

Cientes de aplicaciones

IBM Spectrum Protect puede proteger datos para productos o aplicaciones específicos. Estos clientes se denominan *clientes de aplicaciones*. Para proteger los *datos estructurados* para estos clientes, en otras palabras, los datos de los campos de base de datos, debe hacer copia de seguridad de los componentes específicos para la aplicación. IBM Spectrum Protect puede proteger las siguientes aplicaciones:

- Clientes de IBM Spectrum Protect for Enterprise Resource Planning:
  - Data Protection for SAP HANA
  - Data Protection for SAP for DB2
  - Data Protection for SAP for Oracle
- Clientes de IBM Spectrum Protect for Databases:
  - Data Protection for Microsoft SQL Server
  - Data Protection for Oracle
- Clientes de IBM Spectrum Protect for Mail:
  - Data Protection for IBM® Domino
  - Data Protection for Microsoft Exchange Server

#### Máquinas virtuales

Máquinas virtuales a las que se hace copia de seguridad utilizando el software de cliente de aplicación instalado en la máquina virtual. En el entorno de IBM Spectrum Protect, una máquina virtual puede estar protegida por IBM Spectrum Protect for Virtual Environments.

#### Clientes de sistema

Los clientes siguientes de IBM Spectrum Protect se llaman *clientes del sistema*:

- Todos los clientes que hacen copia de seguridad de datos en archivos y directorios, en otras palabras, *datos no estructurados*, como clientes de archivado y copia de seguridad y clientes de API que están instalados en estaciones de trabajo.
- Un servidor que se incluye en una configuración de volumen virtual de servidor a servidor.
- Una máquina virtual de la que se hace copia de seguridad utilizando el software de cliente de archivado y copia de seguridad instalado en una máquina virtual.

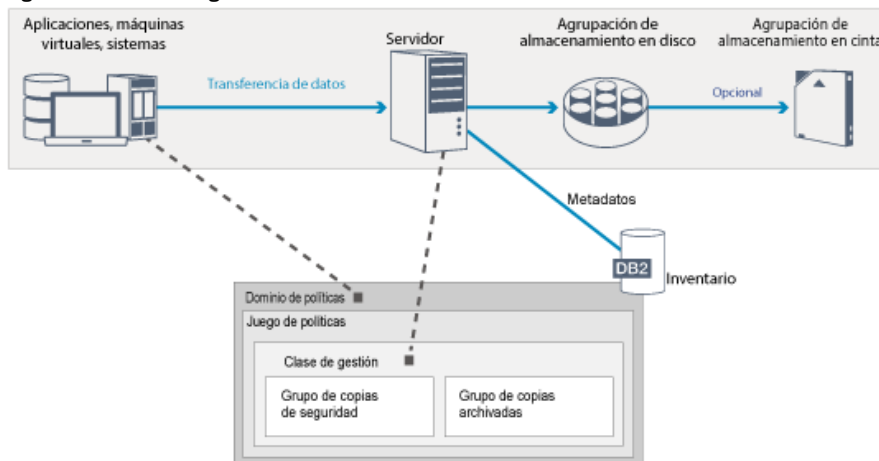
## Procesos para gestionar la protección de datos con IBM Spectrum Protect

El inventario del servidor de IBM Spectrum Protect tiene un rol clave en los procesos para la protección de datos. Defina las políticas que utiliza el servidor para gestionar el almacenamiento de datos.

### Proceso de gestión de datos

Figura 1 muestra el proceso de gestión de datos de IBM Spectrum Protect.

Figura 1. Proceso de gestión de datos



IBM Spectrum Protect utiliza políticas para controlar cómo el servidor almacena y gestiona objetos de datos en varios tipos de soportes y dispositivos de almacenamiento. Asocie un cliente a un dominio de política que contiene un conjunto de políticas activas. Cuando un cliente realiza una copia de seguridad, archivado o migración de un archivo, el archivo se vincula a una clase de gestión en el juego de políticas activo del dominio de políticas. La clase de gestión y los grupos de archivado y copia de seguridad especifican dónde se almacenan los archivos y cómo se gestionan. Si configura el almacenamiento del servidor en una jerarquía, puede migrar los archivos a agrupaciones de almacenamiento diferentes.

### Componentes de inventario



Los siguientes componentes de inventario son clave para el funcionamiento del servidor:

#### Base de datos del servidor

La base de datos del servidor contiene información sobre las operaciones del servidor y datos de cliente. La base de datos almacena información sobre los datos de cliente, denominados *metadatos*. La información sobre los datos del cliente incluye el nombre, el tamaño y el propietario del archivo, así como la clase de gestión, el grupo de copias y la ubicación del archivo en el almacenamiento del servidor. La base de datos incluye la siguiente información necesaria para el funcionamiento del servidor:

- Definiciones de nodos de cliente y administradores
- Políticas y planificaciones.
- Valores del servidor.
- Registros de operaciones de servidor, como registros de actividad y registros de sucesos
- Resultados intermedios para consultas administrativas

#### Registro de recuperación

El servidor registra transacciones de base de datos en el registro de recuperación. El registro de recuperación le ayuda a garantizar que un fallo no deja la base de datos en estado incoherente. El registro de recuperación también se utiliza para mantener la consistencia a través de las operaciones de inicio del servidor. El registro de recuperación consta de los siguientes registros:

##### Registro activo

Este registro registra transacciones actuales en el servidor. Esta información es necesaria para iniciar el servidor y la base de datos después de un desastre.

##### Duplicación de anotaciones (opcional)

La duplicación de anotaciones activas es una copia de las anotaciones activas que puede utilizarse en caso de que no puedan leerse los archivos de anotaciones activas. Todos los cambios que se realizan en el registro activo también se graban en una duplicación de registro. Puede configurar una duplicación de registro activo.

##### Registro de archivos

El registro de archivado contiene copias de archivos de registro cerrados que estuvieron en el registro activo. El registro de archivado se incluye en las copias de seguridad de la base de datos y se utiliza para la recuperación de la base de datos del servidor. Los archivos de registro de archivado que se incluyen en una copia de seguridad de base de datos se podan automáticamente una vez completado un ciclo completo de copia de seguridad de base de datos. El registro de archivado debe tener espacio suficiente para almacenar los archivos de registro para las copias de seguridad de bases de datos.

##### Anotaciones de recuperación de errores de archivado (opcional)

Las anotaciones de recuperación de errores de archivado, también denominadas anotaciones de archivado secundario, son el directorio que usa el servidor para almacenar archivos de anotaciones cuando el directorio de anotaciones de archivado está lleno.

## Gestión de datos basada en políticas

---

En el entorno de IBM Spectrum Protect, una *política* para la gestión de protección de datos contiene reglas que determinan cómo se almacenan y gestionan datos de cliente. El objetivo principal de una política es implementar los siguientes objetivos de gestión de datos:

- Controlar en qué agrupación de almacenamiento están almacenados inicialmente los datos de cliente.
- Definir los criterios de retención que controlarán cuántas copias de objetos se almacenan.
- Definir cuánto tiempo se conservarán las copias de los objetos.

La gestión de los datos basada en políticas le ayuda a centrarse más en los requisitos empresariales para la protección de los datos en lugar de en la gestión de los medios y dispositivos de almacenamiento. Los administradores definen políticas y asignan nodos de cliente a un *dominio de políticas*.

Dependiendo de sus necesidades empresariales, puede tener una política o varias. Dentro de una organización empresarial, por ejemplo, departamentos diferentes con tipos de datos diferentes pueden tener sus propios planes de gestión de almacenamiento personalizados. Las políticas pueden actualizarse y las actualizaciones pueden aplicarse a datos ya gestionados.

Cuando instala IBM Spectrum Protect, ya hay definida una política denominada STANDARD. La política STANDARD proporciona la protección de copia de seguridad básica para las estaciones de trabajo de usuario. Para proporcionar diferentes niveles de servicio para clientes diferentes, puede añadir niveles a la política predeterminada o crear una nueva política.

Cree políticas definiendo los siguientes componentes de política:

#### Dominio de políticas

El dominio de políticas es el método organizativo primario de agrupación de nodos cliente que comparten reglas comunes para la gestión de datos. Aunque se puede definir un nodo de cliente para más de un servidor, el nodo de cliente se puede definir para un solo dominio de políticas en cada servidor.

#### Juego de políticas

Un *conjunto de políticas* es un número de políticas agrupadas para que la política para los nodos de cliente de un dominio se pueda activar o desactivar según sea necesario. Un administrador utiliza un conjunto de políticas para implementar diferentes clases de gestión en funciones de las necesidades del usuario y de la empresa. Un dominio de políticas puede incluir varios conjuntos de políticas, pero solo un conjunto de políticas puede estar activo en el dominio. Cada conjunto de políticas contiene una clase de gestión predeterminada y varias clases de gestión adicionales.

#### Clase de gestión

Una *clase de gestión* es un objeto de política que se puede enlazar a cada categoría de datos para especificar cómo gestiona los datos el servidor. Puede haber una o más clases de gestión. Se asigna una clase de gestión para que sea la clase de gestión predeterminada que utilizan los clientes a menos que sustituyan específicamente el valor determinado para utilizar una clase de gestión específica.

La clase de gestión puede contener un grupo de copias de seguridad, un grupo de copias archivadas y atributos de gestión de espacio. Un grupo de copias determina cómo gestiona el servidor las versiones de copia de seguridad o copias archivadas del archivo. Los atributos de gestión de espacio determinan si el cliente de gestor de espacios puede elegir el archivo para la migración al almacenamiento del servidor, y bajo qué condiciones se migra el archivo.

#### Grupo de copias

Un *grupo de copias* es un conjunto de atributos de una clase de gestión que controla los siguientes factores:

- Dónde almacena el servidor las versiones de los archivos de copia de seguridad o las copias archivadas
- Durante cuánto tiempo mantiene el servidor las versiones de los archivos de copia de seguridad o las copias archivadas
- Cuántas versiones de las copias de seguridad se retienen
- Qué método se utiliza para generar versiones de archivos de copia de seguridad o copias archivadas

## Gestión de la seguridad

---

IBM Spectrum Protect incluye características de seguridad para la inscripción de administradores y usuarios. Una vez que los administradores están registrados, se les debe otorgar autoridad asignándoles una o más clases de privilegios administrativos. Un administrador con un privilegio de sistema puede realizar cualquier función de servidor. Los administradores con privilegios de política, almacenamiento, operador o nodo pueden ejecutar subconjuntos de funciones de servidor. Se puede acceder al servidor mediante los métodos siguientes, cada uno controlado con una contraseña:

- Acceso de administrador para gestionar el servidor
- Acceso de cliente a los nodos para almacenar y recuperar datos

También se incluyen las funciones que pueden ayudar a garantizar la seguridad cuando los clientes se conectan al servidor. Dependiendo de los requisitos empresariales, como administrador es posible elegir uno de los siguientes métodos de inscripción de clientes:

#### Inscripción abierta

Cuando el cliente se conecta por primera vez al servidor, éste solicita al usuario un nombre de nodo, la contraseña y la información de contacto. La inscripción abierta proporciona al usuario los siguientes valores predeterminados:

- El nodo cliente se asigna al dominio de políticas STANDARD.
- El usuario puede definir si los archivos se comprimen para reducir la cantidad de datos que se envían por las redes y el espacio que ocupan los datos en el almacenamiento.
- El usuario puede suprimir copias archivadas de archivos del almacenamiento del servidor, pero no versiones de copia de seguridad de los archivos.

#### Inscripción cerrada

Inscripción cerrada es el método predeterminado para la inscripción de cliente en el servidor. Para este tipo de inscripción, un administrador registra todos los clientes. El administrador puede implementar los siguientes valores:

- Asignar el nodo a cualquier dominio de políticas
- Determinar si el usuario puede utilizar la compresión o no, o si el usuario puede elegir.
- Controlar si el usuario puede suprimir los archivos de copia de seguridad o archivos archivados

Puede aumentar la protección de sus datos y contraseñas utilizando la Capa de sockets seguros (SSL). SSL es la tecnología estándar que utiliza para crear sesiones cifradas para servidores y clientes, y proporciona un canal seguro para comunicarse a través de vías de comunicación abiertas. Con SSL, la identidad del servidor se verifica mediante el uso de certificados digitales. Si se autentica en un servidor LDAP (Lightweight Directory Access Protocol), las contraseñas entre el servidor y el servidor LDAP están protegidas por la Seguridad de la capa de transporte (TLS). El protocolo TLS es el sucesor del protocolo SSL. Cuando un servidor y un cliente se comunican, TLS se asegura de que ningún tercero pueda interceptar los mensajes.

## Interfaces de usuario para entornos de IBM Spectrum Protect

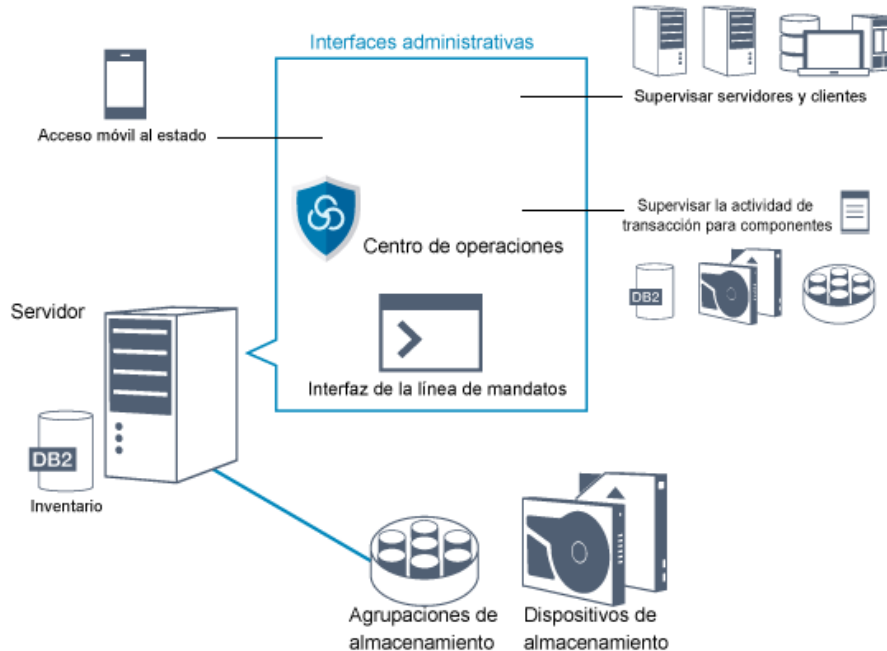
---

Para las tareas de configuración y supervisión, IBM Spectrum Protect proporciona varias interfaces, incluido el Centro de operaciones, una interfaz de línea de mandatos y una interfaz administrativa SQL.

## Interfaces para la gestión de almacenamiento de datos

El Centro de operaciones es la interfaz primaria para que los administradores supervisen y administren los servidores. Una ventaja clave del Centro de operaciones es que se pueden supervisar varios servidores, como se muestra en Figura 1. También puede supervisar y administrar IBM Spectrum Protect desde una interfaz administrativa de línea de mandatos.

Figura 1. Interfaces de usuario para la gestión de datos de almacenamiento



Utilice las interfaces siguientes para interactuar con IBM Spectrum Protect:

### Centro de operaciones

El Centro de operaciones proporcionan acceso móvil y web para la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar el Centro de operaciones para completar ciertas tareas de administración y supervisión, por ejemplo:

- Puede supervisar varios servidores y clientes.
- Puede supervisar la actividad de transacción respecto a componentes específicos en la vía de acceso a datos, como la base de datos del servidor, el registro de recuperación, dispositivos de almacenamiento y agrupaciones de almacenamiento.

### Interfaz de la línea de mandatos

Puede utilizar una interfaz de línea de mandatos para ejecutar tareas de administración para servidores. Puede acceder a la interfaz de línea de mandatos a través del Centro de operaciones o del cliente administrativo de IBM Spectrum Protect.

Acceda a la información en la base de datos del servidor utilizando sentencias SQL

Puede utilizar sentencias SQL SELECT para consultar la base de datos de servidor y visualizar los resultados. Hay disponibles herramientas SQL de terceros para ayudar a los administradores en la gestión de bases de datos.

## Interfaces para la gestión de actividad de cliente

IBM Spectrum Protect proporciona los siguientes tipos de interfaces para la gestión de la actividad de cliente:

- Una interfaz de programación de aplicaciones (API)
- Interfaces gráficas de usuario para clientes
- Interfaz del navegador para el cliente de archivado y copia de seguridad
- Interfaces de línea de mandatos para clientes

## Conceptos de almacenamiento de datos en IBM Spectrum Protect

IBM Spectrum Protect proporciona funciones para almacenar datos en un rango de dispositivo y almacenamiento de soporte.

Para dejar los dispositivos de almacenamiento disponibles para el servidor, debe conectar los dispositivos de almacenamiento y correlacionar las agrupaciones de almacenamiento con clases de dispositivo, bibliotecas y unidades.

- Tipos de dispositivos de almacenamiento  
Puede utilizar varios dispositivos de almacenamiento con IBM Spectrum Protect para cumplir los objetivos de protección de datos específicos.
- Almacenamiento de datos en agrupaciones de almacenamiento  
Las agrupaciones de almacenamiento lógico son los componentes principales del modelo de IBM Spectrum Protect de almacenamiento de datos. Puede optimizar el uso de los dispositivos de almacenamiento manipulando las propiedades de agrupaciones de almacenamiento y volúmenes.
- Transporte de datos a almacenar a través de redes  
En entorno de IBM Spectrum Protect proporciona formas de mover datos de forma segura para almacenarlos a través de varios tipos de redes y configuraciones.

## Tipos de dispositivos de almacenamiento

Puede utilizar varios dispositivos de almacenamiento con IBM Spectrum Protect para cumplir los objetivos de protección de datos específicos.

## Dispositivos de almacenamiento y objetos de almacenamiento

El servidor IBM Spectrum Protect puede conectarse a una combinación de dispositivos de almacenamiento manuales y automatizados. Puede conectar los siguientes tipos de dispositivos de almacenamiento a IBM Spectrum Protect:

- Dispositivos de disco que están conectados directamente, conectados a la SAN o conectados a la red
- Dispositivos de cinta físicos manuales o automatizados
- Dispositivos de cinta virtuales
- Almacenamiento de objetos en la nube

IBM Spectrum Protect representa dispositivos de almacenamiento físicos y soportes con objetos de almacenamiento que define en la base de datos del servidor. Los objetos de almacenamiento clasifican recursos de almacenamiento disponibles y gestiona la migración de un grupo de almacenamiento a otro. La Tabla 1 describe los objetos de almacenamiento en el entorno de almacenamiento del servidor.

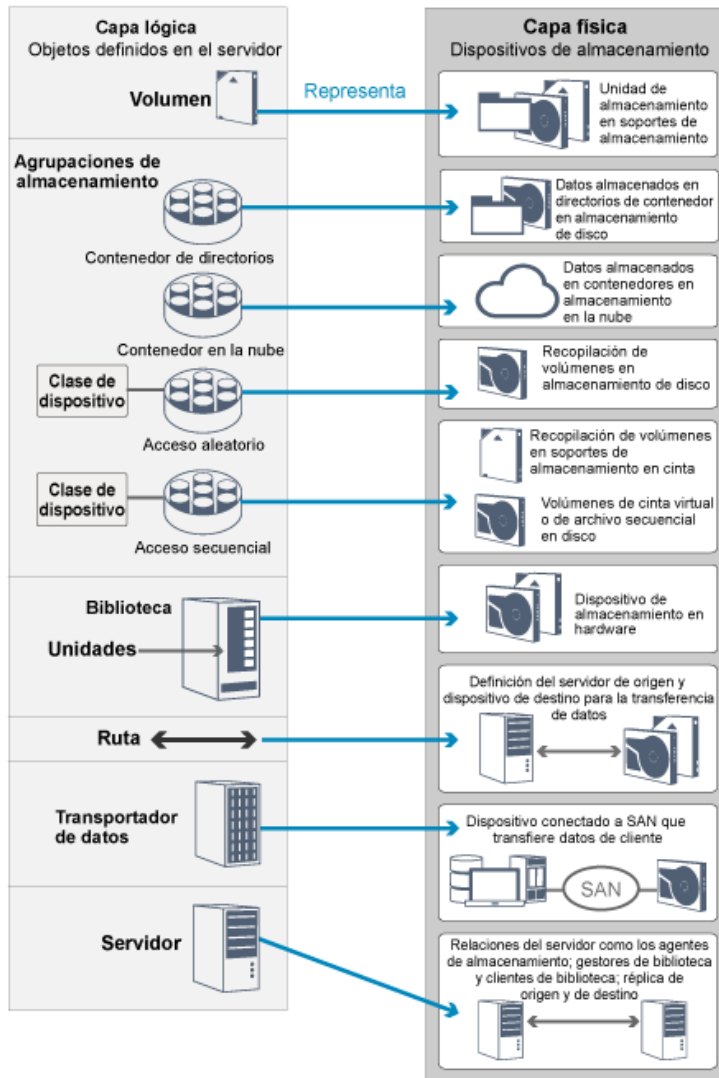
Tabla 1. Objetos de almacenamiento y representaciones

Objeto de almacenamiento	Qué representa este objeto
Volumen	Una unidad discreta de almacenamiento en disco, cinta u otro medio de almacenamiento. Cada volumen se asocia a una sola agrupación de almacenamiento.
Agrupación de almacenamiento	Un conjunto de volúmenes de almacenamiento o contenedores que es el destino utilizado para almacenar datos de cliente. IBM Spectrum Protect utiliza los siguientes tipos de agrupación de almacenamiento: <ul style="list-style-type: none"> <li>• Agrupaciones de almacenamiento de contenedores de directorio</li> <li>• Agrupaciones de almacenamiento de contenedores de nube</li> <li>• Agrupaciones de almacenamiento de acceso secuencial asociadas con una clase de dispositivo.</li> <li>• Agrupaciones de almacenamiento de acceso aleatorio asociadas con una clase de dispositivo.</li> </ul>
Contenedor	Una ubicación de almacenamiento de datos, por ejemplo, un archivo, un directorio o un dispositivo.
Agrupación de almacenamiento de contenedores	Una agrupación de almacenamiento primaria que utiliza un servidor para almacenar datos. Los datos se almacenan en contenedores en directorios de sistemas de archivos o en almacenamiento en la nube. El almacenamiento de los datos se optimiza, si es necesario, en la agrupación de almacenamiento.
Clase de dispositivo	El tipo de dispositivo de almacenamiento que pueden utilizar los volúmenes definidos en una agrupación de almacenamiento de acceso secuencial o aleatorio. Cada clase de dispositivo de tipo de medios extraíbles se asocia a una sola biblioteca.

Objeto de almacenamiento	Qué representa este objeto
Biblioteca	Un dispositivo de almacenamiento. Por ejemplo, una biblioteca puede representar una unidad autónoma, un conjunto de unidades autónomas, un dispositivo automatizado con varias unidades o un conjunto de unidades controlado por un gestor de medios.
Unidad	Un objeto del dispositivo de la biblioteca de cintas que proporciona la capacidad para leer y escribir datos en el soporte de biblioteca de cintas. Cada unidad se asocia a una sola biblioteca.
Vía de acceso	La especificación del origen de datos y el destino del dispositivo. Antes de poder utilizar un dispositivo de almacenamiento, debe definirse una vía de acceso entre el dispositivo y el servidor de origen que está moviendo los datos.
Transportador de datos	Un dispositivo conectado a SAN que se utiliza para transferir datos de cliente. Un transportador de datos sólo se utiliza en una transferencia de datos donde el servidor no está presente, como en un entorno NDMP (Network Data Management Protocol). Los transportadores de datos transfieren datos entre los dispositivos de almacenamiento sin utilizar muchos recursos del servidor, del cliente ni de la red.
Servidor	Servidor gestionado por otro servidor de IBM Spectrum Protect.

El administrador define los objetos de almacenamiento en la capa lógica del servidor, como se ilustra en Figura 1.

Figura 1. Objetos de almacenamiento



## Dispositivos de disco

Puede almacenar datos de cliente en dispositivos de disco con los siguientes tipos de volúmenes:

- Directorios en las agrupaciones de almacenamiento de contenedores de directorio
- Volúmenes de acceso aleatorio de tipo de dispositivo DISK
- Volúmenes de acceso secuencial de tipo de dispositivo FILE

IBM Spectrum Protect ofrece las características siguientes cuando se utilizan agrupaciones de almacenamiento de contenedores de directorio para el almacenamiento de datos:

- Puede aplicar las técnicas de almacenamiento en memoria caché de disco y la optimización de almacenamiento de datos para maximizar el uso del almacenamiento de datos.
- Puede recuperar datos desde el disco mucho más rápido de lo que puede recuperar datos del almacenamiento en cintas.

## Dispositivos de cinta física

En una biblioteca de cintas físicas, la capacidad de almacenamiento se define en términos del número total de volúmenes en la biblioteca. Los dispositivos de cinta física se pueden utilizar para las siguientes actividades:

- Almacenamiento de los datos de cliente de la copia de seguridad, archivados o migrados desde los nodos de cliente
- Almacenamiento de las copias de seguridad de base de datos
- Exportación de datos a otro servidor o almacenamiento externo

El traslado de datos a cinta proporciona los siguientes beneficios:

- Puede conservar los datos para clientes en un dispositivo de disco el mismo tiempo que los datos se mueven a la cinta.
- Puede mejorar el rendimiento de la unidad de cinta clasificando la migración de datos de disco a cinta.

- Puede distribuir las veces en las que las unidades están en uso para mejorar el rendimiento de las unidades de cinta.
- Puede mover los datos de la cinta a almacenes externos.
- Puede limitar el consumo de energía porque los dispositivos de cinta no consumen energía después de que los datos se graban en la cinta.
- Puede aplicar el cifrado proporcionado por el hardware de la unidad de cinta para proteger los datos de la cinta.

En comparación con el almacenamiento de cintas virtuales y de disco equivalente, el coste de la unidad para almacenar datos tiende a ser mucho menor para dispositivos de cinta físicos.

## Bibliotecas virtuales de cintas

Una biblioteca de cintas virtuales (VTL) no utiliza medios de cinta físicos. Cuando utiliza almacenamiento VTL, emula los mecanismos de acceso del hardware de cinta. En una VTL, puede definir volúmenes y unidades para proporcionar una mayor flexibilidad para el entorno de almacenamiento. La capacidad de almacenamiento de una VTL se define en términos de espacio de disco disponible. Puede aumentar o disminuir el número y el tamaño de los volúmenes en el disco.

La definición de una VTL para el servidor IBM Spectrum Protect puede mejorar el rendimiento porque el servidor maneja el proceso de puntos de montaje para las VTL de modo diferente que para las bibliotecas de cintas reales. Aunque las limitaciones lógicas de los dispositivos de cinta aún están presentes, las limitaciones físicas del hardware de cintas reales no se aplican a una VTL, ofreciendo opciones para una mejor escalabilidad. Puede utilizar la VTL de IBM Spectrum Protect cuando se cumplan las siguientes condiciones:

- Sólo se emula un tipo y generación de unidad y soporte en la VTL.
- Cada servidor y agente de almacenamiento con acceso a la VTL tiene vías de acceso definidas para todas las unidades de la biblioteca.

## Almacenamiento de datos en agrupaciones de almacenamiento

Las agrupaciones de almacenamiento lógico son los componentes principales del modelo de IBM Spectrum Protect de almacenamiento de datos. Puede optimizar el uso de los dispositivos de almacenamiento manipulando las propiedades de agrupaciones de almacenamiento y volúmenes.

### Tipos de agrupaciones de almacenamiento

El grupo de agrupaciones de almacenamiento que configura para el servidor se denomina *almacenamiento del servidor*. Puede definir los siguientes tipos de agrupaciones de almacenamiento en el almacenamiento del servidor:

#### Agrupaciones de almacenamiento primarias

Un conjunto con nombre de volúmenes que el servidor utiliza para almacenar versiones de copia de seguridad de archivos, copias archivadas de archivos y archivos que se han migrado desde los nodos cliente.

#### Agrupaciones de almacenamiento de copia

Conjunto con nombre de volúmenes que contienen copias de archivos que residen en agrupaciones de almacenamiento primario. Las agrupaciones de almacenamiento de copias se utilizan solo para realizar copias de seguridad de datos que están almacenados en agrupaciones de almacenamiento primarias. Una agrupación de almacenamiento de copias puede ser el destino para un grupo de copias de seguridad, un grupo de copias archivadas o una clase de gestión de archivos gestionados por espacio.

#### Agrupaciones de almacenamiento de copia de contenedor

Conjunto con nombre de volúmenes que contienen una copia de las extensiones de datos que residen en agrupaciones de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copias de contenedor sólo se utilizan para proteger los datos que están almacenados en agrupaciones de almacenamiento de contenedores de directorio.

#### Agrupaciones de almacenamiento de datos activos

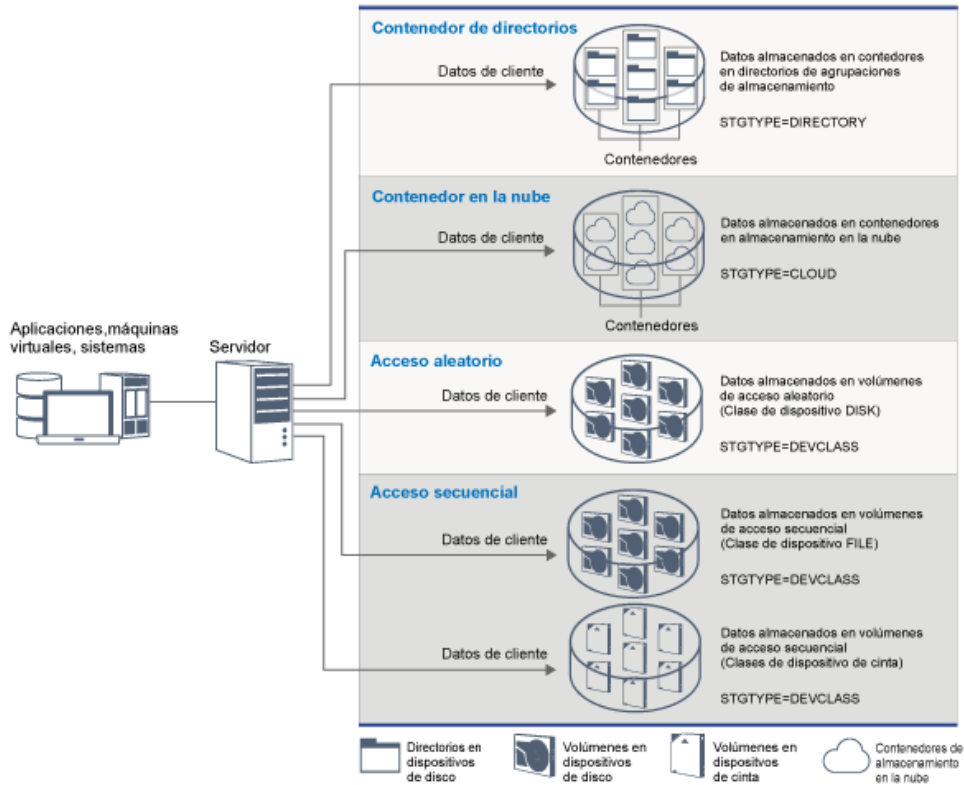
Conjunto denominado de volúmenes de agrupación de almacenamiento que solamente contiene versiones activas de datos de copia de seguridad de cliente.

### Agrupaciones de almacenamiento primarias

Cuando se restauran, se recuperan o se exportan datos de archivos, el archivo solicitado se obtiene de una agrupación de almacenamiento primario. Dependiendo del tipo de agrupación de almacenamiento primario, las agrupaciones de almacenamiento pueden estar en el local o fuera del local. Puede organizar agrupaciones de almacenamiento primarias en una jerarquía de almacenamiento, así esos datos pueden transferirse desde el almacenamiento de disco a un almacenamiento de coste más bajo como los dispositivos de cinta. La Figura 1 ilustra el concepto de agrupaciones de almacenamiento primario.

Figura 1. Agrupaciones de almacenamiento primarias

## Agrupaciones de almacenamiento primario



Puede definir los siguientes tipos de agrupación de almacenamiento primario:

### Agrupaciones de almacenamiento de contenedores de directorio

Una agrupación de almacenamiento que el servidor utiliza para almacenar datos en contenedores en directorios de agrupación de almacenamiento. Los datos que se almacenan en una agrupación de almacenamiento de contenedores de directorios pueden utilizar deduplicación de datos en línea, deduplicación de datos del lado del cliente, compresión en línea o compresión del lado del cliente. La deduplicación de datos en línea o la compresión en línea reduce los datos a la vez que se almacenan. Al utilizar agrupaciones de almacenamiento de contenedores de directorio, elimina la necesidad de reclamación de volumen, que mejora el rendimiento de servidor y reduce el coste del hardware de almacenamiento. Puede proteger y reparar los datos de las agrupaciones de almacenamiento de contenedores de directorio a nivel de la agrupación de almacenamiento.

Restricción: No puede utilizar ninguna de las siguientes funciones con agrupaciones de almacenamiento de contenedores de directorio:

- Migración
- Reclamación
- Agregación
- Proximidad
- Grabación simultánea
- Copia de seguridad de agrupaciones de almacenamiento
- Volúmenes virtuales

### Agrupaciones de almacenamiento de contenedores de nube

Una agrupación de almacenamiento que un servidor utiliza para almacenar datos en almacenamiento en nube. El almacenamiento en la nube puede estar en el local o fuera de este. Las agrupaciones de almacenamiento de contenedores de nube proporcionadas por IBM Spectrum Protect pueden almacenar datos en un almacenamiento en nube que esté basado en objetos. Mediante el almacenamiento de datos en agrupaciones de almacenamiento de contenedores de nube, puede aprovechar las ventajas de coste por unidad que ofrecen las nubes junto con las prestaciones de escalabilidad que proporciona el almacenamiento en nube. IBM Spectrum Protect gestiona las credenciales, la seguridad, las E/S de lectura y escritura y el ciclo de vida de los datos almacenados en la nube. Cuando se implementan agrupaciones de almacenamiento de contenedores de nube en el servidor, puede grabar directamente en la nube configurando una agrupación de almacenamiento de contenedores de nube con las credenciales de la nube. Los datos que se almacenan en una agrupación de almacenamiento de contenedores de nubes pueden utilizar la deduplicación de datos en línea y la compresión en línea. El servidor graba datos deduplicados y cifrados directamente en la nube. Puede hacer la copia de seguridad y la restauración de datos o archivar y recuperar datos directamente de la agrupación de almacenamiento de contenedores de nube.



Puede definir los siguientes tipos de agrupaciones de almacenamiento de contenedores de nubes:

#### En las instalaciones

Puede utilizar el tipo de agrupación de almacenamiento de contenedores de nube en las instalaciones para almacenar datos en una nube privada, lo que aumentará la seguridad y le proporcionará el máximo control sobre los datos. Las desventajas de una nube privada son un mayor coste debido a los requisitos de hardware y el mantenimiento en el local.

#### Fuera de las instalaciones locales

Puede utilizar el tipo de agrupación de almacenamiento de contenedores de nube fuera de las instalaciones para almacenar datos en una nube pública. La ventaja de utilizar una nube pública es que puede conseguir un coste más bajo que en el caso de una nube privada, por ejemplo, al eliminar el mantenimiento. Sin embargo, se debe comparar esta ventaja frente a los posibles problemas de rendimiento debido a las velocidades de conexión y la reducción del control sobre los datos.

#### Agrupaciones de almacenamiento asociadas con clases de dispositivo

Puede definir una agrupación de almacenamiento primario para utilizar los siguientes tipos de dispositivos de almacenamiento:

##### Clase de dispositivo DISK

En un tipo de dispositivo DISK de la agrupación de almacenamiento, los datos se almacenan en bloques de discos de acceso aleatorio. Puede utilizar el almacenamiento en memoria caché en agrupaciones de almacenamiento DISK para aumentar el rendimiento de restauración del cliente con algunas limitaciones en el proceso de servidor. La asignación y el seguimiento de espacio por bloques utiliza más espacio de almacenamiento de base de datos y requiere más potencia de proceso que la asignación y el seguimiento de espacio por volumen.

##### Clase de dispositivo FILE

En un tipo de dispositivo FILE de la agrupación de almacenamiento, los archivos se almacenan en volúmenes secuenciales para un mejor rendimiento secuencial que para el almacenamiento en bloques de discos. Para el servidor, estos archivos tienen las características de un volumen de cinta, por lo que este tipo de agrupación de almacenamiento es más adecuado para la migración a cinta. Los volúmenes FILE son útiles para el *almacenamiento en cámaras de seguridad electrónicas*, donde los datos se transfieren electrónicamente a un sitio remoto en lugar de a un envío físico de cinta. En general, este tipo de agrupación de almacenamiento se prefiere a las agrupaciones de almacenamiento DISK.

El servidor utiliza las siguientes agrupaciones de almacenamiento primario de acceso aleatorio predeterminadas:

##### ARCHIVEPOOL

En la política STANDARD, esta agrupación de almacenamiento es el destino de los archivos que se archivan desde los nodos de cliente.

##### BACKUPPOOL

En la política STANDARD, esta agrupación de almacenamiento es el destino de los archivos de los que se hace copia de seguridad desde los nodos de cliente.

##### SPACEMGPOOL

Esta agrupación de almacenamiento es para archivos gestionados por espacio que se migran desde nodos de cliente de IBM Spectrum Protect for Space Management.

## Agrupaciones de almacenamiento de copia

Las agrupaciones de almacenamiento de copia contienen versiones activas e inactivas de los datos con copia de seguridad procedentes de agrupaciones de almacenamiento primarias. No se puede utilizar una agrupación de almacenamiento de contenedores de directorio como agrupación de almacenamiento de copias. Además, los datos de la agrupación de almacenamiento de contenedores de directorio no se pueden copiar en una agrupación de almacenamiento de copias. Para proteger agrupaciones de almacenamiento de contenedores de directorio, copie los datos en una agrupación de almacenamiento de copias de contenedor. La Figura 2 ilustra el concepto de agrupaciones de almacenamiento de copia.

Figura 2. Agrupaciones de almacenamiento de copia



Las agrupaciones de almacenamiento de copia proporciona un medio de recuperación ante siniestro o anomalías de medios. Por ejemplo, si un cliente intenta recuperar un archivo dañado de la agrupación de almacenamiento primario, el cliente puede restaurar los datos de la agrupación de almacenamiento de copias.

Puede mover los volúmenes de las agrupaciones de almacenamiento de copias fuera de las instalaciones y el servidor aún sigue haciendo seguimiento de los volúmenes. Mover estos volúmenes fuera de las instalaciones proporciona un medio de recuperación ante un desastre interno. Una agrupación de almacenamiento de copias sólo puede utilizar el almacenamiento de acceso secuencial, por ejemplo, una clase de dispositivo de cinta o una clase de dispositivo FILE.

## Agrupaciones de almacenamiento de copia de contenedor

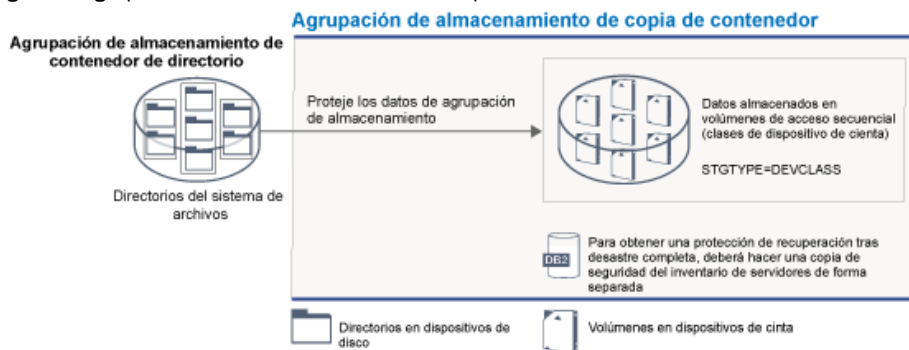
Un servidor puede proteger una agrupación de almacenamiento de contenedores de directorio almacenando copias de los datos en una agrupación de almacenamiento de copias de contenedor. Los datos en las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta, que se pueden almacenar en el local o fuera del local. Los datos dañados en las agrupaciones de almacenamiento de contenedores de directorio se puede reparar utilizando extensiones deduplicadas en agrupaciones de almacenamiento de copia de contenedor. Las agrupaciones de almacenamiento de copia de contenedor proporcionan una alternativa a utilizar un servidor de réplica para proteger los datos en una agrupación de almacenamiento de contenedores de directorio.

Restricción: Si se pierden todos los datos de servidor, las agrupaciones de almacenamiento de copia de contenedor solas no proporcionan el mismo nivel de protección que la réplica:

- Con la réplica, puede restaurar los datos de cliente directamente desde el servidor de destino si el servidor de origen no está disponible.
- Con las agrupaciones de almacenamiento de copia de contenedor, primero debe restaurar el servidor desde una copia de seguridad de base de datos y, a continuación, reparar las agrupaciones de almacenamiento de contenedores de directorio desde los volúmenes de cinta.

La Figura 3 ilustra el concepto de agrupaciones de almacenamiento de copia de contenedor.

Figura 3. Agrupaciones de almacenamiento de copia de contenedor



Dependiendo de la configuración del sistema, puede crear planificaciones de protección para copiar simultáneamente los datos de agrupación de almacenamiento de contenedores de directorio en agrupaciones de almacenamiento de copia de contenedor en el local o fuera del local para satisfacer los requisitos:

- Si la réplica está habilitada, puede crear una agrupación de copia de contenedor fuera del local. La copia fuera del local se puede utilizar para proporcionar protección adicional en un entorno replicado.
- Si la réplica no está habilitada, puede crear una agrupación de almacenamiento en el local y otra fuera del local.

Dependiendo de los recursos y las necesidades del sitio, la capacidad de copiar agrupaciones de almacenamiento de contenedores de directorio en cinta tiene las ventajas siguientes:

- Puede evitar mantener otro servidor y más espacio de almacenamiento de disco.
- Los datos se copian en las agrupaciones de almacenamiento que están definidas en el servidor. El rendimiento no depende de la conexión de red entre servidores ni se ve afectado por dicha conexión.
- Puede satisfacer los requisitos normativos y empresariales para las copias de cinta fuera del local.

## Agrupaciones de almacenamiento de datos activos

Una agrupación de datos activos sólo contiene versiones activas de los datos de copia de seguridad de cliente. En este caso, el servidor no tiene que colocar archivos inactivos antiguos que no se tienen que restaurar. No se puede utilizar una agrupación de almacenamiento de contenedores de directorio como agrupación de almacenamiento de datos activos. Puede utilizar agrupaciones de datos activos para mejorar la eficiencia de las operaciones de almacenamiento de datos y restauración, por ejemplo, este tipo de agrupación de almacenamiento puede ayudarle a lograr los siguientes objetivos:

- Aumentar la velocidad de las operaciones de restauración de datos de cliente
- Reducir el número de volúmenes de almacenamiento en el sitio o fuera del sitio
- Reducir la cantidad de datos que se transfieren al copiar o restaurar archivos almacenados de forma electrónica en una ubicación remota

Los datos migrados mediante clientes de gestión de almacenamiento jerárquico (HSM) y datos de copia archivada no están permitidos en las agrupaciones de datos activos. A medida que las versiones actualizadas de los datos de copia de seguridad van almacenándose en agrupaciones de datos activos, las versiones más antiguas se eliminan cuando los datos que quedan se consolidan desde varios volúmenes de acceso secuencial en menos volúmenes de acceso secuencial nuevos. La Figura 4 ilustra el concepto de agrupaciones de almacenamiento de datos activos.

Figura 4. Agrupaciones de almacenamiento de datos activos



Las agrupaciones de datos activos pueden utilizar cualquier tipo de almacenamiento de acceso secuencial. No obstante, los beneficios de una agrupación de datos activos dependerán del tipo de dispositivo asociado a la agrupación. Por ejemplo, las agrupaciones de datos activos asociadas a una clase de dispositivo FILE resultan ideales para conseguir rápidas operaciones de restauración de cliente por los siguientes motivos:

- Los volúmenes FILE no se han de montar físicamente
- Las sesiones de cliente que se están restaurando desde los volúmenes FILE en una agrupación de datos activos pueden acceder a los volúmenes simultáneamente, lo que mejora el rendimiento de la restauración.

**Información relacionada:**

- ➔ Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de directorio
- ➔ Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de nube

## Transporte de datos a almacenar a través de redes

En entorno de IBM Spectrum Protect proporciona formas de mover datos de forma segura para almacenarlos a través de varios tipos de redes y configuraciones.

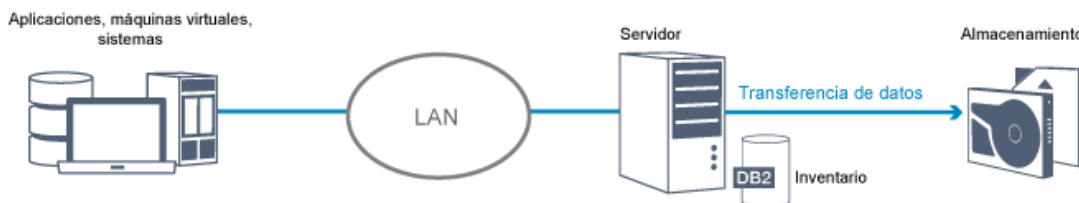
### Configuraciones de red para dispositivos de almacenamiento

IBM Spectrum Protect proporciona métodos para la configuración de clientes y servidores en una red de área local (LAN), en una red de área de almacenamiento (SAN), movimiento de datos sin LAN y como almacenamiento adjunto de red.

Operaciones de copia de seguridad de datos a través de una LAN

Figura 1 muestra la vía de acceso a datos para operaciones de copia de seguridad de IBM Spectrum Protect a través de una LAN.

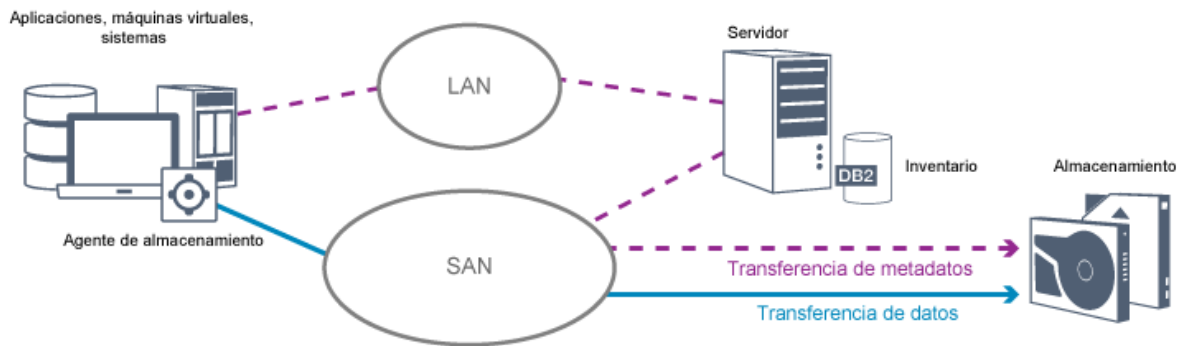
Figura 1. Operaciones de copia de seguridad de IBM Spectrum Protect a través de una LAN



En una configuración de LAN, hay una o más bibliotecas de cintas asociadas con un único servidor IBM Spectrum Protect. En este tipo de configuración, los datos de cliente, el correo electrónico, la conexión de terminal, el programa de aplicación y la información de control de dispositivo deben gestionarse a través de la misma red. La información sobre el control de dispositivos, las copias de seguridad de cliente y la restauración de datos se transfieren a través de la LAN.

Operaciones de copia de seguridad de datos a través de una SAN

Figura 2 muestra la vía de acceso a datos para operaciones de copia de seguridad de IBM Spectrum Protect a través de una SAN. Figura 2. Operaciones de copia de seguridad de IBM Spectrum Protect a través de una SAN



Una red de área de almacenamiento (SAN) es una red de almacenamiento dedicada que puede mejorar el rendimiento del sistema. En una SAN, puede consolidar el almacenamiento y aligerar la distancia, escalabilidad y los límites en el ancho de banda inherentes en entornos de LAN y WAN. Utilizando IBM Spectrum Protect en una SAN, puede beneficiarse de las siguientes funciones:

- Compartir dispositivos de almacenamiento entre varios servidores IBM Spectrum Protect. Los dispositivos que utilizan el tipo de dispositivo GENERICTAPE no se incluyen.
- Mueva datos de un sistema cliente directamente hasta dispositivos de almacenamiento sin utilizar la LAN. El movimiento de datos sin LAN requiere la instalación de un agente de almacenamiento en el sistema cliente. El agente de almacenamiento está disponible con el producto IBM Spectrum Protect for SAN.

A través del agente de almacenamiento, el cliente puede hacer una copia de seguridad y restaurar datos directamente a una biblioteca de cintas o un sistema de archivos compartidos, como GPFS. El servidor IBM Spectrum Protect mantiene la base de datos del servidor y el registro de recuperación, y actúa como gestor de biblioteca para controlar las operaciones de dispositivo. El agente de almacenamiento del cliente gestiona la transferencia de datos al dispositivo de la SAN. Esta implementación libera ancho de banda en la LAN que de lo contrario debe utilizarse para el movimiento de datos de cliente.

- Compartir unidades de cinta y bibliotecas soportadas por el servidor IBM Spectrum Protect.
- Consolidar varios clientes bajo un único nombre de nodo cliente en un clúster de General Parallel File System (GPFS).

#### Almacenamiento conectado a red

Los servidores de archivos de NAS (almacenamiento adjunto de red) son servidores de almacenamiento dedicados cuyos sistemas operativos se optimizan para realizar funciones de servidor de archivos. Normalmente los servidores de archivos de NAS interactúan con IBM Spectrum Protect a través de protocolos de red estándares del sector, como NDMP (protocolo de gestión de datos de red) o como almacenamiento primario para agrupaciones de almacenamiento de acceso aleatorio o de acceso secuencial. IBM Spectrum Protect proporciona los siguientes tipos básicos de configuraciones que utilizan NDMP para hacer copia de seguridad y gestionar servidores de archivos de NAS:

- IBM Spectrum Protect hace copia de seguridad de un servidor de archivos de NAS en un dispositivo de biblioteca adjunto directamente a un servidor de archivos de NAS. El servidor de archivos de NAS, que puede estar lejos del servidor IBM Spectrum Protect, transfiere directamente los datos de copia de seguridad a una unidad de una biblioteca de cintas con conexión SCSI. Los datos están almacenados en agrupaciones de almacenamiento con formato NDMP, de las que se puede hacer copia de seguridad en el soporte de almacenamiento que se pueden mover fuera del sitio como medida de protección en caso de que se produzca un desastre en el sitio.
- IBM Spectrum Protect hace una copia de seguridad de un servidor de archivos de almacenamiento adjunto de red (NAS) sobre la LAN en una jerarquía de agrupación de almacenamiento. En este tipo de configuración, puede almacenar datos de NAS directamente en el disco, ya sea acceso aleatorio o acceso secuencial y, a continuación, migrar los datos a cinta. También puede utilizar este tipo de configuración para la réplica del sistema. También se puede hacer copia de seguridad de los datos en un soporte de almacenamiento que se puede mover fuera del sitio. La ventaja de este tipo de configuración es que le aporta todas las características de gestión de datos asociadas a una jerarquía de agrupaciones de almacenamiento.
- El cliente de IBM Spectrum Protect lee los datos desde el sistema de NAS mediante los protocolos NFS o CIFS y los envía al servidor para almacenarlos.

## Gestión de almacenamiento

Gestiona los dispositivos y soportes utilizados para almacenar datos de cliente a través del servidor IBM Spectrum Protect. El servidor integra la gestión de almacenamiento con las políticas que define para gestionar datos de cliente en las áreas siguientes:

Tipos de dispositivos para almacenamiento del servidor

Con IBM Spectrum Protect se pueden usar dispositivos con conexión directa y con conexión a la red para el almacenamiento del servidor. IBM Spectrum Protect representa dispositivos de almacenamiento físicos y soportes con los siguientes objetos definidos por el administrador.

#### Migración de datos a través de la jerarquía de almacenamiento

Para agrupaciones de almacenamiento primarias que no sean agrupaciones de almacenamiento de contenedores de directorio, puede organizar las agrupaciones de almacenamiento en una o más estructuras jerárquicas. Esta jerarquía de almacenamiento proporciona flexibilidad de varias formas. Por ejemplo, puede establecer una política para hacer copia de seguridad de los datos a disco para operaciones de copia de seguridad más rápidas. El servidor IBM Spectrum Protect puede migrar automáticamente datos desde un disco a una cinta.

#### Eliminación de datos caducados

La política que se define controla el momento en que los datos de cliente caducan automáticamente desde el servidor de IBM Spectrum Protect. Para suprimir datos que son elegibles para la caducidad, un proceso de caducidad del servidor marca los datos como caducados y elimina los metadatos de los datos caducados de la base de datos. A continuación, el espacio que ocupan los datos caducados está disponible para datos nuevos. Puede controlar la frecuencia del proceso de caducidad utilizando una opción de servidor.

#### Reutilización de medios mediante reclamación

Puesto que las políticas del servidor establecen la caducidad de los datos de forma automática, los medios donde se almacenan los datos acumulan espacio no utilizado. Para soporte de almacenamiento distinto de agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de disco aleatorias, el servidor de IBM Spectrum Protect implementa la *reclamación*, un proceso que libera soporte para reutilizarlos sin la rotación de cintas tradicional. La reclamación desfragmenta automáticamente soportes consolidando datos sin caducar en otros soportes cuando el espacio libre de un medio alcanza un nivel definido. A continuación, el servidor puede volver a utilizar los medios reclamados. La reclamación permite a los soportes que circulen automáticamente a través del proceso de gestión de almacenamiento y minimizar el número de soportes necesarios.

## Consolidación de datos de cliente de seguridad

---

Agrupando los datos de cliente a los que ha hecho copia de seguridad, puede minimizar el número de montajes de soporte necesario para la recuperación de cliente. El servidor de IBM Spectrum Protect proporciona los siguientes métodos para agrupar archivos de cliente en soportes de almacenamiento distintos de agrupaciones de almacenamiento de contenedores de directorio:

#### Colocación de datos de cliente

El servidor de IBM Spectrum Protect puede *colocar* datos de cliente; o, en otras palabras, almacenar los datos de cliente en unos pocos volúmenes en lugar de dispersarlos en muchos volúmenes. La colocación por cliente minimiza el número de volúmenes necesario para hacer copia de seguridad y restaurar datos de cliente. La colocación de datos puede aumentar el número de montajes de volumen porque cada cliente puede tener un volumen dedicado en lugar de que los datos de varios clientes se almacenen en el mismo volumen.

Puede establecer el servidor para colocar los datos de cliente cuando se coloquen inicialmente los datos en el almacenamiento del servidor. En una jerarquía de almacenamiento, también puede aproximar los datos cuando el servidor los migre desde la agrupación de almacenamiento inicial a la siguiente agrupación de almacenamiento en la jerarquía de almacenamiento. Puede aplicar la función de proximidad por cliente, por espacio de archivos por cliente o por grupo de clientes. La selección depende del tamaño de los espacios de archivos que se almacenan y los requisitos de restauración.

#### Asociación de agrupaciones de datos activos con varios dispositivos

Las agrupaciones de datos activos son útiles para la restauración rápida de datos de cliente. Los beneficios incluyen una reducción del número de volúmenes de almacenamiento en el sitio o fuera, o la reducción del ancho de banda al copiar o restaurar datos que se han asegurado electrónicamente en una ubicación remota. Las agrupaciones de datos activos que usan soportes extraíbles como cintas, ofrecen beneficios similares. Aunque los dispositivos deben estar montados, el servidor no tiene que colocar archivos antiguos inactivos. Sin embargo, la principal ventaja de utilizar soportes de almacenamiento extraíbles en agrupaciones de datos activos es que el número de volúmenes que se utiliza para el almacenamiento interno y externo se reduce. Si almacena datos en una ubicación remota, puede minimizar la cantidad de datos que se deben transferir copiando y restaurando sólo los datos activos.

#### Creación de un conjunto de copias de seguridad

Un conjunto de copias de seguridad contiene todos los archivos de seguridad activos que existen para el cliente en el almacenamiento del servidor. El conjunto de copias de seguridad es portátil y se mantiene durante el tiempo que se especifique. Un conjunto de copias de seguridad es un añadido para las copias de seguridad que ya están almacenadas y requiere más soporte.

#### Movimiento de datos para un nodo de cliente

Puede consolidar datos para un nodo cliente mediante el traspaso de datos dentro del almacenamiento del servidor. Puede mover un conjunto de copias de seguridad a un soporte diferente, donde el conjunto de copias de seguridad se retiene hasta la

hora que específica. Los datos consolidados puede ayudar a mejorar la eficiencia durante las operaciones de restauración o recuperación de clientes.

## Estrategias de protección de datos con IBM Spectrum Protect

IBM Spectrum Protect proporciona diversas formas de implementar varias estrategias de protección de datos.

Puede configurar IBM Spectrum Protect para enviar datos a dispositivos de almacenamiento que están en el sitio local o en un sitio remoto. Para maximizar la protección de datos, puede configurar la réplica para un servidor remoto.

- Estrategias para minimizar el uso del espacio de almacenamiento para copias de seguridad  
Para minimizar la cantidad de espacio de almacenamiento necesario, IBM Spectrum Protect hace copia de seguridad de los datos utilizando las técnicas de copia de seguridad incremental progresiva y la optimización de almacenamiento de datos.
- Estrategias para protección ante desastres  
IBM Spectrum Protect proporciona estrategias para proteger datos si se produce un desastre. Estas estrategias incluyen la réplica de nodo a un sitio remoto, la protección de agrupación de almacenamiento, la copia de seguridad de base de datos, las transferencias de cintas de copia de seguridad fuera del local y la réplica de dispositivos a un servidor en espera.
- Estrategias para la recuperación tras desastre con IBM Spectrum Protect  
IBM Spectrum Protect proporciona varias formas de recuperar el servidor si se produce un error en la base de datos o las agrupaciones de almacenamiento.

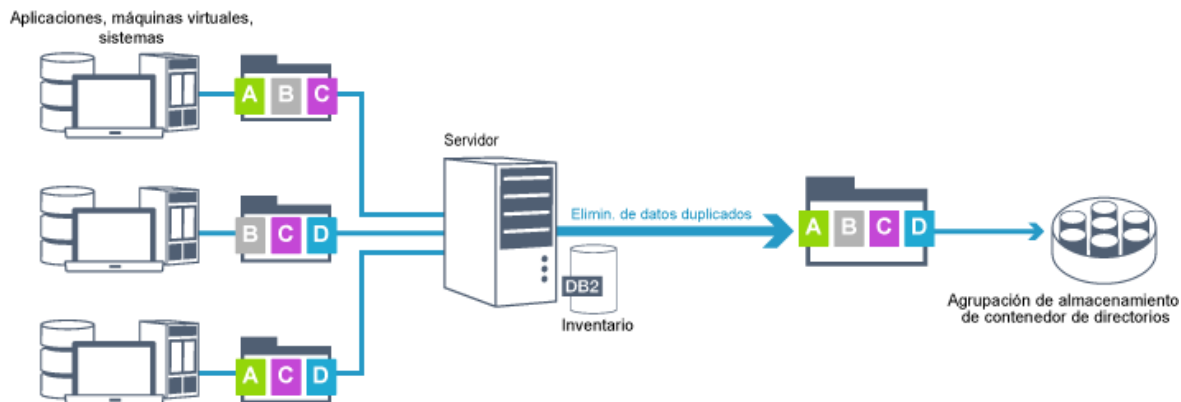
## Estrategias para minimizar el uso del espacio de almacenamiento para copias de seguridad

Para minimizar la cantidad de espacio de almacenamiento necesario, IBM Spectrum Protect hace copia de seguridad de los datos utilizando las técnicas de copia de seguridad incremental progresiva y la optimización de almacenamiento de datos.

### Eliminación de datos duplicados

Cuando el servidor de IBM Spectrum Protect recibe datos de un cliente, dicho servidor identifica las extensiones de datos duplicadas y almacena instancias exclusivas de las extensiones de datos en una agrupación de almacenamiento de contenedores. La técnica de optimización de almacenamiento de datos mejora la utilización del almacenamiento y elimina la necesidad de un dispositivo de optimización de almacenamiento de datos dedicado.

Figura 1. proceso de optimización de almacenamiento de datos



Si se da el mismo patrón de bytes muchas veces, la optimización de almacenamiento de datos reduce enormemente la cantidad de datos que deben almacenarse o transferirse. Además de archivos completos, IBM Spectrum Protect también puede eliminar duplicados de partes de archivos que son comunes con partes de otros archivos.

IBM Spectrum Protect proporciona los siguientes tipos de optimización de almacenamiento de datos:

#### Eliminación de datos duplicados del lado del servidor

El servidor identifica extensiones de datos duplicados y mueve los datos a una agrupación de almacenamiento de contenedores de directorio. El proceso del lado del servidor utiliza la *deduplicación de datos en línea*, donde los datos se deduplican al mismo tiempo que se graban los datos en una agrupación de almacenamiento de contenedores de directorio. Los datos duplicados eliminados también se pueden almacenar en otros tipos de agrupaciones de almacenamiento. La optimización de almacenamiento de datos en línea en el servidor proporciona las siguientes ventajas:

- Elimina la necesidad de reclamación

- Reduce el espacio ocupado por los datos almacenados

#### Eliminación de datos duplicados del lado del cliente

Con este método, el proceso se distribuye entre el servidor y el cliente durante el proceso de una copia de seguridad. El cliente y el servidor identifican y eliminan datos duplicados para ahorrar espacio de almacenamiento en el servidor. En la deduplicación de datos del lado del cliente, solo los datos deduplicados comprimidos se envían al servidor. El servidor almacena los datos en el formato comprimido proporcionado por el cliente. La deduplicación de datos del lado del cliente proporciona las siguientes ventajas:

- Reduce la cantidad de datos que se envía a través de la red de área local (LAN)
- Elimina el tiempo y potencia de proceso extra necesario para eliminar datos duplicados en el servidor
- Mejora el rendimiento de base de datos porque la deduplicación de datos del lado de cliente también está en línea

Puede combinar la deduplicación de datos del lado de cliente y del lado de servidor en el mismo entorno de producción. La capacidad para optimizar datos en el cliente o el servidor proporciona flexibilidad en términos de utilización de recursos, gestión de políticas y protección de datos.

#### Compresión

Utilice la compresión en línea para reducir la cantidad de espacio almacenada en las agrupaciones de almacenamiento de contenedor. Los datos se comprimen a medida que se graban en la agrupación de almacenamiento de contenedores.

Restricción: El servidor IBM Spectrum Protect no puede comprimir datos cifrados.

## Copia de seguridad incremental progresiva

---

En un proceso de copia de seguridad incremental progresiva, el servidor supervisa la actividad de cliente y hace copia de seguridad de cualquier archivo que cambie desde la copia de seguridad completa inicial. Se hace copia de seguridad de todos los archivos, de este modo el servidor no necesita hacer referencia a las versiones base de los archivos. Esta técnica de copia de seguridad elimina la necesidad de varias copias de seguridad completas de los datos de cliente así que ahorra recursos de red y espacio de almacenamiento.

## Estrategias para protección ante desastres

---

IBM Spectrum Protect proporciona estrategias para proteger datos si se produce un desastre. Estas estrategias incluyen la réplica de nodo a un sitio remoto, la protección de agrupación de almacenamiento, la copia de seguridad de base de datos, las transferencias de cintas de copia de seguridad fuera del local y la réplica de dispositivos a un servidor en espera.

### Réplica a un sitio remoto

---

*Réplica de nodo* es el proceso de copia de datos incremental de un servidor a otro servidor. El servidor desde el que se replican datos de cliente se denomina *servidor de réplica de origen*. El servidor al que se replican datos de cliente se denomina *servidor de réplica de destino*. Para la protección ante desastres, el servidor de réplica de destino está en un sitio remoto. Un servidor de réplica puede funcionar como un servidor de origen, un servidor de destino o ambos. Utilice el proceso de réplica para mantener el mismo nivel de archivos en los servidores de origen y de destino.

La réplica de nodo proporciona disponibilidad inmediata de datos mediante la migración tras error. Aunque la réplica de nodo protege a la mayoría de los metadatos, este enfoque no proporciona una protección adecuada frente a los daños en la base de datos. Puede proporcionar una protección más completa mediante la agrupación de almacenamiento para almacenar copias de seguridad de datos.

#### Ventajas

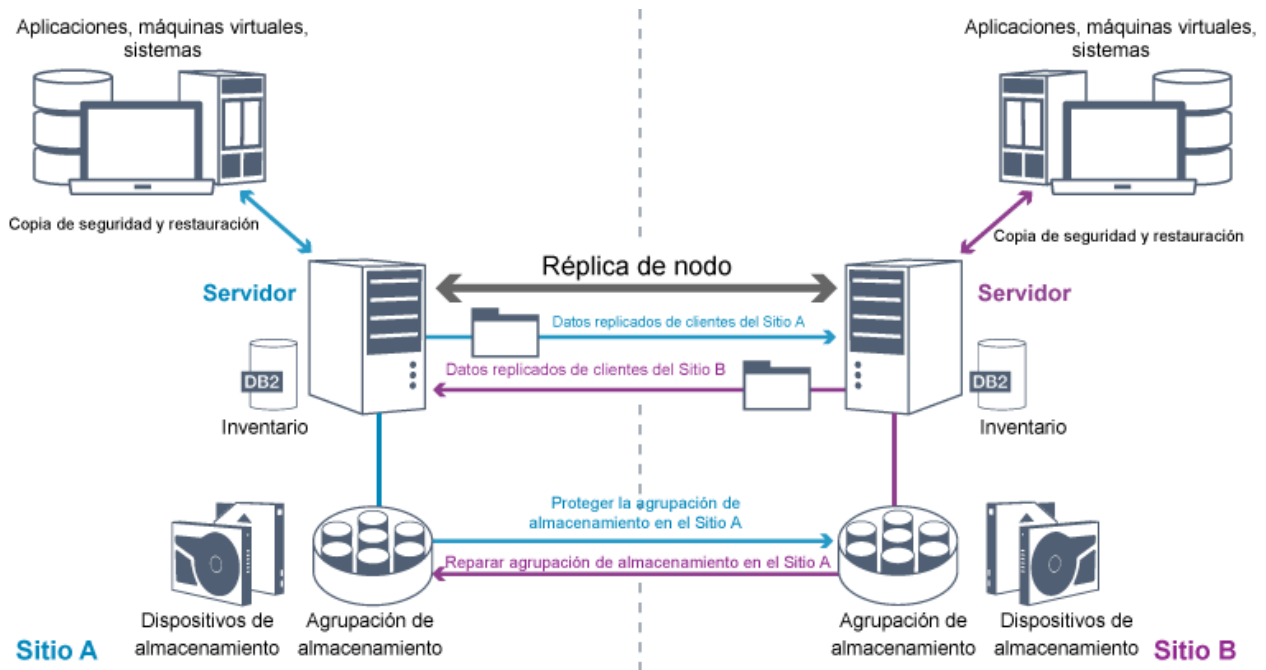
- Migración tras error para que los datos estén disponibles inmediatamente si se produce un desastre.
- Réplica incremental, que acelera la transmisión de datos.
- Transferencia electrónica
- Protege los datos y la mayoría de los metadatos

#### Inconvenientes

- Se deben recuperar tanto los datos como los metadatos.
- Los datos del servidor de origen deben volverse a replicar desde el sitio remoto.

La Figura 1 muestra el proceso de réplica de nodo en un sitio remoto.

Figura 1. Proceso de réplica de nodo



Cuando se replican datos de cliente, sólo se copian los datos que no están en el servidor de destino. Cuando los datos replicados superan el límite de retención, el servidor de destino elimina automáticamente los datos del servidor de origen. Para maximizar la protección de los datos, el servidor local y el servidor remoto se sincronizan; por ejemplo, el Sitio B replica datos del Sitio A y el Sitio A replica datos del Sitio B. Como parte del proceso de réplica, los datos de cliente que se hayan suprimido del servidor de origen también se suprimen en el servidor de destino..

IBM Spectrum Protect proporciona las siguientes funciones de réplica:

- Puede definir políticas respecto al servidor de destino de las siguientes formas:
  - Políticas idénticas en el servidor de origen y el servidor de destino
  - Políticas diferentes en el servidor de origen y el servidor de destino, que cumplen distintos requisitos empresariales.

Si se produce un siniestro y el servidor de origen no está disponible, el cliente puede recuperar los datos del servidor de destino. Si no se puede recuperar el servidor de origen, puede dirigir a los clientes a almacenar datos en el servidor de destino. Cuando se produce una parada, los clientes con copias de seguridad en el servidor de origen pueden migrar automáticamente sus datos para restauración desde el servidor de destino.
- Puede utilizar el proceso de réplica para recuperar archivos dañados de las agrupaciones de almacenamiento. Debe replicar los datos de cliente para el servidor de destino antes de que se produzca un daño en el archivo. Los procesos de réplica posteriores detectan archivos dañados en el servidor de origen y los sustituyen por archivos no dañados del servidor de destino.

## Rol de réplica en la protección ante desastres

Si se produce un desastre, puede recuperar datos replicados desde el sitio remoto y mantener el mismo nivel de archivos en los servidores de origen y de destino. Utilice la réplica para lograr los siguientes objetivos:

- Controlar el rendimiento de red planificando la réplica de nodo en momentos específicos
- Recupere los datos después de una pérdida de sitio.
- Recuperar archivos dañados en el servidor de origen.

## Protección de agrupaciones de almacenamiento

Como parte de una estrategia de recuperación tras desastre, asegúrese de que esté disponible una copia de los datos de copia de seguridad en las agrupaciones de almacenamiento en el sitio remoto.

Ventajas

- Recuperación rápida y reconstrucción del sistema de origen.

Inconvenientes

- Solo se protegen los datos, los metadatos no se protegen.
- Para cada agrupación de almacenamiento, debe definir el medio de almacenamiento.



Se utilizan distintas técnicas para protegerse de la pérdida permanente de datos almacenados en agrupaciones de almacenamiento de contenedores y en agrupaciones de almacenamiento FILE y DISK.

#### Agrupaciones de almacenamiento de contenedores de directorio

Si no necesita replicar todos los datos contenidos en un nodo de cliente, utilice las agrupaciones de almacenamiento de contenedores-directorio para proteger algunas agrupaciones de almacenamiento de contenedores-directorio. Mediante la protección de una agrupación de almacenamiento de contenedores de directorio, no utilice los recursos que replican los datos y metadatos existentes, lo que mejora el rendimiento del servidor.

El método preferido es proteger la agrupación de almacenamiento de contenedores de directorio antes de replicar el nodo de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya están replicadas a través de la protección de agrupación de almacenamiento se omiten, lo que reduce el tiempo de proceso de réplica. Si los datos de la agrupación de almacenamiento de contenedor de directorios se dañan, puede reparar los datos de una copia en una agrupación de almacenamiento de contenedor de directorios.

#### Agrupaciones de almacenamiento de copia de contenedor

Proteja las agrupaciones de almacenamiento de contenedor de directorios copiando los datos de la agrupación de almacenamiento de contenedor de directorios a las agrupaciones de almacenamiento de copia de contenedores. Utilice las agrupaciones de almacenamiento de copia de contenedor para crear hasta dos copias de cinta de una agrupación de almacenamiento de contenedores de directorio. Las copias de cinta se pueden almacenar en el local o fuera del local. Los datos dañados en agrupaciones de almacenamiento de contenedores de directorio pueden repararse utilizando agrupaciones de almacenamiento de copia de contenedor. Las agrupaciones de almacenamiento de copia de contenedor proporcionan una alternativa a utilizar un servidor de réplica para proteger los datos en una agrupación de almacenamiento de contenedores de directorio.

#### Agrupaciones de almacenamiento asociadas con clases de dispositivo FILE y DISK

Para las agrupaciones de almacenamiento asociadas a las clases de dispositivos FILE y DISK, utilice la réplica de nodo para mantener una copia coherente con el nodo de los datos en el servidor de destino. La copia de datos se puede restaurar directamente desde el servidor de destino a las agrupaciones de almacenamiento.

## Copias de seguridad de bases de datos

---

Utilice las copias de seguridad de bases de datos para recuperar el sistema tras un daño en la base de datos. Además, se deben utilizar las operaciones de copia de seguridad de bases de datos para impedir que DB2 se quede sin espacio de registro de archivado. Las operaciones de copia de seguridad de bases de datos no forman parte de la réplica de nodo. Una copia de seguridad de base de datos puede ser completa, incremental o de instantánea. Para prepararse para la recuperación tras desastre, debe restaurarse una copia de las copias de seguridad de la base de datos fuera del local. Para restaurar la base de datos, debe tener los volúmenes de copia de seguridad para la base de datos. La base de datos se puede restaurar desde volúmenes de copia de seguridad mediante una restauración a un momento específico o mediante una operación de restauración más actual.

#### Restauración a un instante específico

Utilice las operaciones de restauración a un momento específico para situaciones como la recuperación tras desastre o para eliminar los efectos de errores que pueden provocar incoherencias en la base de datos. Las operaciones de restauración de la base de datos que utilizan copias de seguridad de instantáneas son una forma de operación de restauración a un momento específico. La operación de restauración a momento específico incluye las acciones siguientes:

- Elimina y vuelve a crear el directorio de registros activos y el directorio de registros de archivado especificados en el archivo dsmserv.opt
- Restaura la imagen de la base de datos desde volúmenes de copia de seguridad a directorios de base de datos grabados en una copia de seguridad de base de datos o en nuevos directorios
- Restaura anotaciones de archivado desde volúmenes de copia de seguridad para el directorio de desbordamiento.
- Utiliza la información de registro desde el directorio de desbordamiento a un momento específico.

#### Restauración más actual

Si desea recuperar la base de datos al momento en que se ha perdido, recupérela a su estado actual. La operación de restauración más actual incluye las acciones siguientes:

- Restaura una imagen de la base de datos desde volúmenes de copia de seguridad a directorios de base de datos grabados en una copia de seguridad de base de datos o en nuevos directorios
- Restaura anotaciones de archivado desde volúmenes de copia de seguridad para el directorio de desbordamiento.
- Utiliza la información de registro desde el directorio de desbordamiento y archiva los registros desde un directorio de registro de archivado.

La restauración más actualizada no elimina ni vuelve a crear el directorio de registros activos ni el directorio de registro de archivado.

## Métodos alternativos para la protección ante desastres

---

Además de la réplica, la protección de agrupación de almacenamiento y las copias de seguridad de bases de datos, puede utilizar los métodos siguientes para proteger datos e implementar la recuperación tras desastre con IBM Spectrum Protect:

Enviando cintas de copia de seguridad a un sitio remoto

Se hace copia de seguridad de los datos a cinta en horas planificadas por el servidor de origen. Las cintas se envían a un sitio remoto. Si se produce un desastre, las cintas se devuelven al sitio del servidor de origen y los datos se restauran en los clientes de origen. Las copias de datos fuera del sitio en una cinta de copia de seguridad también ayudan a recuperarse de ataques de ransomware.

Réplica de dispositivo multisitio a un servidor en espera

En la configuración de dispositivo multisitio, el dispositivo de origen se replica a un servidor remoto en una arquitectura de SAN. En esta configuración, si el hardware de cliente en el sitio original está dañado, el dispositivo de origen puede replicarse desde el servidor en espera en el sitio remoto. Esta configuración proporciona operaciones de copia de seguridad y restauración basadas en disco.

## Comparación de estrategias de configuración de protección

---

Considere los siguientes escenarios de pérdida de datos potencial:

- Los datos de la base de datos están dañados: se puede proteger contra la pérdida de datos en la base de datos mediante una copia de seguridad local de la base de datos.
- Los datos de la agrupación de almacenamiento están dañados: se puede proteger contra la pérdida de datos en agrupaciones de almacenamiento utilizando copias locales de las agrupaciones de almacenamiento o réplicas de nodo.
- Escenario de desastre donde las agrupaciones de almacenamiento y de base de datos locales se pierden: se puede proteger contra un desastre completo utilizando la réplica de nodo o la copia de seguridad tanto de bases de datos como de agrupaciones de almacenamiento.

Las siguientes configuraciones posibles abordan los escenarios de protección de datos más comunes:

Configuraciones solo para protección frente a daños

- Implemente las operaciones de copia de seguridad de base de datos en el local con una agrupación de almacenamiento de copias de contenedores en el sitio para proteger los datos de las agrupaciones de almacenamiento de contenedores de directorios.
- Implementar copia de seguridad de bases de datos local y réplica de nodo local.

Configuraciones para la recuperación tras desastre y la protección frente a daños

- Implemente las operaciones de copia de seguridad de base de datos fuera del local con agrupaciones de almacenamiento de copia de contenedores para proteger los datos en agrupaciones de almacenamiento de contenedores de directorios.
- Implemente las operaciones de copia de seguridad de base de datos en el local y la réplica de nodo fuera del local con una agrupación de almacenamiento de copia de contenedores opcional para acelerar la recuperación de datos dañados.

## Estrategias para la recuperación tras desastre con IBM Spectrum Protect

---

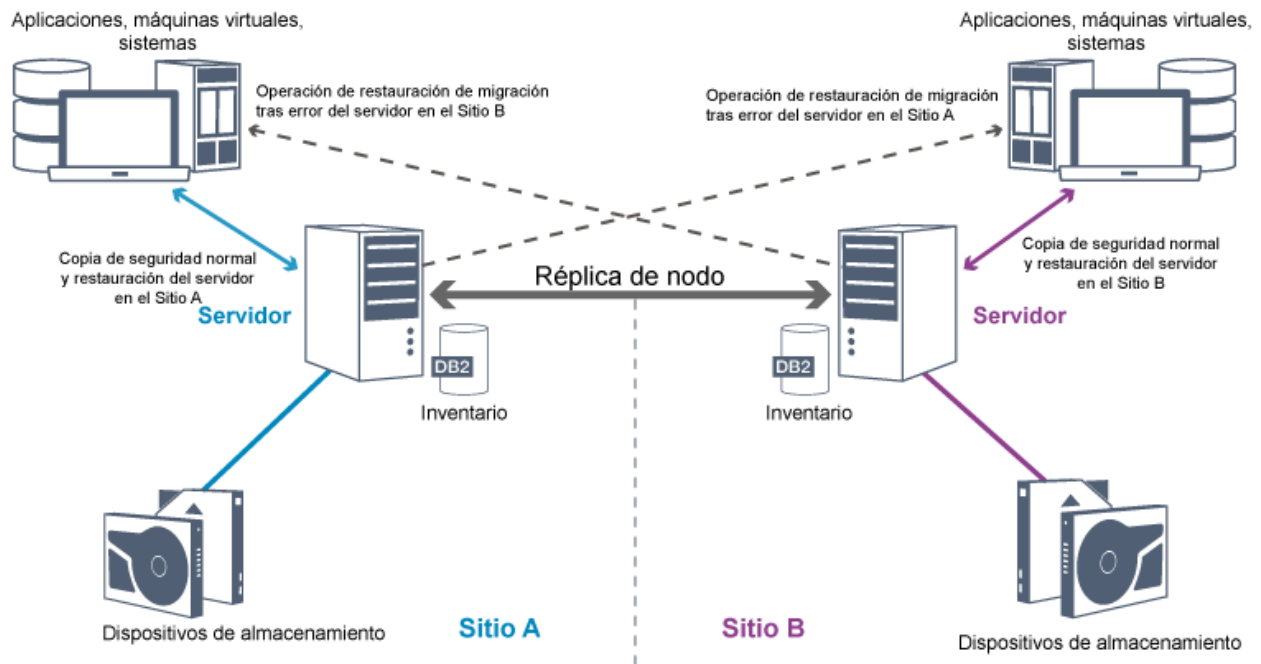
IBM Spectrum Protect proporciona varias formas de recuperar el servidor si se produce un error en la base de datos o las agrupaciones de almacenamiento.

### Migración tras error automática para la recuperación tras desastre

---

La *Migración tras error automática* es una operación que conmuta a un sistema en espera si se produce una interrupción de software, hardware o red. La migración tras error automática se utiliza junto con la réplica de nodo para recuperar datos después de un error del sistema. Figura 1 muestra el proceso de migración tras error automática de IBM Spectrum Protect.

Figura 1. Proceso de migración tras error automática



La migración tras error automática para la recuperación de datos se produce si el servidor de réplica de origen no está disponible debido a un desastre o a una parada del sistema. Durante las operaciones normales, cuando el cliente accede a un servidor de réplica de origen, el cliente recibe información de conexión para el servidor de réplica de destino. El nodo de cliente almacena la información de conexión de migración tras error en el archivo de opciones de cliente.

Durante las operaciones de restauración de cliente, el servidor cambia automáticamente los clientes del servidor de réplica de origen al servidor de réplica de destino y a la inversa. Sólo se puede utilizar un servidor por nodo para la protección de migración tras error en cualquier momento. Cuando se inicia una nueva operación de cliente, el cliente intenta conectarse al servidor de réplica fuente. El cliente reanuda las operaciones en el servidor de origen si está disponible el servidor de réplica fuente.

Para utilizar la migración tras error automática para nodos de cliente replicados, el servidor de réplica de origen, el servidor de réplica de destino y el cliente deben estar en un nivel de V7.1 o posterior. Si alguno de los servidores está en un nivel anterior, la migración tras error automática se inhabilita y debe confiar en un proceso de migración tras error manual.

## Recuperación de componentes de IBM Spectrum Protect

La base de datos, el registro de recuperación y las agrupaciones de almacenamiento son esenciales para el funcionamiento de IBM Spectrum Protect y deben protegerse. Si la base de datos está inutilizable, el servidor entero no está disponible y la recuperación de datos gestionada por el servidor puede resultar difícil o imposible.

Incluso sin la base de datos, los fragmentos de datos o archivos completos se pueden leer desde los volúmenes de agrupación de almacenamiento que no están cifrados y la seguridad se puede ver comprometida. Por lo tanto, siempre debe hacer copia de seguridad de la base de datos. Además, cifre siempre los datos confidenciales utilizando el cliente o el dispositivo de almacenamiento, a menos que el soporte de almacenamiento esté protegido físicamente.

IBM Spectrum Protect proporciona varios métodos de protección de datos, que incluyen copia de seguridad de las agrupaciones de almacenamiento y de la base de datos. Por ejemplo, pueden definirse planificaciones que realicen las operaciones siguientes:

- Después de la copia de seguridad completa inicial de las agrupaciones de almacenamiento, las copias de seguridad de agrupaciones de almacenamiento incrementales se ejecutan cada noche.
- Las copias de seguridad de base de datos incrementales se ejecutan cada noche.
- Las copias de seguridad de base de datos completas se ejecutan una vez a la semana.

Para entornos basados en cinta, puede utilizar el gestor de recuperación tras desastre (DRM), para ayudarle en muchas de las tareas asociadas con la protección y la recuperación de datos. El DRM está disponible con IBM Spectrum Protect Extended Edition.

## Medidas preventivas para la recuperación

La recuperación se basa en las siguientes medidas de precaución:

- Duplicación, mediante la cual el servidor mantiene una copia del registro activo
- Hacer una copia de seguridad de la base de datos.
- Copia de seguridad de las agrupaciones de almacenamiento

- Auditoría de las agrupaciones de almacenamiento de archivos dañados y la recuperación de archivos dañados según convenga
- Copia de seguridad de la configuración de dispositivos y de los archivos de historial de volumen
- Validación de los datos en agrupaciones de almacenamiento mediante la comprobación de redundancia cíclica
- Almacenamiento del archivo cert.kdb en un lugar seguro para garantizar que la capa de sockets seguros (SSL) está protegida

Si está utilizando cinta para el almacenamiento, también puede crear un plan de recuperación tras desastre para que le guíe durante el proceso de recuperación utilizando DRM. Puede utilizar el plan de recuperación tras desastre a efectos de auditoría para certificar la recuperabilidad del servidor. Los métodos de recuperación tras desastre de DRM se basan en la adopción de las medidas siguientes:

- Creación de un archivo de plan de recuperación tras desastre para el servidor
- Copia de seguridad de los datos del servidor en una cinta
- Envío de los datos de copia de seguridad de servidor a un sitio remoto o a otro servidor
- Almacenar la información del sistema cliente
- Definición y seguimiento del soporte de almacenamiento que se utiliza para el almacenamiento y la recuperación de los datos de cliente

## Soluciones de protección de datos de IBM Spectrum Protect

---

Los servidores y clientes de IBM Spectrum Protect proporcionan soluciones de protección de datos para los requisitos de conformidad y empresariales más comunes.

- Selección de una solución de protección de datos para el entorno  
Para ayudarle a desplegar un entorno de protección de datos, revise la información sobre las configuraciones de IBM Spectrum Protect de uso recomendado y seleccione la mejor solución para las necesidades de negocio.
- Solución de disco de sitio único  
Esta solución de protección de datos proporciona almacenamiento de datos asequible en un solo sitio con una configuración de hardware mínima.
- Solución de disco multisitio  
Esta solución de protección de datos proporciona réplica en varios sitios para que cada servidor proteja los datos del otro.
- Solución de cinta  
Esta solución de protección de datos proporciona almacenamiento a soportes de cinta, una opción flexible y asequible para la retención de datos a largo plazo.
- Documentación de la solución de servidor en archivos PDF  
Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

## Selección de una solución de protección de datos para el entorno

---

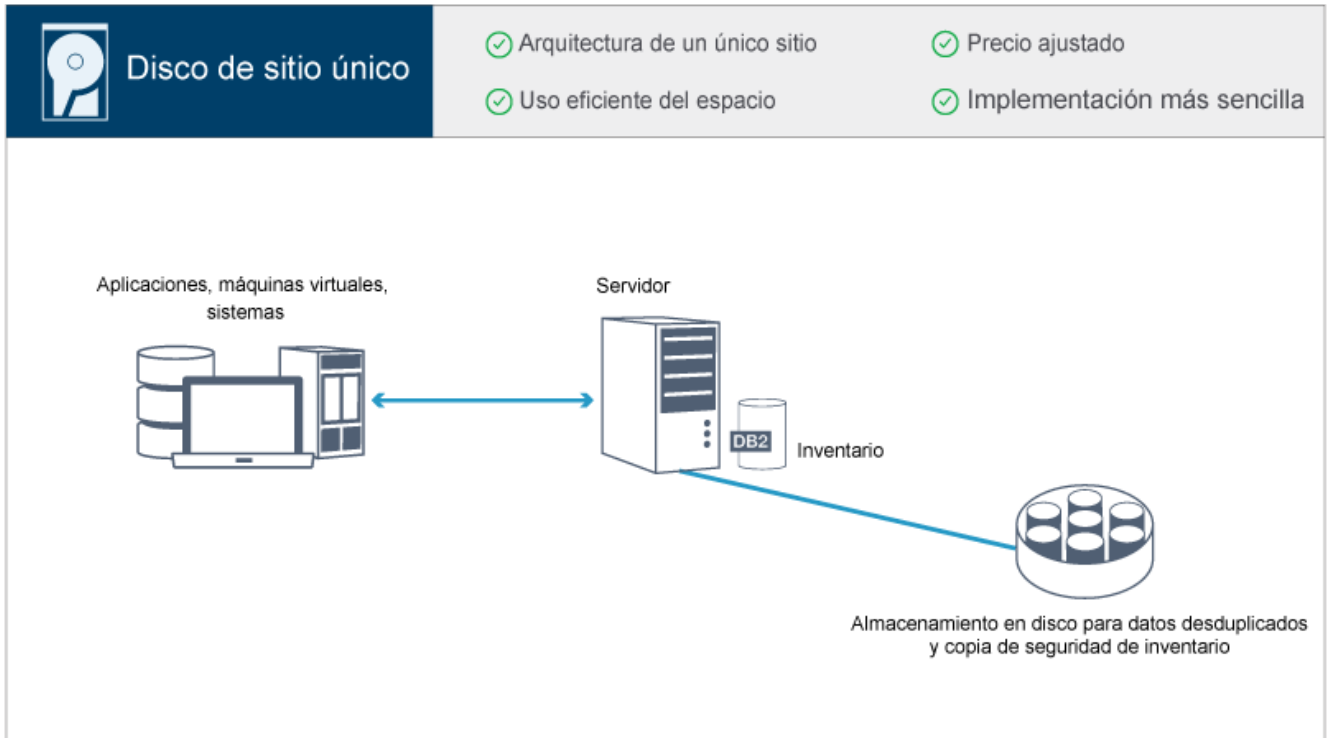
Para ayudarle a desplegar un entorno de protección de datos, revise la información sobre las configuraciones de IBM Spectrum Protect de uso recomendado y seleccione la mejor solución para las necesidades de negocio.

- Implementación basada en disco de una solución de protección de datos para un sitio único  
Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea y proporciona protección para los datos en un único sitio.
- Implementación basada en disco de una solución de protección de datos para varios sitios  
Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea en dos sitios.
- Implementación basada en dispositivo de una solución de protección de datos para varios sitios  
Esta implementación de una solución de protección de datos de IBM Spectrum Protect multisitio utiliza la deduplicación y réplica de datos basadas en dispositivo. Se configura un servidor en espera en un segundo sitio para recuperar datos si el servidor primario no está disponible.
- Implementación basada en cinta de una solución de protección de datos  
Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza uno o más dispositivos de almacenamiento de cinta para hacer copia de seguridad de los datos. La copia de seguridad de cinta proporciona escalabilidad de bajo coste que está optimizada para la retención a largo plazo.
- Comparación de soluciones de protección de datos  
Compare las características clave para cada solución de IBM Spectrum Protect para determinar qué configuración cumple mejor los requisitos de protección de datos. A continuación, revise la documentación disponible para implementar la solución.
- Hoja de ruta para implementar una solución de protección de datos  
Planee e implemente la solución de protección de datos más adecuada para su entorno de negocio con IBM Spectrum Protect.

## Implementación basada en disco de una solución de protección de datos para un sitio único

---

Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea y proporciona protección para los datos en un único sitio.



Esta solución de protección de datos proporciona las siguientes ventajas:

- Hardware de almacenamiento y sistema servidor en un único sitio.
- Uso rentable del almacenamiento mediante la característica de deduplicación de datos.
- Solución con ahorro de espacio y una configuración de hardware mínima.
- Implementación mínima que solo requiere la instalación y la configuración para un único servidor y el hardware de almacenamiento de soporte.

En esta solución, el cliente envía datos al servidor de IBM Spectrum Protect, donde los datos se deduplican y se almacenan en una agrupación de almacenamiento de contenedores de directorios que se implementa en almacenamiento de disco. También se realiza copia de seguridad en el almacenamiento de disco de los datos del inventario. Esta solución es adecuada para entornos de nivel de entrada para los que no se necesita una segunda copia de los datos.

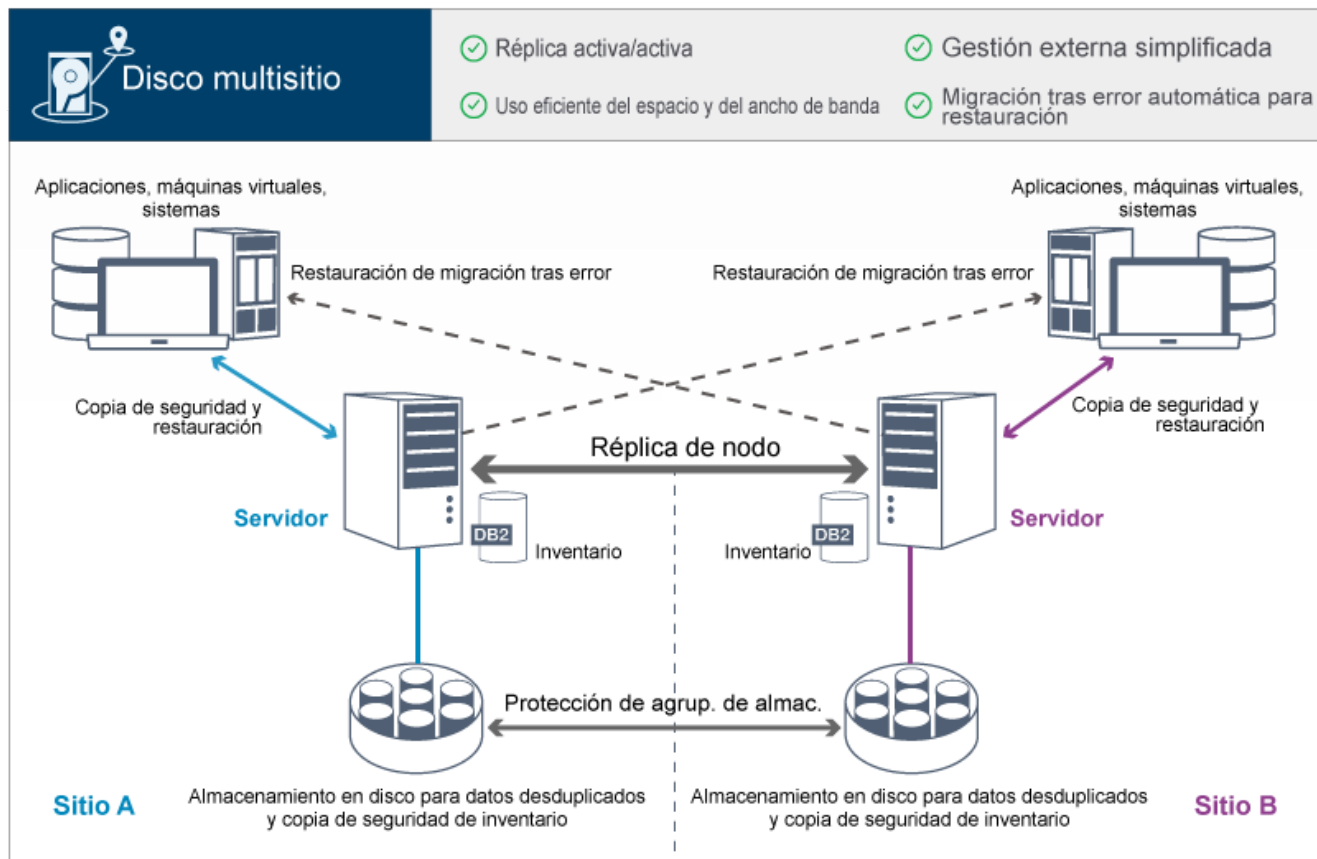
**Referencia relacionada:**

Comparación de soluciones de protección de datos

Hoja de ruta para implementar una solución de protección de datos

## Implementación basada en disco de una solución de protección de datos para varios sitios

Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza la deduplicación y la réplica de datos de datos en línea en dos sitios.



Esta solución de protección de datos proporciona las siguientes ventajas:

- La réplica puede configurarse en ambos sitios para que cada servidor proteja los datos del otro.
- Se simplifica el almacenamiento de datos fuera del sitio de cada ubicación.
- El ancho de banda se utiliza de forma eficaz porque entre los sitios solo se replican datos deduplicados.
- Los clientes pueden realizar una migración tras error automáticamente a un servidor de réplica de destino si el servidor de réplica de origen no está disponible.

En esta solución, los clientes envían datos al servidor de origen, donde los datos se deduplican y se almacenan en una agrupación de almacenamiento de contenedores de directorios que se implementa en el almacenamiento de disco. Los datos se replican en la agrupación de almacenamiento en el servidor de destino para cada sitio. Esta solución es idónea para entornos que necesitan protección frente a desastres. Si se configura la réplica mutua, los clientes en ambos sitios pueden utilizar la recuperación tras error para realizar copias de seguridad continuadas y recuperación de datos desde el servidor disponible en el otro sitio.

**Referencia relacionada:**

Comparación de soluciones de protección de datos

Hoja de ruta para implementar una solución de protección de datos

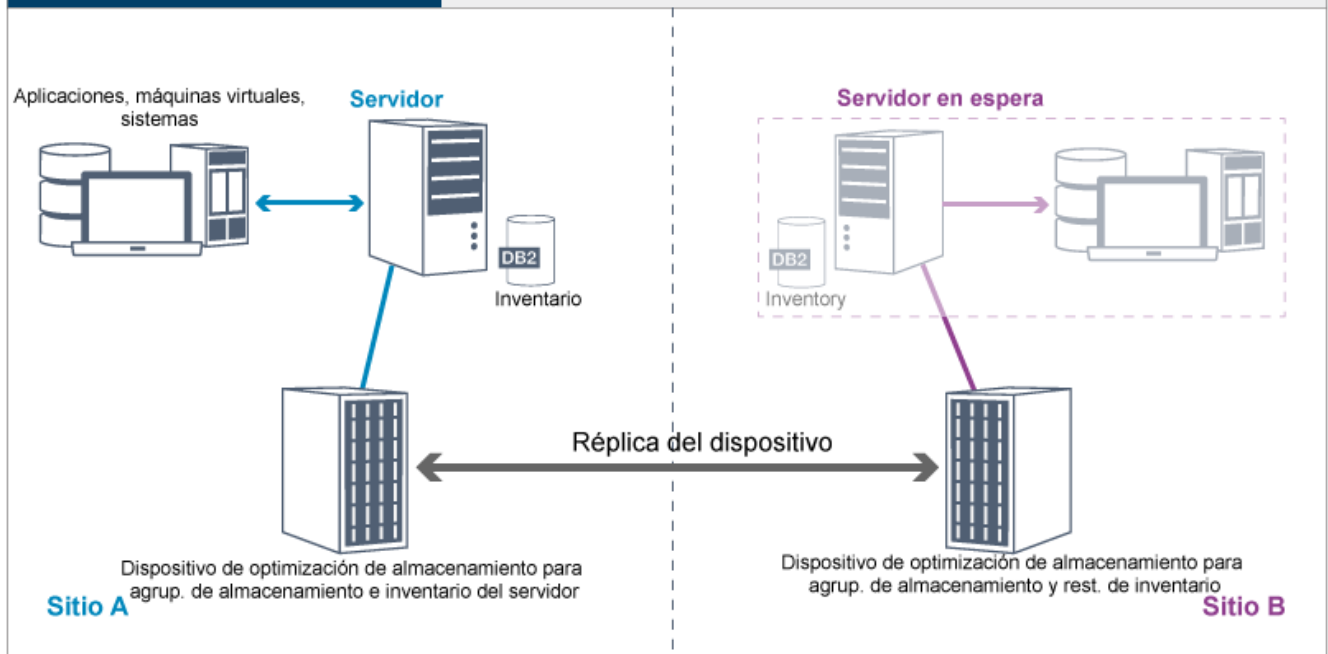
## Implementación basada en dispositivo de una solución de protección de datos para varios sitios

Esta implementación de una solución de protección de datos de IBM Spectrum Protect multisitio utiliza la deduplicación y réplica de datos basadas en dispositivo. Se configura un servidor en espera en un segundo sitio para recuperar datos si el servidor primario no está disponible.



## Dispositivo multisitio

- ✓ Optimizado para copia de seguridad de SAN
- ✓ Réplica basada en dispositivos
- ✓ Uso eficiente del espacio y del ancho de banda
- ✓ Entorno en espera



Esta solución de protección de datos proporciona las siguientes ventajas:

- El rendimiento se optimiza para copias de seguridad en redes de área de almacenamiento (SAN) de alta velocidad y para el uso con IBM Spectrum Protect para SAN cuando se realiza la copia de seguridad de los clientes directamente en dispositivos de cinta virtuales conectados a SAN.
- La réplica rápida basada en dispositivo evita que el servidor tenga que realizar el seguimiento de los metadatos de réplica en la base de datos de servidor.
- El ancho de banda y el espacio de almacenamiento se utilizan de forma eficaz porque entre los sitios solo se replican datos deduplicados.
- Un entorno en espera proporciona la recuperación tras desastre, pero no necesita la cantidad de recursos que se necesitan para un sitio totalmente activo.

En esta configuración de protección de datos, el servidor utiliza dispositivos de hardware para deduplicar y replicar datos. El dispositivo del Sitio A elimina los datos duplicados y, a continuación, los replica en el dispositivo del Sitio B para brindar protección en caso de desastre. Si se produce una anomalía en el Sitio A, active el servidor en espera restaurando la copia de seguridad de base de datos más reciente y activando la copia replicada de los datos.

Para obtener más información sobre cómo configurar bibliotecas virtuales de cintas, consulte Configuración de bibliotecas de cintas virtuales.

### Referencia relacionada:

Comparación de soluciones de protección de datos

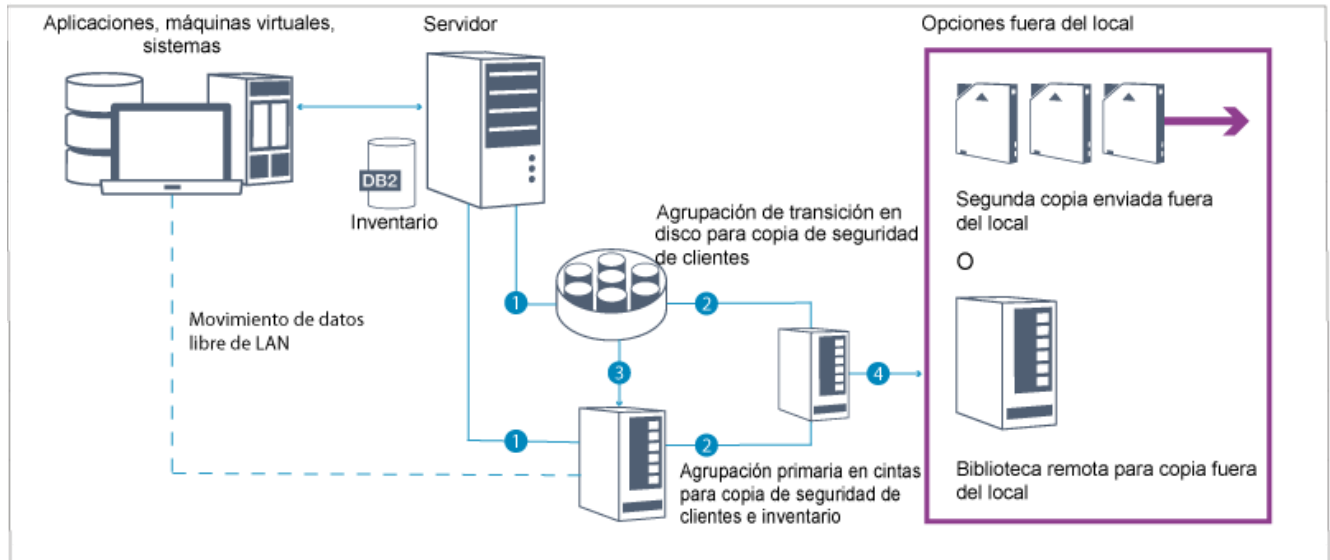
Hoja de ruta para implementar una solución de protección de datos

## Implementación basada en cinta de una solución de protección de datos

Esta implementación de una solución de protección de datos con IBM Spectrum Protect utiliza uno o más dispositivos de almacenamiento de cinta para hacer copia de seguridad de los datos. La copia de seguridad de cinta proporciona escalabilidad de bajo coste que está optimizada para la retención a largo plazo.

Cinta

- ✔ Ideal para retención a largo plazo
- ✔ Escalabilidad a bajo coste
- ✔ Zona de transición disco a agrup. cintas
- ✔ Optimizado para SAN



Esta solución de protección de datos proporciona las siguientes ventajas:

- Se optimiza el rendimiento para operaciones de copia de seguridad en redes de área de almacenamiento (SAN) de alta velocidad directamente a cinta para tipos de datos grandes y para retención de datos a largo plazo.
- Se optimiza el rendimiento para la disponibilidad de datos almacenando copias de datos en ubicaciones externas para la recuperación tras desastre.
- Se consigue una escalabilidad a bajo coste reduciendo la necesidad de hardware de disco adicional y disminuyendo los costes de energía.

**Conceptos relacionados:**

Seleccionar un controlador de dispositivo de cinta

**Tareas relacionadas:**

Creación de estrategias de copia de seguridad

Gestión del inventario de volúmenes

**Referencia relacionada:**

Comparación de soluciones de protección de datos





Instalación y configuración de controladores de dispositivos de cinta

## Comparación de soluciones de protección de datos

Comparar las características clave para cada solución de IBM Spectrum Protect para determinar qué configuración cumple mejor los requisitos de protección de datos. A continuación, revise la documentación disponible para implementar la solución.

	Disco de sitio único	Disco multisitio	Dispositivo multisitio	Cinta
<b>Características destacadas</b>				
Coste	\$	\$\$\$	\$\$\$\$	\$\$
Nivel de protección	Una copia de datos	Dos o más copias de datos	Dos o más copias de datos	Dos o más copias de datos
Recuperación tras desastre	Ninguno	Servidor activo	Servidor en espera	Copias externas
<b>Ventajas principales</b>				
Reducción de datos de borde inicial	✔	✔	✔	✔



	Disco de sitio único	Disco multisitio	Dispositivo multisitio	Cinta
				
Operaciones de copia de seguridad y restauración basadas en disco rápidas y eficaces	✓		✓	
Gestión externa simplificada		✓		
Característica de deduplicación de datos sin ningún coste	✓	✓		
Proceso de réplica incluido sin cargo extra		✓		
Optimización de almacenamiento de datos en el servidor de origen y de destino		✓		
Escalabilidad a bajo coste y optimizada para una retención a largo plazo				✓
<b>Eficiencia y coste</b>				
Optimizado para operaciones de seguridad de red de área de almacenamiento de alta velocidad (SAN)			✓	✓
Optimizado para red de área local de alta velocidad (LAN)	✓	✓	✓	
Optimización de almacenamiento global entre todos los orígenes y tipos de datos	✓	✓	✓	
Réplica eficaz de ancho de banda		✓	✓	
Rebajar costes de energía				✓
Opción de una segunda copia sin hardware de disco extra				✓
<b>Disponibilidad</b>				
Prestación de copia externa		✓	✓	✓
Réplica basada en dispositivos			✓	
Recuperación de cliente desde un servidor de alta disponibilidad		✓		
Destino de duplicación en la nube		✓		
Gestión de políticas de retención independientes para los datos de réplica; capacidad para mantener más o menos datos en el sitio de recuperación		✓		
Réplica a nivel de aplicación; capacidad para elegir qué sistemas y aplicaciones se replican		✓		
<b>Escalabilidad</b>				
Deduplicación de datos globales entre servidores			✓	
Copia de seguridad optimizada para SAN directamente a cinta para tipos de datos grandes				✓
Escalabilidad de petabytes de instancia única				✓

## Acciones siguientes

Revise la documentación disponible para las soluciones en Hoja de ruta para implementar una solución de protección de datos.

### Referencia relacionada:

Implementación basada en disco de una solución de protección de datos para un sitio único

Implementación basada en disco de una solución de protección de datos para varios sitios

Implementación basada en dispositivo de una solución de protección de datos para varios sitios  
Implementación basada en cinta de una solución de protección de datos

## Hoja de ruta para implementar una solución de protección de datos

---

Planee e implemente la solución de protección de datos más adecuada para su entorno de negocio con IBM Spectrum Protect.

### Solución de disco de sitio único

---

Para conocer los pasos que describen cómo planificar, implementar, supervisar y utilizar una solución de disco de sitio único, consulte Solución de disco de sitio único.

### Solución de disco multisitio

---

Para conocer los pasos que describen cómo planificar, implementar, supervisar y utilizar una solución de disco multisitio, consulte Solución de disco multisitio.

### Solución de cinta

---

Para conocer los pasos que describen cómo planificar, implementar, supervisar y utilizar una solución de disco multisitio, consulte Solución de cinta.

### Solución de dispositivo multisitio

---

Para obtener una visión general de las tareas que son necesarias para implementar una solución de dispositivo multisitio, revise los pasos siguientes:

1. Empiece a planificar la solución revisando la información en los siguientes enlaces:
  - o AIX: planificación de la capacidad
  - o Linux: planificación de la capacidad
  - o Windows: planificación de la capacidad
2. Instale el servidor y, opcionalmente, el Centro de operaciones. Revise la información en los siguientes enlaces:
  - o instalación del servidor
  - o Instalación y actualización del Centro de operaciones
3. Configure el servidor para el almacenamiento en una biblioteca virtual de cintas.
  - o Gestión de bibliotecas de cintas virtuales
  - o Conexión de dispositivos de cinta para el servidor

Para obtener orientación sobre cómo mejorar el rendimiento del sistema, consulte Métodos recomendados de configuración.

4. Configure políticas para proteger los datos. Revise la información de Personalización de políticas.
5. Configure planificaciones de cliente. Revise la información de Planificación de copia de seguridad y operaciones de archivado.
6. Instale y configure los clientes. Para determinar el tipo de software de cliente que necesita, revise la información que aparece en Adición de clientes para obtener detalles.
7. Configure la supervisión para el sistema. Revise la información de Supervisión de soluciones de almacenamiento.

#### Referencia relacionada:

Comparación de soluciones de protección de datos  
Implementación basada en disco de una solución de protección de datos para un sitio único  
Implementación basada en disco de una solución de protección de datos para varios sitios  
Implementación basada en dispositivo de una solución de protección de datos para varios sitios  
Implementación basada en cinta de una solución de protección de datos

### Solución de disco de sitio único

---

Esta solución de protección de datos proporciona almacenamiento de datos asequible en un solo sitio con una configuración de hardware mínima.

- Planificación de una solución de protección de datos de disco de sitio único  
Planifique una implementación de protección de datos que incluya un servidor en un único sitio que utilice la deduplicación de datos.
- Implementación de disco de sitio único de una solución de protección de datos  
La solución de disco de sitio único se configura en un sitio y utiliza la deduplicación de datos.

- Supervisión de una solución de disco de sitio único  
Después de implementar una solución de disco en un único sitio con IBM Spectrum Protect, supervise la solución para su funcionamiento correcto. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.
- Gestión de operaciones para una solución de disco de sitio único  
Utilice esta información para gestionar operaciones para una solución de disco de sitio único con IBM Spectrum Protect que incluya un servidor y utilice la eliminación de datos duplicados para una única ubicación.

## Planificación de una solución de protección de datos de disco de sitio único

Planifique una implementación de protección de datos que incluya un servidor en un único sitio que utilice la deduplicación de datos.

### Opciones de implementación

Puede configurar el servidor para una solución de disco de sitio único de las siguientes maneras:

Configure el servidor utilizando el Centro de operaciones y los mandatos de administración

En esta documentación se incluyen los pasos necesarios para configurar un rango de sistemas de almacenamiento y el software de servidor de la solución. Las tareas de configuración se realizan mediante asistentes y opciones del Centro de operaciones y mandatos de IBM Spectrum Protect. Para obtener información sobre cómo empezar, consulte Hoja de vía de acceso de planificación.

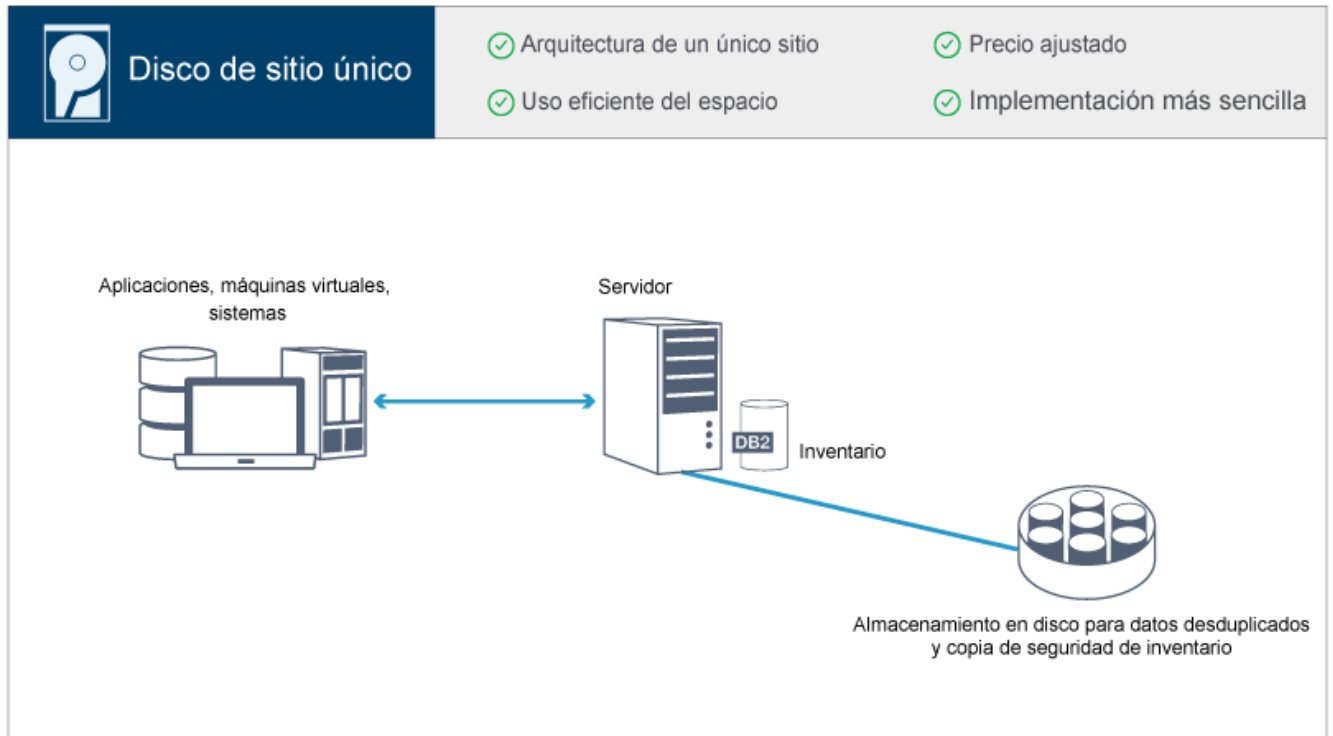
Configure el servidor utilizando scripts automatizados

Para obtener información detallada sobre cómo implementar una solución de disco de sitio único con sistemas de almacenamiento de IBM® Storwize específicos y utilizando scripts automatizados para configurar el servidor, consulte los blueprints de IBM Spectrum Protect. La documentación y los scripts están disponibles en IBM developerWorks en: IBM Spectrum Protect Blueprints.

La documentación blueprint no incluye pasos para la instalación y configuración de Centro de operaciones, o el establecimiento de comunicaciones seguras utilizando la capa de seguridad de transporte (TLS). Se incluye una opción para utilizar Elastic Storage Server, que se basa en la tecnología IBM Spectrum Scale.

### Hoja de vía de acceso de planificación

Planifique una solución de disco en un único sitio revisando el diseño de arquitectura en la siguiente figura y, a continuación, completando las tareas de la hoja de ruta que siguen al diagrama.



Los pasos siguientes son necesarios para planificar un entorno de disco de sitio único.

1. Seleccionar el tamaño de sistema.

2. Cumplir los requisitos de sistema para hardware y software.
3. Registrar valores para la configuración de sistema en las hojas de trabajo de planificación.
4. Planificar el almacenamiento.
5. Planificar la seguridad.
  - a. Planificar los roles de administrador.
  - b. Planificar las comunicaciones seguras.
  - c. Planificar el almacenamiento de datos cifrados.
  - d. Planificar el acceso de cortafuegos.

## Selección de un tamaño del sistema

Seleccione el tamaño del servidor de IBM Spectrum Protect basándose en la cantidad de datos que gestiona y los sistemas que se deben proteger.

### Acerca de esta tarea

Puede utilizar la información de la tabla para determinar el tamaño del servidor que se necesita, en función de la cantidad de datos que gestione.

La tabla siguiente describe el volumen de datos que gestiona un servidor. Esta cantidad incluye todas las versiones. La cantidad diaria de datos es la cantidad de datos nuevos a la que hace copia de seguridad cada día. Los datos gestionados totales y la cantidad diaria de datos nuevos se miden como el tamaño antes de la reducción de datos.

Tabla 1. Determinación del tamaño del servidor

Total de datos gestionados	Cantidad diaria de datos nuevos de los que se debe hacer copia de seguridad	Tamaño de servidor necesario
48 TB - 192 TB	Hasta 10 TB al día	Pequeño
200 TB - 800 TB	10 - 20 TB al día	Mediano
1000 TB - 4000 TB	20 - 100 TB al día	Grande

Los valores de copia de seguridad diaria de la tabla se basan en los resultados de prueba con objetos de 128 MB de tamaño, utilizados por IBM Spectrum Protect for Virtual Environments. Es posible que las cargas de trabajo que constan de objetos que tienen menos de 128 KB no puedan conseguir estos límites diarios.

## Requisitos del sistema para una solución de disco de sitio único

Después de seleccionar la solución IBM Spectrum Protect que mejor se ajuste a los requisitos de protección de datos, revise los requisitos de sistema para planificar la implementación de la solución de protección de datos.

Asegúrese de que el sistema cumple los requisitos previos de hardware y software para el tamaño de servidor que desea utilizar.

- **Requisitos de hardware**  
Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.
- **Requisitos de software**  
La documentación para la solución IBM Spectrum Protect de disco en un único sitio incluye tareas de instalación y configuración para los siguientes sistemas operativos. Debe cumplir los requisitos de software mínimos que se indican.

#### Información relacionada:










[Sistemas operativos admitidos para IBM Spectrum Protect](#)

## Requisitos de hardware

Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

Para obtener una definición de los tamaños de sistema, consulte Selección de un tamaño del sistema.

La tabla siguiente incluye requisitos de hardware mínimos para el servidor y el almacenamiento, en función del tamaño del servidor que planea crear. Si utiliza particiones locales (LPAR) o particiones de trabajo (WPAR), ajuste los requisitos de red para tener en cuenta los tamaños de las particiones.

Componente de hardware	Sistema pequeño	Sistema mediano	Sistema grande
Procesador de servidor	 Sistemas operativos AIX6 núcleos de procesador, 3,42 GHz o más rápido   Sistemas operativos Linux  Sistemas operativos Windows 12 núcleos de procesador, 1,9 GHz o más rápido	 Sistemas operativos AIX8 núcleos de procesador, 3,42 GHz o más rápido   Sistemas operativos Linux  Sistemas operativos Windows 16 núcleos de procesador, 2,0 GHz o más rápido	 Sistemas operativos AIX20 núcleos de procesador, 3,42 GHz   Sistemas operativos Linux  Sistemas operativos Windows 32 núcleos de procesador, 2,0 GHz o más rápido
Memoria de servidor	64 GB RAM	128 GB RAM	192 GB RAM
Red	<ul style="list-style-type: none"> <li>Ethernet de 10 GB (1 puerto)</li> <li>Adaptador de canal de fibra de 8 GB (2 puertos)</li> </ul>	<ul style="list-style-type: none"> <li>Ethernet de 10 GB (2 puertos)</li> <li>Adaptador de canal de fibra de 8 GB (2 puertos)</li> </ul>	<ul style="list-style-type: none"> <li>Ethernet de 10 GB (4 puertos)</li> <li>Adaptador de canal de fibra de 8 GB (4 puertos)</li> </ul>
Almacenamiento	<ul style="list-style-type: none"> <li>1.3 TB de inventario, más espacio para registros de Centro de operaciones.</li> <li>Agrupación de almacenamiento de contenedores de directorio deduplicada de 46 TB</li> </ul>	<ul style="list-style-type: none"> <li>2 TB de inventario, más espacio para registros de Centro de operaciones</li> <li>Agrupación de almacenamiento de contenedores de directorio deduplicada de 200 TB</li> </ul>	<ul style="list-style-type: none"> <li>6 TB de inventario, más espacio para registros de Centro de operaciones</li> <li>Agrupación de almacenamiento de contenedores de directorio deduplicada de 1000 TB</li> </ul>

## Estimación de requisitos de espacio de base de datos para Centro de operaciones

Los requisitos de hardware para Centro de operaciones se incluyen en la tabla anterior, excepto para la base de datos y el espacio de registro de archivado (inventario) que utiliza Centro de operaciones para contener registros para clientes gestionados.

Si no piensa instalar el Centro de operaciones en el mismo sistema que servidor, puede calcular requisitos de sistema por separado. Para calcular requisitos del sistema para Centro de operaciones, consulte la calculadora de requisitos del sistema en la nota técnica 1641684.

La gestión del Centro de operaciones en el servidor es una carga de trabajo que necesita espacio adicional para las operaciones de base de datos. La cantidad de espacio depende del número de clientes supervisados en un servidor. Revise las directrices siguientes para estimar cuánto espacio requiere el servidor.

### Espacio de base de datos

El Centro de operaciones utiliza aproximadamente 1,2 GB de espacio de base de datos por cada 1000 clientes supervisados en un servidor. Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1500 clientes. Esta configuración tiene un total de 6500 clientes en los cuatro servidores y necesita aproximadamente 8,4 GB de espacio de base de datos. Este valor se calcula redondeando los 6500 clientes al 1000 más próximo, que es 7000:

$$7 \times 1.2 \text{ GB} = 8.4 \text{ GB}$$

### Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 8 GB de espacio de registro de archivado cada 24 horas por cada 1000 clientes. En el ejemplo de 6500 clientes en el servidor concentrador y los servidores spoke, se utilizan 56 GB de espacio de registro de archivado a lo largo de un período de 24 horas para el servidor concentrador. Para cada servidor de radio en el ejemplo, el espacio del registro de archivado que se utiliza a lo largo de 24 horas es aproximadamente 16 GB. Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en el requisito de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos:

- servidor concentrador: de 56 GB a 94 GB aproximadamente
- Cada servidor spoke: de 16 GB a 28 GB aproximadamente

Aumente el espacio de registro de archivado para tener espacio suficiente para proporcionar soporte a Centro de operaciones, sin que afecte a las operaciones de servidor existentes.

## Requisitos de software

La documentación para la solución IBM Spectrum Protect de disco en un único sitio incluye tareas de instalación y configuración para los siguientes sistemas operativos. Debe cumplir los requisitos de software mínimos que se indican.

Para obtener información sobre los requisitos de software para los controladores de dispositivo lin\_tape de IBM®, consulte IBM Tape Device Drivers Installation and User's Guide.

### Sistemas AIX

Tipo de software	Requisitos mínimos de software
Sistema operativo	IBM AIX 7.1  Para obtener más información sobre los requisitos del sistema operativo, consulte AIX: requisitos mínimos del sistema para sistemas AIX.
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema antes de instalar o actualizar el servidor de IBM Spectrum Protect . Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.
Tipo de sistema de archivos	Sistemas de archivos JFS2  Los sistemas AIX pueden almacenar en caché una gran cantidad de datos del sistema de archivos y esto puede reducir la memoria que se necesita para el servidor y los procesos de IBM DB2. Para evitar la paginación con el servidor de AIX, utilice la opción de montaje rbrw mount para el sistema de archivos JFS2. Se utiliza menos memoria para la memoria caché de sistema de archivo y hay más disponible para IBM Spectrum Protect.  No utilice las opciones de montaje del sistema de archivos, E/S simultáneas (CIO) y E/S directas (DIO), para sistemas de archivos que contengan la base de datos de IBM Spectrum Protect, registros o volúmenes de agrupaciones de almacenamiento. Estas opciones pueden producir la degradación del rendimiento de muchas operaciones de servidor. IBM Spectrum Protect y DB2 aún pueden utilizar DIO donde sea beneficioso hacerlo, pero IBM Spectrum Protect no necesita las opciones de montaje para aprovechar estas técnicas de forma selectiva.
Otro software	Shell Korn (ksh)

### Sistemas Linux

Tipo de software	Requisitos mínimos de software
Sistema operativo	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	Bibliotecas de GNU C, versión 2.3.3-98.38 o posterior que está instalado en el sistema de IBM Spectrum Protect. Red Hat Enterprise Linux Servers: <ul style="list-style-type: none"><li>• libaio</li><li>• libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits)</li><li>• numactl.x86_64</li></ul>
Tipo de sistema de archivos	Formato de sistemas de archivos relacionados con bases de datos con ext3 o ext4.  Para los sistemas de archivos relacionados con agrupaciones de almacenamiento, utilice XFS.
Otro software	Shell Korn (ksh)

### Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS

Tipo de software	Requisitos mínimos de software
Otro software	Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado.  Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: <ul style="list-style-type: none"> <li>Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada</li> <li>Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador</li> </ul>

**Tareas relacionadas:**

🔗 Establecimiento de las opciones de red de AIX

## Planificación de hojas de trabajo

Utilice las hojas de trabajo de planificación para registrar los valores que se utilizan para configurar el sistema y configurar el servidor de IBM Spectrum Protect. Utilice los valores predeterminados de prácticas recomendadas que aparecen en las hojas de trabajo.

Cada hoja de trabajo le ayuda a prepararse para diferentes partes de la configuración del sistema utilizando valores de las prácticas recomendadas:

**Configuración previa de sistema servidor**

Utilice las hojas de trabajo de configuración previa para planificar los sistemas de archivos y directorios que se crean al configurar sistemas de archivos para IBM Spectrum Protect durante la configuración del sistema. Todos los directorios que crea para el servidor deben estar vacíos.

**Configuración del servidor**

Utilice las hojas de trabajo de configuración cuando configure el servidor. Los valores predeterminados se recomiendan para la mayoría de los elementos, excepto donde se indica.

## AIX

Tabla 1. Hoja de trabajo para configuración previa de un sistema servidor AIX

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo  El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		50 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 2.
Directorio para la instalación del servidor	/		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/usr		Espacio disponible que es necesario para el directorio: 5 GB	

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para la instalación del servidor	/var		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/tmp		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/opt		Espacio disponible que es necesario para el directorio: 10 GB	
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>



Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 2. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 1 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		

Elemento	Valor predeterminado	Valor	Notas
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p>

## Linux

Tabla 3. Hoja de trabajo para la configuración previa de un sistema servidor Linux

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	<p>Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo</p> <p>El número de puerto puede ser un número dentro del rango 1024 - 32767.</p>
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 4.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 4. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 3 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		

Elemento	Valor predeterminado	Valor	Notas
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.  Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

## Windows

Dado que muchos volúmenes se crean para el servidor, configure el servidor utilizando la característica de Windows de correlación de volúmenes de disco con directorios en lugar de letras de unidad.

Por ejemplo, C:\tsminst1\TSMdbpsace00 es el punto de montaje para un volumen con su propio espacio. El volumen se correlaciona con un directorio bajo la unidad C:, pero no ocupa espacio de la unidad C:. La excepción es el directorio de instancia de servidor, C:\tsminst1, que puede ser un punto de montaje o un directorio normal.

Tabla 5. Hoja de trabajo para la configuración previa de un sistema servidor Windows

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo  El número de puerto puede ser un número dentro del rango 1024 - 32767.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para la instancia de servidor	C:\tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 6.
Directorio para el registro activo	C:\tsminst1\TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	
Directorio para el registro de archivado	C:\tsminst1\TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 6. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 5 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	pAssW0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.

Elemento	Valor predeterminado	Valor	Notas
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.  Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

## Planificación de almacenamiento

Elegir la tecnología de almacenamiento más efectiva para componentes de IBM Spectrum Protect para asegurarse de que el rendimiento de servidor y las operaciones son eficientes.

Los dispositivos de hardware de almacenamiento tiene características de rendimiento y capacidad diferentes, lo que determina cómo se pueden utilizar de forma eficaz con IBM Spectrum Protect. Para obtener una orientación general sobre cómo seleccionar el hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

### Base de datos y registro activo

- Utilice un disco rápido para el registro activo y la base de datos de IBM Spectrum Protect, por ejemplo con las siguientes características:
  - Disco de alto rendimiento de 15k rpm con interfaz de canal de fibra o SCSI con conexión en serie (SAS)
  - Disco de estado sólido (SSD)
- Aísle el registro activo de la base de datos a menos que utilice el hardware de flash o SSD
- Al crear matrices para la base de datos, utilice RAID nivel 5

### Agrupación de almacenamiento

- Puede utilizar discos menos caros y más lentos para la agrupación de almacenamiento
- La agrupación de almacenamiento puede compartir discos para el registro de archivado y el almacenamiento de copias de seguridad de base de datos.
- Utilice el nivel RAID 6 para las matrices de agrupación de almacenamiento para añadir protección frente a las anomalías de unidad doble cuando se utilizan tipos de disco de gran tamaño
- Planificación de matrices de almacenamiento  
Prepararse para la configuración de almacenamiento de disco planificando matrices RAID y volúmenes, de acuerdo con el tamaño del sistema IBM Spectrum Protect.

### Referencia relacionada:



## Planificación de la seguridad

Planee proteger la seguridad de los sistemas en la solución IBM Spectrum Protect con controles de acceso y autenticación y tenga en cuenta el cifrado de datos y la transmisión de contraseña.

- Planificación de los roles de administración  
Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.
- Planificación para comunicaciones seguras  
Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.
- Planificación de almacenamiento de datos cifrados  
Determine si la compañía requiere que se cifren los datos almacenados y elija la opción que mejor se adapta a sus necesidades.
- Planificación del acceso de cortafuegos  
Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

## Planificación de los roles de administración

Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.

Puede asignar uno de los siguientes niveles de autorización a los administradores:

### Sistema

Los administradores con autoridad del sistema tienen el nivel de autorización más alto. Los administradores con este nivel pueden realizar cualquier tarea. Pueden gestionar todos los dominios de política y agrupaciones de almacenamiento y otorgar autoridad a otros administradores.

### Política

Los administradores que tienen autorización sobre políticas pueden gestionar todas las tareas relacionadas con la gestión de políticas. Este privilegio puede no tener restricciones o puede estar restringido a dominios de políticas específicos.

### Almacenamiento

Los administradores que tienen autorización de almacenamiento pueden asignar y controlar recursos de almacenamiento para el servidor.

### Operador

Los administradores que tienen autorización de operador pueden controlar la operación inmediata del servidor y la disponibilidad de soporte de almacenamiento como unidades y bibliotecas de cintas.

Los escenarios de Tabla 1 proporcionan ejemplos de por qué es posible que desee asignar distintos niveles de autorización para que los administradores puedan realizar tareas:

Tabla 1. Escenarios para roles de administrador

Escenario	Tipo de ID de administrador a configurar
Un administrador de una pequeña empresa gestiona el servidor y es responsable de todas las actividades del servidor.	<ul style="list-style-type: none"><li>• Autoridad del sistema: 1 ID de administrador</li></ul>
Un administrador para varios servidores también gestiona el sistema en general. Otros diversos administradores gestionan sus propias agrupaciones de almacenamiento.	<ul style="list-style-type: none"><li>• Autoridad del sistema en todos los servidores: 1 ID de administrador para el administrador del sistema general</li><li>• Autoridad de almacenamiento para agrupaciones de almacenamiento designadas: 1 ID de administrador para cada uno de los otros administradores</li></ul>
Un administrador gestiona 2 servidores. Otra persona ayuda con las tareas de administración. Dos ayudantes son responsables de ayudar a garantizar que se hace copia de seguridad de los sistemas importantes. Cada ayudante es responsable de supervisar las copias de seguridad planificadas en uno de los servidores de IBM Spectrum Protect.	<ul style="list-style-type: none"><li>• Autoridad del sistema en ambos servidores: 2 ID de administrador</li><li>• Autoridad de operador: 2 ID de administrador para los ayudantes con acceso al servidor del que cada persona es responsable</li></ul>

## Planificación para comunicaciones seguras

Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.

Determine el nivel de protección necesario para los datos, basándose en las regulaciones y requisitos empresariales bajo los que opera la compañía.

Si su empresa necesita un alto nivel de seguridad para las contraseñas y la transmisión de datos, planee implementar comunicaciones seguras con protocolos de seguridad de la capa de transporte (TLS) o de capa de sockets seguros (SSL).

TLS y SSL proporcionan comunicaciones seguras entre el servidor y el cliente, pero pueden afectar al rendimiento del sistema. Para mejorar el rendimiento del sistema, utilice TLS para autenticarse sin cifrar datos de objetos. Para especificar si el servidor debe utilizar TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor y el parámetro UPDATE SERVER=SSL para la comunicación de servidor a servidor. A partir de la versión V8.1.2, se utiliza TLS para la autenticación predeterminada. Si decide utilizar TLS para cifrar sesiones enteras, utilice el protocolo solo para las sesiones en las que es necesario y añada recursos de procesador en el servidor para gestionar el incremento del tráfico de red. También puede probar otras opciones. Por ejemplo, algunos dispositivos, como los direccionadores o los conmutadores, proporcionan la función TLS o SSL.

Puede utilizar TLS y SSL para proteger todas o algunas de las distintas vías de acceso de comunicación posibles, por ejemplo:

- Centro de operaciones: De navegador a concentrador; de concentrador a radio
- Cliente a servidor
- Servidor a servidor: réplica de nodo en el servidor:

**Tareas relacionadas:**

[Protección de las comunicaciones](#)

## Planificación de almacenamiento de datos cifrados

Determine si la compañía requiere que se cifren los datos almacenados y elija la opción que mejor se adapta a sus necesidades.

Si la empresa requiere que los datos de las agrupaciones de almacenamiento estén cifrados, tiene la opción de utilizar el cifrado IBM Spectrum Protect, o un dispositivo externo como una cinta para el cifrado.

Si elige IBM Spectrum Protect para cifrar los datos, se necesitan recursos informáticos adicionales en el cliente que pueden afectar al rendimiento de los procesos de copia de seguridad y restauración.

**Información relacionada:**

[Nota técnica 1963635](#)

## Planificación del acceso de cortafuegos

Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Tabla 1 describe los puertos utilizados por el servidor, el cliente y el Centro de operaciones.

Tabla 1. Puertos utilizados por el servidor, el cliente y Centro de operaciones

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (TCPPOINT)	1500	Entrada/salida	Cada instancia de servidor necesita un puerto exclusivo. Puede especificar un número de puerto alternativo en lugar del predeterminado. La opción TCPPOINT realiza escuchas para sesiones habilitadas para TCP/IP y SSL desde el cliente. Para el tráfico de cliente administrativo, puede utilizar las opciones TCPADMINPORT y ADMINONCLIENTPORT para definir los valores de puerto.
Puerto solo SSL (SSLTCPPOINT)	No tiene valor predeterminado	Entrada/salida	Este puerto se utiliza si desea restringir la comunicación en el puerto a sesiones solo habilitadas para SSL. Para admitir tanto las comunicaciones SSL como las no SSL, utilice las opciones TCPPOINT o TCPADMINPORT.
SMB	45	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.

Elemento	Valor predeterminado	Dirección	Descripción
NDMP	No tiene valor predeterminado	Entrada/salida	<p>El servidor debe poder abrir una conexión de puerto de control NDMP de salida con el dispositivo NAS. El puerto de control de salida es la dirección de nivel inferior en la definición de transportador de datos para el dispositivo NAS.</p> <p>Durante una restauración NDMP de archivador a servidor, el servidor debe poder abrir una conexión de datos NDMP de salida con el dispositivo NAS. El puerto de conexión de datos que se utiliza durante una restauración puede configurarse en el dispositivo NAS.</p> <p>Durante las copias de seguridad NDMP de archivador a servidor, el dispositivo NAS debe poder abrir conexiones de datos de salida con el servidor y el servidor debe poder aceptar las conexiones de datos NDMP de entrada. Puede utilizar la opción de servidor NDMPPORTRANGE para restringir el conjunto de puertos disponibles para su uso como conexiones de datos NDMP. Puede configurar un cortafuegos para conexiones a estos puertos.</p>
Réplica	No tiene valor predeterminado	Entrada/salida	<p>El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica.</p> <p>Los puertos de entrada para la réplica son los puertos TCP y SSL que el servidor de origen indique en el mandato DEFINE SERVER.</p>
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesión de ejecución larga	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente-servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	El puerto de servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

## Implementación de disco de sitio único de una solución de protección de datos

La solución de disco de sitio único se configura en un sitio y utiliza la deduplicación de datos.

### Hoja de ruta de la implementación

Los pasos siguientes son necesarios para configurar el entorno de disco de sitio único de IBM Spectrum Protect.

1. Configurar el sistema.
  - a. Configurar el hardware de almacenamiento y las matrices de almacenamiento para el tamaño del entorno.
  - b. Instalar el sistema operativo del servidor.
  - c. Configurar la E/S de multivía de acceso.
  - d. Crear el ID de usuario de la instancia de servidor.
  - e. Preparar sistemas de archivos para IBM Spectrum Protect.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
  - a. Completar la configuración inicial del servidor.

- b. Configurar opciones de servidor.
  - c. Configurar la capa de sockets seguros del servidor y el cliente.
  - d. Configurar el Centro de operaciones.
  - e. Registrar la licencia de IBM Spectrum Protect.
  - f. Configurar la eliminación de duplicados de datos.
  - g. Definir las reglas de retención de datos para su empresa.
  - h. Definir programas de mantenimiento del servidor.
  - i. Definir programas de cliente.
4. Instalar y configurar clientes.
    - a. Registrar y asignar clientes a programas.
    - b. Instalar y verificar el servicio de gestión de clientes.
    - c. Configurar el Centro de operaciones para utilizar el servicio de gestión de clientes.
  5. Completar la implementación.

## Configuración del sistema

---

Para configurar el sistema, primero debe configurar el hardware de almacenamiento de disco y el sistema servidor para IBM Spectrum Protect.

- Configuración del hardware de almacenamiento  
Para configurar el hardware de almacenamiento, revise las directrices generales para los sistemas de disco y IBM Spectrum Protect.
- Instalación del sistema operativo del servidor  
Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.
- Configuración de E/S de la multivía de acceso  
puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.
- Creación del ID de usuario para el servidor  
Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.
- Preparación de sistemas de archivos para el servidor  
Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

## Configuración del hardware de almacenamiento

---

Para configurar el hardware de almacenamiento, revise las directrices generales para los sistemas de disco y IBM Spectrum Protect.

### Procedimiento

---

1. Proporcione una conexión entre el servidor y los dispositivos de almacenamiento siguiendo estas directrices:
  - Utilice un conmutador o conexión directa para las conexiones de canal de fibra.
  - Tenga en cuenta el número de puertos que están conectados y la cantidad de ancho de banda que se necesita.
  - Tenga en cuenta el número de puertos en el servidor y el número de puertos de host en el sistema de discos que están conectados.
2. Verifique que los controladores de dispositivo y firmware para el sistema servidor, adaptadores y sistema operativo son actuales y están en los niveles recomendados.
3. Configure matrices de almacenamiento. Asegúrese de que ha planificado correctamente para garantizar un rendimiento óptimo. Consulte el apartado Planificación de almacenamiento para obtener más información al respecto.
4. Asegúrese de que el sistema servidor tiene acceso a los volúmenes de disco que se han creado. Realice los pasos siguientes:
  - a. Si el sistema está conectado a un conmutador de canal de fibra, divida el servidor por zonas para ver los discos.
  - b. Correlacione todos los volúmenes para indicar al sistema de discos que este servidor específico está autorizado para ver cada disco.

## Instalación del sistema operativo del servidor

---

Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Instalación en sistemas AIX  
Complete los pasos siguientes para instalar AIX en el sistema servidor.

- Instalación en sistemas Linux  
Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.
- Instalación en sistemas Windows  
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

## Instalación en sistemas AIX

---

Complete los pasos siguientes para instalar AIX en el sistema servidor.

### Procedimiento

---

1. Instale AIX Versión 7.1, TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.
3. Abra el archivo /etc/hosts y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Habilite los puertos de terminación de E/S de AIX emitiendo el siguiente mandato:

```
chdev -l iocp0 -P
```

El rendimiento de servidor puede verse afectado por la definición de huso horario de Olson.

5. Para optimizar el rendimiento, cambie el formato de huso horario del sistema de Olson a POSIX. Utilice el siguiente formato de mandato para actualizar el valor de huso horario:

```
chtz=local_timezone,date/time,date/time
```

Por ejemplo, si ha vivido en Tucson, Arizona, donde se utiliza la franja horaria de las Rocosas, deberá emitir el siguiente mandato para cambiar el formato POSIX:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Añada una entrada en el .profile del usuario de la instancia para que se defina el entorno siguiente:

```
export MALLOCOPTIONS=multiheap:16
```

7. Defina el sistema para crear archivos principales de aplicación completos. Emita el mandato siguiente:

```
chdev -l sys0 -a fullcore=true -P
```

8. Para las comunicaciones con el servidor y Centro de operaciones, asegúrese de que los siguientes puertos están abiertos en todos los cortafuegos que puedan existir:

- Para las comunicaciones con el servidor, abra el puerto 1500.
- Para las comunicaciones seguras con Centro de operaciones, abra el puerto 11090 en el servidor concentrador.

Si no utiliza los valores de puerto predeterminados, asegúrese de que los puertos que está utilizando están abiertos.

9. Habilite las mejoras de alto rendimiento de TCP. Emita el mandato siguiente:

```
no -p -o rfc1323=1
```

10. Para obtener una fiabilidad y un rendimiento óptimos, vincule cuatro puertos Ethernet de 10 Gb. Utilice la herramienta de la interfaz de gestión del sistema (SMIT) para vincular los puertos utilizando Etherchannel. Durante las pruebas se utilizaron los siguientes valores:

mode	8023ad	
auto_recovery	yes	Habilitar la recuperación automática tras la migración tras error.
backup_adapter	NONE	Adaptador utilizado cuando falla todo el canal.
hash_mode	src_dst_port	Determina cómo se elige el adaptador saliente.
interval	long	Determina el valor de intervalo para IEEE.
mode	8023ad	Modalidad de 802.3ad
		Modalidad de funcionamiento de

netaddr	0	EtherChannel
noloss_failover	yes	Dirección para el ping Habilitar migración tras error sin pérdidas tras anomalía del ping
num_retries	3	Veces que reintentar el ping antes de considerarlo un error
retry_time	1	Tiempo de espera (en segundos) entre pings
use_alt_addr	no	Habilitar dirección EtherChannel alternativa
use_jumbo_frame	no	Habilitar tramas de gran tamaño de Gigabit Ethernet

11. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 1. Si los valores *ulimit* no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 1. Valores de los límites de usuario (*ulimit*)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	<code>ulimit -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	<code>ulimit -Hd</code>
Tamaño de archivo máximo	fsize	Ilimitado	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	nofile	65536	<code>ulimit -Hn</code>
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	<code>ulimit -Ht</code>
Número máximo de procesos de usuario	nproc	16384	<code>ulimit -Hu</code>

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.

### Antes de empezar

El sistema operativo se instalará en los discos duros internos. Configure los discos duros internos utilizando una matriz de hardware de RAID 1. Por ejemplo, si está configurando un sistema pequeño, los dos discos internos de 300 GB se duplican en RAID 1 de modo que aparece disponible un único disco de 300 GB para el instalador del sistema operativo.

### Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
  - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
  - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
  - c. Seleccione las preferencias de idioma y teclado.
  - d. Seleccione la ubicación para establecer el huso horario correcto.
  - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
  - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:
    - El disco local de 300 GB se ha seleccionado como destino de instalación.
    - En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.
Pulse Terminado.
  - g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root. Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato `df` para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

```
[root@tvapp02]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/mapper/rhel-root    50G    3.0G    48G    6% /
devtmpfs                  32G         0    32G    0% /dev
tmpfs                     32G    92K    32G    1% /dev/shm
tmpfs                     32G    8.8M    32G    1% /run
tmpfs                     32G         0    32G    0% /sys/fs/cgroup
/dev/mapper/rhel-home    220G    37M    220G    1% /home
/dev/sda1                 497M   124M    373M   25% /boot
```

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agrega varios puertos subordinados a una sola conexión lógica. El método preferido es utilizar una modalidad de vínculo de 802.3ad, un valor de miimon de 100 y un valor de xmit\_hash\_policy de layer3+4.

Restricción: Para utilizar una conexión de red LACP, debe disponer de un conmutador de red que admita LACP.

Para obtener instrucciones adicionales sobre cómo configurar conexiones de red vinculadas con Red Hat Enterprise Linux Versión 7, consulte Crear una interfaz de acoplamiento de canal.

3. Abra el archivo /etc/hosts y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Instale los componentes que son necesarios para la instalación de servidor. Complete los pasos siguientes para crear un repositorio Yellowdog Updater Modified (YUM) e instale los paquetes de requisitos previos.

- a. Monte el DVD de instalación de Red Hat Enterprise Linux en el directorio del sistema. Por ejemplo, para montarlo en el directorio /mnt, emita el siguiente mandato:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Verifique que el DVD se ha montado emitiendo el mandato mount. Debería ver una salida similar al ejemplo siguiente:

```
/dev/sr0 on /mnt type iso9660
```

- c. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

Si el directorio repos.d no existe, créelo.

- d. Liste el contenido de directorio:

```
ls rhel-source.repo
```

- e. Cambie el nombre del archivo repo original emitiendo el mandato mv. Por ejemplo:

```
mv rhel-source.repo rhel-source.repo.orig
```

- f. Cree un nuevo archivo repo utilizando un editor de texto. Por ejemplo, para utilizar el editor vi, emita el siguiente mandato:

```
vi rhel71_dvd.repo
```

- g. Añada las líneas siguientes al nuevo archivo repo. El parámetro baseurl especifica el punto de montaje del directorio:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

- h. Instale el paquete de requisito previo ksh.x86\_64, emitiendo el mandato yum. Por ejemplo:

```
yum install ksh.x86_64
```

Excepción: No necesita instalar las bibliotecas compat-libstdc++-33-3.2.3-69.el6.i686 y libstdc++-i686 para Red Hat Enterprise Linux Versión 7.1.

5. Cuando se completa la instalación de software, puede restaurar los valores de repositorio YUM originales completando los pasos siguientes:

- a. Desmonte el DVD de instalación de Red Hat Enterprise Linux emitiendo el siguiente mandato:

```
umount /mnt
```

b. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

c. Cambie el nombre del archivo repo que ha creado:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Cambie el nombre del archivo original al nombre original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine si son necesarios cambios de parámetro de kernel. Realice los pasos siguientes:

a. Utilice el mandato `sysctl -a` para listar los valores de parámetro.

b. Analice los resultados utilizando las directrices en Tabla 1 para determinar si es necesario algún cambio.

c. Si se necesitan cambios, establezca los parámetros en el archivo `/etc/sysctl.conf`. Los cambios de archivo se aplican cuando se inicia el sistema.

Consejo: Ajuste automáticamente los valores de parámetros de kernel y elimine la necesidad de actualizaciones manuales en estos valores. En Linux, el software de base de datos DB2 ajusta automáticamente los valores del parámetro de kernel de comunicación entre procesos (IPC) a los valores preferidos. Para obtener más información sobre los valores de parámetros de kernel, busque los parámetros de kernel de Linux en IBM DB2 versión 11.1 Knowledge Center.

Tabla 1. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción	
kernel.shmmni	El número máximo de segmentos.	
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes).  Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.	
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas).	
kernel.sem	(SEMMSL)	
Hay cuatro valores para el parámetro kernel.sem.	El número máximo de semáforos por matriz.	
	(SEMMNS)	El número máximo de semáforos por sistema.
	(SEMOPM)	El número máximo de operaciones por llamada a semáforo.
	(SEMMNI)	El número máximo de matrices.
	kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema.
kernel.msgmax	Tamaño máximo de los mensajes (bytes).	
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes).	
kernel.randomize_va_space	El parámetro <code>kernel.randomize_va_space</code> configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.	
vm.swappiness	El parámetro <code>vm.swappiness</code> define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.	



Parámetro	Descripción
vm.overcommit_memory	El parámetro vm.overcommit_memory influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.

7. Abra puertos de cortafuegos para comunicarse con el servidor. Realice los pasos siguientes:

a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.

Emita el mandato siguiente:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Para utilizar la dirección de puerto predeterminada para las comunicaciones con el servidor, abra el puerto TCP/IP 1500 en el cortafuegos de Linux.

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Si desea utilizar un valor distinto del predeterminado, puede especificar un número en el rango 1024 - 32767. Si abre un puerto distinto del predeterminado, tendrá que especificar ese puerto cuando ejecute el script de configuración.

c. Si piensa utilizar este sistema como concentrador, abra el puerto 11090, que es el puerto predeterminado para las comunicaciones seguras (https).

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Vuelva a cargar las definiciones de cortafuegos para que los cambios entren en vigor.

Emita el mandato siguiente:

```
firewall-cmd --reload
```

8. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 2. Si los valores ulimit no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 2. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	ulimit -Hc
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	ulimit -Hd
Tamaño de archivo máximo	fsize	Ilimitado	ulimit -Hf
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Windows

Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

### Procedimiento

1. Instale Microsoft Windows Server 2012 R2 Standard Edition, de acuerdo con las instrucciones del fabricante.

2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
  - a. Abra el editor de política de seguridad local ejecutando secpol.msc.
  - b. Pulse Políticas locales > Opciones de seguridad y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
    - Modo de aprobación de administrador para la cuenta de administrador integrado
    - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:
  - a. Aplique las últimas actualizaciones de Windows 2012 R2.
  - b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
  - c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
  - d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.
5. Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Backup server port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. En el servidor concentrador de Centro de operaciones, abra el puerto predeterminado para comunicaciones seguras (https) con Centro de operaciones. El número de puerto es 11090. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Centro de operaciones port 11090"
dir=in action=allow protocol=TCP localport=11090
```

## Configuración de E/S de la multivía de acceso

---

puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

- Sistemas AIX
- Sistemas Linux
- Sistemas Windows

## Sistemas AIX

---

### Procedimiento

---

1. Determine la dirección de puerto de canal de fibra que debe utilizar para la definición de host en el subsistema de disco. Emita el mandato lscfg para cada puerto.

- En sistemas pequeños y medianos, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
```

- En sistemas grandes, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"
lscfg -vps -l fcs1 | grep "Network Address"
lscfg -vps -l fcs2 | grep "Network Address"
lscfg -vps -l fcs3 | grep "Network Address"
```

2. Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:

- devices.common.IBM.mpio.rte
- devices.fcp.disk.array.rte
- devices.fcp.disk.rte

3. Emita el mandato cfgmgr para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

4. Para listar los discos disponibles, emita el siguiente mandato:

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```
hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
```

```
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...
```

5. Utilice la salida del mandato `lsdev` para identificar y listar ID de dispositivo para cada dispositivo de disco.

Por ejemplo, un ID de dispositivo podría ser `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

```
lspv -u
```

En un sistema IBM® Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

```
hdisk4 00f8cf083fd97327 None active
      33213600507630081010578000000000003004214503IBMfcp
```

En el ejemplo, `600507630081010578000000000030` es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

Para verificar el tamaño de disco en megabytes y compararlo con el valor que se lista para el sistema, emita el siguiente mandato:

```
bootinfo -s hdisk4
```

## Sistemas Linux

---

### Procedimiento

---

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

```
multipathconf --enable
```

Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los mandatos siguientes:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

```
multipath -l
```

4. Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan.  
Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

```
[root@tapsrv01 code]# multipath -l
36005076802810c50980000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|+- policy='round-robin 0' prio=0 status=active
| |- 2:0:1:18 sdcw 70:64 active undef running
| `-- 4:0:0:18 sdgb 131:112 active undef running
`+- policy='round-robin 0' prio=0 status=enabled
| - 1:0:1:18 sdat 66:208 active undef running
`- 3:0:0:18 sddy 128:0 active undef running
```

a. Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

b. Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato multipath -l.

5. Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 36005076802810c50980000000000012.

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

## Sistemas Windows

### Procedimiento

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
2. Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

```
c:\program files\IBM\SDDSSM\datapath.exe query device
```

3. Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan. Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

```
DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0
```

4. Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 60050763008101057800000000000034

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

5. Para poner los nuevos discos en línea y borrar el atributo de 'sólo lectura', ejecute diskpart.exe con los mandatos siguientes. Repítalo para cada uno de los discos:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
```

```
attribute disk clear readonly
exit
```

## Creación del ID de usuario para el servidor

---

Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.

### Acerca de esta tarea

---

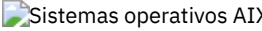
Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado ( \_ ) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.


### Procedimiento

---

1. Utilice mandatos del sistema operativo para crear un ID de usuario.

-  Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

Por ejemplo, para crear el ID de usuario `tsminst1` en el grupo `tsmsrvrs` con una contraseña de `tsminst1`, emita los siguientes mandatos desde un ID de usuario de administración:


 Sistemas operativos AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

 Sistemas operativos Linux

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

-  Cree un ID de usuario y, a continuación, añada el nuevo ID al grupo de administradores. Por ejemplo, para crear el ID de usuario `tsminst1`, emita el siguiente mandato:

```
net user tsminst1 * /add
```

Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Cierre la sesión con el nuevo ID de usuario.

## Preparación de sistemas de archivos para el servidor

---

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

- Preparación de sistemas de archivos en sistemas AIX  
Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.
- Preparación de sistemas de archivos en sistemas Linux  
Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.
- Preparación de sistemas de archivos en sistemas Windows  
Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

# Preparación de sistemas de archivos en sistemas AIX

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

## Procedimiento

1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos *hdiskX* disponibles. Emita los siguientes mandatos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, *hdisk0*.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato `mkvg`, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

Por ejemplo, si los nombres de dispositivo *hdisk4*, *hdisk5* y *hdisk6* corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita `lsvg` para cada grupo de volúmenes que ha creado en el paso anterior.

Por ejemplo:

```
lsvg -p tsmdb
```

La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

```
tsmdb:
PV_NAME  PV STATE   TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active     1631      1631      327..326..326..326..326
hdisk5   active     1631      1631      327..326..326..326..326
hdisk6   active     1631      1631      327..326..326..326..326
```

4. Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato `mklv`. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco.

Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato `crfs`.

Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

```
mount -a
```

7. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado es normalmente un 1%:

```
tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks   Free   %Used   Iused   %Iused   Mounted on
/dev/tsmact00   195.12     194.59    1%      4       1%      /tsminst1/TSMalog
```

- Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios para el servidor.

## Preparación de sistemas de archivos en sistemas Linux

Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

### Procedimiento

- Utilizando la lista de ID de dispositivo que ha generado antes, emita el mandato mkfs para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos xfs:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Puede emitir el mandato mkfs hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

- Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato mkdir para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación.

Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
mkdir /tsminst1
```

Repita el mandato mkdir para cada sistema de archivos.

- Añada una entrada en el archivo /etc/fstab para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.

Por ejemplo:

```
/dev/mapper/36005076802810c509800000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

- Monte los sistemas de archivos que ha añadido al archivo /etc/fstab emitiendo el mandato mount -a.
- Liste todos los sistemas de archivos emitiendo el mandato df. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible. El ejemplo siguiente en un sistema IBM® Storwize muestra que la cantidad de espacio utilizado normalmente es un 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/360050763008101057800000000000003 134G  188M 132G  1%  /tsminst1/TSMalog
```

- Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios para el servidor IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas Windows

Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

### Procedimiento

- Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato md para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
md c:\tsminst1
```

Repita el mandato md para cada sistema de archivos.

2. Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

Vaya a Gestor de servidores > Servicios de archivo y almacenamiento y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

- a. Ponga el disco en línea.
  - b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
  - c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como TSMfile00. No asigna el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como C:\tsminst1\TSMfile00.  
Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.
3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato mountvol y, a continuación, revise la salida. Por ejemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\  
C:\tsminst1\TSMdbspace00\
```

4. Una vez se ha completado la configuración de disco, reinicie el sistema.

## Qué hacer a continuación

---

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

## Instalación del servidor y Centro de operaciones

---

Utilice el asistente gráfico de IBM® Installation Manager para instalar los componentes.

- Instalación en sistemas AIX y Linux  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.
- Instalación en sistemas Windows  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

## Instalación en sistemas AIX y Linux

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.


### Antes de empezar

---

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

### Procedimiento

---


1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.  
Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.
2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package\_name* es el nombre del archivo descargado.

6.  Sistemas operativos AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:



```
lsuser
```

De manera predeterminada, el mandato está habilitado.

7. Cambie al directorio en el que colocó el archivo ejecutable.
8. Inicie el asistente de instalación emitiendo el mandato siguiente:

```
./install.sh
```

Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación



---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.
- Instalación de archivos RPM de requisitos previos para el asistente gráfico  
Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

### Tareas relacionadas:

-  Otros métodos para instalar componentes de IBM Spectrum Protect (AIX)
-  Otros métodos para instalar componentes de IBM Spectrum Protect (Linux)

## Instalación en sistemas Windows

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento

---

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM®.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.

### Tareas relacionadas:

-  Otros métodos para instalar componentes de IBM Spectrum Protect

## Configuración del servidor y el Centro de operaciones

---

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

- Configuración de la instancia de servidor  
Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.
- Instalación del cliente de archivado y copia de seguridad  
Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?
- Configuración de opciones para el servidor  
Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.
- Configuración de comunicaciones seguras con Seguridad de la capa de transporte  
Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.
- Configuración de Centro de operaciones  
Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.
- Registro de la licencia de producto  
Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.
- Configuración de la optimización de almacenamiento de datos  
Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.
- Definición de las reglas de retención de datos para su empresa  
Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.
- Definición de planificaciones para actividades de mantenimiento del servidor  
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.
- Definición de planificaciones de cliente  
Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

## Configuración de la instancia de servidor

---

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

 Sistemas operativos Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:







1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
  - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
  - b. Seleccione Configuración avanzada.
  - c. Seleccione Reglas de entrada.
  - d. Seleccione Nueva regla.
  - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.

3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
  - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
  - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
  - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
  - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada > Inhabilitar > Aceptar.
4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

## Acerca de esta tarea

El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Procedimiento

1. Inicie la versión local del asistente.
  - 

 Abra el programa dsmicfgx en el directorio /opt/tivoli/tsm/server/bin. Este asistente sólo puede ejecutarse como usuario root.
  - 
 Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Planificación de hojas de trabajo para la configuración del sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.
  - 

 En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.
  - 
 Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

## Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

## Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

## Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

## Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo dsmserv.opt.
2. Revise los valores de la tabla siguiente y verifique los valores de opciones de servidor, en base al tamaño del sistema.

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Sí	No	No

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo dsmserv.opt y utilice el mandato SETOPT desde la interfaz de línea de mandatos de administración para establecer las opciones.

Por ejemplo, para actualizar la opción IDLETIMEOUT a 60, emita el siguiente mandato:

```
setopt idletimeout 60
```

- Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

Opción de servidor	Todos los tamaños del sistema
SSLFIPSMODE	NO
TCPPORT	Especifique el número de puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente.
TCPADMINPORT	Especifique la dirección del puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente administrativo de línea de mandatos.

Si alguno de los valores de opción debe actualizarse, edite el archivo dsmserv.opt utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guardé los cambios y cierre el archivo. Si edita el archivo dsmserv.opt directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

#### Referencia relacionada:

- [Referencia de opciones de servidor](#)
- [SETOPT \(Establecer una opción de servidor para actualización dinámica\)](#)

## Configuración de comunicaciones seguras con Seguridad de la capa de transporte

Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

### Acerca de esta tarea

Tal como se indica en la figura siguiente, puede configurar manualmente comunicaciones seguras entre el servidor y el cliente de archivado y copia de seguridad definiendo opciones en los archivos de opciones de servidor y cliente y, después, transfiriendo el certificado firmado automáticamente que se ha generado en el servidor al cliente. Como alternativa, puede obtener y transferir un certificado único que esté firmado por una entidad emisora de certificados (CA).



Para obtener más información sobre cómo configurar el servidor y los clientes para las comunicaciones SSL o TLS, consulte Configuración de agentes, servidores y clientes de almacenamiento, y del Centro de operaciones para conectarse al servidor mediante SSL.

## Configuración de Centro de operaciones

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

### Antes de empezar

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

### Procedimiento

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

```
https://hostname:secure_port/oc
```

donde:

- *nombre\_host* representa el nombre del sistema donde está instalado Centro de operaciones
- *puerto\_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

Por ejemplo, si el nombre de host es tsm.storage.mylocation.com y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

```
https://tsm.storage.mylocation.com:11090/oc
```

Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.

2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor concentrador configurando el protocolo de la capa de sockets seguros (SSL).

Siga las instrucciones que encontrará en Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

Siga las instrucciones que encontrará en Seguimiento del estado del sistema mediante informes de correo electrónico.

- Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador  
Para proteger las comunicaciones entre Centro de operaciones y el servidor concentrador, añada el certificado de seguridad de la capa de transporte (TLS) del servidor concentrador al archivo de almacén de confianza de Centro de operaciones.

## Registro de la licencia de producto

Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.


### Acerca de esta tarea

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

## Procedimiento

---

Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.


1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración  y pulsando Creador de mandatos.
3. Emita el mandato REGISTER LICENSE. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

## Qué hacer a continuación

---

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor se ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
-  Sistemas operativos Linux Si cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

### Referencia relacionada:

 REGISTER LICENSE (Registrar una nueva licencia)

## Configuración de la optimización de almacenamiento de datos

---

Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.

## Antes de empezar

---

Utilice la información de directorio de agrupación de almacenamiento que ha registrado en Planificación de hojas de trabajo para esta tarea.

## Procedimiento

---

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el cursor por encima de Almacenamiento.
3. En la lista que se visualiza, pulse Agrupaciones de almacenamiento.
4. Pulse el botón +Agrupación de almacenamiento.
5. Complete los pasos del asistente Añadir agrupación de almacenamiento:
  - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
  - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
6. Tras configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.

## Definición de las reglas de retención de datos para su empresa

---

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

## Procedimiento

---

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse Detalles.

2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.
3. Pulse el conmutador Configurar y realice los cambios siguientes:
  - o Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedores de directorio.
  - o Cambie el valor de la columna de copias de seguridad a Sin límite.
  - o Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador Configurar para que el conjunto de políticas ya no se pueda editar.
5. Activar el conjunto de políticas pulsando Activar.

**Tareas relacionadas:**

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

## Definición de planificaciones para actividades de mantenimiento del servidor

Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.

### Acerca de esta tarea

Planifique operaciones de mantenimiento de servidor para ejecutar después de operaciones de copia de seguridad de cliente. Puede controlar la temporización de planificaciones estableciendo la hora de inicio en combinación con la duración para cada operación.

El ejemplo siguiente muestra cómo puede planificar las operaciones de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de disco de un sitio único.

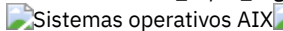
Operación	Planificación
Copia de seguridad del cliente	Empieza a las 22:00.
Proceso para archivos de recuperación tras desastre y de base de datos	<ul style="list-style-type: none"> <li>• La operación de copia de seguridad de base de datos se inicia a las 11:00, o 13 después de iniciar la operación de copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.</li> <li>• La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 17:00 o 6 horas después del inicio de la copia de seguridad de la base de datos.</li> <li>• La supresión del historial de volumen comienza a las 20:00 o 9 horas después del inicio de la operación de copia de seguridad de la base de datos.</li> </ul>
Caducidad de inventario	Se inicia a las 12:00, o 14 horas después del comienzo de la operación de copia de seguridad del cliente. Este proceso se ejecuta hasta completarse.

### Procedimiento


Tras configurar la clase de dispositivo para las operaciones de copia de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato DEFINE SCHEDULE. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.

1. Defina una clase de dispositivo para las operaciones de copia de seguridad. Por ejemplo, utilice el mandato DEFINE DEVCLASS para crear una clase de dispositivo que se denomine DBBACK\_FILEDEV:

```
define devclass dbback_filedev devtype=file
  directory=directorios_copia_seguridad_bd
```

donde *directorios\_copia\_seguridad\_bd* es una lista de los directorios que ha creado para la copia de seguridad de base de datos.  Sistemas operativos AIX/Sistemas operativos Linux Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando por el mandato /tsminst1/TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

 Sistemas operativos Windows Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando con C:\tsminst1\TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

- Establezca la clase de dispositivo para operaciones de copia de seguridad de base de datos automáticas. Utilice el mandato SET DBRECOVERY para especificar la clase de dispositivo que ha creado en el paso anterior. Por ejemplo, si la clase de dispositivo es dbback\_filedev, emita el mandato siguiente:

```
set dbrecovery dbback_filedev
```

- Cree planificaciones para las operaciones de mantenimiento utilizando el mandato DEFINE SCHEDULE. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.

Operación	Mandato de ejemplo
Realizar una copia de seguridad de la base de datos.	<p>Cree una planificación para ejecutar el mandato BACKUP DB. Si está configurando un sistema pequeño, establezca el parámetro COMPRESS en YES.</p> <p>Por ejemplo, en un sistema pequeño, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db   devclass=dbback_filedev type=full numstreams=3 wait=yes   compress=yes" active=yes desc="Back up the database."   startdate=today starttime=11:00:00 duration=45   durunits=minutes</pre>
Realice una copia de seguridad de la información de configuración del dispositivo.	<p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup   devconfig   filenames=devconfig.dat" active=yes desc="Backup the   device   configuration file." startdate=today starttime=17:00:00   duration=45 durunits=minutes</pre>
Haga una copia de seguridad del historial de volumen.	<p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup   volhistory   filenames=volhist.dat" active=yes desc="Back up the   volume   history." startdate=today starttime=17:00:00   duration=45   durunits=minutes</pre>
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	<p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete   volhistory   type=dbb todate=today-6 totime=now" active=yes   desc="Remove   old database backups." startdate=today   starttime=20:00:00   duration=45 durunits=minutes</pre>
Elimine objetos que exceden su retención permitida.	<p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY. Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar:</p> <ul style="list-style-type: none"> <li>o Sistemas pequeños: 10</li> <li>o Sistemas medianos: 30</li> <li>o Sistemas grandes: 40</li> </ul> <p>Por ejemplo, en un sistema de tamaño mediano, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire   inventory   wait=yes resource=30 duration=120" active=yes   desc="Remove expired   objects." startdate=today starttime=12:00:00   duration=45   durunits=minutes</pre>

## Qué hacer a continuación



Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Servidores.
2. Pulse Mantenimiento.

**Referencia relacionada:**

 [DEFINE SCHEDULE](#) (Definir una planificación para un mandato de administración)

## Definición de planificaciones de cliente

---

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

### Procedimiento

---

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de Clientes.
2. Pulse Planificaciones.
3. Pulse +Planificación.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.

## Instalación y configuración de clientes de archivado y copia de seguridad

---

Tras la configuración correcta del sistema servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

### Procedimiento

---

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

### Qué hacer a continuación

---

Registrar y asignar los clientes a planificaciones.

- Registro y asignación de clientes a planificaciones  
Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.
- Instalación del servicio de gestión de cliente  
Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

## Registro y asignación de clientes a planificaciones

---

Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.

### Antes de empezar

---

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

### Procedimiento

---

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre\_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Clientes.
  - b. En la tabla Clientes, pulse + Cliente.
  - c. Complete los pasos en el asistente Añadir cliente:
    - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
    - ii. En la ventana Configuración, copie los valores de opción TCPSEVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.  
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
    - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
    - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
    - v. Pulse Añadir cliente.

## Instalación del servicio de gestión de cliente

Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

### Procedimiento

Instale el servicio de gestión de cliente en el mismo sistema que el cliente de archivado y copia de seguridad completando los pasos siguientes:

1. Descargue el paquete de instalación para el servicio de gestión de cliente desde un sitio de descarga de IBM® como por ejemplo IBM Passport Advantage® o IBM Fix Central. Busque un nombre de archivo que sea similar a *<versión>-IBM\_Spectrum\_Protect-CMS-sistema\_operativo.bin*.
  2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
  3. Extraiga el contenido del archivo del paquete de instalación.
  4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
  5. Para instalar el servicio de gestión de cliente, siga las instrucciones del asistente del Gestor de instalación de IBM. Si el Gestor de instalación de IBM no está instalado en el sistema cliente, debe seleccionar el Gestor de instalación de IBM y los Servicios de gestión de cliente de IBM Spectrum Protect.
- Verificación de que el servicio de gestión de clientes está instalado correctamente  
Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.
  - Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente  
Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

#### Tareas relacionadas:

- 🔗 Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas

## Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.

### Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

```
dir_instalación_cliente/cms/bin/CmsConfig.sh list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
```

```
Capabilities: [LOG_QUERY]
```

```
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

- En los sistemas cliente Windows, emita el mandato siguiente:

```
dir_instalación_cliente\cms\bin\CmsConfig.bat list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
C:\"Archivos de programa"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
```

```
Capabilities: [LOG_QUERY]
```

```
Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt
```

```
Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

```
Log File: C:\Program Files\Tivoli\TSM\baclient\dmsched.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo client-configuration.xml. Para obtener instrucciones para configurar este archivo, consulte Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato CmsConfig verify para comprobar que una definición de nodo se ha creado correctamente en el archivo client-configuration.xml.

## Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente

---

Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

## Antes de empezar

Asegúrese de que el servicio de gestión de cliente está instalado y se ha iniciado en el sistema cliente. Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de cliente no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
  - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse por una red, mientras que el servicio de gestión de cliente se comunica por la otra red.
  - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, se le asigna dinámicamente al sistema cliente una dirección IP, que se guarda en el servidor durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

## Procedimiento

Para configurar Centro de operaciones para utilizar el servicio de gestión de cliente, complete los pasos siguientes:

1. En la página Clientes de Centro de operaciones, seleccione el cliente.
2. Pulse Detalles > Propiedades.
3. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de cliente en el sistema cliente. La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	<code>https://server.example.com</code>
Con el nombre de host de DNS y puerto no predeterminado	<code>https://server.example.com:1599</code>
Con la dirección IP y puerto no predeterminado	<code>https://192.0.2.0:1599</code>

4. Pulse Guardar.

## Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

## Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

## Procedimiento

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
  - a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
  - b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
  - c. Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.  
Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.
2. Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de disco de sitio único.

## Supervisión de una solución de disco de sitio único

Después de implementar una solución de disco en un único sitio con IBM Spectrum Protect, supervise la solución para su funcionamiento correcto. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

## Acerca de esta tarea

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar un informe de correo electrónico diario que resume el estado del sistema.

En algunos casos, es posible que desee utilizar herramientas de supervisión avanzadas para completar tareas de supervisión o resolución de problemas específicas.

Consejo: Si piensa diagnosticar problemas con clientes de archivado y copia de seguridad en sistemas operativos Linux o Windows, instale los servicios de gestión de cliente de IBM Spectrum Protect en cada sistema donde esté instalado un cliente de archivado y copia de seguridad. De esta forma, puede garantizar que el botón Diagnosticar está disponible en Centro de operaciones para diagnosticar problemas con los clientes de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.

## Procedimiento

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación diaria.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación periódica.
3. Para verificar que la solución de IBM Spectrum Protect cumple con los requisitos de licencia, siga las instrucciones que encontrará en Verificación de la conformidad de licencia.
4. Si desea configurar el Centro de operaciones para generar informes de estado de correo electrónico, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

## Qué hacer a continuación

Resuelva cualquier problema que encuentre. Para resolver un problema cambiando la configuración de la solución, siga las instrucciones que encontrará en Gestión de operaciones para una solución de disco de sitio único. Los siguientes recursos están también disponibles:

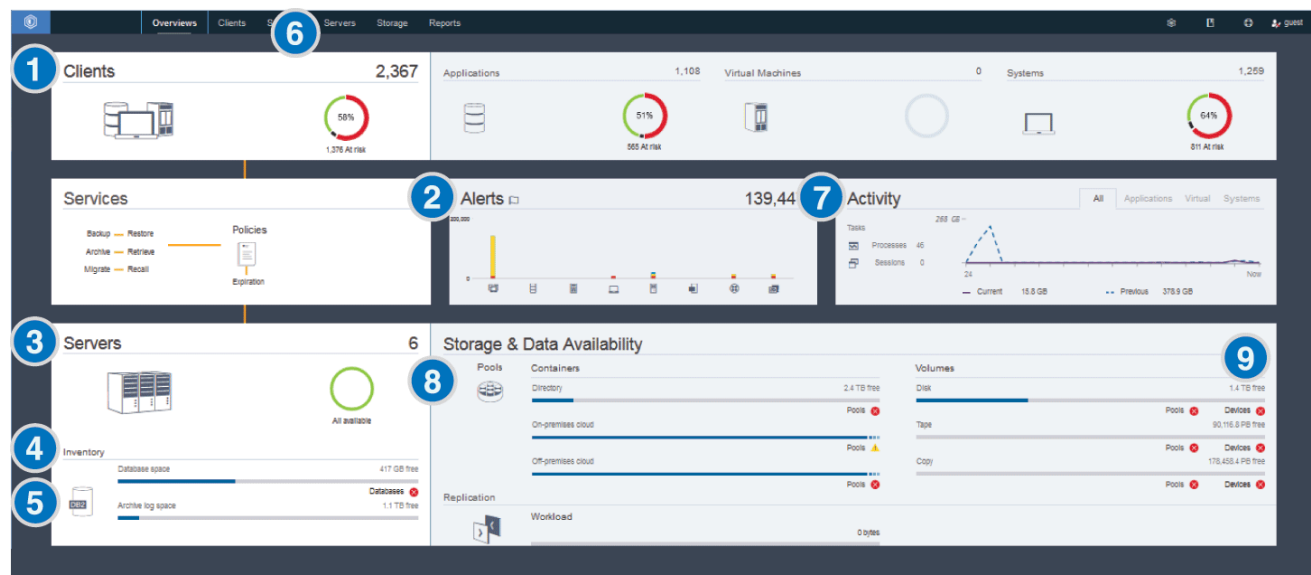
- Para resolver problemas de rendimiento, consulte Rendimiento.
- Para resolver otros tipos de problemas, consulte Resolución de problemas.


## Lista de comprobación de supervisión diaria

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.









Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.





Tabla 1. Tareas de supervisión diarias

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>1</b> Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Clientes, seleccione el cliente y pulse Detalles.</li> <li>2. Para diagnosticar un problema, pulse Diagnóstico.</li> </ol>	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>
<p><b>2</b> Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Alertas.</li> <li>2. En la tabla Alertas, seleccione una alerta.</li> <li>3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.</li> </ol>
<p><b>3</b> Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> <li>1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible.</li> <li>2. Para ver información adicional, pulse el área Servidores.</li> <li>3. Seleccione un servidor en la tabla Servidores y pulse Detalles.</li> </ol>	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione un servidor y pulse Detalles.</li> <li>2. Para actualizar las propiedades de servidor, pulse Propiedades.</li> </ol>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> <li>o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado.</li> <li>o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor.</li> <li>o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio.</li> <li>o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC.</li> <li>o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio.</li> </ul> </li> </ol>	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>5</b> Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.</li> </ol>	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione una fila y pulse Detalles.</li> <li>2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad.</li> </ol> <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Servidores.</li> <li>2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad.</li> </ol> <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la barra de menú, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY DB: <pre>query db f=d</pre> </li> <li>3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.</li> </ol>
<p><b>6</b> Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse Servidores &gt; Mantenimiento.</li> <li>2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial.</li> <li>3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.</li> </ol>	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>7 Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> <li>Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad.</li> <li>Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.</li> </ul>	<ul style="list-style-type: none"> <li>Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente.</li> <li>Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.</li> </ul>
<p>8 Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<ol style="list-style-type: none"> <li>Si se indican problemas en el área Almacenamiento &amp; Disponibilidad de datos, pulse Agrupaciones para ver los detalles: <ul style="list-style-type: none"> <li>Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible.</li> <li>Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura.</li> </ul> </li> <li>Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</li> </ol>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento &amp; Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> <li>En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes.</li> <li>En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios.</li> <li>Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.</li> </ul>

## Lista de comprobación de supervisión periódica

Para asegurarse de que la solución IBM Spectrum Protect opera correctamente, complete las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.










Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
Supervise el rendimiento del sistema.	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Visión general, pulse Clientes. Busque el servidor asociado al cliente.</li> <li>2. Pulse Servidores. Seleccione el servidor y pulse Detalles.</li> <li>3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse Tareas completadas.</li> <li>4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones que encontrará en QUERY ACTLOG (Consultar las anotaciones de actividades).</li> <li>5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa.</li> </ol> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Visión general, pulse Clientes.</li> <li>2. Seleccione un cliente de archivado y copia de seguridad y pulse Detalles.</li> <li>3. Para recuperar registros de cliente, pulse Diagnóstico.</li> </ol>	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte Resolución de problemas de rendimiento comunes del cliente.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte Identificación de cuellos de botella de rendimiento.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte Rendimiento.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse Agrupaciones.</li> <li>2. Seleccione una agrupación y pulse Vista rápida.</li> <li>3. En el área Optimización de almacenamiento de datos, vea la fila Espacio guardado.</li> </ol>	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores de nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones que encontrará en GENERATE DEDUPSTATS (Generar estadísticas de deduplicación de datos respecto a una agrupación de almacenamiento de contenedores de directorio).</li> <li>3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones que encontrará en QUERY DEDUPSTATS (Consultar las estadísticas de deduplicación de datos).</li> </ol>
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory  query option devconfig</pre> </li> <li>3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.</li> </ol> <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine si está disponible espacio suficiente para el sistema de archivos del directorio de la instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad.</li> </ul> <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux /home/tsminst1/tsminst1</li> <li>•  Sistemas operativos Windows C:\tsminst1</li> </ul> <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

<b>Tarea</b>	<b>Procedimientos básicos</b>	<b>Procedimientos avanzados y solución de problemas</b>
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Clientes.</li> <li>2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente.</li> <li>3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades.</li> <li>4. En el área Última sesión, visualice la fila Enviado a cliente.</li> </ol>	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones.</li> <li>2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles.</li> </ol>	<p>Sugerencias:</p> <ul style="list-style-type: none"> <li>• Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> <li>3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>.</li> </ol> </li> <li>• Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>.</li> <li>• Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> </ol> </li> </ul> <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> <li>• Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.</li> </ul>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes &gt; Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones.</li> <li>2. Seleccione una planificación y pulse Detalles.</li> <li>3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila.</li> <li>4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado.</li> <li>5. Pulse Guardar.</li> </ol>
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores &gt; Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).</li> </ol>

**Referencia relacionada:**

QUERY ACTLOG (Consultar las anotaciones de actividades)

➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

➔ QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

## Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

### Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

**Licencia de capacidad frontal**

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

**Licencia de capacidad de programa de fondo**

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

**Licencia de PVU**

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.



Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

## Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
<b>Modelo frontal</b>	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
<b>Modelo suplementario</b>	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
<b>Modelo de PVU</b>	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.</p>

## Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

### Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.



- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

## Acerca de esta tarea

---

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

## Procedimiento

---

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:


1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.  
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

## Resultados

---

Los informes habilitados se envían según los valores especificados.

### Referencia relacionada:

 UPDATE ADMIN (Actualizar un administrador)

## Gestión de operaciones para una solución de disco de sitio único

---

Utilice esta información para gestionar operaciones para una solución de disco de sitio único con IBM Spectrum Protect que incluya un servidor y utilice la eliminación de datos duplicados para una única ubicación.

- **Gestión del Centro de operaciones**  
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.
- **Protección de aplicaciones, máquinas virtuales y sistemas**  
El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.
- **Gestión del almacenamiento de datos**  
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Protección del servidor IBM Spectrum Protect**  
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**  
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**  
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**  
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Implementación de un plan de recuperación tras desastre**  
Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.
- **Recuperación de paradas del sistema**  
Para soluciones de disco de sitio único de IBM Spectrum Protect, puede recuperar el inventario localmente únicamente y restaurar la base de datos para proteger los datos.

## Gestión del Centro de operaciones

---

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke  
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web  
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Reinicio del asistente de configuración inicial  
Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.
- Cambio del servidor concentrador  
Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.
- Restauración de la configuración a un estado de preconfiguración  
Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

## Adición y eliminación de servidores spoke

---

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

### Acerca de esta tarea

---

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio  
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke  
Puede eliminar un servidor spoke del Centro de operaciones.

## Adición de un servidor de radio

---

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

### Antes de empezar

---

Las comunicaciones entre el servidor spoke y el servidor concentrador deben asegurarse utilizando el protocolo de Seguridad de la capa de transporte (TLS). Para asegurar las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

### Procedimiento

---

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
  - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
  - Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.  
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente a 14 días, si configura el servidor como un servidor de radio.

## Eliminación de un servidor spoke

---

Puede eliminar un servidor spoke del Centro de operaciones.

### Acerca de esta tarea

---

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

### Procedimiento

---

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre\_grupo* representa el nombre del grupo supervisado y *nombre\_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```

## Inicio y detención del servidor web


---

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.


### Procedimiento

---

1. Detener el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation\_dir/ui/utils*, donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:


```
./stopserver.sh
```

-  Sistemas operativos Linux Emita el mandato siguiente:

```
service opscenter.rc stop
```

-  Sistemas operativos Windows En la ventana Servicios, detenga el servicio de IBM Spectrum Protect Operations Center.

2. Inicie el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation\_dir/ui/utils*, donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

```
./startserver.sh
```

-  Sistemas operativos Linux Emita los mandatos siguientes:

Inicie el servidor:


```
service opscenter.rc start
```

Reinicie el servidor:

```
service opscenter.rc restart
```

Determine si el servidor se está ejecutando:

```
service opscenter.rc status
```

-  Sistemas operativos Windows En la ventana Servicios, inicie el servicio IBM Spectrum Protect Operations Center.

## Reinicio del asistente de configuración inicial

---

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

### Antes de empezar

---

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:

- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.







### Acerca de esta tarea

---

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

### Procedimiento

---

1. Detenga el servidor web de Centro de operaciones.
  2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde *installation\_dir* representa el directorio en el que está instalado Centro de operaciones:
    -  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/Liberty/usr/servers/guiServer*
    -  Sistemas operativos Windows *dir\_instalación\ui\Liberty\usr\servers\guiServer*
- Por ejemplo:
-  Sistemas operativos AIX  Sistemas operativos Linux *opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer*
  -  Sistemas operativos Windows *c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer*
3. En el directorio *guiServer*, elimine el archivo *serverConnection.properties*.
  4. Inicie el servidor web Centro de operaciones.
  5. Abra el Centro de operaciones.
  6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
  7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

## Cambio del servidor concentrador

---

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

### Procedimiento

---

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

**Tareas relacionadas:**

Reinicio del asistente de configuración inicial

## Restauración de la configuración a un estado de preconfiguración

---

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

### Procedimiento

---

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
  - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

Consejo: *IBM-OC-nombre\_servidor\_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
  - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: *IBM-OC-nombre\_servidor\_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

- e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

- f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restaure los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.

**Tareas relacionadas:**

Reinicio del asistente de configuración inicial

Inicio y detención del servidor web

## Protección de aplicaciones, máquinas virtuales y sistemas

---

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes  
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Gestión de operaciones de cliente  
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.
- Gestión de actualizaciones del cliente  
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- Poner fuera de servicio un nodo cliente  
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- Desactivación de datos para liberar espacio de almacenamiento  
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

## Adición de clientes

---

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

### Acerca de esta tarea

---

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

**Nodos de cliente de aplicaciones**

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

## Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones que encontrará en Selección del software de cliente y planificación de la instalación.
2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones que encontrará en Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones que encontrará en Instalación y configuración de clientes.

## Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

### Acerca de esta tarea

La práctica preferida es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente para poder configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración en la documentación de producto para asegurarse de que se puede producir las operaciones planificadas.

## Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de archivado y copia de seguridad realiza la copia de seguridad y el archivado de archivos y directorios de los servidores de archivos y las estaciones de trabajo en el almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none"><li>• Requisitos del cliente de archivado y copia de seguridad</li><li>• Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li><li>• Instalación del cliente de archivado y copia de seguridad de Windows</li></ul>
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM software de base de datos DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li></ul>

Objetivo	Producto y descripción	Instrucciones de instalación
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se han completado sin concluir servidores IBM Domino.	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> </ul>
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se han completado sin concluir servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de DB2 en el servidor IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de Informix en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection for SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales almacenadas en un servidor centralizado, crear políticas de copia de seguridad y restaurar máquinas virtuales o archivos individuales.</p> <p>De forma alternativa, utilice el cliente de archivado y copia de seguridad para hacer la copia de seguridad y restauración de una máquina virtual de VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for Microsoft Hyper-V</li> <li>• Instalación y actualización de Data Protection for VMware</li> <li>• Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)</li> </ul>

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

## Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente



Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

## Antes de empezar

---

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

## Acerca de esta tarea

---

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el periodo de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro de cliente, se asigna un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activas* activo.

Cuando un cliente realiza la copia de seguridad o el archivado de un archivo, el archivo se vincula a una clase de gestión del conjunto de políticas activas activo del dominio de políticas. Una *clase de gestión* es el conjunto de claves de reglas para gestionar los datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo local editable del sistema cliente y en un conjunto de opciones de cliente en el servidor. Las opciones del conjunto de opciones de cliente en el servidor pueden alterar temporalmente las opciones del archivo de opciones del cliente local o añadirse a dichas opciones.

## Procedimiento

---

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

## Visualización de políticas

---

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

## Procedimiento

---

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
  - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
  - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
  - c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

## Edición de políticas

---

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

## Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

## Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

## Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
<b>Añadir una clase de gestión</b>	<ol style="list-style-type: none"><li>a. En la tabla Conjuntos de políticas, pulse +Clase de gestión.</li><li>b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión.</li><li>c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada.</li><li>d. Pulse Añadir.</li></ol>
<b>Suprimir una clase de gestión</b>	En la columna Clase de gestión, pulse -. Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.
<b>Establecer una clase de gestión como clase de gestión predeterminada</b>	En la columna Predeterminada para la clase de gestión, pulse el botón de selección. Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.
<b>Modificar una clase de gestión</b>	Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.

6. Pulse Guardar.  
Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:
  - a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
  - b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.

- c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

## Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

### Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


### Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


### Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menú Centro de operaciones. Pulse Planificaciones.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
<b>Modificar una planificación</b>	<ol style="list-style-type: none"><li>a. En la vista Planificaciones, seleccione la planificación y pulse Detalles.</li><li>b. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas.</li><li>c. Modifique los valores de la planificación y pulse Guardar.</li></ol>
<b>Crear una planificación</b>	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
  - a. En la página Visión general del Centro de operaciones, pase el ratón por encima del icono de configuración  y pulse Creador de mandatos.
  - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

#### Tareas relacionadas:

-  Ajuste de la planificación para las operaciones diarias

## Registro de clientes

Registrar un cliente para garantizar que el cliente pueda conectarse con el servidor y el servidor pueda proteger los datos de cliente.

### Antes de empezar

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

## Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre\_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Clientes.
  - b. En la tabla Clientes, pulse + Cliente.
  - c. Complete los pasos en el asistente Añadir cliente:
    - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
    - ii. En la ventana Configuración, copie los valores de opción TCPSEVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.  
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
    - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
    - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
    - v. Pulse Añadir cliente.

### Referencia relacionada:

- 🔗 Opción Tcpserveraddress
- 🔗 Opción Tcpport
- 🔗 Opción Nodename
- 🔗 Opción Deduplication

## Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

## Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:
  - o Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li><li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li></ul> Para obtener información sobre el despliegue manual de actualizaciones de clientes del servidor, consulte los documentos siguientes: <ul style="list-style-type: none"><li>■ Para los servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.</li><li>■ Para servidores IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0, y servidores V8.1.1, consulte la nota técnica 1673299.</li></ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"><li>■ Instalación de Data Protection for Oracle</li><li>■ Instalación de Data Protection for SQL Server en Windows Server Core</li></ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"><li>■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li><li>■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li><li>■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>

Software	Enlace a instrucciones
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li> </ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> <li>■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li> <li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul>
Si planea crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo de cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> <li>■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments</li> </ul> <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSEVERADDRESS, TCPSPORT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (Registro de clientes).
  - Para los clientes que están instalados en un sistema operativo AIX, Linux o Mac OS X, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
  - Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt. De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de clientes en el cliente. Siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones que encontrará en Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones que encontrará en Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
  - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

## Qué hacer a continuación

Si necesita cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones que encontrará en Modificación del ámbito de una copia de seguridad de cliente.

## Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

## Acerca de esta tarea

El método preferido es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Utilizando el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que las operaciones planificadas se pueden producir.

Si la empresa utiliza una herramienta de planificación de terceros como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Normalmente, las herramientas de planificación de terceros inician los programas cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

## Procedimiento

---

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones para el sistema operativo que está instalado en el nodo cliente.

### AIX y Oracle Solaris

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- Para permitir que el aceptador de cliente se inicie automáticamente después del reinicio de un sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```

### Linux

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente iniciando sesión con el ID de usuario `root` y emitiendo el mandato siguiente:

```
service dsmcad start
```

- Para permitir que el aceptador de cliente pueda iniciarse automáticamente después del reinicio de un sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

## MAC OS X

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- b. Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- c. Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- d. Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- e. Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

## Windows

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- b. Consulte la información en la página Asistente del planificador y pulse Siguiente.
- c. En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- d. En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- e. Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- f. Complete la configuración paso a paso a través del asistente.
- g. Actualice el archivo de opciones de cliente, dsm.opt, y configure la opción passwordaccess como generate.
- h. Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- i. Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El servicio de planificador se ha iniciado y detenido automáticamente mediante el servicio aceptador de cliente, según sea necesario.

## Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

---

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

### Antes de empezar

---

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores de opción en el archivo de opciones de cliente que ha obtenido durante ese proceso. Puede utilizar los valores para especificar puertos.

### Acerca de esta tarea

---

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

### Procedimiento

---

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción tcpport en el archivo de opciones de cliente. La opción tcpport del archivo de opciones de cliente debe coincidir con la opción TCPPORT en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción httpport en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción webports en el archivo de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción tcpadminport de cliente debe coincidir con el valor de la opción de servidor TCPADMINPORT. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.

## Gestión de operaciones de cliente

---

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

### Acerca de esta tarea

---

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- Evaluación de errores en registros de errores de cliente  
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- Detención y reinicio del aceptador de cliente  
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- Restablecimiento de contraseñas  
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- Modificación del ámbito de una copia de seguridad de cliente  
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

## Evaluación de errores en registros de errores de cliente

---

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

### Antes de empezar

---

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación Instalación del servicio de gestión de cliente. Para obtener instrucciones sobre cómo verificar la instalación, consulte Verificación de que el servicio de gestión de clientes está instalado correctamente.

### Procedimiento

---

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Detalles.
  3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
  4. Revise los mensajes de registro recuperados.  
Sugerencias:
    - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.



- Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.

- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

## Detención y reinicio del aceptador de cliente

---

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

### Acerca de esta tarea

---

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

### Procedimiento

---

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
  - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Para iniciar el aceptador de cliente, emita el mandato siguiente:


```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.

- c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Iniciar y Aceptar.

**Referencia relacionada:**

 Resolución de problemas de planificación del cliente

## Restablecimiento de contraseñas

---

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

### Procedimiento

---

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nodo cliente y *nueva\_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como `generar` en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva\_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:

1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nombre del nodo y *nueva\_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como `generar` en el archivo de opciones del cliente.

## Modificación del ámbito de una copia de seguridad de cliente

---

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

### Acerca de esta tarea

---

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete

de licencia, también podrá reducir los costes de licencia.

## Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones que encontrará en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Para obtener información detallada al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción dominio. Siga las instrucciones que encontrará en Opción de cliente Domain.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

## Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

### Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

## Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>• Actualización del cliente de archivado y copia de seguridad</li></ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li></ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"><li>• Actualización de Data Protection for SQL Server</li><li>• Instalación de Data Protection for Oracle</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li></ul>

Software	Enlace a instrucciones
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> <li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> <li>• Instalación y actualización de Data Protection for VMware</li> <li>• Instalación de Data Protection for Microsoft Hyper-V</li> </ul>

## Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

### Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

## Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
  1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
  2. Pulse Más > Poner fuera de servicio.
- Para que un nodo cliente quede fuera de servicio utilizando un mandato administrativo, realice una de las siguientes acciones:
  - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
  - Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
  - Un valor null especifica que el nodo no está fuera de servicio.
  - Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

Proceso proceso	Descripción proceso	Estado proceso
----- 3	----- DECOMMISSION NODE	----- Número de objetos de copia de seguridad desactivados para el nodo NODE1: 8 objetos desactivados.

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

### Referencia relacionada:

[DECOMMISSION NODE \(Poner fuera de servicio un nodo de cliente\)](#)

[DECOMMISSION VM \(Poner fuera de servicio una máquina virtual\)](#)

## Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando

caduca. De este modo, puede liberar espacio en el servidor.

## Acerca de esta tarea

---

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

## Procedimiento

---

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.  
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

### Referencia relacionada:

 [DEACTIVATE DATA \(Desactivar datos para un nodo de cliente\)](#)


## Gestión del almacenamiento de datos

---

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Auditoría de un contenedor de la agrupación de almacenamiento  
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.
- Gestión de la capacidad de inventario  
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- Gestión del uso de la memoria y del procesador  
Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.
- Ajuste de actividades planificadas  
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

### Referencia relacionada:

 [Tipos de agrupaciones de almacenamiento](#)

## Auditoría de un contenedor de la agrupación de almacenamiento

---

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.

## Acerca de esta tarea

---

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

## Procedimiento

---

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 000000000000076c.dcf:

```
audit container c:\tsm-storage\07\000000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

## Qué hacer a continuación

---

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Emita el mandato AUDIT CONTAINER y especifique el nombre del contenedor.

### Referencia relacionada:

- 🔗 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- 🔗 QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

## Gestión de la capacidad de inventario

---

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

### Antes de empezar

---

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

### Procedimiento

---

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
    - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
    - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.
- Sugerencias:
- El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
  - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
  - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
  - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.

- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:

Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPAC1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
```

```

db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX

```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
  5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la compresión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la compresión del registro de archivado de forma inmediata sin detener el servidor.

#### Referencia relacionada:

- ➔ ACTIVELOGSIZE, opción de servidor
- ➔ EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- ➔ SETOPT (Establecer una opción de servidor para actualización dinámica)

## Gestión del uso de la memoria y del procesador

Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.



## Antes de empezar

---

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos admitidos para IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

## Procedimiento

---

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

## Ajuste de actividades planificadas

---

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

## Procedimiento

---

1. Supervise el rendimiento de sistema de forma periódica para asegurarse de que las tareas de copia de seguridad y mantenimiento se completan correctamente. Para obtener más información sobre supervisión, consulte Supervisión de una solución de disco de sitio único.
2. Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, tal vez tenga que revisar la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
  - El número de clientes aumenta.
  - La cantidad de datos de los que se hace copia de seguridad aumenta.
  - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución tiene problemas de rendimiento. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
  - b. Pulse Detalles.
  - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos.Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.
4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
  - a. Copia de seguridad de la base de datos
  - b. Ejecutar la caducidad para eliminar las copias de seguridad de cliente y las copias de archivo de archivado del almacenamiento de servidor.

### Conceptos relacionados:

[Rendimiento](#)

### Tareas relacionadas:

[Deduplicación de datos \(V7.1.1\)](#)

## Protección del servidor IBM Spectrum Protect

---

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- Conceptos sobre la seguridad  
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- Gestión de administradores  
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

- Cambio de los requisitos de contraseña  
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- Protección del servidor en el sistema  
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

## Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

### Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

### Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

### Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.

Característica	Más información
Caducidad de la contraseña predeterminada	90 días.  El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

## Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos de cliente	<ul style="list-style-type: none"> <li>• REGISTER NODE</li> <li>• UPDATE NODE</li> </ul>
Administradores	<ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul>
Servidores	<ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul>


Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

### Tareas relacionadas:

 Protección de las comunicaciones

## Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

### Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:  a. Registre el administrador y especifique Pa\$#\$twO como contraseña ejecutando el siguiente mandato: <pre>register admin admin1 Pa\$#\$twO</pre> b. Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre>
Cambie los permisos del administrador.	Cambie el nivel de autorización de un administrador, ADMIN1.  • Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> • Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <pre>revoke authority admin1 classes=system</pre>
Elimine administradores.	Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect: <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.

## Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

### Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

### Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
-------	---------------

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</p> <p>c. Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</p> <p>El valor predeterminado en la instalación es 0.</p>
Establezca una longitud mínima para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establezca el número de caracteres en el campo Longitud de contraseña mínima.</p>
Establezca el periodo de caducidad para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establecer el número de días en el campo Caducidad común de la contraseña.</p>
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.</p> <p>Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

**Conceptos relacionados:**

- 🔗 Autenticación de usuarios de IBM Spectrum Protect utilizando un servidor LDAP
- 🔗 Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

## Protección del servidor en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

### Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor  
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.
- Limitación de acceso a través de restricciones de puerto  
Limitar acceso al servidor aplicando restricciones de puerto.

## Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

### Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
  - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
  - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grabe en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique el parámetro BACKUPINITIATION=root:

```
update node backupinitiation=root
```

## Limitación de acceso a través de restricciones de puerto

Limitar acceso al servidor aplicando restricciones de puerto.

### Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

### Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPSPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPSPORT.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPSPORT y SSLTCPSPORT.
SSLTCPSPORT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.
SSLTCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPSPORT y SSLTCPSPORT.

#### Referencia relacionada:

Planificación del acceso de cortafuegos

# Detención e inicio del servidor

---

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

## Antes de empezar

---

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**  
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- **Inicio del servidor para tareas de mantenimiento o reconfiguración**  
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Detención del servidor

---

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

## Acerca de esta tarea

---

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

## Procedimiento

---

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:
  - a. En la página *Visión general del Centro de operaciones*, vea el área *Actividad* para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.
  - b. Vea el gráfico en el área *Actividad* para comparar la cantidad de tráfico de red durante los periodos siguientes:
    - El periodo actual, es decir, el periodo de 24 horas más reciente
    - El periodo anterior, es decir, 24 horas antes del periodo actualSi el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.
  - c. En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.
3. Espere hasta que las sesiones de nodo cliente se completen o cáncelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:
  - En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*.
  - Pulse el separador *Tareas activas* y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - Pulse *Cancelar*.
  - Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.

Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.

4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

## Inicio del servidor para tareas de mantenimiento o reconfiguración

---

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, dsmserv.opt, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

### Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

### Qué hacer a continuación




---

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:

-  Sistemas operativos AIX Inicio de la instancia de servidor
-  Sistemas operativos Linux Inicio de la instancia de servidor
-  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

## Planificación para actualizar el servidor

---

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

### Acerca de esta tarea

---



Siga estas directrices:

- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

## Procedimiento




---

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.  
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

## Qué hacer a continuación

---

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

### Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

## Preparación para una parada o actualización de sistema

---

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

## Acerca de esta tarea

---

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor.

## Procedimiento

---

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
  - a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
  - b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - c. Pulse Cancelar.

2. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

## Implementación de un plan de recuperación tras desastre

---

Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

## Acerca de esta tarea

---

Determine los requisitos que necesita para recuperación tras desastre identificando las prioridades empresariales respecto a la recuperación de nodo de cliente, los sistemas que utiliza para recuperar datos y si los nodos de cliente tienen conectividad con el

servidor de recuperación. Utilice la réplica y la protección de agrupación de almacenamiento para proteger datos. También debe determinar la frecuencia con la que se protegen las agrupaciones de almacenamiento de contenedores de directorio.

- Realización de la obtención de detalles de recuperación  
Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

## Recuperación de paradas del sistema

Para soluciones de disco de sitio único de IBM Spectrum Protect, puede recuperar el inventario localmente únicamente y restaurar la base de datos para proteger los datos.

### Procedimiento

Utilice uno de los métodos siguientes para recuperar el inventario para un sitio local, basado en el tipo de información del que se hace copia de seguridad.

Restricción: Puesto que las soluciones de disco de sitio único no tienen una segunda copia de la agrupación de almacenamiento, no puede restaurar las agrupaciones de almacenamiento. Para revisar la arquitectura de las soluciones de disco, consulte Selección de una solución de IBM Spectrum Protect.

Tabla 1. Escenarios para la recuperación tras un desastre

Escenario	Procedimiento
El sistema está inaccesible y desea restaurar localmente a una versión anterior utilizando las herramientas del sistema.	<ul style="list-style-type: none"> <li>• Utilice IBM Spectrum Protect para hacer copia de seguridad del servidor a otro servidor.</li> <li>• Utilice las herramientas del sistema operativo para hacer copia de seguridad y restaurar el sistema a una versión anterior.</li> </ul>
Se ha producido una parada o desastre y desea restaurar datos desde las versiones de copia de seguridad de los datos.	<ul style="list-style-type: none"> <li>• Para hacer copia de seguridad de un cliente, en la página Clientes de TSM de Centro de operaciones, seleccione los clientes a los que desea hacer copia de seguridad y pulse Hacer copia de seguridad.</li> <li>• En la página Servidores de TSM de Centro de operaciones, seleccione el servidor de cuya base de datos desea hacer copia de seguridad. Pulse Copia de seguridad y siga las instrucciones que encontrará en la ventana Copia de seguridad de la base de datos del servidor.</li> </ul> <p>Para restaurar una agrupación de almacenamiento de una versión de copia de seguridad de la agrupación de almacenamiento, debe restaurar la base de datos. Emita el mandato DSMSERV RESTORE DB para restaurar la base de datos y las agrupaciones de almacenamiento asociadas a una versión de copia de seguridad.</p>

- Restauración de la base de datos  
Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

#### Referencia relacionada:

- ➔ [AUDIT CONTAINER](#) (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- ➔ [DSMSERV RESTORE DB](#) (Restaurar la base de datos)

## Solución de disco multisitio

Esta solución de protección de datos proporciona réplica en varios sitios para que cada servidor proteja los datos del otro.

- Planificación de una solución de protección de datos de disco multisitio  
Planifique una solución de protección de datos de disco multisitio con servidores en dos sitios que utilizan la deduplicación y la réplica de datos.
- Implementación de disco multisitio de una solución de protección de datos  
La solución de disco multisitio se configura en dos sitios y utiliza la deduplicación y réplica de datos.
- Supervisión de una solución de disco multisitio  
Después de implementar una solución de disco multisitio con IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.
- Gestión de operaciones para una solución de disco multisitio  
Utilice esta información para gestionar operaciones para una solución de disco multisitio con IBM Spectrum Protect que incluye un servidor y utiliza la eliminación de datos duplicados para varias ubicaciones.

## Planificación de una solución de protección de datos de disco multisitio

---

Planifique una solución de protección de datos de disco multisitio con servidores en dos sitios que utilizan la deduplicación y la réplica de datos.

### Métodos de implementación

---

Puede configurar servidores para una solución de disco multisitio de las maneras siguientes:

Configure servidores utilizando los mandatos de Centro de operaciones y administrativos

Puede configurar un rango de sistemas de almacenamiento y el software de servidor para la solución. Las tareas de configuración se realizan mediante asistentes y opciones del Centro de operaciones y mandatos de IBM Spectrum Protect. Para obtener información sobre cómo empezar, consulte Hoja de vía de acceso de planificación.

Configure los servidores utilizando scripts automatizados

Para obtener instrucciones detalladas sobre la configuración con sistemas de almacenamiento de IBM® Storwize específicos y utilizando scripts automatizados para configurar cada servidor, consulte los blueprints de IBM Spectrum Protect. La documentación y los scripts están disponibles en IBM developerWorks en: IBM Spectrum Protect Blueprints.

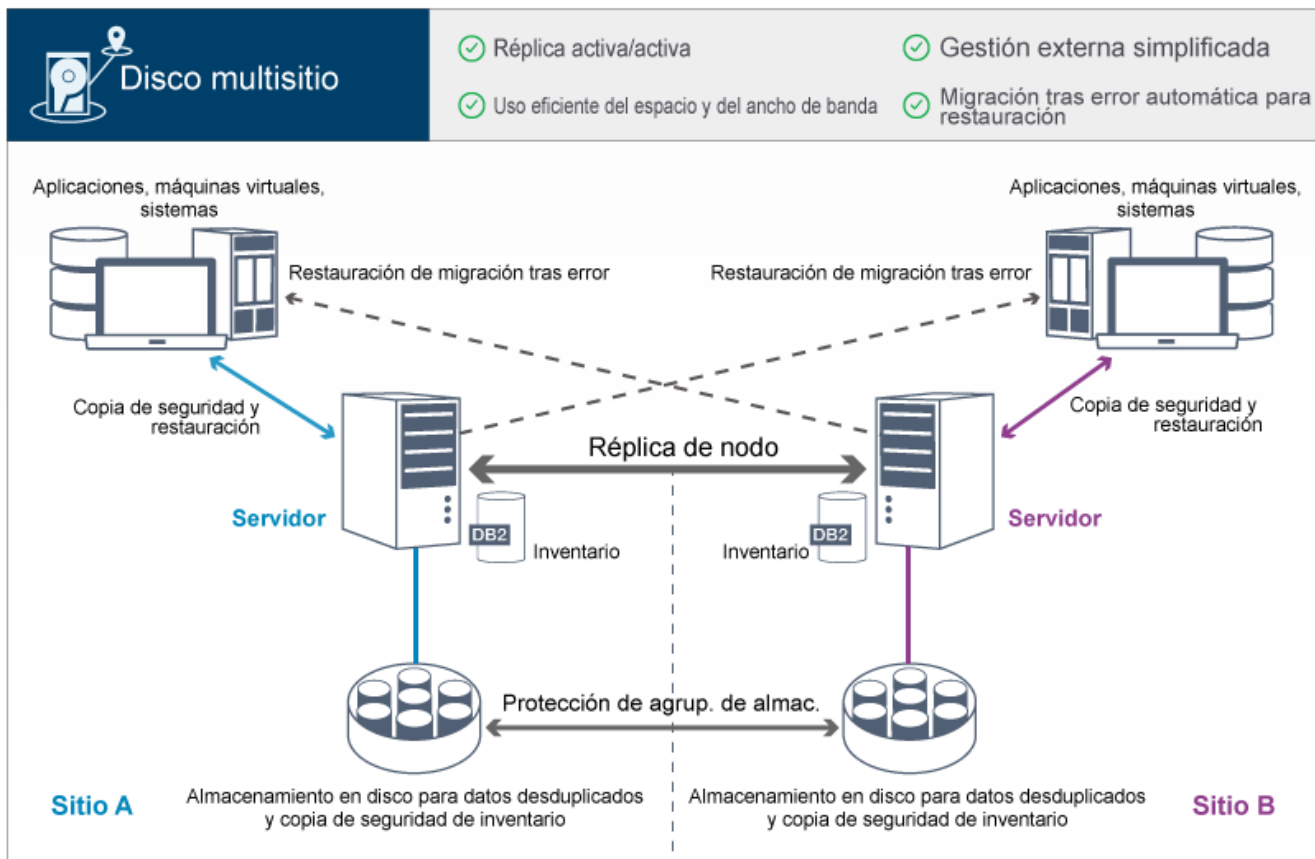
La documentación blueprint no incluye pasos para la instalación y configuración de Centro de operaciones, o el establecimiento de comunicaciones seguras utilizando la capa de seguridad de transporte (TLS). La réplica se configura utilizando mandatos después de que se haya configurado cada servidor. Se incluye una opción para utilizar Elastic Storage Server, que se basa en la tecnología IBM Spectrum Scale.

### Hoja de vía de acceso de planificación

---

Planifique una solución de disco multisitio revisando el diseño de arquitectura en la siguiente figura y, a continuación, completando las tareas de la hoja de ruta que siguen al diagrama.

Figura 1. Solución de disco multisitio



Los pasos siguientes son necesarios para planificar correctamente un entorno de disco multisitio.

1. Seleccionar el tamaño de sistema.
2. Planificar los sitios.
3. Cumplir los requisitos de sistema para hardware y software.
4. Registrar valores para la configuración de sistema en las hojas de trabajo de planificación.
5. Planificar el almacenamiento.
6. Planificar la seguridad.
  - a. Planificar los roles de administrador.
  - b. Planificar las comunicaciones seguras.
  - c. Planificar el almacenamiento de datos cifrados.
  - d. Planificar el acceso de cortafuegos.

## Selección de un tamaño del sistema

Seleccione el tamaño del servidor de IBM Spectrum Protect basándose en la cantidad de datos que gestiona y los sistemas que se deben proteger.

### Acerca de esta tarea

Puede utilizar la información de la tabla para determinar el tamaño del servidor que se necesita, en función de la cantidad de datos que gestione.

La tabla siguiente describe el volumen de datos que gestiona un servidor. Esta cantidad incluye todas las versiones. La cantidad diaria de datos es la cantidad de datos nuevos a la que hace copia de seguridad cada día. Los datos gestionados totales y la cantidad diaria de datos nuevos se miden como el tamaño antes de la reducción de datos.

Tabla 1. Determinación del tamaño del servidor

Total de datos gestionados	Cantidad diaria de datos nuevos de los que se debe hacer copia de seguridad	Tamaño de servidor necesario
48 TB - 192 TB	Hasta 10 TB al día	Pequeño
200 TB - 800 TB	10 - 20 TB al día	Mediano
1000 TB - 4000 TB	20 - 100 TB al día	Grande

Los valores de copia de seguridad diaria de la tabla se basan en los resultados de prueba con objetos de 128 MB de tamaño, utilizados por IBM Spectrum Protect for Virtual Environments. Es posible que las cargas de trabajo que constan de objetos que tienen menos de 128 KB no puedan conseguir estos límites diarios.

## Planificación de los sitios

---

Revise los casos de uso y evalúe los factores para proporcionar la protección de datos más eficiente para la solución de disco multisitio para IBM Spectrum Protect.

### Casos de uso

---

La solución de disco multisitio crea al menos una copia de los datos de copia de seguridad. Si los servidores de IBM Spectrum Protect están en ubicaciones independientes, la réplica de copia de seguridad se mantiene fuera del local. Aunque su compañía puede beneficiarse de una solución de disco multisitio por diversos motivos, los motivos más comunes para utilizar una solución de disco multisitio incluyen los siguientes escenarios de réplica:

#### Réplica del sitio primario en el sitio de recuperación tras desastre

En este escenario, los datos de los que se hace una copia de seguridad desde el sitio primario, Sitio A, se replican en un servidor en el sitio secundario de recuperación tras desastre, sitio B. Si se produce un siniestro en el sitio A, como por ejemplo una anomalía del servidor, puede utilizar el servidor en el Sitio B para recuperar sistemas. De forma alternativa, puede utilizar el servidor en el Sitio A para restaurar los datos de agrupación de almacenamiento primario en el Sitio B, por ejemplo después de una anomalía de almacenamiento de disco en el Sitio B.

#### Réplica mutua en dos sitios activos

En este escenario, los servidores realizan la copia de seguridad de los datos locales de cada sitio tanto en el Sitio A como en el Sitio B. Los datos de los que se hace copia de seguridad desde el Sitio A se replican en el Sitio B y los datos de los que se ha hecho copia de seguridad desde el Sitio B se replican en el Sitio A. Si los datos de los que se ha hecho copia de seguridad se pierden en el Sitio A, puede utilizar el servidor en el Sitio B para recuperar los datos de agrupación de almacenamiento en el servidor en el Sitio A. Si el Sitio A ya no está disponible, puede recuperar los datos replicados para el Sitio A en un sistema nuevo del sitio B. Debe dimensionar los recursos de servidor para asegurarse de que ambos servidores tienen suficiente capacidad para realizar la copia de seguridad y la restauración de todos los nodos de cliente como parte del plan de recuperación tras desastre.

#### Proteger servidores remotos en el sitio primario

En este escenario, debe configurar servidores remotos que son relativamente pequeños para replicar los datos de copia de seguridad en un servidor más grande en el sitio primario. Si el ancho de banda es limitado, puede que no sea práctico restaurar sistemas en los sitios remotos. En este caso, es aconsejable recuperar sistemas en el sitio primario antes de replicar los datos de copia de seguridad en los servidores remotos.

## Factores que deben evaluarse

---

Antes de implementar una solución de disco multisitio, evalúe los factores siguientes:

#### Ancho de banda de red

La red debe tener suficiente ancho de banda para las transferencias de datos esperadas entre nodos, para la réplica y para las operaciones de restauración entre sitios que son necesarias para la recuperación tras desastre. Antes de continuar con la prueba de rendimiento de réplica, asegúrese de que la red puede manejar el tráfico de réplica. Calcule el ancho de banda de red necesario para el requisito de estado estable aplicando las directrices de Estimación de ancho de banda de red necesario para la réplica (V7.1.1).

La conexión de red es con frecuencia un recurso compartido. Planee la hora del día para planificar la ejecución de la réplica de nodo a fin de evitar un conflicto con otros usuarios de recurso. Asimismo, los controles de red pueden limitar la actividad a sólo una parte del ancho de banda. No hay controles en IBM Spectrum Protect para restringir el uso de red.

#### Recursos para la réplica inicial

Para configurar la solución de protección de datos entre dos sitios, debe replicar los datos inicialmente del Sitio A en el servidor de destino del sitio B. Para garantizar que la réplica inicial se realiza correctamente, debe determinar si tiene el ancho de banda de red, los recursos de procesador y el tiempo disponible para replicar los datos. Es posible que tenga que planificar la réplica de las copias de seguridad completas iniciales a lo largo de varios días. Si no se puede ampliar la planificación para las copias de seguridad iniciales, puede replicar datos del Sitio A en el Sitio B sin utilizar la red. Por ejemplo, puede exportar e importar los datos de copia de seguridad utilizando soportes o temporalmente puede ubicar los servidores de origen y destino en el mismo sitio.

## Ingestión de datos diaria

Para la solución de disco multisitio, la ingestión de datos diaria y la retención de datos total deben estar dentro de la capacidad de las configuraciones. Por ejemplo, una configuración grande tiene una capacidad de ingestión de datos de hasta 100 TB por día, incluida la réplica de nodos. En los casos en que los requisitos de copia de seguridad superan la capacidad de un solo servidor, puede configurar una solución que utilice varios servidores para alcanzar la capacidad necesaria.

## Configuración del servidor

La configuración de servidor debe cumplir o superar los requisitos para la solución de disco multisitio.

## Réplica única de datos de copia de seguridad

La solución de disco multisitio es más eficaz cuando una única copia fuera de sitio de los datos de copia de seguridad cumple los requisitos de protección de datos y mitigación de riesgos. En este caso, la única copia de los datos se mantiene fuera del local en la ubicación de un servidor de réplica.

### Referencia relacionada:

Requisitos del sistema para una solución de disco multisitio

## Requisitos del sistema para una solución de disco multisitio

Después de seleccionar la solución IBM Spectrum Protect que mejor se ajuste a los requisitos de protección de datos, revise los requisitos de sistema para planificar la implementación de la solución de protección de datos.

Asegúrese de que el sistema cumple los requisitos previos de hardware y software para el tamaño de servidor que desea utilizar.

- **Requisitos de hardware**  
Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.
- **Requisitos de software**  
La documentación para la solución de disco multisitio de IBM Spectrum Protect incluye las tareas de instalación y configuración para los siguientes sistemas operativos. Debe cumplir los requisitos de software mínimos que se indican.

### Información relacionada:










[Sistemas operativos admitidos para IBM Spectrum Protect](#)

## Requisitos de hardware

Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

Para obtener una definición de los tamaños de sistema, consulte Selección de un tamaño del sistema.

La tabla siguiente incluye requisitos de hardware mínimos para el servidor y el almacenamiento, en función del tamaño del servidor que planea crear. Si utiliza particiones locales (LPAR) o particiones de trabajo (WPAR), ajuste los requisitos de red para tener en cuenta los tamaños de las particiones.

Componente de hardware	Sistema pequeño	Sistema mediano	Sistema grande
Procesador de servidor	 Sistemas operativos AIX6 núcleos de procesador, 3,42 GHz o más rápido   Sistemas operativos Linux  Sistemas operativos Windows 12 núcleos de procesador, 1,9 GHz o más rápido	 Sistemas operativos AIX8 núcleos de procesador, 3,42 GHz o más rápido   Sistemas operativos Linux  Sistemas operativos Windows 16 núcleos de procesador, 2,0 GHz o más rápido	 Sistemas operativos AIX20 núcleos de procesador, 3,42 GHz   Sistemas operativos Linux  Sistemas operativos Windows 32 núcleos de procesador, 2,0 GHz o más rápido
Memoria de servidor	64 GB RAM	128 GB RAM	192 GB RAM
Red	<ul style="list-style-type: none"><li>• Ethernet de 10 GB (1 puerto)</li><li>• Adaptador de canal de fibra de 8 GB (2 puertos)</li></ul>	<ul style="list-style-type: none"><li>• Ethernet de 10 GB (2 puertos)</li><li>• Adaptador de canal de fibra de 8 GB (2 puertos)</li></ul>	<ul style="list-style-type: none"><li>• Ethernet de 10 GB (4 puertos)</li><li>• Adaptador de canal de fibra de 8 GB (4 puertos)</li></ul>

Componente de hardware	Sistema pequeño	Sistema mediano	Sistema grande
Almacenamiento	<ul style="list-style-type: none"> <li>• 1.3 TB de inventario, más espacio para registros de Centro de operaciones.</li> <li>• Agrupación de almacenamiento de contenedores de directorio deduplicada de 46 TB</li> </ul>	<ul style="list-style-type: none"> <li>• 2 TB de inventario, más espacio para registros de Centro de operaciones</li> <li>• Agrupación de almacenamiento de contenedores de directorio deduplicada de 200 TB</li> </ul>	<ul style="list-style-type: none"> <li>• 6 TB de inventario, más espacio para registros de Centro de operaciones</li> <li>• Agrupación de almacenamiento de contenedores de directorio deduplicada de 1000 TB</li> </ul>

## Estimación de requisitos de espacio de base de datos para Centro de operaciones

Los requisitos de hardware para Centro de operaciones se incluyen en la tabla anterior, excepto para la base de datos y el espacio de registro de archivado (inventario) que utiliza Centro de operaciones para contener registros para clientes gestionados.

Si no piensa instalar el Centro de operaciones en el mismo sistema que servidor, puede calcular requisitos de sistema por separado. Para calcular requisitos del sistema para Centro de operaciones, consulte la calculadora de requisitos del sistema en la nota técnica 1641684.

La gestión del Centro de operaciones en el servidor es una carga de trabajo que necesita espacio adicional para las operaciones de base de datos. La cantidad de espacio depende del número de clientes supervisados en un servidor. Revise las directrices siguientes para estimar cuánto espacio requiere el servidor.

### Espacio de base de datos

El Centro de operaciones utiliza aproximadamente 1,2 GB de espacio de base de datos por cada 1000 clientes supervisados en un servidor. Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1500 clientes. Esta configuración tiene un total de 6500 clientes en los cuatro servidores y necesita aproximadamente 8,4 GB de espacio de base de datos. Este valor se calcula redondeando los 6500 clientes al 1000 más próximo, que es 7000:

$$7 \times 1.2 \text{ GB} = 8.4 \text{ GB}$$

### Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 8 GB de espacio de registro de archivado cada 24 horas por cada 1000 clientes. En el ejemplo de 6500 clientes en el servidor concentrador y los servidores spoke, se utilizan 56 GB de espacio de registro de archivado a lo largo de un período de 24 horas para el servidor concentrador.

Para cada servidor de radio en el ejemplo, el espacio del registro de archivado que se utiliza a lo largo de 24 horas es aproximadamente 16 GB. Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en el requisito de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos:

- servidor concentrador: de 56 GB a 94 GB aproximadamente
- Cada servidor spoke: de 16 GB a 28 GB aproximadamente

Aumente el espacio de registro de archivado para tener espacio suficiente para proporcionar soporte a Centro de operaciones, sin que afecte a las operaciones de servidor existentes.

## Requisitos de hardware para el segundo servidor

Si tiene planificado configurar los sitios, de forma que todo lo del primer sitio se duplica en el segundo sitio, los requisitos de hardware son idénticos en ambos sitios. Si sólo desea replicar un subconjunto de datos para el segundo sitio, los requisitos de almacenamiento y red se pueden reducir.

## Requisitos de software

La documentación para la solución de disco multisitio de IBM Spectrum Protect incluye las tareas de instalación y configuración para los siguientes sistemas operativos. Debe cumplir los requisitos de software mínimos que se indican.

Para obtener información sobre los requisitos de software para los controladores de dispositivo lin\_tape de IBM®, consulte IBM Tape Device Drivers Installation and User's Guide.

## Sistemas AIX

Tipo de software	Requisitos mínimos de software
Sistema operativo	IBM AIX 7.1  Para obtener más información sobre los requisitos del sistema operativo, consulte AIX: requisitos mínimos del sistema para sistemas AIX.
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema antes de instalar o actualizar el servidor de IBM Spectrum Protect . Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.
Tipo de sistema de archivos	Sistemas de archivos JFS2  Los sistemas AIX pueden almacenar en caché una gran cantidad de datos del sistema de archivos y esto puede reducir la memoria que se necesita para el servidor y los procesos de IBM DB2. Para evitar la paginación con el servidor de AIX, utilice la opción de montaje rbrw mount para el sistema de archivos JFS2. Se utiliza menos memoria para la memoria caché de sistema de archivo y hay más disponible para IBM Spectrum Protect.  No utilice las opciones de montaje del sistema de archivos, E/S simultáneas (CIO) y E/S directas (DIO), para sistemas de archivos que contengan la base de datos de IBM Spectrum Protect, registros o volúmenes de agrupaciones de almacenamiento. Estas opciones pueden producir la degradación del rendimiento de muchas operaciones de servidor. IBM Spectrum Protect y DB2 aún pueden utilizar DIO donde sea beneficioso hacerlo, pero IBM Spectrum Protect no necesita las opciones de montaje para aprovechar estas técnicas de forma selectiva.
Otro software	Shell Korn (ksh)

## Sistemas Linux

Tipo de software	Requisitos mínimos de software
Sistema operativo	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	Bibliotecas de GNU C, versión 2.3.3-98.38 o posterior que está instalado en el sistema de IBM Spectrum Protect. Red Hat Enterprise Linux Servers: <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits)</li> <li>• numactl.x86_64</li> </ul>
Tipo de sistema de archivos	Formato de sistemas de archivos relacionados con bases de datos con ext3 o ext4.  Para los sistemas de archivos relacionados con agrupaciones de almacenamiento, utilice XFS.
Otro software	Shell Korn (ksh)

## Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS
Otro software	Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado.  Se deben desactivar las siguientes políticas de Control de la cuenta de usuario: <ul style="list-style-type: none"> <li>• Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada</li> <li>• Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador</li> </ul>

### Tareas relacionadas:

- 🔗 Establecimiento de las opciones de red de AIX



## Planificación de hojas de trabajo

Utilice las hojas de trabajo de planificación para registrar los valores que se utilizan para configurar el sistema y configurar el servidor de IBM Spectrum Protect. Utilice los valores predeterminados de prácticas recomendadas que aparecen en las hojas de trabajo.

Cada hoja de trabajo le ayuda a prepararse para diferentes partes de la configuración del sistema utilizando valores de las prácticas recomendadas:

### Configuración previa de sistema servidor

Utilice las hojas de trabajo de configuración previa para planificar los sistemas de archivos y directorios que se crean al configurar sistemas de archivos para IBM Spectrum Protect durante la configuración del sistema. Todos los directorios que crea para el servidor deben estar vacíos.

### Configuración del servidor

Utilice las hojas de trabajo de configuración cuando configure el servidor. Los valores predeterminados se recomiendan para la mayoría de los elementos, excepto donde se indica.

## AIX

Tabla 1. Hoja de trabajo para configuración previa de un sistema servidor AIX

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo  El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		50 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 2.
Directorio para la instalación del servidor	/		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/usr		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/var		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/tmp		Espacio disponible que es necesario para el directorio: 5 GB	
Directorio para la instalación del servidor	/opt		Espacio disponible que es necesario para el directorio: 10 GB	

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 2. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 1 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		

Elemento	Valor predeterminado	Valor	Notas
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p>

## Linux

Tabla 3. Hoja de trabajo para la configuración previa de un sistema servidor Linux

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	<p>Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo</p> <p>El número de puerto puede ser un número dentro del rango 1024 - 32767.</p>
Directorio para la instancia de servidor	/home/tsminst1/tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 4.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para el registro activo	/tsminst1/TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	
Directorio para el registro de archivado	/tsminst1/TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	/tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	/tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	/tsminst1/TSMbkup00 /tsminst1/TSMbkup01 /tsminst1/TSMbkup02 /tsminst1/TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 4. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 3 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	tsmsrvrs		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		

Elemento	Valor predeterminado	Valor	Notas
Contraseña del servidor	passwd0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passwd0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.  Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.

## Windows

Dado que muchos volúmenes se crean para el servidor, configure el servidor utilizando la característica de Windows de correlación de volúmenes de disco con directorios en lugar de letras de unidad.

Por ejemplo, C:\tsminst1\TSMdbpsace00 es el punto de montaje para un volumen con su propio espacio. El volumen se correlaciona con un directorio bajo la unidad C:, pero no ocupa espacio de la unidad C:. La excepción es el directorio de instancia de servidor, C:\tsminst1, que puede ser un punto de montaje o un directorio normal.

Tabla 5. Hoja de trabajo para la configuración previa de un sistema servidor Windows

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo  El número de puerto puede ser un número dentro del rango 1024 - 32767.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorio para la instancia de servidor	C:\tsminst1		25 GB	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 6.
Directorio para el registro activo	C:\tsminst1\TSMalog		<ul style="list-style-type: none"> <li>• Pequeños y mediano: 140 GB</li> <li>• Grande: 300 GB</li> </ul>	
Directorio para el registro de archivado	C:\tsminst1\TSMarchlog		<ul style="list-style-type: none"> <li>• Pequeño: 1 TB</li> <li>• Mediano: 3 TB</li> <li>• Grande: 4 TB</li> </ul>	
Directorios para la base de datos	C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 1 TB</li> <li>• Mediano: Al menos 2 TB</li> <li>• Grande: Al menos 4 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 4 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 8 sistemas de archivos</li> </ul>
Directorios para almacenamiento	C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 38 TB</li> <li>• Mediano: Al menos 180 TB</li> <li>• Grande: Al menos 500 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para almacenamiento, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 10 sistemas de archivos</li> <li>• Mediano: Al menos 20 sistemas de archivos</li> <li>• Grande: Al menos 40 sistemas de archivos</li> </ul>



Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Notas
Directorios para la copia de seguridad de base de datos	C:\tsminst1\TSMbkup00 C:\tsminst1\TSMbkup01 C:\tsminst1\TSMbkup02 C:\tsminst1\TSMbkup03		<p>Espacio total mínimo para todos los directorios:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 3 TB</li> <li>• Mediano: Al menos 10 TB</li> <li>• Grande: Al menos 16 TB</li> </ul>	<p>Cree un número mínimo de sistemas de archivos para hacer copia de seguridad de la base de datos, dependiendo del tamaño del sistema:</p> <ul style="list-style-type: none"> <li>• Pequeño: Al menos 2 sistemas de archivos</li> <li>• Mediano: Al menos 4 sistemas de archivos</li> <li>• Grande: Al menos 4 sistemas de archivos, pero preferiblemente 6</li> </ul> <p>El primer directorio de la copia de seguridad de la base de datos también se utiliza para el directorio de migración tras error del registro de archivado y una segunda copia de los archivos de historial de volumen y de configuración de dispositivo.</p>

Tabla 6. Hoja de trabajo para la configuración de IBM Spectrum Protect

Elemento	Valor predeterminado	Valor	Notas
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 5 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	pAssWOrd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.

Elemento	Valor predeterminado	Valor	Notas
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	22:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p>

## Planificación de almacenamiento

Elegir la tecnología de almacenamiento más efectiva para componentes de IBM Spectrum Protect para asegurarse de que el rendimiento de servidor y las operaciones son eficientes.

Los dispositivos de hardware de almacenamiento tiene características de rendimiento y capacidad diferentes, lo que determina cómo se pueden utilizar de forma eficaz con IBM Spectrum Protect. Para obtener una orientación general sobre cómo seleccionar el hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

### Base de datos y registro activo

- Utilice un disco rápido para el registro activo y la base de datos de IBM Spectrum Protect, por ejemplo con las siguientes características:
  - Disco de alto rendimiento de 15k rpm con interfaz de canal de fibra o SCSI con conexión en serie (SAS)
  - Disco de estado sólido (SSD)
- Aísle el registro activo de la base de datos a menos que utilice el hardware de flash o SSD
- Al crear matrices para la base de datos, utilice RAID nivel 5

### Agrupación de almacenamiento

- Puede utilizar discos menos caros y más lentos para la agrupación de almacenamiento
- La agrupación de almacenamiento puede compartir discos para el registro de archivado y el almacenamiento de copias de seguridad de base de datos.
- Utilice el nivel RAID 6 para las matrices de agrupación de almacenamiento para añadir protección frente a las anomalías de unidad doble cuando se utilizan tipos de disco de gran tamaño
- Planificación de matrices de almacenamiento
  - Prepararse para la configuración de almacenamiento de disco planificando matrices RAID y volúmenes, de acuerdo con el tamaño del sistema IBM Spectrum Protect.

### Referencia relacionada:

## Planificación de la seguridad

Planee proteger la seguridad de los sistemas en la solución IBM Spectrum Protect con controles de acceso y autenticación y tenga en cuenta el cifrado de datos y la transmisión de contraseña.

- Planificación de los roles de administración  
Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.
- Planificación para comunicaciones seguras  
Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.
- Planificación de almacenamiento de datos cifrados  
Determine si la compañía requiere que se cifren los datos almacenados y elija la opción que mejor se adapta a sus necesidades.
- Planificación del acceso de cortafuegos  
Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

## Planificación de los roles de administración

Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.

Puede asignar uno de los siguientes niveles de autorización a los administradores:

### Sistema

Los administradores con autoridad del sistema tienen el nivel de autorización más alto. Los administradores con este nivel pueden realizar cualquier tarea. Pueden gestionar todos los dominios de política y agrupaciones de almacenamiento y otorgar autoridad a otros administradores.

### Política

Los administradores que tienen autorización sobre políticas pueden gestionar todas las tareas relacionadas con la gestión de políticas. Este privilegio puede no tener restricciones o puede estar restringido a dominios de políticas específicos.

### Almacenamiento

Los administradores que tienen autorización de almacenamiento pueden asignar y controlar recursos de almacenamiento para el servidor.

### Operador

Los administradores que tienen autorización de operador pueden controlar la operación inmediata del servidor y la disponibilidad de soporte de almacenamiento como unidades y bibliotecas de cintas.

Los escenarios de Tabla 1 proporcionan ejemplos de por qué es posible que desee asignar distintos niveles de autorización para que los administradores puedan realizar tareas:

Tabla 1. Escenarios para roles de administrador

Escenario	Tipo de ID de administrador a configurar
Un administrador de una pequeña empresa gestiona el servidor y es responsable de todas las actividades del servidor.	<ul style="list-style-type: none"> <li>• Autoridad del sistema: 1 ID de administrador</li> </ul>
Un administrador para varios servidores también gestiona el sistema en general. Otros diversos administradores gestionan sus propias agrupaciones de almacenamiento.	<ul style="list-style-type: none"> <li>• Autoridad del sistema en todos los servidores: 1 ID de administrador para el administrador del sistema general</li> <li>• Autoridad de almacenamiento para agrupaciones de almacenamiento designadas: 1 ID de administrador para cada uno de los otros administradores</li> </ul>
Un administrador gestiona 2 servidores. Otra persona ayuda con las tareas de administración. Dos ayudantes son responsables de ayudar a garantizar que se hace copia de seguridad de los sistemas importantes. Cada ayudante es responsable de supervisar las copias de seguridad planificadas en uno de los servidores de IBM Spectrum Protect.	<ul style="list-style-type: none"> <li>• Autoridad del sistema en ambos servidores: 2 ID de administrador</li> <li>• Autoridad de operador: 2 ID de administrador para los ayudantes con acceso al servidor del que cada persona es responsable</li> </ul>

## Planificación para comunicaciones seguras

Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.

Determine el nivel de protección necesario para los datos, basándose en las regulaciones y requisitos empresariales bajo los que opera la compañía.

Si su empresa necesita un alto nivel de seguridad para las contraseñas y la transmisión de datos, planee implementar comunicaciones seguras con protocolos de seguridad de la capa de transporte (TLS) o de capa de sockets seguros (SSL).

TLS y SSL proporcionan comunicaciones seguras entre el servidor y el cliente, pero pueden afectar al rendimiento del sistema. Para mejorar el rendimiento del sistema, utilice TLS para autenticarse sin cifrar datos de objetos. Para especificar si el servidor debe utilizar TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor y el parámetro UPDATE SERVER=SSL para la comunicación de servidor a servidor. A partir de la versión V8.1.2, se utiliza TLS para la autenticación predeterminada. Si decide utilizar TLS para cifrar sesiones enteras, utilice el protocolo solo para las sesiones en las que es necesario y añada recursos de procesador en el servidor para gestionar el incremento del tráfico de red. También puede probar otras opciones. Por ejemplo, algunos dispositivos, como los direccionadores o los conmutadores, proporcionan la función TLS o SSL.

Puede utilizar TLS y SSL para proteger todas o algunas de las distintas vías de acceso de comunicación posibles, por ejemplo:

- Centro de operaciones: De navegador a concentrador; de concentrador a radio
- Cliente a servidor
- Servidor a servidor: réplica de nodo en el servidor:

**Tareas relacionadas:**

[Protección de las comunicaciones](#)

## Planificación de almacenamiento de datos cifrados

Determine si la compañía requiere que se cifren los datos almacenados y elija la opción que mejor se adapta a sus necesidades.

Si la empresa requiere que los datos de las agrupaciones de almacenamiento estén cifrados, tiene la opción de utilizar el cifrado IBM Spectrum Protect, o un dispositivo externo como una cinta para el cifrado.

Si elige IBM Spectrum Protect para cifrar los datos, se necesitan recursos informáticos adicionales en el cliente que pueden afectar al rendimiento de los procesos de copia de seguridad y restauración.

**Información relacionada:**

[Nota técnica 1963635](#)

## Planificación del acceso de cortafuegos

Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Tabla 1 describe los puertos utilizados por el servidor, el cliente y el Centro de operaciones.

Tabla 1. Puertos utilizados por el servidor, el cliente y Centro de operaciones

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (TCPPOINT)	1500	Entrada/salida	Cada instancia de servidor necesita un puerto exclusivo. Puede especificar un número de puerto alternativo en lugar del predeterminado. La opción TCPPOINT realiza escuchas para sesiones habilitadas para TCP/IP y SSL desde el cliente. Para el tráfico de cliente administrativo, puede utilizar las opciones TCPADMINPORT y ADMINONCLIENTPORT para definir los valores de puerto.
Puerto solo SSL (SSLTCPPOINT)	No tiene valor predeterminado	Entrada/salida	Este puerto se utiliza si desea restringir la comunicación en el puerto a sesiones solo habilitadas para SSL. Para admitir tanto las comunicaciones SSL como las no SSL, utilice las opciones TCPPOINT o TCPADMINPORT.
SMB	45	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.

Elemento	Valor predeterminado	Dirección	Descripción
NDMP	No tiene valor predeterminado	Entrada/salida	<p>El servidor debe poder abrir una conexión de puerto de control NDMP de salida con el dispositivo NAS. El puerto de control de salida es la dirección de nivel inferior en la definición de transportador de datos para el dispositivo NAS.</p> <p>Durante una restauración NDMP de archivador a servidor, el servidor debe poder abrir una conexión de datos NDMP de salida con el dispositivo NAS. El puerto de conexión de datos que se utiliza durante una restauración puede configurarse en el dispositivo NAS.</p> <p>Durante las copias de seguridad NDMP de archivador a servidor, el dispositivo NAS debe poder abrir conexiones de datos de salida con el servidor y el servidor debe poder aceptar las conexiones de datos NDMP de entrada. Puede utilizar la opción de servidor NDMPPORTRANGE para restringir el conjunto de puertos disponibles para su uso como conexiones de datos NDMP. Puede configurar un cortafuegos para conexiones a estos puertos.</p>
Réplica	No tiene valor predeterminado	Entrada/salida	<p>El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica.</p> <p>Los puertos de entrada para la réplica son los puertos TCP y SSL que el servidor de origen indique en el mandato DEFINE SERVER.</p>
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesión de ejecución larga	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente-servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	El puerto de servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

## Implementación de disco multisitio de una solución de protección de datos

La solución de disco multisitio se configura en dos sitios y utiliza la deduplicación y réplica de datos.

### Hoja de ruta de la implementación

Los pasos siguientes son necesarios para configurar un entorno de disco multisitio.

1. Configurar el sistema.
  - a. Configurar el hardware de almacenamiento y las matrices de almacenamiento para el tamaño del entorno.
  - b. Instalar el sistema operativo del servidor.
  - c. Configurar la E/S de multivía de acceso.
  - d. Crear el ID de usuario de la instancia de servidor.
  - e. Preparar sistemas de archivos para IBM Spectrum Protect.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
  - a. Completar la configuración inicial del servidor.
  - b. Configurar opciones de servidor.
  - c. Configurar la capa de sockets seguros del servidor y el cliente.

- d. Configurar el Centro de operaciones.
  - e. Registrar la licencia de IBM Spectrum Protect.
  - f. Configurar la eliminación de duplicados de datos.
  - g. Definir las reglas de retención de datos para su empresa.
  - h. Definir programas de mantenimiento del servidor.
  - i. Definir programas de cliente.
4. Instalar y configurar clientes.
    - a. Registrar y asignar clientes a programas.
    - b. Instalar y verificar el servicio de gestión de clientes.
    - c. Configurar el Centro de operaciones para utilizar el servicio de gestión de clientes.
  5. Configurar el segundo servidor.
    - a. Configuración de la comunicación de SSL entre el servidor central y el servidor spoke.
    - b. Añadir el segundo servidor como servidor spoke.
    - c. Habilitar la duplicación.
  6. Completar la implementación.

## Configuración del sistema

---

Para configurar el sistema, primero debe configurar el hardware de almacenamiento de disco y el sistema servidor para IBM Spectrum Protect.

- Configuración del hardware de almacenamiento  
Para configurar el hardware de almacenamiento, revise las directrices generales para los sistemas de disco y IBM Spectrum Protect.
- Instalación del sistema operativo del servidor  
Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.
- Configuración de E/S de la multivía de acceso  
puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.
- Creación del ID de usuario para el servidor  
Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.
- Preparación de sistemas de archivos para el servidor  
Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

## Configuración del hardware de almacenamiento

---


Para configurar el hardware de almacenamiento, revise las directrices generales para los sistemas de disco y IBM Spectrum Protect.

### Procedimiento

---

1. Proporcione una conexión entre el servidor y los dispositivos de almacenamiento siguiendo estas directrices:
  - Utilice un conmutador o conexión directa para las conexiones de canal de fibra.
  - Tenga en cuenta el número de puertos que están conectados y la cantidad de ancho de banda que se necesita.
  - Tenga en cuenta el número de puertos en el servidor y el número de puertos de host en el sistema de discos que están conectados.
2. Verifique que los controladores de dispositivo y firmware para el sistema servidor, adaptadores y sistema operativo son actuales y están en los niveles recomendados.
3. Configure matrices de almacenamiento. Asegúrese de que ha planificado correctamente para garantizar un rendimiento óptimo. Consulte el apartado Planificación de almacenamiento para obtener más información al respecto.
4. Asegúrese de que el sistema servidor tiene acceso a los volúmenes de disco que se han creado. Realice los pasos siguientes:
  - a. Si el sistema está conectado a un conmutador de canal de fibra, divida el servidor por zonas para ver los discos.
  - b. Correlacione todos los volúmenes para indicar al sistema de discos que este servidor específico está autorizado para ver cada disco.

#### Tareas relacionadas:

 Configuración del almacenamiento

## Instalación del sistema operativo del servidor

---

Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Instalación en sistemas AIX  
Complete los pasos siguientes para instalar AIX en el sistema servidor.
- Instalación en sistemas Linux  
Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.
- Instalación en sistemas Windows  
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

## Instalación en sistemas AIX

---

Complete los pasos siguientes para instalar AIX en el sistema servidor.

### Procedimiento

---

1. Instale AIX Versión 7.1, TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.
3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Habilite los puertos de terminación de E/S de AIX emitiendo el siguiente mandato:

```
chdev -l iocp0 -P
```

El rendimiento de servidor puede verse afectado por la definición de huso horario de Olson.

5. Para optimizar el rendimiento, cambie el formato de huso horario del sistema de Olson a POSIX. Utilice el siguiente formato de mandato para actualizar el valor de huso horario:

```
chtz=local_timezone,date/time,date/time
```

Por ejemplo, si ha vivido en Tucson, Arizona, donde se utiliza la franja horaria de las Rocosas, deberá emitir el siguiente mandato para cambiar el formato POSIX:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Añada una entrada en el `.profile` del usuario de la instancia para que se defina el entorno siguiente:

```
export MALLOCOPTIONS=multiheap:16
```

7. Defina el sistema para crear archivos principales de aplicación completos. Emita el mandato siguiente:

```
chdev -l sys0 -a fullcore=true -P
```

8. Para las comunicaciones con el servidor y Centro de operaciones, asegúrese de que los siguientes puertos están abiertos en todos los cortafuegos que puedan existir:

- Para las comunicaciones con el servidor, abra el puerto 1500.
- Para las comunicaciones seguras con Centro de operaciones, abra el puerto 11090 en el servidor concentrador.

Si no utiliza los valores de puerto predeterminados, asegúrese de que los puertos que está utilizando están abiertos.

9. Habilite las mejoras de alto rendimiento de TCP. Emita el mandato siguiente:

```
no -p -o rfc1323=1
```

10. Para obtener una fiabilidad y un rendimiento óptimos, vincule cuatro puertos Ethernet de 10 Gb. Utilice la herramienta de la interfaz de gestión del sistema (SMIT) para vincular los puertos utilizando Etherchannel. Durante las pruebas se utilizaron los siguientes valores:

<code>mode</code>	<code>8023ad</code>	
<code>auto_recovery</code>	<code>yes</code>	Habilitar la recuperación automática tras la migración tras error.
<code>backup_adapter</code>	<code>NONE</code>	Adaptador utilizado cuando falla todo el canal.

hash_mode	src_dst_port	Determina cómo se elige el adaptador saliente.
interval	long	Determina el valor de intervalo para IEEE.
mode	8023ad	Modalidad de 802.3ad Modalidad de funcionamiento de EtherChannel
netaddr	0	Dirección para el ping
noloss_failover	yes	Habilitar migración tras error sin pérdidas tras anomalía del ping
num_retries	3	Veces que reintentar el ping antes de considerarlo un error
retry_time	1	Tiempo de espera (en segundos) entre pings
use_alt_addr	no	Habilitar dirección EtherChannel alternativa
use_jumbo_frame	no	Habilitar tramas de gran tamaño de Gigabit Ethernet

11. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 1. Si los valores *ulimit* no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 1. Valores de los límites de usuario (*ulimit*)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	<code>ulimit -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	<code>ulimit -Hd</code>
Tamaño de archivo máximo	fsize	Ilimitado	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	nofile	65536	<code>ulimit -Hn</code>
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	<code>ulimit -Ht</code>
Número máximo de procesos de usuario	nproc	16384	<code>ulimit -Hu</code>

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.

### Antes de empezar

El sistema operativo se instalará en los discos duros internos. Configure los discos duros internos utilizando una matriz de hardware de RAID 1. Por ejemplo, si está configurando un sistema pequeño, los dos discos internos de 300 GB se duplican en RAID 1 de modo que aparece disponible un único disco de 300 GB para el instalador del sistema operativo.

### Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contenga Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
  - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
  - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
  - c. Seleccione las preferencias de idioma y teclado.
  - d. Seleccione la ubicación para establecer el huso horario correcto.
  - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
  - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:
    - El disco local de 300 GB se ha seleccionado como destino de instalación.
    - En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.



Pulse Terminado.

g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root. Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato df para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

```
[root@tvapp02]# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root     50G   3.0G   48G   6% /
devtmpfs                  32G    0    32G   0% /dev
tmpfs                     32G   92K   32G   1% /dev/shm
tmpfs                     32G   8.8M   32G   1% /run
tmpfs                     32G    0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home     220G   37M   220G   1% /home
/dev/sdal                  497M  124M   373M  25% /boot
```

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agrega varios puertos subordinados a una sola conexión lógica. El método preferido es utilizar una modalidad de vínculo de 802.3ad, un valor de miimon de 100 y un valor de xmit\_hash\_policy de layer3+4.

Restricción: Para utilizar una conexión de red LACP, debe disponer de un conmutador de red que admita LACP.

Para obtener instrucciones adicionales sobre cómo configurar conexiones de red vinculadas con Red Hat Enterprise Linux Versión 7, consulte Crear una interfaz de acoplamiento de canal.

3. Abra el archivo /etc/hosts y complete las siguientes acciones:

- o Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- o Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Instale los componentes que son necesarios para la instalación de servidor. Complete los pasos siguientes para crear un repositorio Yellowdog Updater Modified (YUM) e instale los paquetes de requisitos previos.

a. Monte el DVD de instalación de Red Hat Enterprise Linux en el directorio del sistema. Por ejemplo, para montarlo en el directorio /mnt, emita el siguiente mandato:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

b. Verifique que el DVD se ha montado emitiendo el mandato mount. Debería ver una salida similar al ejemplo siguiente:

```
/dev/sr0 on /mnt type iso9660
```

c. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

Si el directorio repos.d no existe, créelo.

d. Liste el contenido de directorio:

```
ls rhel-source.repo
```

e. Cambie el nombre del archivo repo original emitiendo el mandato mv. Por ejemplo:

```
mv rhel-source.repo rhel-source.repo.orig
```

f. Cree un nuevo archivo repo utilizando un editor de texto. Por ejemplo, para utilizar el editor vi, emita el siguiente mandato:

```
vi rhel71_dvd.repo
```

g. Añada las líneas siguientes al nuevo archivo repo. El parámetro baseurl especifica el punto de montaje del directorio:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

h. Instale el paquete de requisito previo ksh.x86\_64, emitiendo el mandato yum. Por ejemplo:

```
yum install ksh.x86_64
```

Excepción: No necesita instalar las bibliotecas compat-libstdc++-33-3.2.3-69.el6.i686 y libstdc++.i686 para Red Hat Enterprise Linux Versión 7.1.

5. Cuando se completa la instalación de software, puede restaurar los valores de repositorio YUM originales completando los pasos siguientes:

a. Desmunte el DVD de instalación de Red Hat Enterprise Linux emitiendo el siguiente mandato:

```
umount /mnt
```

b. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

c. Cambie el nombre del archivo repo que ha creado:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

d. Cambie el nombre del archivo original al nombre original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine si son necesarios cambios de parámetro de kernel. Realice los pasos siguientes:

a. Utilice el mandato `sysctl -a` para listar los valores de parámetro.

b. Analice los resultados utilizando las directrices en Tabla 1 para determinar si es necesario algún cambio.

c. Si se necesitan cambios, establezca los parámetros en el archivo `/etc/sysctl.conf`. Los cambios de archivo se aplican cuando se inicia el sistema.

Consejo: Ajuste automáticamente los valores de parámetros de kernel y elimine la necesidad de actualizaciones manuales en estos valores. En Linux, el software de base de datos DB2 ajusta automáticamente los valores del parámetro de kernel de comunicación entre procesos (IPC) a los valores preferidos. Para obtener más información sobre los valores de parámetros de kernel, busque los parámetros de kernel de Linux en IBM DB2 versión 11.1 Knowledge Center.

Tabla 1. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción
kernel.shmmni	El número máximo de segmentos.
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes).  Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas).
kernel.sem	(SEMMSL)
Hay cuatro valores para el parámetro kernel.sem.	El número máximo de semáforos por matriz.
	(SEMMNS)
	El número máximo de semáforos por sistema.
	(SEMOPM)
	El número máximo de operaciones por llamada a semáforo.
	(SEMMNI)
	El número máximo de matrices.
kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema.
kernel.msgmax	Tamaño máximo de los mensajes (bytes).
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes).
kernel.randomize_va_space	El parámetro kernel.randomize_va_space configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.

Parámetro	Descripción
vm.swappiness	El parámetro vm.swappiness define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.
vm.overcommit_memory	El parámetro vm.overcommit_memory influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.

7. Abra puertos de cortafuegos para comunicarse con el servidor. Realice los pasos siguientes:

a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.

Emita el mandato siguiente:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Para utilizar la dirección de puerto predeterminada para las comunicaciones con el servidor, abra el puerto TCP/IP 1500 en el cortafuegos de Linux.

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Si desea utilizar un valor distinto del predeterminado, puede especificar un número en el rango 1024 - 32767. Si abre un puerto distinto del predeterminado, tendrá que especificar ese puerto cuando ejecute el script de configuración.

c. Si piensa utilizar este sistema como concentrador, abra el puerto 11090, que es el puerto predeterminado para las comunicaciones seguras (https).

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

d. Vuelva a cargar las definiciones de cortafuegos para que los cambios entren en vigor.

Emita el mandato siguiente:

```
firewall-cmd --reload
```

8. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 2. Si los valores ulimit no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 2. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	ulimit -Hc
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	ulimit -Hd
Tamaño de archivo máximo	fsize	Ilimitado	ulimit -Hf
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Windows

Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

## Procedimiento

---

1. Instale Microsoft Windows Server 2012 R2 Standard Edition, de acuerdo con las instrucciones del fabricante.
2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
  - a. Abra el editor de política de seguridad local ejecutando secpol.msc.
  - b. Pulse Políticas locales > Opciones de seguridad y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
    - Modo de aprobación de administrador para la cuenta de administrador integrado
    - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:
  - a. Aplique las últimas actualizaciones de Windows 2012 R2.
  - b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
  - c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
  - d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.
5. Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Backup server port 1500"  
dir=in action=allow protocol=TCP localport=1500
```

6. En el servidor concentrador de Centro de operaciones, abra el puerto predeterminado para comunicaciones seguras (https) con Centro de operaciones. El número de puerto es 11090. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Centro de operaciones port 11090"  
dir=in action=allow protocol=TCP localport=11090
```

## Configuración de E/S de la multivía de acceso

---

puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

- Sistemas AIX
- Sistemas Linux
- Sistemas Windows

## Sistemas AIX

---

### Procedimiento

---

1. Determine la dirección de puerto de canal de fibra que debe utilizar para la definición de host en el subsistema de disco. Emita el mandato `lscfg` para cada puerto.

- En sistemas pequeños y medianos, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"
```

- En sistemas grandes, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"  
lscfg -vps -l fcs2 | grep "Network Address"  
lscfg -vps -l fcs3 | grep "Network Address"
```

2. Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:

- `devices.common.IBM.mpio.rte`
- `devices.fcp.disk.array.rte`
- `devices.fcp.disk.rte`

3. Emita el mandato `cfgmgr` para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

4. Para listar los discos disponibles, emita el siguiente mandato:

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```

hdisk0 Available 00-00-00 SAS Disk Drive
hdisk1 Available 00-00-00 SAS Disk Drive
hdisk2 Available 01-00-00 SAS Disk Drive
hdisk3 Available 01-00-00 SAS Disk Drive
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk
...

```

5. Utilice la salida del mandato `lsdev` para identificar y listar ID de dispositivo para cada dispositivo de disco.

Por ejemplo, un ID de dispositivo podría ser `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

```
lspv -u
```

En un sistema IBM® Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

```

hdisk4 00f8cf083fd97327 None active
        33213600507630081010578000000000003004214503IBMfcp

```

En el ejemplo, `6005076300810105780000000000030` es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

Para verificar el tamaño de disco en megabytes y compararlo con el valor que se lista para el sistema, emita el siguiente mandato:

```
bootinfo -s hdisk4
```

## Sistemas Linux

---

### Procedimiento

---

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

```
multipathconf --enable
```

Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

```

defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}

```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los mandatos siguientes:

```

systemctl enable multipathd.service
systemctl start multipathd.service

```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

```
multipath -l
```

- Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan. Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
  size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  `-- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  `-- 3:0:0:18 sddy 128:0 active undef running
```

- Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

```
echo "-- --" > /sys/class/scsi_host/host0/scan
echo "-- --" > /sys/class/scsi_host/host1/scan
echo "-- --" > /sys/class/scsi_host/host2/scan
```

También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

- Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato `multipath -l`.
- Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 36005076802810c509800000000000012.

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

## Sistemas Windows

### Procedimiento

- Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
- Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

- Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan. Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

```
DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0
```

- Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 60050763008101057800000000000034

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

- Para poner los nuevos discos en línea y borrar el atributo de 'sólo lectura', ejecute `diskpart` con los mandatos siguientes. Repítalo para cada uno de los discos:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
```

```
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

## Creación del ID de usuario para el servidor

---

Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.

### Acerca de esta tarea

---

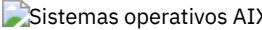
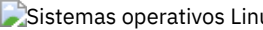
Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado ( \_ ) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.


### Procedimiento

---


1. Utilice mandatos del sistema operativo para crear un ID de usuario.

-  Sistemas operativos AIX  Sistemas operativos Linux Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

Por ejemplo, para crear el ID de usuario *tsminst1* en el grupo *tsmsrvrs* con una contraseña de *tsminst1*, emita los siguientes mandatos desde un ID de usuario de administración:


 Sistemas operativos AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

 Sistemas operativos Linux

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

-  Sistemas operativos Windows Cree un ID de usuario y, a continuación, añada el nuevo ID al grupo de administradores. Por ejemplo, para crear el ID de usuario *tsminst1*, emita el siguiente mandato:

```
net user tsminst1 * /add
```

Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Cierre la sesión con el nuevo ID de usuario.

## Preparación de sistemas de archivos para el servidor

---

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

- Preparación de sistemas de archivos en sistemas AIX  
Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.
- Preparación de sistemas de archivos en sistemas Linux  
Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum

Protect.

- Preparación de sistemas de archivos en sistemas Windows  
Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas AIX

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

### Procedimiento

1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos *hdiskX* disponibles. Emita los siguientes mandatos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, *hdisk0*.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato `mkvg`, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

Por ejemplo, si los nombres de dispositivo *hdisk4*, *hdisk5* y *hdisk6* corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita `lsvg` para cada grupo de volúmenes que ha creado en el paso anterior.

Por ejemplo:

```
lsvg -p tsmdb
```

La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

```
tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631      1631      327..326..326..326..326
hdisk5   active    1631      1631      327..326..326..326..326
hdisk6   active    1631      1631      327..326..326..326..326
```

4. Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato `mklv`. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco.

Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato `crfs`.

Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

```
mount -a
```



7. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado es normalmente un 1%:

```
tapsrv07> df -g /tsminst1/*
Filesystem      GB blocks   Free    %Used   Iused   %Iused   Mounted on
/dev/tsmact00   195.12    194.59    1%      4       1%      /tsminst1/TSMalog
```

8. Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios para el servidor IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas Linux

---

Debe formatear los sistemas de archivos `ext4` o `xfs` en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

### Procedimiento

---

1. Utilizando la lista de ID de dispositivo que ha generado antes, emita el mandato `mkfs` para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos `ext4`:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos `xfs`:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Puede emitir el mandato `mkfs` hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

2. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato `mkdir` para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación.

Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
mkdir /tsminst1
```

Repita el mandato `mkdir` para cada sistema de archivos.

3. Añada una entrada en el archivo `/etc/fstab` para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.

Por ejemplo:

```
/dev/mapper/36005076802810c5098000000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Monte los sistemas de archivos que ha añadido al archivo `/etc/fstab` emitiendo el mandato `mount -a`.
5. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente en un sistema IBM® Storwize muestra que la cantidad de espacio utilizado normalmente es un 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem      Size  Used Avail Use% Mounted on
/dev/mapper/3600507630081010578000000000000003 134G  188M 132G   1%  /tsminst1/TSMalog
```

6. Compruebe que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura a los directorios de IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas Windows

---

Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

### Procedimiento

---

1. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato `md` para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
md c:\tsminst1
```

Repita el mandato md para cada sistema de archivos.

2. Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

Vaya a Gestor de servidores > Servicios de archivo y almacenamiento y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

- a. Ponga el disco en línea.
- b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
- c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como TSMfile00. No asigna el nuevo volumen a la letra de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como C:\tsminst1\TSMfile00.  
Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.

3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato mountvol y, a continuación, revise la salida. Por ejemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\  
C:\tsminst1\TSMdbspace00\
```

4. Una vez se ha completado la configuración de disco, reinicie el sistema.

## Qué hacer a continuación

---

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

## Instalación del servidor y Centro de operaciones

---

Utilice el asistente gráfico de IBM® Installation Manager para instalar los componentes.

- Instalación en sistemas AIX y Linux  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema de servidor.
- Instalación en sistemas Windows  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema servidor.

## Instalación en sistemas AIX y Linux

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema de servidor.

### Antes de empezar

---

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

### Procedimiento

---

1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.

Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.


2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package\_name* es el nombre del archivo descargado.

6.  Sistemas operativos AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:

```
lsuser
```

De manera predeterminada, el mandato está habilitado.

7. Cambie al directorio en el que colocó el archivo ejecutable.
8. Inicie el asistente de instalación emitiendo el mandato siguiente:

```
./install.sh
```

Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación



---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.
- Instalación de archivos RPM de requisitos previos para el asistente gráfico  
Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

### Tareas relacionadas:

-  Otros métodos para instalar componentes de IBM Spectrum Protect (AIX)
-  Otros métodos para instalar componentes de IBM Spectrum Protect (Linux)

## Instalación en sistemas Windows

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el primer sistema servidor.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento

---

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación


---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM®.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.

#### Tareas relacionadas:

 Otros métodos para instalar componentes de IBM Spectrum Protect

## Configuración del servidor y el Centro de operaciones

---

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

- Configuración de la instancia de servidor  
Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.
- Instalación del cliente de archivado y copia de seguridad  
Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?
- Configuración de opciones para el servidor  
Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.
- Configuración de comunicaciones seguras con Seguridad de la capa de transporte  
Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.
- Configuración de Centro de operaciones  
Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.
- Registro de la licencia de producto  
Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.
- Configuración de la optimización de almacenamiento de datos  
Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.
- Definición de las reglas de retención de datos para su empresa  
Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.
- Definición de planificaciones para actividades de mantenimiento del servidor  
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.
- Definición de planificaciones de cliente  
Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

## Configuración de la instancia de servidor

---

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

 Sistemas operativos Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:







1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.

2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
  - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
  - b. Seleccione Configuración avanzada.
  - c. Seleccione Reglas de entrada.
  - d. Seleccione Nueva regla.
  - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
  - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
  - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
  - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
  - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada > Inhabilitar > Aceptar.
4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.

## Acerca de esta tarea

El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Procedimiento

1. Inicie la versión local del asistente.
  -   Abra el programa dsmsicfgx en el directorio /opt/tivoli/tsm/server/bin. Este asistente sólo puede ejecutarse como usuario root.
  -  Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Planificación de hojas de trabajo para la configuración del sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.
  -   En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.
  -  Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

## Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

## Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

## Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

## Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo dsmserv.opt.
2. Revise los valores de la tabla siguiente y verifique los valores de opciones de servidor, en base al tamaño del sistema.

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
--------------------	--------------------------	--------------------------	-------------------------

Opción de servidor	Valor de sistema pequeño	Valor de sistema mediano	Valor de sistema grande
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072	131072	262144
ARCHLOGCOMPRESS	Sí	No	No
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCPIP	TCPIP	TCPIP
COMMTIMEOUT	3600	3600	3600
DEDUPREQUIRESBACKUP	No	No	No
DEVCONFIG	devconf.dat	devconf.dat	devconf.dat
EXPINTERVAL	0	0	0
IDLETIMEOUT	60	60	60
MAXSESSIONS	250	500	1000
NUMOPENVOLSALLOWED	20	20	20
TCPADMINPORT	1500	1500	1500
TCPPORT	1500	1500	1500
VOLUMEHISTORY	volhist.dat	volhist.dat	volhist.dat

Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo dmserv.opt y utilice el mandato SETOPT desde la interfaz de línea de mandatos de administración para establecer las opciones.

Por ejemplo, para actualizar la opción IDLETIMEOUT a 60, emita el siguiente mandato:

```
setopt idletimeout 60
```

- Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

Opción de servidor	Todos los tamaños del sistema
SSLFIPSMODE	NO
TCPPORT	Especifique el número de puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente.
TCPADMINPORT	Especifique la dirección del puerto en el que el servidor espera las solicitudes para TCP/IP y las sesiones habilitadas para SSL desde el cliente administrativo de línea de mandatos.

Si alguno de los valores de opción debe actualizarse, edite el archivo dmserv.opt utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guardé los cambios y cierre el archivo. Si edita el archivo dmserv.opt directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

#### Referencia relacionada:

- [Referencia de opciones de servidor](#)
- [SETOPT \(Establecer una opción de servidor para actualización dinámica\)](#)

## Configuración de comunicaciones seguras con Seguridad de la capa de transporte

Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

## Acerca de esta tarea

A partir de IBM Spectrum Protect versión 8.1.2, SSL está habilitada de forma predeterminada, y el servidor y cliente de archivado y copia de seguridad de IBM Spectrum Protect se configuran automáticamente para comunicarse entre ellos utilizando el protocolo TLS 1.2.

Tal como se indica en la figura siguiente, puede configurar manualmente comunicaciones seguras entre el servidor y el cliente de archivado y copia de seguridad definiendo opciones en los archivos de opciones de servidor y cliente y, después, transfiriendo el certificado firmado automáticamente que se ha generado en el servidor al cliente. Como alternativa, puede obtener y transferir un certificado único que esté firmado por una entidad emisora de certificados (CA).



Para obtener más información sobre cómo configurar el servidor y los clientes para las comunicaciones SSL o TLS, consulte Configuración de agentes, servidores y clientes de almacenamiento, y del Centro de operaciones para conectarse al servidor mediante SSL.

## Configuración de Centro de operaciones

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

### Antes de empezar

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

### Procedimiento

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

```
https://hostname:secure_port/oc
```

donde:

- *nombre\_host* representa el nombre del sistema donde está instalado Centro de operaciones
- *puerto\_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

Por ejemplo, si el nombre de host es `tsm.storage.mylocation.com` y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

```
https://tsm.storage.mylocation.com:11090/oc
```

Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.

2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor concentrador configurando el protocolo de la capa de sockets seguros (SSL).

Siga las instrucciones que encontrará en Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

Siga las instrucciones que encontrará en Seguimiento del estado del sistema mediante informes de correo electrónico.

- Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador  
Para proteger las comunicaciones entre Centro de operaciones y el servidor concentrador, añada el certificado de seguridad de la capa de transporte (TLS) del servidor concentrador al archivo de almacén de confianza de Centro de operaciones.

## Registro de la licencia de producto

---

Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.

### Acerca de esta tarea


---

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

### Procedimiento

---

Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.


1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración  y pulsando Creador de mandatos.
3. Emita el mandato REGISTER LICENSE. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

### Qué hacer a continuación

---

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor se ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
-  Sistemas operativos Linux Si cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

#### Referencia relacionada:

 REGISTER LICENSE (Registrar una nueva licencia)

## Configuración de la optimización de almacenamiento de datos

---

Crear una agrupación de almacenamiento de contenedores de directorio y al menos un directorio para utilizar la deduplicación de datos en línea.

### Antes de empezar

---

Utilice la información de directorio de agrupación de almacenamiento que ha registrado en Planificación de hojas de trabajo para esta tarea.

### Procedimiento

---

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el cursor por encima de Almacenamiento.
3. En la lista que se visualiza, pulse Agrupaciones de almacenamiento.
4. Pulse el botón +Agrupación de almacenamiento.
5. Complete los pasos del asistente Añadir agrupación de almacenamiento:
  - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
  - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
6. Tras configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.



## Definición de las reglas de retención de datos para su empresa

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

### Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.
3. Pulse el conmutador Configurar y realice los cambios siguientes:
  - Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedores de directorio.
  - Cambie el valor de la columna de copias de seguridad a Sin límite.
  - Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador Configurar para que el conjunto de políticas ya no se pueda editar.
5. Activar el conjunto de políticas pulsando Activar.

#### Tareas relacionadas:

Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

## Definición de planificaciones para actividades de mantenimiento del servidor

Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.

### Acerca de esta tarea

Planifique operaciones de mantenimiento de servidor para ejecutar después de operaciones de copia de seguridad de cliente. Puede controlar la temporización de planificaciones estableciendo la hora de inicio en combinación con la duración para cada operación.

El ejemplo siguiente muestra cómo puede planificar procesos de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de disco multisitio.

Operación	Planificación
Copia de seguridad del cliente	Empieza a las 22:00.
Réplica de nodo	Se inicia a las 08:00, o 10 horas después del comienzo de la copia de seguridad de cliente.
Proceso para archivos de recuperación tras desastre y de base de datos	<ul style="list-style-type: none"><li>• La copia de seguridad de base de datos se inicia a las 11:00, o 13 horas después del comienzo de la copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.</li><li>• La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 17:00 o 6 horas después del inicio de la copia de seguridad de la base de datos.</li><li>• La supresión del historial de volumen comienza a las 20:00 o 9 horas después del inicio de la copia de seguridad de la base de datos.</li></ul>
Caducidad de inventario	Empieza a las 12:00, o 14 horas después del inicio de la ventana de copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.



### Procedimiento

Tras configurar la clase de dispositivo para las operaciones de copia de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato DEFINE SCHEDULE. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.


1. Defina una clase de dispositivo para las operaciones de copia de seguridad. Por ejemplo, utilice el mandato DEFINE DEVCLASS para crear una clase de dispositivo que se denomine DBBACK\_FILEDEV:

```
define devclass dbback_filedev devtype=file
  directory=directorios_copia_seguridad_bd
```

donde *directorios\_copia\_seguridad\_bd* es una lista de los directorios que ha creado para la copia de seguridad de base de datos.

  Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando por el mandato /tsminst1/TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory=/tsminst1/TSMbkup00,
  /tsminst1/TSMbkup01,/tsminst1/TSMbkup02,
  /tsminst1/TSMbkup03"
```

 Por ejemplo, si tiene cuatro directorios para copias de seguridad de base de datos, empezando con C:\tsminst1\TSMbkup00, emita el mandato siguiente:

```
define devclass dbback_filedev devtype=file
  directory="c:\tsminst1\TSMbkup00,
  c:\tsminst1\TSMbkup01,c:\tsminst1\TSMbkup02,c:\tsminst1\TSMbkup03"
```

2. Establezca la clase de dispositivo para operaciones de copia de seguridad de base de datos automáticas. Utilice el mandato SET DBRECOVERY para especificar la clase de dispositivo que ha creado en el paso anterior. Por ejemplo, si la clase de dispositivo es dbback\_filedev, emita el mandato siguiente:

```
set dbrecovery dbback_filedev
```

3. Cree planificaciones para las operaciones de mantenimiento utilizando el mandato DEFINE SCHEDULE. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.  
Consejo: Cree la planificación para la réplica por separado en un paso posterior, al utilizar Centro de operaciones para configurar la réplica.

Operación	Mandato de ejemplo
Realizar una copia de seguridad de la base de datos.	<p>Cree una planificación para ejecutar el mandato BACKUP DB. Si está configurando un sistema pequeño, establezca el parámetro COMPRESS en YES.</p> <p>Por ejemplo, en un sistema pequeño, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db   devclass=dbback_filedev type=full numstreams=3 wait=yes   compress=yes" active=yes desc="Back up the database."   startdate=today starttime=11:00:00 duration=45   durunits=minutes</pre>
Realice una copia de seguridad de la información de configuración del dispositivo.	<p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup   devconfig   filenames=devconfig.dat" active=yes desc="Backup the   device   configuration file." startdate=today starttime=17:00:00   duration=45 durunits=minutes</pre>
Haga una copia de seguridad del historial de volumen.	<p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup   volhistory   filenames=volhist.dat" active=yes desc="Back up the   volume   history." startdate=today starttime=17:00:00   duration=45   durunits=minutes</pre>
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	<p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete   volhistory   type=dbb todate=today-6 totime=now" active=yes   desc="Remove   old database backups." startdate=today   starttime=20:00:00   duration=45 durunits=minutes</pre>

Operación	Mandato de ejemplo
Elimine objetos que exceden su retención permitida.	<p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY. Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar:</p> <ul style="list-style-type: none"> <li>○ Sistemas pequeños: 10</li> <li>○ Sistemas medianos: 30</li> <li>○ Sistemas grandes: 40</li> </ul> <p>Por ejemplo, en un sistema de tamaño mediano, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory wait=yes resource=30 duration=120" active=yes desc="Remove expired objects." startdate=today starttime=12:00:00 duration=45 durunits=minutes</pre>

## Qué hacer a continuación

Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Servidores.
2. Pulse Mantenimiento.

### Referencia relacionada:

[DEFINE SCHEDULE](#) (Definir una planificación para un mandato de administración)

## Definición de planificaciones de cliente

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

### Procedimiento

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de Clientes.
2. Pulse Planificaciones.
3. Pulse +Planificación.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.

## Instalación y configuración de clientes de archivado y copia de seguridad

Tras la configuración correcta del sistema servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

### Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

## Qué hacer a continuación

Registrar y asignar los clientes a planificaciones.

- Registro y asignación de clientes a planificaciones  
Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.
- Instalación del servicio de gestión de cliente  
Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas

operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

## Registro y asignación de clientes a planificaciones

---

Añada y registre cliente mediante Centro de operaciones utilizando el asistente Añadir cliente.

### Antes de empezar

---

Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

### Procedimiento

---

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre\_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Clientes.
  - b. En la tabla Clientes, pulse + Cliente.
  - c. Complete los pasos en el asistente Añadir cliente:
    - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
    - ii. En la ventana Configuración, copie los valores de opción TCPSERVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.  
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
    - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
    - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
    - v. Pulse Añadir cliente.

## Instalación del servicio de gestión de cliente

---

Instale el servicio de gestión de cliente para clientes de archivado y copia de seguridad que se ejecutan en los sistemas operativos Linux y Windows. El servicio de gestión de cliente recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y deja la información disponible en el Centro de operaciones para la funcionalidad de supervisión básica.

### Procedimiento

---

Instale el servicio de gestión de cliente en el mismo sistema que el cliente de archivado y copia de seguridad completando los pasos siguientes:

1. Descargue el paquete de instalación para el servicio de gestión de cliente desde un sitio de descarga de IBM® como por ejemplo IBM Passport Advantage® o IBM Fix Central. Busque un nombre de archivo que sea similar a *<versión>-IBM\_Spectrum\_Protect-CMS-sistema\_operativo.bin*.
2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
3. Extraiga el contenido del archivo del paquete de instalación.
4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
5. Para instalar el servicio de gestión de cliente, siga las instrucciones del asistente del Gestor de instalación de IBM. Si el Gestor de instalación de IBM no está instalado en el sistema cliente, debe seleccionar el Gestor de instalación de IBM y los Servicios de gestión de cliente de IBM Spectrum Protect.

- Verificación de que el servicio de gestión de clientes está instalado correctamente  
Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.
- Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente  
Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

#### Tareas relacionadas:

[Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas](#)

## Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de cliente para recopilar información de diagnóstico sobre un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de cliente está instalado y configurado correctamente.

### Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

```
dir_instalación_cliente/cms/bin/CmsConfig.sh list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

La salida es similar al texto siguiente:

Listado de la configuración de CMS

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys

  Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252

  Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

- En los sistemas cliente Windows, emita el mandato siguiente:

```
dir_instalación_cliente\cms\bin\CmsConfig.bat list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
C:\"Archivos de programa"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

Listado de la configuración de CMS

```
server1.example.com:1500 NO_SSL HOSTNAME
Capabilities: [LOG_QUERY]
  Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt

  Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252

  Log File: C:\Program Files\Tivoli\TSM\baclient\dmsched.log
            en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:

```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo client-configuration.xml. Para obtener instrucciones para configurar este archivo, consulte Configuración del servicio de gestión clientes para instalaciones de cliente personalizadas. Puede utilizar el mandato CmsConfig verify para comprobar que una definición de nodo se ha creado correctamente en el archivo client-configuration.xml.

## Configuración de Centro de operaciones para utilizar el servicio de gestión de cliente

Si no ha utilizado la configuración predeterminada para el servicio de gestión de cliente, debe configurar Centro de operaciones para acceder al servicio de gestión de cliente.

### Antes de empezar

Asegúrese de que el servicio de gestión de cliente está instalado y se ha iniciado en el sistema cliente. Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de cliente no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
  - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse por una red, mientras que el servicio de gestión de cliente se comunica por la otra red.
  - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, se le asigna dinámicamente al sistema cliente una dirección IP, que se guarda en el servidor durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

### Procedimiento

Para configurar Centro de operaciones para utilizar el servicio de gestión de cliente, complete los pasos siguientes:

1. En la página Clientes de Centro de operaciones, seleccione el cliente.
2. Pulse Detalles > Propiedades.
3. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de cliente en el sistema cliente. La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	https://server.example.com
Con el nombre de host de DNS y puerto no predeterminado	https://server.example.com:1599
Con la dirección IP y puerto no predeterminado	https://192.0.2.0:1599

4. Pulse Guardar.

### Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

## Configuración del segundo servidor

Después de completar la configuración para el primer servidor del sistema, configure el segundo servidor.

### Procedimiento

Complete las instrucciones de las secciones siguientes:

1. Para configurar un segundo servidor que sea igual que el primer servidor, complete las instrucciones de las secciones siguientes:
  - a. Configuración del sistema
  - b. Instalación del servidor y Centro de operaciones

Sólo un servidor de la solución de disco multisitio está configurada como el servidor concentrador, de modo que no necesita instalar el Centro de operaciones en el segundo servidor. Cuando seleccione los paquetes de instalación para instalar en el segundo servidor, no seleccione el Centro de operaciones.
  - c. Configuración del servidor y el Centro de operaciones

Sáltese las tareas para configurar el Centro de operaciones.
  - d. Instalación y configuración de clientes de archivado y copia de seguridad
2. Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke
3. Añadir un segundo servidor como servidor spoke
4. Habilitación de réplica

## Configuración de las comunicaciones SSL entre el servidor concentrador y un servidor spoke

Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke utilizando el protocolo de Seguridad de la capa de transporte (TLS), debe definir el certificado del servidor spoke en el servidor concentrador. También debe configurar Centro de operaciones para supervisar el servidor spoke.

### Procedimiento

1. En el servidor spoke, cambie al directorio de la instancia del servidor spoke.
2. Especifique el certificado cert256.arm necesario como certificado predeterminado en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

3. Verifique los certificados en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

4. Transfiera de forma el archivo cert256.arm del servidor de radio al servidor central.
5. En el servidor concentrador, cambie el directorio de la instancia del servidor concentrador.
6. Defina el certificado de servidor spoke para el servidor concentrador. Emita el mandato siguiente desde el directorio de instancia de servidor concentrador, donde *nombre\_servidor\_spoke* es el nombre del servidor spoke y *spoke\_cert256.arm* es el nombre de archivo del certificado de servidor spoke.

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii  
-label spoke_servername -file spoke_cert256.arm
```

El servidor de radio no requiere el certificado del servidor central para la comunicación del servidor central al de radio. Sin embargo, otras configuraciones de servidor que requieren servidores de definición cruzada requieren que el servidor de radio tenga el certificado de servidor concentrador.

7. Reinicie el servidor central y el servidor de radio.
8. Para el servidor concentrador, emita el mandato DEFINE SERVER, según el siguiente ejemplo:

```
DEFINE SERVER spoke_servername HLA=spoke_address  
LLA=spoke_SS LTCADMINPort SERVERPA=contraseña_servidorespoke
```

Consejo: De manera predeterminada la comunicación del servidor se cifra, excepto cuando el servidor está enviando o recibiendo datos de objeto. Los datos de objeto se envían y reciben mediante TCP/IP. Al elegir no cifrar los datos, el rendimiento del servidor es similar al de la comunicación por una sesión TCP/IP y la sesión es segura. Para cifrar toda la comunicación con el servidor especificado, incluso cuando el servidor está enviando y recibiendo datos de objeto, especifique el parámetro SSL=YES en el mandato DEFINE SERVER.

9. En la barra de menús de Centro de operaciones, pulse Servidores.

En la tabla de la página Servidores, el servidor de radio que ha definido en el paso 8, normalmente, tiene un estado de "No supervisado". En función del valor del intervalo de renovación de estado, es posible que no vea el servidor spoke inmediatamente.

10. Pulse en el servidor spoke para resaltarlo el elemento, y en la monitor de la tabla, pulse Supervisar spoke.

**Referencia relacionada:**

- ➔ DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)
- ➔ QUERY OPTION (Consultar opciones del servidor)

## Añadir un segundo servidor como servidor spoke

---

Después de configurar ambos servidores en el entorno, añada el segundo servidor como servidor spoke al servidor concentrador.

### Procedimiento

---

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pulse Servidores.
3. Realice uno de los siguientes pasos:
  - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
  - Si el servidor que desea añadir no se muestra en la tabla, pulse +Spoke.
4. Realice los pasos del asistente de configuración de spoke.

## Habilitación de réplica

---

Para proteger los datos, habilite la réplica de nodo, además de proteger las agrupaciones de almacenamiento.

### Procedimiento

---

Para habilitar la réplica de nodo para todos los clientes registrados para el servidor de origen, complete los pasos siguientes:

1. Abra el Centro de operaciones.
2. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
3. En la página Réplica, pulse + Par de servidores.
4. Realice los pasos del asistente Añadir par de servidores:
  - Establezca el servidor de origen como el primer servidor que ha configurado para la solución de disco multisitio. El servidor de destino es el segundo servidor.
  - Establezca que la planificación de réplica de nodo se inicie 10 horas después de la ventana de copia de seguridad de cliente, basándose en las actividades de mantenimiento de servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.
  - El asistente configura planificaciones de protección de agrupación de almacenamiento, en función de la cantidad de datos que se están protegiendo y de cuándo se planifica la réplica de cliente.

### Qué hacer a continuación

---

Si piensa configurar la réplica mutua entre dos sitios, ejecute el asistente Añadir par de servidores de nuevo y establezca el segundo servidor como el origen y el primer servidor como el destino.

## Finalización de la implementación

---

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

### Procedimiento

---

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.
  - a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
  - b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
  - c. Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.

Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.



2. Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de disco multisitio.

## Supervisión de una solución de disco multisitio

---

Después de implementar una solución de disco multisitio con IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

### Acerca de esta tarea

---

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar un informe de correo electrónico diario que resume el estado del sistema.

En algunos casos, es posible que desee utilizar herramientas de supervisión avanzadas para completar tareas de supervisión o resolución de problemas específicas.

Consejo: Si piensa diagnosticar problemas con clientes de archivado y copia de seguridad en sistemas operativos Linux o Windows, instale los servicios de gestión de cliente de IBM Spectrum Protect en cada sistema donde esté instalado un cliente de archivado y copia de seguridad. De esta forma, puede garantizar que el botón Diagnosticar está disponible en Centro de operaciones para diagnosticar problemas con los clientes de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.

### Procedimiento

---

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación de supervisión diaria.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación de supervisión periódica.
3. Para verificar que la solución de IBM Spectrum Protect cumple con los requisitos de licencia, siga las instrucciones que encontrará en Verificación de la conformidad de licencia.
4. Si desea configurar el Centro de operaciones para generar informes de estado de correo electrónico, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

### Qué hacer a continuación

---

Resuelva cualquier problema que encuentre. Para resolver un problema cambiando la configuración de la solución, siga las instrucciones que encontrará en Gestión de operaciones para una solución de disco multisitio. Los siguientes recursos están también disponibles:

- Para resolver problemas de rendimiento, consulte Rendimiento.
- Para resolver otros tipos de problemas, consulte Resolución de problemas.

## Lista de comprobación de supervisión diaria


---

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.









Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.





La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.


Tabla 1. Tareas de supervisión diarias

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>1</b> Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Clientes, seleccione el cliente y pulse Detalles.</li> <li>2. Para diagnosticar un problema, pulse Diagnóstico.</li> </ol>	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>
<p><b>2</b> Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Alertas.</li> <li>2. En la tabla Alertas, seleccione una alerta.</li> <li>3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.</li> </ol>
<p><b>3</b> Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> <li>1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible.</li> <li>2. Para ver información adicional, pulse el área Servidores.</li> <li>3. Seleccione un servidor en la tabla Servidores y pulse Detalles.</li> </ol>	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione un servidor y pulse Detalles.</li> <li>2. Para actualizar las propiedades de servidor, pulse Propiedades.</li> </ol>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> <li>o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado.</li> <li>o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor.</li> <li>o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio.</li> <li>o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC.</li> <li>o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio.</li> </ul> </li> </ol>	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>5</b> Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.</li> </ol>	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione una fila y pulse Detalles.</li> <li>2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad.</li> </ol> <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Servidores.</li> <li>2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad.</li> </ol> <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la barra de menú, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY DB: <pre>query db f=d</pre> </li> <li>3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.</li> </ol>
<p><b>6</b> Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse Servidores &gt; Mantenimiento.</li> <li>2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial.</li> <li>3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.</li> </ol>	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>7</b> Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> <li>• Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad.</li> <li>• Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.</li> </ul>	<ul style="list-style-type: none"> <li>• Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente.</li> <li>• Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.</li> </ul>
<p><b>8</b> Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<ol style="list-style-type: none"> <li>1. Si se indican problemas en el área Almacenamiento &amp; Disponibilidad de datos, pulse Agrupaciones para ver los detalles: <ul style="list-style-type: none"> <li>◦ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible.</li> <li>◦ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura.</li> </ul> </li> <li>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</li> </ol>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>
<p><b>9</b> Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento &amp; Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> <li>• En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes.</li> <li>• En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios.</li> <li>• Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.</li> </ul>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>10</b> Supervise los procesos de réplica de nodo.</p>	<ol style="list-style-type: none"> <li>1. Para obtener el estado global de los procesos de réplica de nodo, vea el área Réplica en la página Centro de operaciones Descripción general.</li> <li>2. Para ver información sobre cada par de servidores replicados, pulse el área de réplica.</li> <li>3. Para ver la cantidad de datos que se ha duplicado durante las dos últimas semanas y la velocidad de la duplicación, seleccione un par de servidores y pulse Detalles.</li> <li>4. Para ver la información de réplica para un cliente, en la página Centro de operaciones Descripción general, pulse Clientes. Vea la información en la columna Carga de trabajo de réplica.</li> </ol>	<p>Para la supervisión avanzadas, vea la información sobre cómo ejecutar y finalizar procesos de réplica de nodos utilizando mandatos:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general del Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY REPLICATION. Para obtener instrucciones, consulte QUERY REPLICATION (Consultar los procesos de réplica de nodos). Si la operación de réplica se ha completado satisfactoriamente, el valor de <code>Total de archivos a replicar</code> coincide con el valor de <code>Total de archivos replicados</code>.</li> </ol> <p>Para mostrar mensajes que están relacionados con el proceso de duplicación de un nodo en un servidor de réplica de origen o destino, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Visión general del Centro de operaciones pulse Servidores.</li> <li>2. Seleccione el servidor de réplica de origen o destino y pulse Detalles: <ul style="list-style-type: none"> <li>o Para ver tareas activas, pulse Tareas activas, seleccione la tarea y verifique que se muestra el estado En ejecución. Para obtener detalles, consulte los registros de actividad relacionados.</li> <li>o Para ver las tareas completadas, pulse Tareas completadas, seleccione la tarea y asegúrese de que se visualiza el estado Completado. Para obtener detalles, consulte los registros de actividad relacionados.</li> </ul> </li> </ol>

## Lista de comprobación de supervisión periódica

Para asegurarse de que la solución opera correctamente, complete las tareas en la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.




Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.







Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>. Busque el servidor asociado al cliente.</li> <li>2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>.</li> <li>3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>.</li> <li>4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones que encontrará en QUERY ACTLOG (Consultar las anotaciones de actividades).</li> <li>5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa.</li> </ol> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>.</li> <li>2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>.</li> <li>3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>.</li> </ol>	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento comunes del cliente</i>.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> <li>1. En la página <i>Centro de operaciones Descripción general</i>, pulse <i>Agrupaciones</i>.</li> <li>2. Seleccione una agrupación y pulse <i>Vista rápida</i>.</li> <li>3. En el área <i>Optimización de almacenamiento de datos</i>, vea la fila <i>Espacio guardado</i>.</li> </ol>	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores de nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la página <i>Descripción general de Centro de operaciones</i>, pase el ratón sobre el icono de configuración  y pulse <i>Creador de mandatos</i>.</li> <li>2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones que encontrará en GENERATE DEDUPSTATS (Generar estadísticas de deduplicación de datos respecto a una agrupación de almacenamiento de contenedores de directorio).</li> <li>3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones que encontrará en QUERY DEDUPSTATS (Consultar las estadísticas de deduplicación de datos).</li> </ol>


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory  query option devconfig</pre> </li> <li>3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.</li> </ol> <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	



Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine si está disponible espacio suficiente para el sistema de archivos del directorio de la instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad.</li> </ul> <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux /home/tsminst1/tsminst1</li> <li>•  Sistemas operativos Windows C:\tsminst1</li> </ul> <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

<b>Tarea</b>	<b>Procedimientos básicos</b>	<b>Procedimientos avanzados y solución de problemas</b>
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Clientes.</li> <li>2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente.</li> <li>3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades.</li> <li>4. En el área Última sesión, visualice la fila Enviado a cliente.</li> </ol>	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones.</li> <li>2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles.</li> </ol>	<p>Sugerencias:</p> <ul style="list-style-type: none"> <li>• Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> <li>3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>.</li> </ol> </li> <li>• Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>.</li> <li>• Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> </ol> </li> </ul> <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> <li>• Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.</li> </ul>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes &gt; Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones.</li> <li>2. Seleccione una planificación y pulse Detalles.</li> <li>3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila.</li> <li>4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado.</li> <li>5. Pulse Guardar.</li> </ol>
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores &gt; Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).</li> </ol>

**Referencia relacionada:**

QUERY ACTLOG (Consultar las anotaciones de actividades)

➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

➔ QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

## Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

### Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

#### Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

#### Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

#### Licencia de PVU

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.



Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

## Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
<b>Modelo frontal</b>	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
<b>Modelo suplementario</b>	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
<b>Modelo de PVU</b>	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.</p>

## Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

### Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.

- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

## Acerca de esta tarea

---

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

## Procedimiento

---

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:


1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.  
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

## Resultados

---

Los informes habilitados se envían según los valores especificados.

### Referencia relacionada:

 UPDATE ADMIN (Actualizar un administrador)

## Gestión de operaciones para una solución de disco multisitio

---

Utilice esta información para gestionar operaciones para una solución de disco multisitio con IBM Spectrum Protect que incluye un servidor y utiliza la eliminación de datos duplicados para varias ubicaciones.

- **Gestión del Centro de operaciones**  
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.
- **Protección de aplicaciones, máquinas virtuales y sistemas**  
El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.
- **Gestión del almacenamiento de datos**  
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Gestión de la réplica**  
Utilice la réplica para la recuperación de datos en el sitio de recuperación tras desastre y para mantener el mismo nivel de archivos en los servidores de origen y de destino. Puede gestionar réplicas en el nivel de nodo. También puede proteger datos en el nivel de agrupación de almacenamiento.
- **Protección del servidor**  
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**  
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**  
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**  
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Implementación de un plan de recuperación tras desastre**  
Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

- Recuperación de pérdida de datos o de paradas del sistema  
Puede utilizar IBM Spectrum Protect para recuperar los datos que se han perdido al producirse un siniestro o una parada del sistema. Puede recuperar agrupaciones de almacenamiento de contenedores de directorio, datos de cliente y bases de datos.

## Gestión del Centro de operaciones

---

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke  
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web  
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Reinicio del asistente de configuración inicial  
Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.
- Cambio del servidor concentrador  
Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.
- Restauración de la configuración a un estado de preconfiguración  
Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

## Adición y eliminación de servidores spoke

---

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

### Acerca de esta tarea

---

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio  
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke  
Puede eliminar un servidor spoke del Centro de operaciones.

## Adición de un servidor de radio

---

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

### Antes de empezar

---

Las comunicaciones entre el servidor spoke y el servidor concentrador deben asegurarse utilizando el protocolo de Seguridad de la capa de transporte (TLS). Para asegurar las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

### Procedimiento

---

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
  - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.

- Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.  
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente a 14 días, si configura el servidor como un servidor de radio.

## Eliminación de un servidor spoke

---

Puede eliminar un servidor spoke del Centro de operaciones.

### Acerca de esta tarea

---

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

### Procedimiento

---

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.

3. Emita el mandato siguiente en el servidor concentrador, donde *nombre\_grupo* representa el nombre del grupo supervisado y *nombre\_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```

## Inicio y detención del servidor web


---

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Es posible que tenga que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.


### Procedimiento

---

1. Detener el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation\_dir/ui/utls*, donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:


```
./stopserver.sh
```

-  Sistemas operativos Linux Emita el mandato siguiente:

```
service opscenter.rc stop
```


-  Sistemas operativos Windows En la ventana Servicios, detenga el servicio de IBM Spectrum Protect Operations Center.

2. Inicie el servidor web.

-  Sistemas operativos AIX Desde el directorio */installation\_dir/ui/utls*, donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:



```
./startserver.sh
```

-  Sistemas operativos Linux Emita los mandatos siguientes:

Inicie el servidor:


```
service opscenter.rc start
```

Reinicie el servidor:

```
service opscenter.rc restart
```

Determine si el servidor se está ejecutando:

```
service opscenter.rc status
```

-  Sistemas operativos Windows En la ventana Servicios, inicie el servicio IBM Spectrum Protect Operations Center.

## Reinicio del asistente de configuración inicial

---

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

### Antes de empezar

---

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:

- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.







### Acerca de esta tarea

---

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

### Procedimiento

---

1. Detenga el servidor web de Centro de operaciones.
  2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde *installation\_dir* representa el directorio en el que está instalado Centro de operaciones:
    -  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/Liberty/usr/servers/guiServer*
    -  Sistemas operativos Windows *dir\_instalación\ui\Liberty\usr\servers\guiServer*
- Por ejemplo:
-  Sistemas operativos AIX  Sistemas operativos Linux *opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer*
  -  Sistemas operativos Windows *c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer*
3. En el directorio *guiServer*, elimine el archivo *serverConnection.properties*.
  4. Inicie el servidor web Centro de operaciones.
  5. Abra el Centro de operaciones.
  6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
  7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

## Cambio del servidor concentrador

---

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

## Procedimiento

---

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

### Tareas relacionadas:

Reinicio del asistente de configuración inicial

## Restauración de la configuración a un estado de preconfiguración

---

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

## Procedimiento

---

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
  - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

Consejo: *IBM-OC-nombre\_servidor\_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

Atención: No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
  - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

Consejo: *IBM-OC-nombre\_servidor\_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

- e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

Atención: No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

Atención: No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restaure los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```

5. Reinicie el asistente de configuración inicial del Centro de operaciones.

#### Tareas relacionadas:

Reinicio del asistente de configuración inicial  
Inicio y detención del servidor web

## Protección de aplicaciones, máquinas virtuales y sistemas

---

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes  
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Gestión de operaciones de cliente  
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.
- Gestión de actualizaciones del cliente  
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- Poner fuera de servicio un nodo cliente  
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- Desactivación de datos para liberar espacio de almacenamiento  
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

## Adición de clientes

---

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

### Acerca de esta tarea

---

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

## Procedimiento

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones que encontrará en Selección del software de cliente y planificación de la instalación.
2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones que encontrará en Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones que encontrará en Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones que encontrará en Instalación y configuración de clientes.

## Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

### Acerca de esta tarea

La práctica preferida es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente para poder configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración en la documentación de producto para asegurarse de que se puede producir las operaciones planificadas.

## Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de archivado y copia de seguridad realiza la copia de seguridad y el archivado de archivos y directorios de los servidores de archivos y las estaciones de trabajo en el almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none"> <li>• Requisitos del cliente de archivado y copia de seguridad</li> <li>• Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li> <li>• Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul>

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM software de base de datos DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li> </ul>
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection for IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se han completado sin concluir servidores IBM Domino.	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> </ul>
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se han completado sin concluir servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de DB2 en el servidor IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de archivado y copia de seguridad puede utilizarse para hacer una copia de seguridad de los datos de Informix en el servidor de IBM Spectrum Protect.	Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection for SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect for Databases: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales almacenadas en un servidor centralizado, crear políticas de copia de seguridad y restaurar máquinas virtuales o archivos individuales.</p> <p>De forma alternativa, utilice el cliente de archivado y copia de seguridad para hacer la copia de seguridad y restauración de una máquina virtual de VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for Microsoft Hyper-V</li> <li>• Instalación y actualización de Data Protection for VMware</li> <li>• Instalación de clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)</li> </ul>

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

## Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

---

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

### Antes de empezar

---

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

### Acerca de esta tarea

---

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el periodo de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro de cliente, se asigna un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas activas* activo.

Cuando un cliente realiza la copia de seguridad o el archivado de un archivo, el archivo se vincula a una clase de gestión del conjunto de políticas activas activo del dominio de políticas. Una *clase de gestión* es el conjunto de claves de reglas para gestionar los datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo local editable del sistema cliente y en un conjunto de opciones de cliente en el servidor. Las opciones del conjunto de opciones de cliente en el servidor pueden alterar temporalmente las opciones del archivo de opciones del cliente local o añadirse a dichas opciones.

### Procedimiento

---

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

## Visualización de políticas

---

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

### Procedimiento

---

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
  - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
  - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas

- activas se resaltan.
- c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

## Edición de políticas

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

### Antes de empezar

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

### Acerca de esta tarea

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

### Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
<b>Añadir una clase de gestión</b>	<ol style="list-style-type: none"> <li>a. En la tabla Conjuntos de políticas, pulse +Clase de gestión.</li> <li>b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión.</li> <li>c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada.</li> <li>d. Pulse Añadir.</li> </ol>
<b>Suprimir una clase de gestión</b>	<p>En la columna Clase de gestión, pulse -.</p> <p>Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.</p>
<b>Establecer una clase de gestión como clase de gestión predeterminada</b>	<p>En la columna Predeterminada para la clase de gestión, pulse el botón de selección.</p> <p>Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.</p>
<b>Modificar una clase de gestión</b>	<p>Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.</p>

6. Pulse Guardar.
 

Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos

completando los pasos siguientes:

- a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
- b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.
- c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

## Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

### Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


### Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


### Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menú Centro de operaciones. Pulse Planificaciones.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
<b>Modificar una planificación</b>	<ol style="list-style-type: none"><li>a. En la vista Planificaciones, seleccione la planificación y pulse Detalles.</li><li>b. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas.</li><li>c. Modifique los valores de la planificación y pulse Guardar.</li></ol>
<b>Crear una planificación</b>	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
  - a. En la página Visión general del Centro de operaciones, pase el ratón por encima del icono de configuración  y pulse Creador de mandatos.
  - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

#### Tareas relacionadas:

 Ajuste de la planificación para las operaciones diarias

## Registro de clientes

Registrar un cliente para garantizar que el cliente pueda conectarse con el servidor y el servidor pueda proteger los datos de cliente.

### Antes de empezar



Determine si el cliente requiere un ID de usuario administrativo con autorización de propietario de cliente en el nodo de cliente. Para determinar qué clientes requieren un ID de usuario administrativo, consulte nota técnica 7048963.

Restricción: Para algunos tipos de clientes, el nombre de nodo de cliente y el ID de usuario administrativo deben coincidir. No se pueden autenticar los clientes utilizando el método de autenticación Lightweight Directory Access Protocol que se ha introducido en V7.1.7. Para obtener detalles sobre este método de autenticación, lo que a veces se denomina modalidad integrada, consulte Autenticación de los usuarios mediante una base de datos Active Directory.

## Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente necesita un ID de usuario administrativo, registre el cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node nombre_nodo contraseña userid=nombre_nodo
```

donde *nombre\_nodo* especifica el nombre de nodo y *contraseña* especifica la contraseña del nodo. Para obtener información detallada al respecto, consulte el apartado Registrar un nodo.

- Si el cliente no requiere un ID de usuario administrativo, registre el cliente mediante el asistente Agregar cliente de Centro de operaciones. Realice los pasos siguientes:

- a. En la barra de menús de Centro de operaciones, pulse Clientes.
- b. En la tabla Clientes, pulse + Cliente.
- c. Complete los pasos en el asistente Añadir cliente:
  - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de duplicados de datos del lado del cliente, active la casilla de verificación Habilitar.
  - ii. En la ventana Configuración, copie los valores de opción TCPSEVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.  
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
  - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
  - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
  - v. Pulse Añadir cliente.

### Referencia relacionada:

- [Opción Tcpserveraddress](#)
- [Opción Tcpport](#)
- [Opción Nodename](#)
- [Opción Deduplication](#)

## Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

## Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:
  - o Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li><li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li></ul> Para obtener información sobre el despliegue manual de actualizaciones de clientes del servidor, consulte los documentos siguientes: <ul style="list-style-type: none"><li>■ Para los servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.</li><li>■ Para servidores IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0, y servidores V8.1.1, consulte la nota técnica 1673299.</li></ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"><li>■ Instalación de Data Protection for Oracle</li><li>■ Instalación de Data Protection for SQL Server en Windows Server Core</li></ul>

Software	Enlace a instrucciones
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> <li>■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li> </ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> <li>■ Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux</li> <li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul>
Si planea crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo de cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> <li>■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments</li> </ul> <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSEVERADDRESS, TCPSPORT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (Registro de clientes).
  - Para los clientes que están instalados en un sistema operativo AIX, Linux o Mac OS X, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
  - Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt.

De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de clientes en el cliente. Siga las instrucciones que encontrará en Instalación del servicio de gestión de cliente.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones que encontrará en Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones que encontrará en Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
  - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

## Qué hacer a continuación

Para cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones que encontrará en Modificación del ámbito de una copia de seguridad de cliente.

## Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

## Acerca de esta tarea

---

El método preferido es instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Utilizando el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect for Databases, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que las operaciones planificadas se pueden producir.

Si la empresa utiliza una herramienta de planificación de terceros como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Normalmente, las herramientas de planificación de terceros inician los programas cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

## Procedimiento

---

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones para el sistema operativo que está instalado en el nodo cliente.

### AIX y Oracle Solaris

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- Para permitir que el aceptador de cliente se inicie automáticamente después del reinicio de un sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```

### Linux

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente iniciando sesión con el ID de usuario root y emitiendo el mandato siguiente:

```
service dsmcad start
```

- g. Para permitir que el aceptador de cliente pueda iniciarse automáticamente después del reinicio de un sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

#### MAC OS X

- En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

#### Windows

- En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- Consulte la información en la página Asistente del planificador y pulse Siguiente.
- En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- Complete la configuración paso a paso a través del asistente.
- Actualice el archivo de opciones de cliente, dsm.opt, y configure la opción passwordaccess como generate.
- Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El servicio de planificador se ha iniciado y detenido automáticamente mediante el servicio aceptador de cliente, según sea necesario.

## Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

---

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

### Antes de empezar

---

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores de opción en el archivo de opciones de cliente que ha obtenido durante ese proceso. Puede utilizar los valores para especificar puertos.

### Acerca de esta tarea

---

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

### Procedimiento

---

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente

Especifique el puerto utilizando la opción `tcpport` en el archivo de opciones de cliente. La opción `tcpport` del archivo de opciones de cliente debe coincidir con la opción `TCPPORT` en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas

Especifique el puerto para la estación de trabajo remota estableciendo la opción `httpport` en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

Puertos TCP/IP para la estación de trabajo remota

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción `webports` en el archivo de opciones de cliente de la estación de trabajo remota.

Puerto TCP/IP para sesiones de administración

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción `tcpadminport` de cliente debe coincidir con el valor de la opción de servidor `TCPADMINPORT`. De esta forma, puede asegurar las sesiones administrativas dentro de una red privada.

## Gestión de operaciones de cliente

---

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

### Acerca de esta tarea

---

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- Evaluación de errores en registros de errores de cliente  
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- Detención y reinicio del aceptador de cliente  
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- Restablecimiento de contraseñas  
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- Modificación del ámbito de una copia de seguridad de cliente  
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

## Evaluación de errores en registros de errores de cliente

---

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

### Antes de empezar

---

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación Instalación del servicio de gestión de cliente. Para obtener instrucciones sobre cómo verificar la instalación, consulte Verificación de que el servicio de gestión de clientes está instalado correctamente.

### Procedimiento

---

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Detalles.
  3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
  4. Revise los mensajes de registro recuperados.
 

Sugerencias:

    - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
    - Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.
  5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.
 

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

## Detención y reinicio del aceptador de cliente

---

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

### Acerca de esta tarea

---

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

### Procedimiento

---

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
  - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

## Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Iniciar y Aceptar.

### Referencia relacionada:

[Resolución de problemas de planificación del cliente](#)

## Restablecimiento de contraseñas

---

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

### Procedimiento

---

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nodo cliente y *nueva\_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como *generar* en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva\_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:
  1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
  2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
  3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nombre del nodo y *nueva\_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción passwordaccess como *generar* en el archivo de opciones del cliente.

## Modificación del ámbito de una copia de seguridad de cliente

---

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

## Acerca de esta tarea

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

## Procedimiento

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones que encontrará en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Para obtener información detallada al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción dominio. Siga las instrucciones que encontrará en Opción de cliente Domain.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

## Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

## Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

## Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>• Actualización del cliente de archivado y copia de seguridad</li></ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li></ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"><li>• Actualización de Data Protection for SQL Server</li><li>• Instalación de Data Protection for Oracle</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>



Software	Enlace a instrucciones
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li> <li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li> </ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> <li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li> </ul>
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"> <li>• Instalación y actualización de Data Protection for VMware</li> <li>• Instalación de Data Protection for Microsoft Hyper-V</li> </ul>

## Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

### Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

## Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:

1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
  2. Pulse Más > Poner fuera de servicio.
- Para poner fuera de servicio un nodo cliente utilizando un mandato administrativo, complete los pasos siguientes:
    1. Determine si el nodo cliente se ha configurado para la réplica de nodo emitiendo el mandato QUERY NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, ejecute el siguiente mandato:

```
query node austin format=detailed
```

Revise el campo de salida de Estado de réplica.

2. Si el nodo cliente se ha configurado para la réplica, elimine el nodo cliente de la réplica emitiendo el mandato REMOVE REPLNODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
remove replnode austin
```

3. Realice una de las siguientes acciones:

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:
  - Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
  - Un valor null especifica que el nodo no está fuera de servicio.
  - Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

Proceso	Descripción proceso	Estado proceso
proceso		

-----

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

**Referencia relacionada:**

- 🔗 DECOMMISSION NODE (Poner fuera de servicio un nodo de cliente)
- 🔗 DECOMMISSION VM (Poner fuera de servicio una máquina virtual)
- 🔗 QUERY NODE (Consultar nodos)
- 🔗 REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)

## Desactivación de datos para liberar espacio de almacenamiento

---

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

### Acerca de esta tarea

---

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

### Procedimiento

---

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.  
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

**Referencia relacionada:**

- 🔗 DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

## Gestión del almacenamiento de datos

---

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Auditoría de un contenedor de la agrupación de almacenamiento  
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.
- Gestión de la capacidad de inventario  
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- Gestión del uso de la memoria y del procesador  
Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.
- Ajuste de actividades planificadas  
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

**Referencia relacionada:**

- 🔗 Tipos de agrupaciones de almacenamiento

# Auditoría de un contenedor de la agrupación de almacenamiento

---

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre información de base de datos y un contenedor en una agrupación de almacenamiento.

## Acerca de esta tarea

---

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

## Procedimiento

---

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 00000000000076c.dcf:

```
audit container c:\tsm-storage\07\00000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

## Qué hacer a continuación

---

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración. Puede reparar el contenido de la agrupación de almacenamiento utilizando el mandato REPAIR STGPOOL.

Restricción: Solo puede reparar el contenido de la agrupación de almacenamiento si ha protegido dicha agrupación de almacenamiento mediante el mandato PROTECT STGPOOL.

### Referencia relacionada:

- ➔ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)
- ➔ QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

# Gestión de la capacidad de inventario

---

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

## Antes de empezar

---

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

## Procedimiento

---

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
    - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
    - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.
- Sugerencias:

- El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
  - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
    - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
    - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.
- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:

Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
  5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

**Referencia relacionada:**

- ➔ ACTIVELOGSIZE, opción de servidor
- ➔ EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- ➔ SETOPT (Establecer una opción de servidor para actualización dinámica)

## Gestión del uso de la memoria y del procesador

---

Asegúrese de que gestiona requisitos de memoria y el uso de procesador para garantizar que el servidor puede completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

### Antes de empezar

---

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos admitidos para IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

### Procedimiento

---

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

## Ajuste de actividades planificadas

---

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

### Procedimiento

---

1. Supervise el rendimiento del sistema de forma periódica para asegurarse de que las tareas de copia de seguridad de cliente y de mantenimiento de servidor se completan satisfactoriamente. Siga las instrucciones que encontrará en Supervisión de una solución de disco multisitio.
2. Opcional: Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, revise la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
  - El número de clientes aumenta.
  - La cantidad de datos de los que se hace copia de seguridad aumenta.
  - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución está funcionando en el nivel esperado. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
  - b. Pulse Detalles.
  - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos.Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.

4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
  - a. Proteger agrupaciones de almacenamiento.
  - b. Replicar datos de nodo.
  - c. Realizar una copia de seguridad de la base de datos.
  - d. Ejecutar el proceso de caducidad para eliminar copias de seguridad de cliente y copias de archivo de archivado del almacenamiento de servidor.

Consejo: Planificar que las tareas de mantenimiento se inicien a una hora adecuada y en la secuencia correcta. Por ejemplo, planificar tareas de réplica después de que las copias de seguridad de cliente se completen satisfactoriamente.
- Traslado de clientes de un servidor a otro
 

Para evitar quedarse sin espacio en un servidor o para resolver problemas de carga de trabajo, es posible que tenga que mover los nodos cliente de un servidor a otro.

**Conceptos relacionados:**

➔ Rendimiento

**Tareas relacionadas:**

Definición de planificaciones para actividades de mantenimiento del servidor

➔ Deduplicación de datos (V7.1.1)

## Gestión de la réplica

Utilice la réplica para la recuperación de datos en el sitio de recuperación tras desastre y para mantener el mismo nivel de archivos en los servidores de origen y de destino. Puede gestionar réplicas en el nivel de nodo. También puede proteger datos en el nivel de agrupación de almacenamiento.

- Compatibilidad de réplica
 

Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino son compatibles para la réplica.
- Habilitación de la réplica de nodo
 

Puede habilitar la réplica de nodo para proteger los datos.
- Protección de datos en agrupaciones de almacenamiento de contenedor de directorios
 

Proteja los datos de agrupaciones de almacenamiento de contenedor de directorios para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedor de directorios.
- Modificación de los valores de réplica
 

Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.
- Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino
 

Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

## Compatibilidad de réplica

Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino son compatibles para la réplica.

Tabla 1. Compatibilidad de réplica de versiones de servidor

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V6.3.0 - V6.3.2	V6.3.0 - V6.3.2
V6.3.3	V6.3.3 o niveles posteriores de V6.3
V6.3.4 o niveles posteriores de V6.3	V6.3.4 o posterior
V7.1	V7.1 o posterior
V7.1.1	V7.1 o posterior
V7.1.3	V7.1.3 o posterior
V7.1.4	V7.1.3 o posterior
V7.1.5	V7.1.3 o posterior
V7.1.6	V7.1.3 o posterior

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V7.1.7	V7.1.3 o posterior
V8.1	V7.1.3 o posterior
V8.1.1	V7.1.3 o posterior
V8.1.2	V7.1.3 o posterior

## Habilitación de la réplica de nodo

---

Puede habilitar la réplica de nodo para proteger los datos.

### Antes de empezar

---

Asegúrese de que los servidores de origen y destino son compatibles para la réplica.

### Acerca de esta tarea

---

Replique el nodo de cliente para replicar todos los datos de cliente, incluyendo metadatos. De forma predeterminada, la réplica de nodo está inhabilitada, cuando se inicia el servidor por primera vez.

Sugerencias:

- Para reducir el tiempo de proceso de réplica, proteja la agrupación de almacenamiento antes de replicar los nodos de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya se han replicado a través de la protección de agrupación de almacenamiento se omiten.
- La réplica requiere cantidades aumentadas de memoria y ancho de banda suficiente para completar el proceso. Cambie el tamaño de la base de datos y sus registros para garantizar que las transacciones se pueden completar.

### Procedimiento

---


Para habilitar la réplica de nodo, complete los siguientes pasos en Centro de operaciones:

- En la página Servidores, pulse Detalles.
- En la página Detalles, pulse Propiedades.
- En la sección Réplica, seleccione Habilitada en el campo Réplica de salida.
- Pulse Guardar.

### Qué hacer a continuación

---

Realice las acciones siguientes:

- Para verificar que la réplica es correcta, revise Lista de comprobación de supervisión diaria.
-  Sistemas operativos Linux Si el servidor de IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología de Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos con el servidor remoto. Siga las instrucciones que encontrará en Determinación de si la tecnología de Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

#### Referencia relacionada:

Compatibilidad de réplica

## Protección de datos en agrupaciones de almacenamiento de contenedor de directorios

---

Proteja los datos de agrupaciones de almacenamiento de contenedor de directorios para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedor de directorios.

### Antes de empezar

---

Asegúrese de que exista al menos una agrupación de contenedores en directorios en el servidor de réplica de destino. Cuando habilita la réplica en el Centro de operaciones, puede planificar la protección de agrupación de almacenamiento. Para configurar la réplica y habilitar la protección de agrupación de almacenamiento, complete los siguientes pasos:



1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
2. En la página de réplica, pulse Par de servidores.
3. Complete los pasos del asistente Añadir par de servidores.

## Acerca de esta tarea

---

La protección de una agrupación de almacenamiento de contenedores de directorios hace copias de seguridad de extensiones en otra agrupación de almacenamiento y puede mejorar el rendimiento para la réplica de nodos. Cuando se inicia la réplica de nodo, se omiten las extensiones de datos de las que ya se han hecho copias de seguridad a través de la protección de la agrupación de almacenamiento, lo cual reduce el tiempo de proceso de la réplica. Puede planificar la protección de agrupaciones de almacenamiento varias veces al día para estar al día con los cambios realizados en los datos.

Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor. Debe utilizar agrupaciones de almacenamiento de contenedores de directorios si solo desea proteger y realizar la copia de seguridad de la agrupación de almacenamiento.

Estrategia de protección alternativa: Como alternativa al uso de la réplica, puede proteger los datos de las agrupaciones de almacenamiento de contenedores de directorios copiando los datos en agrupaciones de almacenamiento de copia de contenedor. Los datos de las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta. Las copias de cinta que se almacenan fuera del local proporcionan protección de recuperación tras desastre adicional en un entorno replicado.

## Procedimiento

---

1. Como alternativa para habilitar la protección de agrupación de almacenamiento, puede utilizar el mandato PROTECT STGPOOL desde el servidor de origen para realizar la copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedor de directorios. Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio denominada POOL1, emita el siguiente mandato:

```
protect stgpool pool1
```

Como parte de la operación del mandato PROTECT STGPOOL, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato AUDIT CONTAINER podría identificar daños en la agrupación de almacenamiento de destino antes de que se emite el mandato PROTECT STGPOOL.

2. Opcional: Si las extensiones dañadas se han reparado en la agrupación de almacenamiento de destino y protege varias agrupaciones de almacenamiento de origen en una agrupación de almacenamiento de destino, complete los pasos siguientes para garantizar una reparación completa:
  - a. Emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen para reparar el máximo daño posible.
  - b. Vuelva a emitir el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen. Para esta segunda operación, utilice el parámetro FORCERECONCILE=YES. Este paso garantiza que las reparaciones de otras agrupaciones de origen se reconocen correctamente para todas las agrupaciones de almacenamiento de origen.

## Resultados

---


Si una agrupación de almacenamiento de contenedores de directorios está protegida, puede reparar la agrupación de almacenamiento si se producen daños, emitiendo el mandato REPAIR STGPOOL.

Restricción: Si duplica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorios, no puede reparar la agrupación de almacenamiento.


## Qué hacer a continuación


---

Realice las acciones siguientes:

1. Para ver el estado de la carga de trabajo de la réplica, siga las instrucciones que encontrará en Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor de IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología de Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos con el servidor remoto. Siga las instrucciones que encontrará en Determinación de si la tecnología de Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

### Referencia relacionada:

 Reparación y recuperación de datos

 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

🔗 PROTECT STGPOOL (Proteger datos de agrupación de almacenamiento)

**Información relacionada:**

🔗 Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de directorio

🔗 Preguntas más frecuentes sobre agrupaciones de almacenamiento de contenedores de nube

## Modificación de los valores de réplica

Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.

### Acerca de esta tarea

Es posible que tenga que personalizar los valores de réplica en los siguientes escenarios:

- Cambios en las prioridades de datos
- Cambios en reglas de réplica
- Requisito para que un servidor diferente sea el servidor de destino
- Procesos planificados que afectan de forma negativa al rendimiento de servidor

### Procedimiento

Utilice Centro de operaciones para modificar valores de réplica.

Tarea	Procedimiento
Cambiar una regla de réplica.	<ol style="list-style-type: none"><li>En la página Servidores, pulse Detalles.</li><li>En la página Detalles, pulse Propiedades.</li><li>En la sección Réplica, elija la regla de réplica que desea aplicar: Regla de archivado predeterminada, Regla de copia de seguridad predeterminada, o Regla de gestión de espacio predeterminada.</li><li>Pulse Guardar.</li></ol>
Especifique el tiempo que se retienen los registros de réplica.	<ol style="list-style-type: none"><li>En la página Servidores, pulse Detalles.</li><li>En la página Detalles, pulse Propiedades.</li><li>En la sección Réplica, entre el número de días que deben retenerse los registros de réplica en el campo Retener historial de réplica. Sino, seleccione la casilla de verificación No retener si no necesita registros de réplica.</li><li>Pulse Guardar.</li></ol>
Especifique un servidor de réplica de destino.	<ol style="list-style-type: none"><li>En la página Servidores, pulse Detalles.</li><li>En la página Detalles, pulse Propiedades.</li><li>En la sección Réplica, especifique el servidor de destino.</li><li>Pulse Guardar.</li></ol>
Cancele un proceso de réplica.	<ol style="list-style-type: none"><li>En la página Servidores, pulse Tareas activas.</li><li>Seleccione el proceso o sección que desea cancelar.</li><li>Pulse Cancelar.</li></ol>

## Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino

Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

### Procedimiento

1. Desde el servidor de réplica fuente, valide la configuración de réplica y verifique que el servidor de réplica de origen se puede comunicar con el servidor de réplica de destino emitiendo el mandato VALIDATE REPLICATION. Por ejemplo, valide la configuración utilizando el nombre de un nodo de cliente que se está duplicando:

```
validate replication node1 verifyconnection=yes
```

2. Desde el servidor de réplica fuente, emita el mandato VALIDATE REPLPOLICY para revisar las diferencias entre las políticas en los servidores de réplica fuente y de destino. Por ejemplo, para mostrar las diferencias entre las políticas en el servidor de origen y el servidor de destino, CVT\_SRV2, emita el mandato siguiente desde el servidor de origen:

```
validate replpolicy cvt_srv2
```

3. Actualice las políticas en el servidor de destino, si es necesario.

Consejo: Puede utilizar Centro de operaciones para modificar las políticas en el servidor de destino. Siga las instrucciones que encontrará en Edición de políticas.

Por ejemplo, para mantener versiones inactivas de archivos durante un periodo de tiempo más corto en el servidor de destino que en el servidor de origen, reduzca el valor de Copias de seguridad en las clases de gestión que se aplican a datos de cliente replicados.

4. Permita al servidor de réplica de destino utilizar sus políticas para gestionar los datos del nodo de cliente replicado emitiendo el mandato SET DISSIMILARPOLICIES en el servidor de origen. Por ejemplo, para habilitar las políticas en el servidor de réplica de destino, CVT\_SRV2, emita el mandato siguiente en el servidor de origen:

```
set dissimilarpolicies cvt_srv2 on
```

La próxima vez que se ejecuta el proceso de réplica, se utilizan las políticas en el servidor de réplica de destino para gestionar los datos del nodo del cliente duplicado.

Consejo: Si configura la réplica utilizando el Centro de operaciones y las políticas en los servidores de réplica de origen y destino no coinciden, se utiliza la política especificada para el servidor de réplica de origen. Si ha habilitado las políticas en el servidor de réplica de destino utilizando el mandato SET DISSIMILARPOLICIES, se utiliza la política especificada para el servidor de réplica de destino. Si el servidor de réplica de destino no tiene la política que utiliza el nodo en servidor de réplica de origen, se utiliza la política STANDARD.

#### Referencia relacionada:

- EXPORT POLICY (Exportar información de política)
- SET DISSIMILARPOLICIES (Habilitar las políticas en el servidor de réplica de destino para gestionar daños replicados)
- VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)
- VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

## Protección del servidor

---

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- Conceptos sobre la seguridad  
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- Gestión de administradores  
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.
- Cambio de los requisitos de contraseña  
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- Protección de IBM Spectrum Protect en el sistema  
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

## Conceptos sobre la seguridad

---

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

## Seguridad de la capa de transporte

---

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

## Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

## Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días.  El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

## Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL,

se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos de cliente	<ul style="list-style-type: none"> <li>REGISTER NODE</li> <li>UPDATE NODE</li> </ul>
Administradores	<ul style="list-style-type: none"> <li>REGISTER ADMIN</li> <li>UPDATE ADMIN</li> </ul>
Servidores	<ul style="list-style-type: none"> <li>DEFINE SERVER</li> <li>UPDATE SERVER</li> </ul>

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

#### Tareas relacionadas:

[Protección de las comunicaciones](#)

## Gestión de administradores

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

### Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	<p>Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:</p> <ol style="list-style-type: none"> <li>Registre el administrador y especifique Pa\$# \$twO como contraseña ejecutando el siguiente mandato: <pre>register admin admin1 Pa\$# \$twO</pre> </li> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> </li> </ol>

Tarea	Procedimiento
Cambie los permisos del administrador.	<p>Cambie el nivel de autorización de un administrador, ADMIN1.</p> <ul style="list-style-type: none"> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> </li> <li>Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <pre>revoke authority admin1 classes=system</pre> </li> </ul>
Elimine administradores.	<p>Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect:</p> <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	<p>Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.</p>

## Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

### Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

### Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</li> <li>Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</li> </ol> <p>El valor predeterminado en la instalación es 0.</p>
Establezca una longitud mínima para las contraseñas.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>Establezca el número de caracteres en el campo Longitud de contraseña mínima.</li> </ol>
Establezca el periodo de caducidad para las contraseñas.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>Establecer el número de días en el campo Caducidad común de la contraseña.</li> </ol>

Tarea	Procedimiento
Inhabilitar la autenticación de contraseña.	De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.  Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.
Establecer un método de autenticación predeterminado.	Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:  <code>set defaultauthentication local</code>  Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:  <code>update node authentication=local</code>

**Conceptos relacionados:**

- Autenticación de usuarios de IBM Spectrum Protect utilizando un servidor LDAP
- Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1)

## Protección de IBM Spectrum Protect en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

### Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor  
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.
- Limitación de acceso a través de restricciones de puerto  
Limitar acceso al servidor aplicando restricciones de puerto.

## Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

### Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
  - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
  - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grave en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique

el parámetro BACKUPINITIATION=root:  
update node backupinitiation=root

## Limitación de acceso a través de restricciones de puerto

Limitar acceso al servidor aplicando restricciones de puerto.

### Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

### Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPPOINT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPPOINT.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPOINT y SSLTCPPOINT.
SSLTCPPOINT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.
SSLTCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPOINT y SSLTCPPOINT.

**Referencia relacionada:**

Planificación del acceso de cortafuegos

## Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

### Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**  
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.
- **Inicio del servidor para tareas de mantenimiento o reconfiguración**  
Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Detención del servidor



Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

## Acerca de esta tarea

---

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

## Procedimiento

---

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:
  - a. En la página *Visión general* del Centro de operaciones, vea el área *Actividad* para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.
  - b. Vea el gráfico en el área *Actividad* para comparar la cantidad de tráfico de red durante los periodos siguientes:
    - El periodo actual, es decir, el periodo de 24 horas más reciente
    - El periodo anterior, es decir, 24 horas antes del periodo actualSi el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.
  - c. En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.
3. Espere hasta que las sesiones de nodo cliente se completen o cancélelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:
  - En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*.
  - Pulse el separador *Tareas activas* y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - Pulse *Cancelar*.
  - Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.  
Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.
4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

## Inicio del servidor para tareas de mantenimiento o reconfiguración

---

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente

- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, `dsm serv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

## Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsm serv maintenance
```

Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.




## Qué hacer a continuación

---

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
  -  Sistemas operativos AIX Inicio de la instancia de servidor
  -  Sistemas operativos Linux Inicio de la instancia de servidor
  -  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

## Planificación para actualizar el servidor

---

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

## Acerca de esta tarea

---

Siga estas directrices:

- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

## Procedimiento




---

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.  
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.


## Qué hacer a continuación

---

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

#### Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

## Preparación para una parada o actualización de sistema

---

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

### Acerca de esta tarea

---

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor.

### Procedimiento

---

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
  - a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
  - b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - c. Pulse Cancelar.
2. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

## Implementación de un plan de recuperación tras desastre

---

Implemente una estrategia de recuperación tras desastre para recuperar las aplicaciones si se produce un desastre y para garantizar una alta disponibilidad del servidor.

### Acerca de esta tarea

---

Determine los requisitos que necesita para recuperación tras desastre identificando las prioridades empresariales respecto a la recuperación de nodo de cliente, los sistemas que utiliza para recuperar datos y si los nodos de cliente tienen conectividad con el servidor de recuperación. Utilice la réplica y la protección de agrupación de almacenamiento para proteger datos. También debe determinar la frecuencia con la que se protegen las agrupaciones de almacenamiento de contenedores de directorio.

- Realización de la obtención de detalles de recuperación  
Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

## Recuperación de pérdida de datos o de paradas del sistema

---

Puede utilizar IBM Spectrum Protect para recuperar los datos que se han perdido al producirse un siniestro o una parada del sistema. Puede recuperar agrupaciones de almacenamiento de contenedores de directorio, datos de cliente y bases de datos.

### Antes de empezar

---

Planifique las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Emita los mandatos PROTECT STGPOOL y REPLICATE NODE como parte de la planificación. Proteja la agrupación de almacenamiento antes de replicar el nodo de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya están replicadas a través de la protección de agrupación de almacenamiento se omiten, lo que reduce el tiempo de proceso de réplica.

### Procedimiento

---

Utilice los siguientes métodos de recuperación basándose en el componente que debe recuperar.

<b>Componente a recuperar</b>	<b>Procedimiento</b>	<b>Más información</b>
Agrupación de almacenamiento de contenedores de directorio	<p>Para recuperar agrupaciones de almacenamiento de contenedores de directorio, complete los siguientes pasos:</p> <ul style="list-style-type: none"><li>a. Explore las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio utilizando el mandato AUDIT CONTAINER y especificando el parámetro ACTION=SCANALL.</li><li>b. Repare las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio utilizando el mandato REPAIR STGPPOOL. Restricción: Solo puede reparar una agrupación de almacenamiento si dicha agrupación de almacenamiento está protegida.</li><li>c. Elimine las extensiones de datos dañadas utilizando el mandato AUDIT CONTAINER y especificando el parámetro ACTION=REMOVEDAMAGED.</li></ul>	Reparación de agrupaciones de almacenamiento


Componente a recuperar	Procedimiento	Más información
Datos de cliente	<p>Requisitos previos:</p> <ul style="list-style-type: none"> <li>El servidor de réplica de origen, el servidor de réplica de destino y el cliente deben estar en el nivel V7.1 o posterior. Si alguno de los servidores está en un nivel anterior, la migración tras error automática se inhabilita y debe confiar en la migración tras error manual.</li> </ul> <p>Configure manualmente el cliente para migrar tras error automáticamente al servidor de destino para la recuperación de datos.</p> <p>Si ha habilitado el cliente para una migración tras error de cliente automatizada, puede recuperar los datos utilizando la función de migración tras error automática. Puede verificar que la opción <code>usereplicationfailover</code> no está en el archivo de opciones de cliente o está establecida en <code>si</code>. Recupere datos del servidor de destino cuando el servidor de destino no esté disponible debido a una parada utilizando la migración tras error automática.</p> <p>Consejo:</p> <ul style="list-style-type: none"> <li>Utilice el mandato <code>SET FAILOVERHLADDRESS</code> para especificar la dirección IP para el servidor de réplica durante la migración tras error, si la dirección es diferente de la dirección IP especificada para el proceso de réplica.</li> </ul>	<ul style="list-style-type: none"> <li>Recuperación de datos dañados de una copia replicada</li> <li><code>SET FAILOVERHLADDRESS</code> (Establecer una dirección de alto nivel de migración tras error)</li> </ul>
Base de datos	<p>Requisitos previos:</p> <ul style="list-style-type: none"> <li>Para restaurar la base de datos después de un siniestro, debe tener una copia del archivo de configuración del dispositivo actual. El archivo de configuración del dispositivo no se puede volver a crear.</li> <li>Asegúrese de que tiene una versión de seguridad de la base de datos.</li> </ul> <p>Restaura la base de datos de IBM Spectrum Protect al estado más actual o a un punto específico en el tiempo utilizando el programa de utilidad del servidor <code>DSMSERV RESTORE DB</code>.</p>	<p><code>DSMSERV RESTORE DB</code> (Restaurar la base de datos)</p>


- Restauración de la base de datos  
Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base

de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

- Recuperación de datos dañados de una copia replicada  
Si no hay disponible un servidor de réplica de origen, puede recuperar los datos dañados de la copia replicada almacenada en el servidor de réplica de destino.
- Reparación de agrupaciones de almacenamiento  
Si se ha producido un desastre o parada del sistema, puede reparar las extensiones de datos duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio.

**Referencia relacionada:**

 [AUDIT CONTAINER](#) (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

 [DSMSERV RESTORE DB](#) (Restaurar la base de datos)

## Restauración de la base de datos

---

Es posible que tenga que restaurar la base de datos de IBM Spectrum Protect después de un siniestro. Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Debe tener volúmenes de copia de seguridad de base de datos de instantánea, completos o incrementales para restaurar la base de datos.

### Antes de empezar

---

Si los directorios de la base de datos y el registro de recuperación se han perdido, vuelva a crearlos antes de emitir el programa de utilidad del servidor DSMSERV RESTORE DB. Por ejemplo, utilice los mandatos siguientes:

 **Sistemas operativos Linux**

```
mkdir /tsmdb001
mkdir /tsmdb002
mkdir /tsmdb003
mkdir /activelog
mkdir /archlog
mkdir /archfaillog
```

 **Sistemas operativos Windows**

```
mkdir e:\tsm\db001
mkdir f:\tsm\db001
mkdir g:\tsm\db001
mkdir h:\tsm\activelog
mkdir i:\tsm\archlog
mkdir j:\tsm\archfaillog
```

**Restricciones:**

- Para restaurar la base de datos a la versión más reciente, debe ubicar el directorio de registro de archivado. Si no puede ubicar el directorio, puede restaurar la base de datos sólo en un momento específico.
- No puede utilizar la capa de sockets seguros (SSL) para las operaciones de restauración de la base de datos.
- Si el nivel de release de la copia de seguridad de base de datos es diferente del nivel de release del servidor que se está restaurando, no puede restaurar la base de datos del servidor. Por ejemplo, si está utilizando un servidor de la Versión 8.1 e intenta restaurar una base de datos de la Versión 7.1, se produce un error.

### Acerca de esta tarea

---

Las operaciones de restauración en un momento específico se utilizan generalmente para situaciones como la recuperación tras desastre o para eliminar los efectos de errores que pueden provocar incoherencias en la base de datos. Para recuperar la base de datos al instante en que se ha perdido la base de datos, recupérela a su estado actual.

### Procedimiento

---

Utilice el programa de utilidad del servidor DSMSERV RESTORE DB para restaurar la base de datos. En función de la versión de la base de datos que desee restaurar, elija uno de los siguientes métodos:

- Restaure una base de datos a su versión más reciente. Por ejemplo, utilice este mandato:

```
dsmserv restore db
```

- Restaura una base de datos a un momento específico. Por ejemplo, para restaurar la base de datos a una serie de copias de seguridad que se ha creado el 19 de abril de 2015, utilice el siguiente mandato:

```
dmserv restore db todate=04/19/2015
```

## Qué hacer a continuación

Si ha restaurado la base de datos y existen agrupaciones de almacenamiento de contenedores de directorio en el servidor, debe identificar las incoherencias entre la base de datos y el sistema de archivos.

1. Si ha restaurado la base de datos a un punto en el tiempo y no ha retardado la reutilización de la agrupación de almacenamiento de contenedores de directorio, debe auditar todos los contenedores. Para auditar todos los contenedores, emita el siguiente mandato:

```
audit container stgpool
```

2. Si el servidor no puede identificar contenedores en el sistema, complete los pasos siguientes para mostrar una lista de contenedores:

- a. Desde un cliente administrativo, emita el mandato siguiente:


```
select container_name from containers
```

- b. Desde el sistema de archivos, emita el siguiente mandato para el directorio de la agrupación de almacenamiento en el servidor de origen:

Consejo: El directorio de la agrupación de almacenamiento se visualiza en la salida del mandato:

 Sistemas operativos AIX  Sistemas operativos Linux


```
[root@source]$ ls -l
```

 Sistemas operativos Windows


```
c:\source_stgpool\dir\00>dir
```


- c. Compare los contenedores listados en el sistema de archivos y el servidor.
- d. Emita el mandato AUDIT CONTAINER y especifique el contenedor que falta de la salida del servidor. Especifique el parámetro ACTION=REMOVEDAMAGED para suprimir el contenedor.
- e. Para asegurarse de que los contenedores se suprimen en el sistema de archivos, revise los mensajes que se muestran.

### Tareas relacionadas:

 Réplica de datos de nodo de cliente después de una restauración de la base de datos (V7.1.1)

### Referencia relacionada:

 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

 DSMSEV RESTORE DB (Restaurar la base de datos)

## Recuperación de datos dañados de una copia replicada

Si no hay disponible un servidor de réplica de origen, puede recuperar los datos dañados de la copia replicada almacenada en el servidor de réplica de destino.

### Antes de empezar

El nombre del servidor que especifica con el mandato SET REPLSERVER debe coincidir con el nombre de una definición de servidor existente. También debe ser el nombre del servidor que se va a utilizar como servidor de réplica de destino. Si el nombre de servidor especificado por este mandato no coincide con el nombre de servidor de una definición de servidor existente, el mandato falla.

Consejo:

- Tenga cuidado cuando cambie o elimine un servidor de réplica de destino. Si cambia un servidor de réplica de destino, los datos de nodo cliente replicados se envían a un servidor de réplica de destino diferente. Si elimina un servidor de réplica de destino, los datos del nodo cliente no se replican.

### Procedimiento

1. Verifique el estado de réplica de los datos en el servidor de destino. El estado indica si la réplica de copia de seguridad más reciente se ha replicado en el servidor secundario.
2. Restaura los datos desde un servidor de réplica de destino estableciendo el servidor de réplica de origen como servidor de réplica de destino. Por ejemplo, si desea establecer el servidor de réplica de origen como servidor de réplica de destino, server1,

emita el siguiente mandato:

```
set replserver server1
```

## Qué hacer a continuación

---

Al restaurar la base de datos de IBM Spectrum Protect en un servidor de réplica de origen, la réplica se inhabilita automáticamente. Antes de volver a habilitar la réplica, determine si las copias de datos que están en el servidor de réplica de destino son necesarias.

### Tareas relacionadas:

🔗 Réplica de datos de nodo de cliente después de una restauración de la base de datos (V7.1.1)

## Reparación de agrupaciones de almacenamiento

---

Si se ha producido un desastre o parada del sistema, puede reparar las extensiones de datos duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio.

## Antes de empezar

---

Identifique las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio utilizando el mandato AUDIT CONTAINER. Mediante la identificación de las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar.

Antes de reparar una agrupación de almacenamiento, asegúrese de que la agrupación de almacenamiento esté protegida mediante el mandato PROTECT STGPOOL.

## Procedimiento

---

1. Para reparar una agrupación de almacenamiento de contenedores de directorio, utilice el mandato REPAIR STGPOOL. Por ejemplo, para reparar una agrupación de almacenamiento, STGPOOL1, emita el mandato siguiente:

```
repair stgpool stgpool1
```

2. Si la agrupación de almacenamiento dañada se especifica como una agrupación de almacenamiento de destino en el mandato PROTECT STGPOOL para una o varias agrupaciones de almacenamiento de origen, emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen.
3. Para asegurarse de que todos los datos dañados se identifiquen y reparen desde otras agrupaciones de almacenamiento de origen, emita el mandato PROTECT STGPOOL de nuevo desde todas las agrupaciones de almacenamiento de origen y especifique el parámetro FORCERECONCILE=YES.
4. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.
5. Si la agrupación de almacenamiento dañada es una agrupación de almacenamiento de destino para la réplica de nodos de uno o varios servidores de origen, emita el mandato REPLICATE NODE de nuevo desde todos los servidores de origen.
6. Cuando el daño esté reparado, emita el mandato PROTECT STGPOOL para asegurarse de que la agrupación de almacenamiento esté protegida en otra agrupación de almacenamiento de contenedores de directorios.

## Qué hacer a continuación

---

Asegúrese de que las extensiones de datos no dañadas se visualizan en la salida utilizando el mandato QUERY DAMAGED.

### Referencia relacionada:

🔗 Reparación y recuperación de datos

🔗 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

🔗 QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores de nube)

🔗 REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

## Solución de cinta

---

Esta solución de protección de datos proporciona almacenamiento a soportes de cinta, una opción flexible y asequible para la retención de datos a largo plazo.

- Planificación de una solución de protección de datos basada en cinta  
Planifique una solución de protección de datos que incluya operaciones de copia de seguridad de disco a cinta y de disco a disco



a cinta para optimizar el almacenamiento.

- Implementación de una solución de protección de datos basada en cinta  
Implemente la solución basada en cinta, que utiliza copia de seguridad 'de disco a disco a cinta' y disco intermedio para optimizar el almacenamiento. Al implementar la solución de cinta, puede habilitar la retención de datos a largo plazo y lograr una escalabilidad de bajo coste.
- Supervisión de una solución de cinta  
Tras implementar una solución basada en cinta de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.
- Gestión de operaciones para una solución de cinta  
Utilice esta información para gestionar las operaciones para una implementación de cinta para un servidor IBM Spectrum Protect.

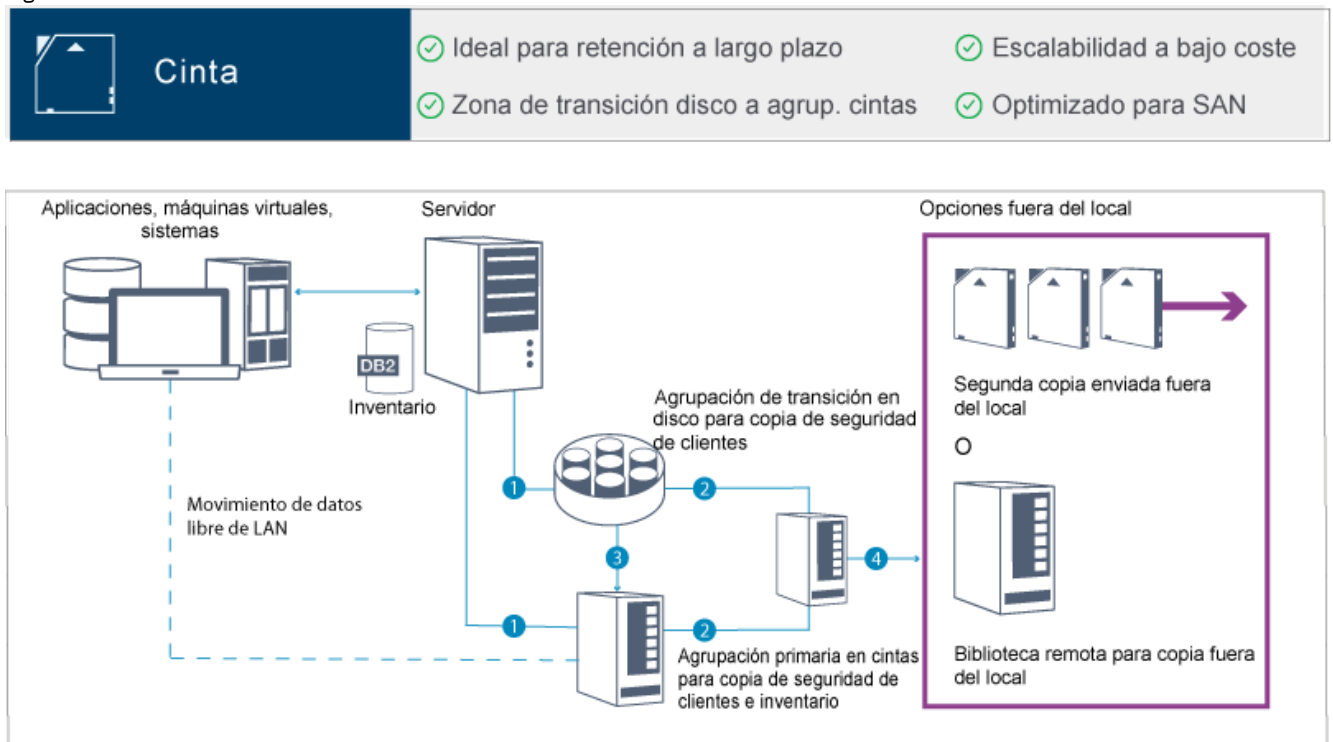
## Planificación de una solución de protección de datos basada en cinta

Planifique una solución de protección de datos que incluya operaciones de copia de seguridad de disco a cinta y de disco a disco a cinta para optimizar el almacenamiento.

### Hoja de vía de acceso de planificación

Planifique la solución de cinta revisando el diseño de la arquitectura en Figura 1 y completando después las tareas de la hoja de ruta que siguen al diagrama.

Figura 1. Solución de cinta



En esta configuración de protección de datos, el servidor utiliza hardware de almacenamiento de disco y de cinta. Se utiliza la transferencia de agrupaciones de almacenamiento, en la que los datos de cliente se almacenan inicialmente en agrupaciones de almacenamiento de disco y, a continuación, se migran a las agrupaciones de almacenamiento de cinta. Para la recuperación tras desastre, los volúmenes de cinta se pueden almacenar fuera del local. Las opciones fuera del local incluyen que un transportista mueva físicamente una segunda copia fuera del local o electrónicamente copias de cámara de seguridad fuera del local a una biblioteca remota.

Consejo: La solución descrita no incluye réplica de nodo. Sin embargo, si quiere utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento de disco a disco, asegúrese de que la operación de réplica esté completada antes de migrar los datos de disco a disco. También puede utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento en un dispositivo de cinta local a una agrupación de almacenamiento de copia en un dispositivo de cinta local. Para planificar una solución basada en cinta, complete las tareas siguientes:

1. Ajustese a los requisitos de sistema para hardware y software.
2. Registre los valores de configuración del sistema en las hojas de trabajo de planificación.

3. Planifique el almacenamiento en disco.
4. Planifique el almacenamiento en cinta.
5. Planifique la seguridad.

## Requisitos de planificación de cinta

---

Antes de implementar una solución de cinta, revise las directrices generales sobre los requisitos del sistema. Determine si realizar una copia de seguridad de los datos en un disco o en una cinta, o si combinar ambos sistemas.

### Ancho de banda de red

La red debe tener suficiente ancho de banda para las transferencias de datos esperadas entre el cliente y el servidor, para la réplica y para las operaciones de restauración entre sitios que son necesarias para la recuperación tras desastre. Utilice una red de área de almacenamiento (SAN) para transferir datos entre el servidor, los dispositivos de disco y los dispositivos de cinta. Para obtener más información, consulte Requisitos de hardware.

### Migración de datos

Migre todos los datos de disco a cinta a diario. Especifique una clase de dispositivo FILE para las agrupaciones de almacenamiento basadas en disco. Planifique la migración para controlar cuándo se produce el procesamiento. Para impedir la migración automática basada en el umbral de migración, especifique un valor de 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG cuando emita el mandato DEFINE STGPOOL. Debe mantener al menos el 20% de las unidades de cinta disponibles para operaciones de restauración. Para utilizar hasta el 80% de las unidades de cinta disponibles y mejorar el rendimiento, especifique el parámetro MIGPROCESS.

Considere la siguiente información en base al tipo de datos que se migran:

- Utilice una cinta para realizar una copia de seguridad de los datos de clientes que tienen objetos de gran tamaño, como bases de datos.  
Consejo: Consulte con el fabricante de unidades y cintas cuál es el tamaño de la base de datos adecuada para grabar a cinta.
- Utilice un disco para realizar una copia de seguridad de los datos de clientes que tienen objetos más pequeños.
- Para realizar una copia de seguridad de los datos directamente en una cinta, utilice el movimiento de datos sin LAN. Para obtener más información, consulte Configuración del movimiento de datos sin LAN.
- No realice la copia de seguridad de máquinas virtuales a cintas. Utilice una agrupación de almacenamiento basada en disco individual que no migre a una agrupación de almacenamiento basada en cinta. Para obtener más información sobre soporte de máquina virtual, consulte nota técnica 1239546.

### Capacidad de agrupación de almacenamiento

Mantenga suficiente capacidad de la agrupación de almacenamiento para permitir 2 días de copias de seguridad de cliente y un almacenamiento intermedio de 20%. Es posible que tenga planificar copias de seguridad completas durante varios días para asegurarse de que tiene suficiente espacio de agrupación de almacenamiento.

### unidades de cinta

Revise las especificaciones del fabricante y estime la capacidad de una unidad de cinta. Determine la cantidad de espacio necesaria para operaciones de copia de seguridad y migración. Reserve el 20% de unidades de cinta para operaciones de restauración.

### Referencia relacionada:

 [MIGRATE STGPOOL \(Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente\)](#)

## Requisitos del sistema para una solución basada en cinta

---

Se proporcionan los requisitos de hardware y software para una solución de almacenamiento basada en cintas que tiene una tasa de ingestión de datos de 14 TB por hora.

Revise la información para determinar los requisitos de hardware y software para su entorno de almacenamiento. Es posible que tenga que realizar ajustes basados en el tamaño de su sistema.

- **Requisitos de hardware**  
Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.
- **Requisitos de software**  
La documentación para la solución basada en cinta de IBM Spectrum Protect incluye tareas de instalación y configuración para sistemas operativos IBM® AIX, Linux y Microsoft Windows. Debe cumplir los requisitos de software mínimos que se indican.

## Requisitos de hardware




---

Los requisitos de hardware para la solución IBM Spectrum Protect se basan en el tamaño del sistema. Elija componentes equivalentes o mejores que los listados para garantizar un rendimiento óptimo para el entorno.

Para obtener más información sobre la planificación de dispositivos de disco, consulte Planificación del almacenamiento en disco.

Para obtener más información sobre la planificación de dispositivos de cinta, consulte Planificación del almacenamiento en cinta.

La tabla siguiente incluye requisitos de hardware mínimos para el servidor y el almacenamiento. Si utiliza particiones locales (LPAR) o particiones de trabajo (WPAR), ajuste los requisitos de red para tener en cuenta los tamaños de las particiones. Las cifras de la tabla se basan en una tasa de ingestión de datos de 14 TB por hora.

Componente de hardware	Requisitos del sistema
Procesador de servidor	<p> Sistemas operativos AIX 8 núcleos de procesador, 3,42 GHz o más rápido.</p> <p>Por ejemplo, utilice un servidor basado en procesador POWER8.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows 16 núcleos de procesador, 2,0 GHz o más rápido.</p> <p>Por ejemplo, utilice un procesador Intel Xeon.</p>
Memoria de servidor	64 GB de RAM.
Red	<p>El siguiente dimensionamiento gestiona aproximadamente 14 TB de datos por hora:</p> <ul style="list-style-type: none"> <li>• 10 Gb de Ethernet (un mínimo de cuatro puertos)</li> <li>• 8 Gb de adaptador de canal de fibra (un mínimo de cuatro puertos)</li> </ul> <p>El número de puertos depende del porcentaje de ingestión de datos diario en agrupaciones de almacenamiento de disco en comparación con almacenamiento de cinta.</p> <p>Utilice adaptadores de canal de fibra distintos para los datos de cinta y de disco.</p>
Almacenamiento	<p><b>Disco</b></p> <p>En función de la cantidad de datos que esté grabando en el disco, especifique el número de discos que necesita.</p> <p>Asegúrese de que el rendimiento de entrada/salida (E/S) secuencial de la red de área de almacenamiento (SAN) se corresponde con el rendimiento de E/S de la red de la fila anterior.</p> <p>Por ejemplo, si tiene que realizar la copia de seguridad de 10 TB de datos en un período de cuatro horas, el rendimiento es de aproximadamente 700 MB por segundo. En este caso, el servidor requiere una red frontal (vía de acceso de cliente a servidor) que admita un rendimiento mínimo de 700 MB por segundo. El SAN de fondo (la vía de acceso del servidor al dispositivo de almacenamiento) también debe admitir un rendimiento mínimo de 700 MB por segundo.</p> <p>Para calcular la velocidad de disco necesaria, utilice las siguientes fórmulas:</p> $\frac{\text{cantidad total de ingestión de datos diaria} - \text{cantidad de ingestión de datos diaria directamente en cinta}}{(\text{Número de horas para operaciones de copia de seguridad de cliente})} = \text{Megabytes de ingestión de datos en disco por hora}$ $\frac{\text{Megabytes de ingestión de datos en disco por hora}}{(3600 \text{ segundos por hora})} = \text{Megabytes de ingestión de datos por segundo que debe soportar la tecnología de disco}$ <p><b>Cinta</b></p> <p>Seleccione la tecnología de cinta que mejor se ajuste a los requisitos empresariales. Por ejemplo, utilice las unidades de cinta IBM Linear Tape-Open (LTO) o IBM TS1150. Asegúrese de que dispone de suficientes puntos de montaje para las operaciones de copia de seguridad de cliente y para la migración. Para obtener más información sobre la planificación de almacenamiento en cinta, consulte Planificación del almacenamiento en cinta. Para obtener una lista de dispositivos de cinta soportados, consulte IBM® Support Portal for IBM Spectrum Protect.</p> <p>Consejo: Para optimizar el movimiento de datos, utilice el movimiento de datos sin LAN.</p>

Componente de hardware	Requisitos del sistema
Adaptadores de E/S de SAN	<p>Separe la entrada/salida de cinta y de disco. Para obtener más información sobre la selección de un adaptador, consulte la documentación para productos de hardware Brocade y para las soluciones de almacenamiento de IBM Storwize.</p> <p>Disco</p> <p>Utilice al menos dos adaptadores.</p> <p>Cinta</p> <p>Utilice al menos dos adaptadores.</p>

## Estimación de requisitos de espacio para Centro de operaciones

Los requisitos de hardware para Centro de operaciones se incluyen en la tabla anterior, excepto para la base de datos y el espacio de registro de archivado (inventario) que utiliza Centro de operaciones para contener registros para clientes gestionados.

Si no piensa instalar el Centro de operaciones en el mismo sistema que el servidor IBM Spectrum Protect, puede calcular los requisitos de sistema por separado. Para calcular requisitos del sistema para Centro de operaciones, consulte la calculadora de requisitos del sistema en la nota técnica 1641684.

La gestión de Centro de operaciones en el servidor IBM Spectrum Protect es una carga de trabajo que requiere espacio adicional para operaciones de base de datos en el servidor spoke y el servidor concentrador. La cantidad de espacio en el servidor concentrador para el registro de archivado es mayor si el servidor concentrador está supervisando uno o más servidores spoke. Revise las siguientes directrices para calcular cuánto espacio necesita el servidor IBM Spectrum Protect.

### Espacio de base de datos para el Centro de operaciones

El Centro de operaciones utiliza aproximadamente 4,4 GB de espacio de base de datos por cada 1000 clientes supervisados en un servidor. Este cálculo se aplica a servidores concentradores y servidores spoke dentro de una configuración.

Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1000 clientes. Esta configuración tiene un total de 5000 clientes en los cuatro servidores. Cada servidor spoke necesita 4,4 GB de espacio de base de datos. Si los servidores spoke están en IBM Spectrum Protect versión 8.1.2 o posterior, el servidor concentrador necesita 8,8 GB de espacio de base de datos para supervisar solo a sus 2000 clientes:

$$(4,4 \text{ GB} \times 2) = 8,8 \text{ GB}$$

### Espacio de base de datos para datos gestionados

*Datos gestionados* es la cantidad de datos protegidos, incluyendo la cantidad de datos para todas las versiones retenidas.

- Para tipos de clientes que realizan una copia de seguridad siempre incremental, se puede utilizar la siguiente fórmula para calcular el total de datos gestionados:

$$\text{Frontal} + (\text{frontal} \times \text{tasa de cambio} \times (\text{retención} - 1))$$

Por ejemplo, si realiza la copia de seguridad de 100 TB de datos frontales, usa un periodo de retención de 30 días y cuenta con una tasa de cambio del 5%, calcule el total de datos gestionados mediante las siguientes cifras:

$$100 \text{ TB} + (100 \text{ TB} \times 0,05 \times (30-1)) = 245 \text{ TB de total de datos gestionados}$$

- Para tipos de clientes que realizan una copia de seguridad completa a diario, se puede utilizar la siguiente fórmula para calcular el total de datos gestionados:

$$\text{Frontal} \times \text{retención} \times (1 + \text{tasa de cambio})$$

Por ejemplo, si realiza la copia de seguridad de 10 TB de datos frontales, usa un periodo de retención de 30 días y cuenta con una tasa de cambio del 3%, calcule el total de datos gestionados mediante las siguientes cifras:

$$10 \text{ TB} \times 30 \times (1 + .03) = 309 \text{ TB de total de datos gestionados}$$

Datos no estructurados, promedio de tamaño de objeto: 4 MB

Datos estructurados, promedio de tamaño de objeto: 128 MB

Datos no estructurados, número de objetos =

$$(245 \text{ TB} \times 1024 \times 1024) / 4 \text{ MB} = 64225280$$

Datos estructurados, número de objetos =

$$(309 \text{ TB} \times 1024 \times 1024) / 128 \text{ MB} = 2531328$$

Número total de objetos: 66756608

Coste de los datos gestionados (1 KB por objeto) =

$$(66756608 \text{ KB}) / (1024 \times 1024) = 63,66 \text{ GB}$$

Planifique un 20% de espacio adicional para que los sistemas de base de datos no estén al 100% de capacidad:

$$\text{Requisitos de almacenamiento físico del total de la base de datos} = (\text{espacio de datos gestionados} + \text{espacio del centro de operaciones}) \times (1,20)$$

Para este ejemplo, debe calcular el espacio utilizando las siguientes cifras:

$$(66,33 \text{ GB} + 8,4 \text{ GB}) \times 1,20 = 76,41 \text{ GB}$$

### Espacio de registro de archivado

El Centro de operaciones utiliza aproximadamente 18 GB de espacio de registro de archivado cada 24 horas, por servidor, para cada 1000 clientes supervisados en dicho servidor. Además, para cada 1000 clientes que se supervisan en servidores spoke, se utiliza espacio de registro de archivado adicional en el servidor concentrador. Para servidores spoke en versión V8.1.2 o posterior, esta cantidad añadida es de 1,2 GB de espacio de registro de archivado en el servidor concentrador por 1000 clientes supervisados cada 24 horas.

Por ejemplo, considere un servidor concentrador con 2000 clientes que gestione también tres servidores spoke, cada uno de ellos con 1000 clientes. Esta configuración tiene un total de 5000 clientes en los cuatro servidores. Puede calcular el espacio de registro de archivado para el servidor concentrador utilizando la fórmula siguiente:

$$((18 \text{ GB} \times 2) + (1,2 \text{ GB} \times 3)) = 39,6 \text{ GB de espacio de registro de archivado}$$

Estas estimaciones se basan en el intervalo de recopilación de estados predeterminado de 5 minutos. Si reduce el intervalo de recopilación de uno cada 5 minutos a uno cada 3 minutos, aumentan los requisitos de espacio. Los siguientes ejemplos muestran el aumento aproximado en los requisitos de espacio de registro con un intervalo de recopilación de una vez cada 3 minutos para una configuración en la que se supervisan servidores spoke V8.1.2 o versiones posteriores:

- Servidor concentrador: en el rango 39,6 GB - 66 GB
- Cada servidor spoke: en el rango 18 GB - 30 GB

Asigne espacio de registro de archivado para que pueda dar soporte al Centro de operaciones sin que afecte a las operaciones de servidor.

## Requisitos de software

La documentación para la solución basada en cinta de IBM Spectrum Protect incluye tareas de instalación y configuración para sistemas operativos IBM® AIX, Linux y Microsoft Windows. Debe cumplir los requisitos de software mínimos que se indican.

Para obtener información sobre los requisitos de software para los controladores de dispositivo lin\_tape de IBM, consulte IBM Tape Device Drivers Installation and User's Guide.

### Sistemas AIX

Tipo de software	Requisitos mínimos de software
Sistema operativo	IBM AIX 7.1  Para obtener más información sobre los requisitos del sistema operativo, consulte AIX: requisitos mínimos del sistema para sistemas AIX.
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema antes de instalar o actualizar el servidor de IBM Spectrum Protect . Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.

Tipo de software	Requisitos mínimos de software
Tipo de sistema de archivos	<p>Sistemas de archivos JFS2</p> <p>Los sistemas AIX pueden almacenar en caché una gran cantidad de datos del sistema de archivos y esto puede reducir la memoria que se necesita para el servidor y los procesos de IBM DB2. Para evitar la paginación con el servidor de AIX, utilice la opción de montaje rbrw mount para el sistema de archivos JFS2. Se utiliza menos memoria para la memoria caché de sistema de archivo y hay más disponible para IBM Spectrum Protect.</p> <p>No utilice las opciones de montaje del sistema de archivos, E/S simultáneas (CIO) y E/S directas (DIO), para sistemas de archivos que contengan la base de datos de IBM Spectrum Protect, registros o volúmenes de agrupaciones de almacenamiento. Estas opciones pueden producir la degradación del rendimiento de muchas operaciones de servidor. IBM Spectrum Protect y DB2 aún pueden utilizar DIO donde sea beneficioso hacerlo, pero IBM Spectrum Protect no necesita las opciones de montaje para aprovechar estas técnicas de forma selectiva.</p>
Otro software	Shell Korn (ksh)

## Sistemas Linux

Tipo de software	Requisitos mínimos de software
Sistema operativo	Red Hat Enterprise Linux 7 (x86_64)
Bibliotecas	<p>Bibliotecas de GNU C, versión 2.3.3-98.38 o posterior que está instalado en el sistema de IBM Spectrum Protect.</p> <p>Red Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits)</li> <li>• numactl.x86_64</li> </ul>
Tipo de sistema de archivos	<p>Formato de sistemas de archivos relacionados con bases de datos con ext3 o ext4.</p> <p>Para los sistemas de archivos relacionados con agrupaciones de almacenamiento, utilice XFS.</p>
Otro software	Shell Korn (ksh)

## Sistemas Windows

Tipo de software	Requisitos mínimos de software
Sistema operativo	Microsoft Windows Server 2012 R2 (64-bit) o Windows Server 2016
Tipo de sistema de archivos	NTFS
Otro software	<p>Windows 2012 R2 o Windows 2016 con .NET Framework 3.5 está instalado o habilitado.</p> <p>Se deben desactivar las siguientes políticas de Control de la cuenta de usuario:</p> <ul style="list-style-type: none"> <li>• Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada</li> <li>• Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador</li> </ul>

## Planificación de hojas de trabajo

Utilice las hojas de trabajo de planificación para registrar los valores que se utilizan para configurar el sistema y configurar el servidor de IBM Spectrum Protect. Utilice los valores predeterminados de prácticas recomendadas que aparecen en las hojas de trabajo.

Cada hoja de trabajo le ayuda a prepararse para diferentes partes de la configuración del sistema utilizando valores de las prácticas recomendadas:

Configuración previa de sistema servidor





Utilice las hojas de trabajo de configuración previa para planificar los sistemas de archivos y directorios que se crean al configurar sistemas de archivos para IBM Spectrum Protect durante la configuración del sistema. Todos los directorios que crea para el

servidor deben estar vacíos.

Configuración del servidor

Utilice las hojas de trabajo de configuración cuando configure el servidor. Los valores predeterminados se recomiendan para la mayoría de los elementos, excepto donde se indica.

Tabla 1. Hoja de trabajo para la configuración previa de un sistema servidor

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Más información
Dirección de puerto TCP/IP para comunicaciones con el servidor	1500		No aplicable.	Asegúrese de que este puerto está disponible cuando instala y configura el sistema operativo.  El número de puerto puede ser un número dentro del rango 1024 - 32767.
Directorio para la instancia de servidor	 Sistemas operativos AIX  Sistemas operativos Linux /home/tsminst1/tsminst1   Sistemas operativos Windows C:\tsminst1		 Sistemas operativos AIX 50 GB.   Sistemas operativos Linux  Sistemas operativos Windows 25 GB.	Si cambia el valor para el directorio de instancia de servidor respecto al valor predeterminado, modifique también el valor de propietario de instancia de DB2 en Tabla 2.
Directorio para la instalación del servidor	<ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux/</li> <li>•  Sistemas operativos Windows</li> <li>• C:</li> </ul>		 Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.   Sistemas operativos Linux  Sistemas operativos Windows Espacio mínimo requerido para el directorio: 30 GB.	
Directorio para la instalación del servidor	/usr		 Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	 Sistemas operativos AIX/var		 Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	 Sistemas operativos AIX/tmp		 Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 5 GB.	
Directorio para la instalación del servidor	 Sistemas operativos AIX/opt		 Sistemas operativos AIX Espacio disponible que es necesario para el directorio: 10 GB.	
Directorio para el registro activo	 Sistemas operativos AIX  Sistemas operativos Linux /tsminst1/TSMalog   Sistemas operativos Windows C:\tsminst1\TSMalog		128 GB.	Cuando crea el registro activo durante la configuración inicial del servidor, establezca el tamaño en 128 GB.

Elemento	Valor predeterminado	Valor	Tamaño mínimo de directorio	Más información
Directorio para el registro de archivado	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMarchlog  Sistemas operativos Windows C:\tsminst1\TSMarchlog		3 TB.	
Directorios para la base de datos	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMdbspace00 /tsminst1/TSMdbspace01 /tsminst1/TSMdbspace02 /tsminst1/TSMdbspace03  Sistemas operativos Windows C:\tsminst1\TSMdbspace00 C:\tsminst1\TSMdbspace01 C:\tsminst1\TSMdbspace02 C:\tsminst1\TSMdbspace03		Para obtener instrucciones sobre cómo calcular los requisitos de espacio, consulte Requisitos de hardware.	Cree cuatro sistemas de archivos para la base de datos.
Directorios para almacenamiento	Sistemas operativos AIX Sistemas operativos Linux /tsminst1/TSMfile00 /tsminst1/TSMfile01 /tsminst1/TSMfile02 /tsminst1/TSMfile03 ...  Sistemas operativos Windows C:\tsminst1\TSMfile00 C:\tsminst1\TSMfile01 C:\tsminst1\TSMfile02 C:\tsminst1\TSMfile03 ...		Determine la capacidad total mínima para todos los directorios utilizando el siguiente cálculo:  Diariamente porcentaje de datos ingeridos que se graban en el disco + 20% = capacidad mínima total	El método preferido consiste en definir al menos un directorio para cada dispositivo de cinta.







Tabla 2. Hoja de trabajo para la configuración de IBM Spectrum Protect







Elemento	Valor predeterminado	Valor	Más información
Propietario de instancia de DB2	tsminst1		Si ha cambiado el valor para el directorio de instancia de servidor en Tabla 1 respecto al valor predeterminado, modifique también el valor para el propietario de instancia de DB2.
Contraseña de propietario de instancia de DB2	Sistemas operativos AIX Sistemas operativos Linux passw0rd Sistemas operativos Windows pAssW0rd		Seleccione un valor diferente al predeterminado para la contraseña de propietario de instancia. Asegúrese de que registra este valor en una ubicación segura.
Grupo primario para el propietario de instancia de DB2	Sistemas operativos AIX Sistemas operativos Linux tsmrsvr		
Nombre del servidor	El valor predeterminado para el nombre del servidor es el nombre de host del sistema.		
Contraseña del servidor	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de servidor. Asegúrese de que registra este valor en una ubicación segura.



Elemento	Valor predeterminado	Valor	Más información
ID de administrador: ID de usuario para la instancia de servidor	admin		
Contraseña de ID de administrador	passw0rd		Seleccione un valor diferente al predeterminado para la contraseña de administrador. Asegúrese de que registra este valor en una ubicación segura.
Hora de inicio de la planificación	23:00		<p>La hora de inicio de la planificación predeterminada empieza en la fase de cargar de trabajo de cliente, que es predominantemente la fase de actividades de archivado y copia de seguridad del cliente. Durante la fase de carga de trabajo del cliente, los recursos del servidor admiten las operaciones del cliente. Normalmente, estas operaciones se completan durante la ventana de planificación nocturna.</p> <p>Las planificaciones de las operaciones de mantenimiento de servidor se definen para empezar 10 horas después del inicio de la ventana de copia de seguridad de cliente.</p> <p>En esta guía, la hora sugerida de inicio de operaciones de copia de seguridad de cliente es 23:00.</p>

Tabla 3. Hoja de trabajo para la configuración de cinta

Elemento	Valor predeterminado	Valor	Más información
Archivos de dispositivos de robótica	<p>Dispositivos de IBM® con un controlador de dispositivo de cinta de IBM:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX /dev/smcX</li> <li>•  Sistemas operativos Linux /dev/IBMchangerX</li> <li>•  Sistemas operativos Windows ChangerX</li> </ul> <p>Dispositivos no IBM con un controlador de dispositivo IBM Spectrum Protect</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX /dev/lbX</li> <li>•  Sistemas operativos Linux /dev/tsmcsi/lbX</li> <li>•  Sistemas operativos Windows lbA.B.C.D</li> </ul>		<p>Para definir manualmente los archivos de dispositivo de biblioteca, utilice los siguientes mandatos:</p> <ul style="list-style-type: none"> <li>• DEFINE LIBRARY</li> <li>• DEFINE DRIVE</li> <li>• DEFINE PATH</li> </ul> <p>Para SCSI, puede utilizar el mandato PERFORM LIBACTION para definir todas las unidades y sus vías de acceso para una única biblioteca en un paso. Para utilizar este mandato para definir todas las unidades y vías de acceso, la opción SANDISCOVERY debe estar admitida y habilitada.</p>

Elemento	Valor predeterminado	Valor	Más información
unidades de cinta	<p>Dispositivos de IBM con un controlador de dispositivo de cinta de IBM:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX /dev/rmtX</li> <li>•  Sistemas operativos Linux /dev/IBMtapeX</li> <li>•  Sistemas operativos Windows TapeX</li> </ul> <p>Dispositivos no IBM con un controlador de dispositivo IBM Spectrum Protect</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX /dev/mtX</li> <li>•  Sistemas operativos Linux /dev/tmscsi/mtX</li> <li>•  Sistemas operativos Windows mtA.B.C.D</li> </ul>		

## Planificación del almacenamiento en disco

Elegir la tecnología de almacenamiento más efectiva para componentes de IBM Spectrum Protect para asegurarse de que el rendimiento de servidor y las operaciones son eficientes.

Los dispositivos de hardware de almacenamiento tiene características de rendimiento y capacidad diferentes, lo que determina cómo se pueden utilizar de forma eficaz con IBM Spectrum Protect. Para obtener una orientación general sobre cómo seleccionar el hardware de almacenamiento apropiado y configurar la solución, revise las directrices siguientes.

Base de datos, registro activo y registro de archivado

- Utilice un disco de estado sólido (SSD) o un disco rápido de 15.000 rpm para el registro activo y la base de datos de IBM Spectrum Protect.
- Al crear matrices para la base de datos, utilice RAID nivel 5.
- Utilice discos separados para el almacenamiento de copia de seguridad de la base de datos y el registro de archivado.

Agrupación de almacenamiento

Utilice el nivel RAID 6 para las matrices de agrupación de almacenamiento para añadir protección frente a las anomalías de unidad doble cuando se utilizan tipos de disco de gran tamaño.

- Planificación de matrices de almacenamiento  
Prepararse para la configuración de almacenamiento de disco planificando matrices RAID y volúmenes, de acuerdo con el tamaño del sistema IBM Spectrum Protect.

## Planificación del almacenamiento en cinta

Determine qué dispositivos de cinta utilizar y cómo configurarlos. Para optimizar el rendimiento del sistema, planifique utilizar dispositivos de cinta rápidos y de gran capacidad. Suministre suficientes unidades de cinta para cumplir los requisitos empresariales.

- Dispositivos de cinta y bibliotecas soportados  
El servidor puede utilizar una amplia variedad de dispositivos de cinta y bibliotecas. Seleccione dispositivos de cinta y bibliotecas que cumplan sus requisitos de negocio.
- Configuraciones de dispositivos de cinta soportadas  
Revise la información sobre las redes de área local (LAN) y las redes de área de almacenamiento (SAN). Para optimizar el movimiento de datos, planifique la configuración del movimiento de datos sin LAN. Además, considere si utilizar el uso compartido de bibliotecas.
- Definiciones necesarias para dispositivos de almacenamiento en cinta  
Para que el servidor de IBM Spectrum Protect pueda utilizar un dispositivo de cinta, debe configurar el dispositivo en el sistema

operativo y en el servidor. Durante el proceso de planificación, determine qué definiciones se necesitan para sus dispositivos de almacenamiento en cinta.

- Planificación de la jerarquía de agrupaciones de almacenamiento

Planifique la jerarquía de agrupaciones de almacenamiento para asegurarse de que los datos se migran a diario de disco a cinta. La migración libera espacio en el dispositivo de disco y mueve los datos a la cinta para la retención a largo plazo. De esta manera, podrá aprovechar la escalabilidad, la rentabilidad y las características de seguridad del almacenamiento de cintas.




- Almacenamiento de datos fuera del local

Para facilitar la recuperación de datos y como parte de la estrategia de recuperación tras desastre, almacene copias de cinta fuera del local.

## Dispositivos de cinta y bibliotecas soportados

El servidor puede utilizar una amplia variedad de dispositivos de cinta y bibliotecas. Seleccione dispositivos de cinta y bibliotecas que cumplan sus requisitos de negocio.

Para obtener una lista de dispositivos soportados y formatos de clase de dispositivo válidos, consulte el sitio web de su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos soportados para AIX y Windows
-  Sistemas operativos Linux Dispositivos soportados para Linux

Para obtener más información acerca de los dispositivos y objetos de almacenamiento, consulte Tipos de dispositivos de almacenamiento.

Cada uno de los dispositivos definidos para IBM Spectrum Protect está asociado a una *clase de dispositivo*. Dicha clase de dispositivo especifica un tipo de dispositivo e información de gestión de medios, como por ejemplo el formato de grabación, la capacidad estimada y los prefijos de etiquetas.

El *tipo de dispositivo* identifica a un dispositivo como miembro de un grupo que comparte características de medios semejantes. Por ejemplo, el tipo de dispositivo LTO se aplica a todas las generaciones de unidades de cinta LTO.

Una clase de dispositivo para una unidad de cinta también debe especificar una biblioteca. Una *biblioteca física* es un conjunto de una o varias unidades que comparten requisitos semejantes de montaje de medios. Es decir, la unidad la puede montar un operador o un mecanismo de montaje automatizado.

Una *definición de objeto de biblioteca* especifica el tipo de biblioteca y otras características asociadas con el tipo de biblioteca.

La tabla siguiente muestra los tipos de biblioteca preferidos para una solución de cinta IBM Spectrum Protect versión 8.1.2.

Tabla 1. Tipos de biblioteca para una solución de cinta IBM Spectrum Protect 8.1.2

Tipo de biblioteca	Descripción	Más información
SCSI	<p>Una biblioteca SCSI se controla mediante una interfaz SCSI, conectada directamente al host del servidor a través de cables SCSI o mediante una red de área de almacenamiento. Un robot u otro mecanismo maneja automáticamente el montaje y el desmontaje de los volúmenes de cinta.</p> <p>Si crea distintos tipos de unidades para una biblioteca SCSI, crea múltiples bibliotecas lógicas que no se pueden dividir entre distintos tipos de unidades. Una biblioteca SCSI puede contener unidades de tecnologías mixtas, incluyendo unidades LTO Ultrium y unidades DLT (Digital Linear Tape). Por ejemplo:</p> <ul style="list-style-type: none"> <li>• La biblioteca Oracle StorageTek L700</li> <li>• El dispositivo de cinta IBM® 3592</li> </ul>	<p>Configuración de bibliotecas para su uso por parte de un servidor</p> <p>Las restricciones se aplican cuando combina distintas generaciones de medios y unidades. Para obtener más información, consulte:</p> <ul style="list-style-type: none"> <li>• Combinación de generaciones de unidades y medios 3592 en una sola biblioteca</li> <li>• Combinación de unidades y medios LTO en una biblioteca</li> </ul>
Compartidas	<p>Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI. La biblioteca se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas.</p> <p>Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas. Las bibliotecas compartidas hacen referencia a un gestor de bibliotecas.</p>	

## Configuraciones de dispositivos de cinta soportadas

---

Revise la información sobre las redes de área local (LAN) y las redes de área de almacenamiento (SAN). Para optimizar el movimiento de datos, planifique la configuración del movimiento de datos sin LAN. Además, considere si utilizar el uso compartido de bibliotecas.

Seleccione la configuración de dispositivo que se ajuste a sus requisitos empresariales.

- **Movimiento de datos sin LAN y basados en LAN**  
Puede mover datos entre clientes y dispositivos de almacenamiento que estén conectados a una red de área local (LAN), o a dispositivos de almacenamiento conectados a una red de área de almacenamiento (SAN), conocido como movimiento de datos sin LAN.
- **Compartición de bibliotecas**  
Puede optimizar la eficiencia de su solución de cinta configurando la compartición de biblioteca. La compartición de biblioteca permite que diversos servidores de IBM Spectrum Protect utilicen la misma biblioteca de cintas y las mismas unidades en una red de área de almacenamiento (SAN) y permite mejorar el rendimiento de los procesos de copia de seguridad y recuperación y la utilización del hardware de cintas.
- **Movimiento de datos sin LAN**  
IBM Spectrum Protect proporciona la capacidad para un cliente, a través de un agente de almacenamiento, de hacer copia de seguridad y restaurar datos directamente a una biblioteca de cintas en una SAN. Este tipo de movimiento de datos también se conoce como movimiento de datos sin LAN.
- **Mezcla de tipos de dispositivos en una biblioteca**  
IBM Spectrum Protect admite mezclar diferentes tipos de dispositivos en una sola biblioteca automatizada, si la biblioteca puede distinguir entre los diferentes medios para los diferentes tipos de dispositivos. Para simplificar el proceso de configuración, no planifique mezclar distintos tipos de dispositivos en una misma biblioteca. Si tiene que combinar tipos de dispositivos, revise las restricciones.

## Movimiento de datos sin LAN y basados en LAN

---

Puede mover datos entre clientes y dispositivos de almacenamiento que estén conectados a una red de área local (LAN), o a dispositivos de almacenamiento conectados a una red de área de almacenamiento (SAN), conocido como movimiento de datos sin LAN.

En una configuración de LAN convencional, hay una o más bibliotecas de cintas asociadas con un único servidor IBM Spectrum Protect. El movimiento de datos sin LAN pone el ancho de banda disponible para otros usos y disminuye la carga en el servidor IBM Spectrum Protect.

En una configuración de LAN, los datos de cliente, el correo electrónico, la conexión de terminal, el programa de aplicación y la información de control de dispositivo deben gestionarse a través de la misma red. La información sobre el control de dispositivos, las copias de seguridad de cliente y la restauración de datos se transfieren a través de la LAN.

Una red de área de almacenamiento (SAN) es una red de almacenamiento dedicada que puede mejorar el rendimiento del sistema.

Utilizando IBM Spectrum Protect en una SAN, puede beneficiarse de las siguientes funciones:

- **Compartir dispositivos de almacenamiento entre varios servidores de IBM Spectrum Protect.**  
Restricción: Un dispositivo de almacenamiento con tipo de dispositivo GENERICTAPE no se puede compartir entre servidores.
- **Mover los datos de cliente de IBM Spectrum Protect directamente a los dispositivos de almacenamiento (movimiento de datos sin LAN) configurando un agente de almacenamiento en el sistema cliente.**

En una SAN, puede compartir unidades de cinta y bibliotecas soportadas por el servidor de IBM Spectrum Protect, incluyendo la mayoría de dispositivos de cinta SCSI.

Cuando los servidores IBM Spectrum Protect comparten una cinta SCSI, un servidor, el *gestor de biblioteca*, posee y controla el dispositivo. Los agentes de almacenamiento, junto con otros servidores de IBM Spectrum Protect que comparten esta biblioteca, son los *agentes de biblioteca*. Un cliente de biblioteca solicita recursos de biblioteca compartida como, por ejemplo, unidades o medios, al gestor de bibliotecas, pero utiliza los recursos de forma independiente. El gestor de bibliotecas coordina el acceso a estos recursos. Los servidores de IBM Spectrum Protect que se define como clientes de biblioteca utilizan comunicaciones de servidor a servidor para ponerse en contacto con el gestor de bibliotecas y solicitar el servicio de dispositivos. Los datos se traspan por la SAN entre los servidores y el dispositivo de almacenamiento.

Requisito: Si define un servidor de gestor de biblioteca que se comparte con el servidor IBM Spectrum Protect, la opción SANDISCOVERY se debe establecer en ENCENDIDO. De forma predeterminada, esta opción está establecida en OFF.

Los servidores de IBM Spectrum Protect utilizan las características siguientes cuando comparten una biblioteca automatizada:

**Particionamiento del inventario de volúmenes**

El inventario de volúmenes de medios de la biblioteca compartida está particionado entre los servidores. O bien un servidor es propietario de un volumen determinado, o el volumen se encuentra en la agrupación de reutilización global. Ningún servidor es

propietario de la agrupación de reutilizables.

Acceso a unidad serializado

Sólo un servidor accede a una unidad de cintas cada vez. El acceso a unidades está serializado. IBM Spectrum Protect controla el acceso a unidades para que los servidores no desmonten los volúmenes de otros servidores ni graben en unidades donde otros servidores montan sus volúmenes.

Acceso a montaje serializado

El cambiador automático de la biblioteca efectúa una única operación de montaje o desmontaje cada vez. El gestor de biblioteca completa todas las operaciones de montaje para proporcionar esta serialización.

## Compartición de bibliotecas

Puede optimizar la eficiencia de su solución de cinta configurando la compartición de biblioteca. La compartición de biblioteca permite que diversos servidores de IBM Spectrum Protect utilicen la misma biblioteca de cintas y las mismas unidades en una red de área de almacenamiento (SAN) y permite mejorar el rendimiento de los procesos de copia de seguridad y recuperación y la utilización del hardware de cintas.

Cuando los servidores de IBM Spectrum Protect comparten una biblioteca, un servidor se configura como el gestor de bibliotecas y controla las operaciones de la biblioteca como, por ejemplo, el montaje y desmontaje. El gestor de bibliotecas también controla la propiedad del volumen y el inventario de la biblioteca. Otros servidores están configurados como clientes de biblioteca y utilizan las comunicaciones de servidor a servidor para ponerse en contacto con el gestor de bibliotecas y solicitar recursos.

Los clientes de biblioteca debe estar de la misma versión o de una versión anterior que el servidor del gestor de biblioteca. Un gestor de biblioteca no puede admitir clientes de biblioteca de una versión posterior. Para obtener más información, consulte Compatibilidad del agente de almacenamiento y el cliente de biblioteca con un servidor de IBM Spectrum Protect.

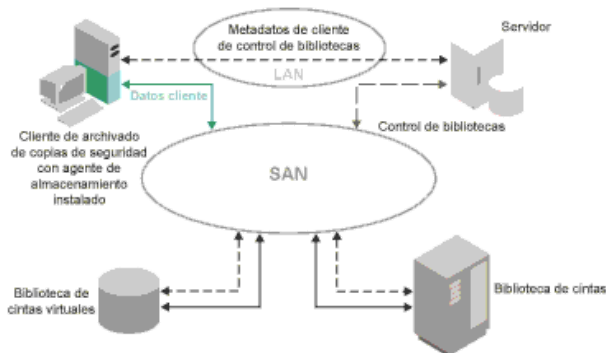
## Movimiento de datos sin LAN

IBM Spectrum Protect proporciona la capacidad para un cliente, a través de un agente de almacenamiento, de hacer copia de seguridad y restaurar datos directamente a una biblioteca de cintas en una SAN. Este tipo de movimiento de datos también se conoce como movimiento de datos sin LAN.

Restricción: Los dispositivos de almacenamiento Centera no pueden ser destinos para las operaciones fuera de la LAN.

La Figura 1 muestra una configuración de SAN en la que un cliente accede directamente a una cinta para leer o grabar datos.

Figura 1. Movimiento de datos sin LAN



El movimiento de datos sin LAN requiere la instalación de un agente de almacenamiento en el sistema cliente. El servidor mantiene la base de datos, las anotaciones de recuperación y el gestor de biblioteca para controlar las operaciones de los dispositivos. El agente de almacenamiento del cliente gestiona la transferencia de datos al dispositivo de la SAN. Esta implementación libera ancho de banda de la LAN que, de otro modo, se utilizaría para la transferencia de datos del cliente.

## Mezcla de tipos de dispositivos en una biblioteca

IBM Spectrum Protect admite mezclar diferentes tipos de dispositivos en una sola biblioteca automatizada, si la biblioteca puede distinguir entre los diferentes medios para los diferentes tipos de dispositivos. Para simplificar el proceso de configuración, no planifique mezclar distintos tipos de dispositivos en una misma biblioteca. Si tiene que combinar tipos de dispositivos, revise las restricciones.

Las bibliotecas con esta capacidad son los modelos que tienen unidades incorporadas mixtas, o que admiten la adición de unidades mixtas. Para obtener información sobre modelos específicos, consulte la documentación del fabricante. Para obtener más información

acerca de las bibliotecas probadas en IBM Spectrum Protect con mezcla de tipos de dispositivos, consulte la información para su sistema operativo:

- Dispositivos de IBM Spectrum Protect admitidos AIX, HP-UX, Solaris y Windows
- Dispositivos de IBM Spectrum Protect admitidos para Linux

Por ejemplo, puede tener unidades LTO Ultrium y unidades TS4500 de IBM en una biblioteca única definida en el servidor de IBM Spectrum Protect.

- Diferentes generaciones de medios en una biblioteca  
El servidor de IBM Spectrum Protect permite mezclar tipos de dispositivo en una biblioteca automatizada, pero normalmente no se admite mezclar distintas generaciones del mismo tipo de unidad. Las nuevas unidades no pueden grabar en los formatos de medios más antiguos y las unidades antiguas no pueden leer los formatos nuevos. Las unidades LTO Ultrium no son una excepción a esta regla.
- Mezcla de medios y agrupaciones de almacenamiento  
Puede optimizar la eficiencia de su solución de cinta no mezclando formatos de medios en una misma agrupación de almacenamiento. En lugar de mezclar distintos formatos, correlacione cada formato de medio con una agrupación de almacenamiento distinta utilizando su propia clase de dispositivo. Esta restricción también se aplica a los formatos LTO.

## Diferentes generaciones de medios en una biblioteca

---

El servidor de IBM Spectrum Protect permite mezclar tipos de dispositivo en una biblioteca automatizada, pero normalmente no se admite mezclar distintas generaciones del mismo tipo de unidad. Las nuevas unidades no pueden grabar en los formatos de medios más antiguos y las unidades antiguas no pueden leer los formatos nuevos. Las unidades LTO Ultrium no son una excepción a esta regla.

Si la tecnología de unidad nueva no puede grabar en medios que se hayan formateado con unidades de generaciones anteriores, los medios más antiguos deben marcarse como de sólo lectura para evitar problemas en las operaciones de servidor. Asimismo, las unidades más antiguas deben retirarse de la biblioteca, o bien del servidor. Por ejemplo, el servidor de IBM Spectrum Protect no admite el uso de unidades Oracle StorageTek 9940A con unidades 9940B en combinación con otros tipos de dispositivos en una misma biblioteca.

En general, IBM Spectrum Protect no admite mezclar distintas generaciones de unidades y medios LTO Ultrium. No obstante, se admiten las mezclas siguientes:

- LTO Ultrium Generación 3 (LTO-3) con LTO Ultrium Generación 4 (LTO-4)
- LTO Ultrium Generación 4 (LTO-4) con LTO Ultrium Generación 5 (LTO-5)
- LTO Ultrium Generación 5 (LTO-5) con LTO Ultrium Generación 6 (LTO-6)
- LTO Ultrium Generación 6 (LTO-6) con LTO Ultrium Generación 7 (LTO-7)

El servidor admite estas mezclas porque las distintas unidades pueden leer y grabar en medios diferentes. Si tiene previsto actualizar todas las unidades a generación 4 (o generación 5, 6 o 7), debe suprimir todas las definiciones de unidades LTO Ultrium existentes y las vías de acceso asociadas a las mismas. A continuación, puede definir las nuevas unidades y vías de acceso para Generación 4 (o Generación 5, 6, o 7).

Restricciones que se aplican a una combinación de medios y unidades de cinta LTO Ultrium

- Las unidades LTO-5 solo pueden leer medios LTO-3. Si mezcla unidades y medios LTO-3 con unidades y medios LTO-5 en una única biblioteca, deberá marcar los medios LTO-3 media como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-3.
- Las unidades LTO-6 solo pueden leer medios LTO-4. Si mezcla unidades y medios LTO-4 con unidades y medios LTO-6 en una sola biblioteca, deberá marcar los medios LTO-4 como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-4.
- Las unidades LTO-7 solo pueden leer medios LTO-5. Si mezcla unidades y medios LTO-5 con unidades y medios LTO-7 en una sola biblioteca, deberá marcar los medios LTO-5 como sólo lectura. Debe extraer todos los volúmenes reutilizables de LTO-5.

Restricciones que se aplican a unidades de cinta LTO Ultrium de mezcla de generaciones en una biblioteca

Debe utilizar cartuchos de cinta que sean una generación anterior a la unidad de cinta. Una unidad de cinta de generación posterior puede leer y grabar datos en un cartucho de cinta de generación anterior. Por ejemplo, si una biblioteca tiene unidades de cinta LTO-7 y LTO-6, debe utilizar cartuchos de cinta LTO-6. Tanto las unidades de cinta LTO-7 como LTO-6 pueden leer y grabar datos en cartuchos de cinta LTO-6.

Restricciones que se aplican a cartuchos de cinta LTO Ultrium de mezcla de generaciones en una biblioteca

Debe utilizar un cartucho de cinta que sea de la misma generación que la unidad de cinta, o una generación anterior. Por ejemplo, si una biblioteca tiene unidades de cinta LTO-7, puede utilizar cartuchos de cinta LTO-7 o una combinación de cartuchos de cinta LTO-7 y LTO-6. Si esta biblioteca tiene cartuchos de cinta LTO-7, LTO-6 y LTO-5, debe cambiar el modo de acceso a READONLY para los cartuchos de cinta LTO-5.

Para obtener más información sobre consideraciones adicionales al mezclar generaciones de LTO Ultrium, consulte Definición de las clases de dispositivo LTO.

Cuando utilice IBM Spectrum Protect, no puede mezclar unidades que sean 3592, TS1130, TS1140, TS1150, ni generaciones de unidades posteriores. Utilice una de las tres configuraciones especiales. Para obtener información detallada al respecto, consulte el apartado Definición de clases de dispositivo 3592.

Si tiene previsto cifrar volúmenes en una biblioteca, no mezcle las generaciones de medios en la biblioteca.

## Mezcla de medios y agrupaciones de almacenamiento

Puede optimizar la eficiencia de su solución de cinta no mezclando formatos de medios en una misma agrupación de almacenamiento. En lugar de mezclar distintos formatos, correlacione cada formato de medio con una agrupación de almacenamiento distinta utilizando su propia clase de dispositivo. Esta restricción también se aplica a los formatos LTO.

Varias agrupaciones de almacenamiento y sus clases de dispositivo de distintos tipos pueden apuntar a la misma biblioteca que puede admitirlos, tal como se describe en Diferentes generaciones de medios en una biblioteca.

Puede migrar a una nueva generación de tipos de soporte dentro de la misma agrupación de almacenamiento realizando los pasos siguientes:

1. Sustituya todas las unidades más antiguas por las unidades de generaciones más recientes dentro de la biblioteca. Las unidades se deben mezclar.
2. Marque los volúmenes existentes con los formatos más antiguos como de sólo lectura si la nueva unidad no puede añadir esas cintas en el formato antiguo. Si la nueva unidad puede grabar en los medios existentes en su formato antiguo, este paso no es necesario, aunque el Paso 1 sí lo es. Si es necesario mantener varias generaciones de unidades diferentes que se pueden leer pero no grabar dentro de la misma biblioteca, utilice agrupaciones de almacenamiento diferentes.






## Definiciones necesarias para dispositivos de almacenamiento en cinta

Para que el servidor de IBM Spectrum Protect pueda utilizar un dispositivo de cinta, debe configurar el dispositivo en el sistema operativo y en el servidor. Durante el proceso de planificación, determine qué definiciones se necesitan para sus dispositivos de almacenamiento en cinta.


Consejo: Puede utilizar el mandato PERFORM LIBACTION para simplificar el proceso en el que añade dispositivos a los tipos de biblioteca SCSI y VTL.

La Tabla 1 resume las definiciones obligatorias para diferentes tipos de dispositivos.

Tabla 1. Definiciones necesarias para los dispositivos de almacenamiento

Dispositivo	Tipos de dispositivo	Definiciones necesarias			
		Biblioteca	Unidad	Vía de acceso	Clase de dispositivo
Disco magnético	DISK	—	—	—	Sí <sup>1</sup>
	FILE <sup>2</sup>	—	—	—	Sí
	 Sistemas operativos AIX  Sistemas operativos Windows CENTERA  Sistemas operativos LinuxCENTERA <sup>3</sup>	—	—	—	Sí
Cinta	<ul style="list-style-type: none"> <li>• 3590</li> <li>• 3592</li> <li>• DLT</li> <li>• LTO</li> <li>• NAS</li> <li>• VOLSAFE</li> </ul>  Sistemas operativos AIX  Sistemas operativos Windows GENERICTAPE ECARTRIDGE <sup>4</sup>	Sí	Sí	Sí	Sí

Dispositivo	Tipos de dispositivo	Definiciones necesarias			
		Biblioteca	Unidad	Vía de acceso	Clase de dispositivo
Medios extraíbles (sistema de archivos)	REMOVABLEFILE	Sí	Sí	Sí	Sí


1. La clase de dispositivo DISK ya existe en el momento de la instalación y no se puede modificar.
2. Se requieren bibliotecas, unidades y vías de acceso FILE para compartir con los agentes de almacenamiento.
3.  Sistemas operativos Linux El tipo de dispositivo CENTERA está disponible solo para sistemas Linux x86\_64.
4. El tipo de dispositivo ECARTRIDGE es para unidades de cinta de cartucho Oracle StorageTek como unidades 9840 y T10000.

## Planificación de la jerarquía de agrupaciones de almacenamiento

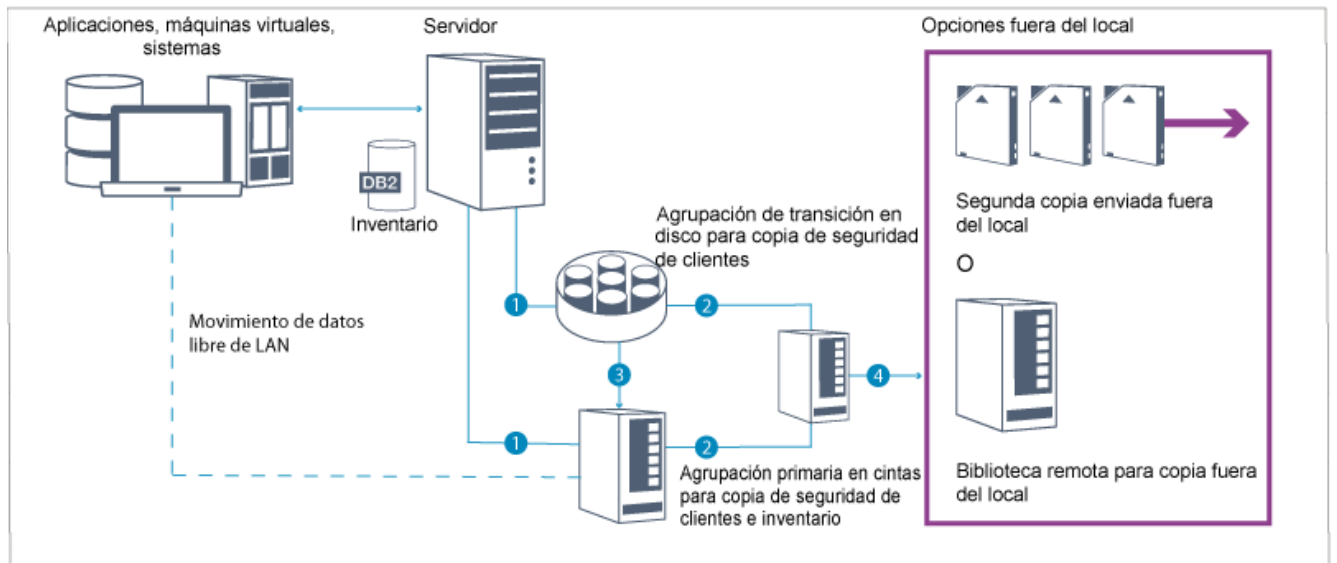
Planifique la jerarquía de agrupaciones de almacenamiento para asegurarse de que los datos se migran a diario de disco a cinta. La migración libera espacio en el dispositivo de disco y mueve los datos a la cinta para la retención a largo plazo. De esta manera, podrá aprovechar la escalabilidad, la rentabilidad y las características de seguridad del almacenamiento de cintas.

### Antes de empezar

La jerarquía de agrupaciones de almacenamiento ayuda a gestionar el flujo de datos. Para comprender el flujo de datos, revise Figura 1. Figura 1. Solución de cinta


Cinta

- ✔ Ideal para retención a largo plazo
- ✔ Escalabilidad a bajo coste
- ✔ Zona de transición disco a agrup. cintas
- ✔ Optimizado para SAN



Los pasos siguientes corresponden a los números de la figura:

1. El servidor recibe datos de los clientes (aplicaciones, máquinas virtuales o sistemas) y almacena los datos en agrupaciones de almacenamiento primaria. En función del tipo de cliente, los datos se almacenan en una agrupación de almacenamiento primaria en disco o cinta.
2. La copia de seguridad de los datos en disco y cinta se realiza en una agrupación de almacenamiento de copias en cinta.
3. Los datos de la agrupación de almacenamiento primaria en disco se migran a diario a la agrupación de almacenamiento primaria en cinta.
4. Los datos de la agrupación de almacenamiento de copias en cinta se mueva fuera de local para dar soporte a la retención a largo plazo y a la recuperación tras desastre.

### Procedimiento

Para planificar la jerarquía de agrupaciones de almacenamiento, responda a las siguientes preguntas:

- a. ¿Qué clientes deben realizar copias de seguridad de los datos en discos, y qué clientes en cinta?



- o El método preferido es realizar una copia de seguridad de los clientes que alojan objetos grandes, como bases de datos, en cinta.
- o El método preferido es realizar una copia de seguridad de todos los demás clientes en el disco.
- o La copia de seguridad de los clientes de máquina virtual (VM) se puede realizar en disco o cinta. El método preferido es realizar una copia de seguridad de un cliente de máquina virtual en una agrupación de almacenamiento de disco independiente, que no se migra a cinta. Si tiene que migrar un cliente de máquina virtual en cinta, cree una agrupación de almacenamiento de disco más pequeña para albergar los archivos de control de VMware. Esta agrupación de almacenamiento de disco más pequeña no se puede migrar a cinta. Para obtener más información sobre cómo hacer copia de seguridad de un cliente de máquina virtual en cinta, consulte Directrices del soporte de cinta y nota técnica 1239546.

Consejo: Si muchos clientes tienen que realizar la copia de seguridad de datos en una única agrupación de almacenamiento, considere la posibilidad de utilizar una agrupación de almacenamiento en disco porque puede especificar muchos puntos de montaje. Puede especificar un valor máximo de 999 para el parámetro MAXNUMMP en el mandato REGISTER NODE.

- b. ¿Cuáles son las consideraciones para especificar la capacidad de las agrupaciones de almacenamiento basadas en disco?

Como mínimo, planifique suficiente capacidad para almacenar datos de un único día de operaciones de copia de seguridad. El método preferido es planificar capacidad suficiente para almacenar datos de dos días de operaciones de copia de seguridad y añadir un 20% de almacenamiento intermedio.

- c. ¿Cuáles son las consideraciones para especificar la clase de dispositivo para la agrupación de almacenamiento basada en disco?

El método preferido es especificar una clase de dispositivo FILE. Establezca el parámetro MOUNTLIMIT en 4000. Asegúrese también de que el nodo tenga un número lo suficientemente alto de puntos de montaje, que podrá especificar utilizando el parámetro MAXNUMMP en el mandato REGISTER NODE.

- d. ¿Debe especificarse la deduplicación de datos para la agrupación de almacenamiento de disco?

No, porque los datos se almacenan en el disco sólo un día antes de que los datos se migren a cinta.

- e. ¿Debe especificarse la migración automática de datos en base al umbral de migración?

No. En cambio, planifique una migración diaria utilizando el mandato MIGRATE STGPOOL. (para impedir la migración automática basada en el umbral de migración, especifique un valor de 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG cuando emita el mandato DEFINE STGPOOL.)

- f. ¿Debe especificarse un retardo en la migración?

El método preferido consiste en especificar la migración desde el disco a la cinta a diario, y no especificar un retardo de migración, lo que requiere planificación adicional. Para obtener más información sobre retardos en la migración, consulte Migración de archivos en una jerarquía de agrupaciones de almacenamiento.

- g. ¿Cómo se puede calcular el número de unidades de cinta?

- i. Determine la velocidad de transferencia de datos nativos de la unidad revisando la documentación del fabricante. Para obtener un cálculo aproximado de la velocidad de transferencia de datos constante en el entorno de almacenamiento, reste el 30% de la velocidad de transferencia de datos nativos.
- ii. Calcule la velocidad necesaria de la ingestión de datos por el servidor. A continuación, divida esta cifra entre la velocidad de transferencia de datos constante de un único dispositivo de cinta. El resultado es el número mínimo de unidades para dar soporte a la ingestión de datos.
- iii. Calcule el número de puntos de montaje necesarios por los clientes que realizan la copia de seguridad de datos en cinta, incluyendo aquellos clientes que utilizan varias sesiones. Puede distribuir los puntos de montaje a través de la ventana de copia de seguridad, teniendo en cuenta que es probable que los clientes realicen copias de seguridad de objetos de gran tamaño, que pueden utilizar la mayoría de la ventana.
- iv. Calcule los requisitos de rendimiento y puntos de montaje que son necesarios para tareas de mantenimiento, como la migración de disco a cinta y las copias de cinta a cinta. Al realizar la copia de seguridad de datos a cinta, puede evitar el proceso de migración pero realizar copias de cinta a cinta doblará el requisito de unidad de cintas.
- v. Calcule el número de unidades adicionales que pueden necesitarse, por ejemplo:
  - Si una unidad de cintas funciona mal, el problema afectará al número de puntos de montaje disponibles y a la velocidad de ingestión. Considere el suministro de unidades de repuesto. Por ejemplo, si necesita cinco unidades de cinta para las operaciones normales, considere el suministro de dos unidades de repuesto.
  - Las operaciones de restauración y recuperación pueden requerir unidades de cinta adicionales si tiene previsto ejecutar las operaciones simultáneamente con la ingestión de datos y las operaciones de mantenimiento. Si es necesario, suministre unidades de cinta adicionales y asegúrese de que no se utilicen cuando inicie las operaciones de restauración o recuperación.

- h. ¿Qué alternativas están disponibles para optimizar las operaciones de restauración?

Puede utilizar la función de proximidad para mejorar el rendimiento del sistema y optimizar la organización de datos. La función de proximidad puede reducir el número de volúmenes a los que se debe acceder cuando debe restaurarse una gran cantidad de datos:

- Para agrupaciones de almacenamiento basadas en disco, el método preferido es utilizar la función de proximidad por nodo. El servidor almacena los datos del nodo en el menor número posible de volúmenes.
- Para agrupaciones de almacenamiento basadas en cinta, el método preferido es utilizar la función de proximidad por grupo. La proximidad por grupo genera una reducción de la capacidad de cinta no utilizada, lo que permite más datos colocados en cintas individuales.

Para obtener más información sobre la función de proximidad, consulte Optimización de operaciones habilitando la función de proximidad de los archivos de cliente.

Si es un administrador del sistema con experiencia, es posible que tenga previstas acciones adicionales para optimizar las operaciones de restauración. Consulte Optimización de las operaciones de restauración para clientes, Técnicas de copia de seguridad de archivo y MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial).

## Almacenamiento de datos fuera del local

---

Para facilitar la recuperación de datos y como parte de la estrategia de recuperación tras desastre, almacene copias de cinta fuera del local.

Utilice la función del gestor recuperación tras desastre (DRM) para configurar y generar automáticamente un plan de recuperación tras desastre que contenga la información, los scripts y los procedimientos necesarios para restaurar automáticamente los datos del cliente de recuperación y servidor tras un desastre. Elija entre una de las siguientes opciones de almacenamiento de datos fuera del local como estrategia de recuperación tras desastre para proteger las copias de cinta:

**Cámaras de seguridad fuera del local desde un único sitio de producción**

Volúmenes de almacenamiento, como cartuchos de cinta y volúmenes de soporte, se guardan en una cámara de seguridad fuera del local. Un transportista transporta los datos desde una instalación de almacenamiento fuera del local al sitio de recuperación. Si se produce un desastre, los volúmenes se vuelven a enviar al sitio de producción una vez restaurados el hardware y el servidor de IBM Spectrum Protect.

**Cámaras de seguridad fuera del local con un sitio de recuperación**

Un transportista mueve volúmenes de almacenamiento desde el sitio de producción hasta una instalación de almacenamiento fuera del local. Al implantar un sitio de recuperación dedicado, puede reducir el tiempo de recuperación, en comparación con un único sitio de producción. Sin embargo, esta opción incrementa el coste de la recuperación tras desastre porque debe mantenerse más hardware y software. Por ejemplo, el sitio de recuperación debe tener dispositivos de cinta compatibles y el software del servidor de IBM Spectrum Protect. Para poder recuperar el sitio de producción, el hardware y el software en el sitio de recuperación deben estar configurados y en ejecución.

**Cámara de seguridad electrónica**

Para utilizar la cámara de seguridad electrónica como estrategia de recuperación tras desastre, el sitio de recuperación debe tener un servidor IBM Spectrum Protect en ejecución. Los datos críticos se guardan en una cámara de seguridad electrónica desde el sitio de producción hasta el sitio de recuperación. DRM también se utiliza para el almacenamiento en cámaras de seguridad fuera del local de datos no críticos. La cámara de seguridad electrónica mueve los datos críticos fuera del local más rápidamente y con más frecuencia que los métodos de transportista tradicional. El tiempo de recuperación se reduce porque los datos críticos ya están almacenados en el sitio de recuperación. Sin embargo, como el sitio de recuperación se ejecuta de forma continua, el coste de la estrategia de recuperación tras desastre es más caro que el almacenamiento en cámaras de seguridad fuera del local.

### Conceptos relacionados:

Preparación ante desastres y recuperación tras desastres mediante DRM

## Planificación de la seguridad

---

Planee proteger la seguridad de los sistemas en la solución IBM Spectrum Protect con controles de acceso y autenticación y tenga en cuenta el cifrado de datos y la transmisión de contraseña.

- **Planificación de los roles de administración**  
Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.
- **Planificación para comunicaciones seguras**  
Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.
- **Planificación de almacenamiento de datos cifrados**  
Determine si la compañía requiere que se cifren los datos almacenados y elija el método que mejor se adapta a sus necesidades.
- **Planificación del acceso de cortafuegos**  
Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

## Planificación de los roles de administración

Defina los niveles de autorización que desea asignar a los administradores que tienen acceso a la solución IBM Spectrum Protect.

Puede asignar uno de los siguientes niveles de autorización a los administradores:

### Sistema

Los administradores con autoridad del sistema tienen el nivel de autorización más alto. Los administradores con este nivel pueden realizar cualquier tarea. Pueden gestionar todos los dominios de política y agrupaciones de almacenamiento y otorgar autoridad a otros administradores.

### Política

Los administradores que tienen autorización sobre políticas pueden gestionar todas las tareas relacionadas con la gestión de políticas. Este privilegio puede no tener restricciones o puede estar restringido a dominios de políticas específicos.

### Almacenamiento

Los administradores que tienen autorización de almacenamiento pueden asignar y controlar recursos de almacenamiento para el servidor.

### Operador

Los administradores que tienen autorización de operador pueden controlar la operación inmediata del servidor y la disponibilidad de soporte de almacenamiento como unidades y bibliotecas de cintas.

Los escenarios de Tabla 1 proporcionan ejemplos de por qué es posible que desee asignar distintos niveles de autorización para que los administradores puedan realizar tareas:

Tabla 1. Escenarios para roles de administrador

Escenario	Tipo de ID de administrador a configurar
Un administrador de una pequeña empresa gestiona el servidor y es responsable de todas las actividades del servidor.	<ul style="list-style-type: none"><li>Autoridad del sistema: 1 ID de administrador</li></ul>
Un administrador para varios servidores también gestiona el sistema en general. Otros diversos administradores gestionan sus propias agrupaciones de almacenamiento.	<ul style="list-style-type: none"><li>Autoridad del sistema en todos los servidores: 1 ID de administrador para el administrador del sistema general</li><li>Autoridad de almacenamiento para agrupaciones de almacenamiento designadas: 1 ID de administrador para cada uno de los otros administradores</li></ul>
Un administrador gestiona 2 servidores. Otra persona ayuda con las tareas de administración. Dos ayudantes son responsables de ayudar a garantizar que se hace copia de seguridad de los sistemas importantes. Cada ayudante es responsable de supervisar las copias de seguridad planificadas en uno de los servidores de IBM Spectrum Protect.	<ul style="list-style-type: none"><li>Autoridad del sistema en ambos servidores: 2 ID de administrador</li><li>Autoridad de operador: 2 ID de administrador para los ayudantes con acceso al servidor del que cada persona es responsable</li></ul>

### Tareas relacionadas:

Gestión de administradores

## Planificación para comunicaciones seguras

Planifique la protección de las comunicaciones entre los componentes de la solución IBM Spectrum Protect.

Determine el nivel de protección necesario para los datos, basándose en las regulaciones y requisitos empresariales bajo los que opera la compañía.

Si su empresa necesita un alto nivel de seguridad para las contraseñas y la transmisión de datos, planee implementar comunicaciones seguras con protocolos de seguridad de la capa de transporte (TLS) o de capa de sockets seguros (SSL).

TLS y SSL proporcionan comunicaciones seguras entre el servidor y el cliente, pero pueden afectar al rendimiento del sistema. Para mejorar el rendimiento del sistema, utilice TLS para autenticarse sin cifrar datos de objetos. Para especificar si el servidor debe utilizar TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor y el parámetro UPDATE SERVER=SSL para la comunicación de servidor a servidor. A partir de la versión V8.1.2, se utiliza TLS para la autenticación predeterminada. Si decide utilizar TLS para cifrar sesiones enteras, utilice el protocolo solo para las sesiones en las que es necesario y añada recursos de procesador en el servidor para gestionar el incremento del tráfico de red. También puede probar otras opciones. Por ejemplo, algunos dispositivos, como los direccionadores o los conmutadores, proporcionan la función TLS o SSL.

Puede utilizar TLS y SSL para proteger todas o algunas de las distintas vías de acceso de comunicación posibles, por ejemplo:

- Centro de operaciones: De navegador a concentrador; de concentrador a radio
- Cliente a servidor

- Servidor a servidor: réplica de nodo en el servidor:

#### Tareas relacionadas:

Configuración de comunicaciones seguras con Seguridad de la capa de transporte

## Planificación de almacenamiento de datos cifrados

Determine si la compañía requiere que se cifren los datos almacenados y elija el método que mejor se adapta a sus necesidades.

Tabla 1. Selección de un método de cifrado de datos

Requisito empresarial	Método de cifrado	Información adicional
Proteger los datos a nivel de cliente.	Cifrado del cliente de IBM Spectrum Protect	Puede cifrar los datos al nivel de archivos utilizando una lista de inclusión/exclusión. De este modo, puede mantener un alto grado de control sobre los datos que estén cifrados. Se necesitan recursos informáticos adicionales en el cliente que pueden afectar al rendimiento de los procesos de copia de seguridad y restauración. Para obtener más información acerca de este método, consulte Cifrado de cliente de IBM Spectrum Protect.
Proteger los datos de volúmenes de agrupación de almacenamiento en una unidad de cintas.	Método de aplicación	Cuando se utiliza el método de aplicaciones, IBM Spectrum Protect gestiona las claves de cifrado para proteger los datos de los volúmenes de agrupación de almacenamiento. Preste especial atención para proteger las copias de seguridad de las bases de datos porque las claves de cifrado se almacenan en la base de datos del servidor. Si no dispone de acceso a las copias de seguridad de la base de datos y a las claves de cifrado coincidentes, no podrá restaurar los datos. No puede utilizar este método para cifrar copias de seguridad de bases de datos, datos exportados o conjuntos de copias de seguridad. Para obtener más información sobre el método Aplicación, consulte Métodos de cifrado de cinta.
Proteger los datos en una unidad de cintas.	Método de biblioteca	Cuando se utiliza el método Biblioteca, la biblioteca gestiona las claves de cifrado. Puede cifrar los datos de las agrupaciones de almacenamiento y otros datos en una unidad de cintas. Puede controlar qué volúmenes se cifran utilizando sus números de serie de código de barras. Para obtener más información sobre el método Biblioteca, consulte Métodos de cifrado de cinta.
Proteger los datos en una unidad de cintas.	Método de sistema	Cuando utilice el método Sistema, un controlador de dispositivo o el sistema operativo AIX gestiona el cifrado. Este método de cifrado sólo está disponible en el sistema operativo AIX. Puede cifrar los datos de las agrupaciones de almacenamiento y otros datos en una unidad de cintas. Para obtener más información sobre el método Sistema, consulte Métodos de cifrado de cinta.

## Planificación del acceso de cortafuegos

Determine los cortafuegos que se han configurado y los puertos que deben estar abiertos para que funcione la solución IBM Spectrum Protect.

Tabla 1 describe los puertos utilizados por el servidor, el cliente y el Centro de operaciones.

Tabla 1. Puertos utilizados por el servidor, el cliente y Centro de operaciones

Elemento	Valor predeterminado	Dirección	Descripción
Puerto base (TCPPOINT)	1500	Entrada/salida	Cada instancia de servidor necesita un puerto exclusivo. Puede especificar un número de puerto alternativo. La opción TCPPOINT realiza escuchas para sesiones habilitadas para TCP/IP y SSL desde el cliente. Puede utilizar la opción TCPADMINPORT y la opción ADMINONCLIENTPORT para establecer los valores de puerto para el tráfico de cliente administrativo.
Puerto solo SSL (SSLTCPPOINT)	No tiene valor predeterminado	Entrada/salida	Este puerto se utiliza si desea restringir la comunicación en el puerto a sesiones solo habilitadas para SSL. Un servidor puede soportar las comunicaciones SSL y no SSL utilizando las opciones TCPPOINT o TCPADMINPORT.

Elemento	Valor predeterminado	Dirección	Descripción
SMB	45	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SSH	22	Entrada/salida	Este puerto lo utilizan los asistentes de configuración que se comunican utilizando protocolos nativos con varios hosts.
SMTP	25	Saliente	Este puerto se utiliza para enviar alertas de correo electrónico desde el servidor.
Réplica	No tiene valor predeterminado	Entrada/salida	El puerto y el protocolo correspondientes al puerto de salida para la réplica de datos se definen mediante el mandato DEFINE SERVER que se utiliza para configurar la réplica.  Los puertos de entrada para la réplica son los puertos TCP y SSL que están especificados para el servidor de origen en el mandato DEFINE SERVER.
Puerto de planificación del cliente	Puerto de cliente: 1501	Saliente	El cliente escucha en el puerto que se menciona y comunica el número de puerto al servidor. El servidor establece contacto con el cliente si se utiliza la planificación solicitada por servidor. Puede especificar un número de puerto alternativo en el archivo de opciones de cliente.
Sesiones de larga ejecución	Valor de KEEPALIVE: YES	Saliente	Cuando se habilita la opción KEEPALIVE, los paquetes de estado activo se envían durante las sesiones cliente/servidor para impedir que el software de cortafuegos cierre las conexiones inactivas de larga ejecución.
Centro de operaciones	HTTPS: 11090	Entrante	Estos puertos se utilizan por parte del navegador web de Centro de operaciones. Puede especificar un número de puerto alternativo.
Puerto de servicio de gestión de clientes	Puerto de cliente: 9028	Entrante	Si tiene previsto utilizar servicios de gestión de cliente de IBM Spectrum Protect, el puerto servicio de gestión de clientes debe ser accesible desde el Centro de operaciones. Asegúrese de que los cortafuegos no puedan impedir las conexiones. El servicio de gestión de clientes utiliza el puerto TCP del servidor para el nodo cliente para la autenticación utilizando una sesión administrativa.

**Tareas relacionadas:**

➤ Recopilación de información de diagnóstico con servicios de gestión de cliente de IBM Spectrum Protect

**Referencia relacionada:**

➤ ADMINONCLIENTPORT, opción de servidor

➤ DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

➤ TCPADMINPORT, opción de servidor

➤ TCPPORT, opción de servidor

## Implementación de una solución de protección de datos basada en cinta

Implemente la solución basada en cinta, que utiliza copia de seguridad 'de disco a disco a cinta' y disco intermedio para optimizar el almacenamiento. Al implementar la solución de cinta, puede habilitar la retención de datos a largo plazo y lograr una escalabilidad de bajo coste.



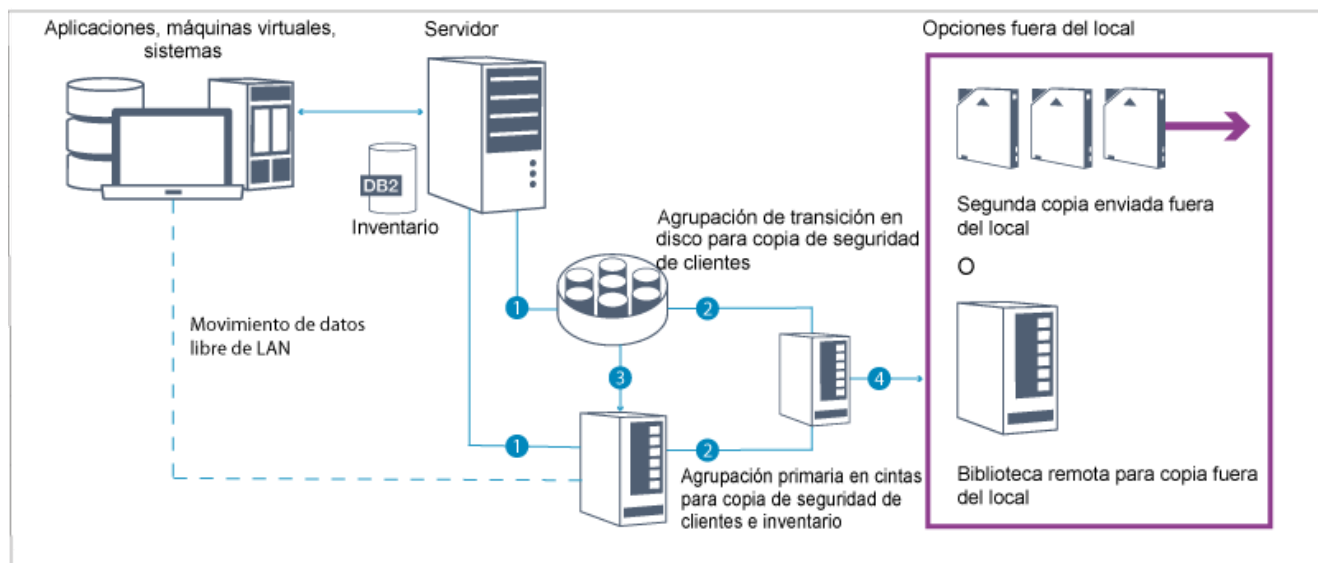
## Cinta

✓ Ideal para retención a largo plazo

✓ Escalabilidad a bajo coste

✓ Zona de transición disco a agrup. cintas

✓ Optimizado para SAN



Consejo: La solución descrita no incluye réplica de nodo. Sin embargo, si quiere utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento de disco a disco, asegúrese de que la operación de réplica esté completada antes de migrar los datos de disco a disco. También puede utilizar la réplica de nodo para realizar la copia de seguridad de una agrupación de almacenamiento en un dispositivo de cinta local a una agrupación de almacenamiento de copia en un dispositivo de cinta local.

## Hoja de ruta de la implementación

Se requieren los siguientes pasos para configurar una solución basada en cinta.

1. Configurar el sistema.
2. Instalar el servidor y el Centro de operaciones.
3. Configurar el servidor y el Centro de operaciones.
4. Conectar dispositivos de cinta para el servidor.
5. Configurar bibliotecas de cintas para su uso por parte de un servidor.
6. Configurar una jerarquía de agrupaciones de almacenamiento.
7. Instalar y configurar clientes.
8. Configurar el movimiento de datos sin LAN.
9. Seleccionar un método de cifrado y configurar el cifrado.
10. Definir operaciones de almacenamiento en cinta.
11. Completar la implementación.

## Configuración del sistema

Para configurar el sistema, primero debe configurar el hardware de almacenamiento de disco y el sistema servidor para IBM Spectrum Protect.

### Acerca de esta tarea

Consejo: Se describen los procedimientos para configurar el sistema de almacenamiento de disco y servidor. Para empezar a configurar dispositivos de cinta, consulte Conexión de dispositivos de cinta para el servidor.

- Configuración del hardware de almacenamiento  
Para optimizar el almacenamiento de disco, revise las directrices para configurar el almacenamiento de disco con IBM Spectrum Protect. A continuación, proporcione una conexión entre el servidor y los dispositivos de almacenamiento de disco y complete otras tareas de configuración.
- Instalación del sistema operativo del servidor  
Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Configuración de E/S de la multivía de acceso  
puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.
- Creación del ID de usuario para el servidor  
Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.
- Preparación de sistemas de archivos para el servidor  
Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

## Configuración del hardware de almacenamiento

---

Para optimizar el almacenamiento de disco, revise las directrices para configurar el almacenamiento de disco con IBM Spectrum Protect. A continuación, proporcione una conexión entre el servidor y los dispositivos de almacenamiento de disco y complete otras tareas de configuración.

### Antes de empezar

---

Para obtener directrices sobre cómo configurar el almacenamiento en disco, consulte Lista de comprobación para agrupaciones de almacenamiento en DISK o FILE

### Procedimiento

---

1. Proporcione una conexión entre el servidor y los dispositivos de almacenamiento siguiendo estas directrices:
  - Utilice un conmutador o conexión directa para las conexiones de canal de fibra.
  - Tenga en cuenta el número de puertos que están conectados y la cantidad de ancho de banda que se necesita.
  - Tenga en cuenta el número de puertos en el servidor y el número de puertos de host en el sistema de discos que están conectados.
2. Verifique que los controladores de dispositivo y firmware para el sistema servidor, adaptadores y sistema operativo son actuales y están en los niveles recomendados.
3. Configure matrices de almacenamiento. Asegúrese de que ha planificado correctamente para garantizar un rendimiento óptimo. Para obtener más información, consulte Planificación del almacenamiento en disco.
4. Asegúrese de que el sistema servidor tiene acceso a los volúmenes de disco que se han creado. Realice los pasos siguientes:
  - a. Si el sistema está conectado a un conmutador de canal de fibra, divida el servidor por zonas para ver los discos.
  - b. Correlacione todos los volúmenes para indicar al sistema de discos que este servidor específico está autorizado para ver cada disco.
5. Asegúrese de que los dispositivos de cinta y de disco utilicen distintos puertos de adaptador de bus de host (HBA). Controle la E/S de disco y cinta utilizando la SAN.

#### Tareas relacionadas:

Configuración de E/S de la multivía de acceso

## Instalación del sistema operativo del servidor

---

Instale el sistema operativo en el sistema servidor y asegúrese de que se cumplan los requisitos del servidor de IBM Spectrum Protect. Ajuste los valores del sistema operativo siguiendo las instrucciones.

- Instalación en sistemas AIX  
Complete los pasos siguientes para instalar AIX en el sistema servidor.
- Instalación en sistemas Linux  
Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.
- Instalación en sistemas Windows  
Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

## Instalación en sistemas AIX

---

Complete los pasos siguientes para instalar AIX en el sistema servidor.

### Procedimiento

---

1. Instale AIX Versión 7.1, TL4, SP2 o posterior de acuerdo con las instrucciones del fabricante.
2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

- Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- Verifique que el archivo contiene una entrada para `localhost` con una dirección de `127.0.0.1`. Por ejemplo:

```
127.0.0.1 localhost
```

4. Habilite los puertos de terminación de E/S de AIX emitiendo el siguiente mandato:

```
chdev -l iocp0 -P
```

El rendimiento de servidor puede verse afectado por la definición de huso horario de Olson.

5. Para optimizar el rendimiento, cambie el formato de huso horario del sistema de Olson a POSIX. Utilice el siguiente formato de mandato para actualizar el valor de huso horario:

```
chtz=local_timezone,date/time,date/time
```

Por ejemplo, si ha vivido en Tucson, Arizona, donde se utiliza la franja horaria de las Rocosas, deberá emitir el siguiente mandato para cambiar el formato POSIX:

```
chtz MST7MDT,M3.2.0/2:00:00,M11.1.0/2:00:00
```

6. Añada una entrada en el `.profile` del usuario de la instancia para que se defina el entorno siguiente:

```
export MALLOCOPTIONS=multiheap:16
```

7. Defina el sistema para crear archivos principales de aplicación completos. Emita el mandato siguiente:

```
chdev -l sys0 -a fullcore=true -P
```

8. Para las comunicaciones con el servidor y Centro de operaciones, asegúrese de que los siguientes puertos están abiertos en todos los cortafuegos que puedan existir:

- Para las comunicaciones con el servidor, abra el puerto 1500.
- Para las comunicaciones seguras con Centro de operaciones, abra el puerto 11090 en el servidor concentrador.

Si no utiliza los valores de puerto predeterminados, asegúrese de que los puertos que está utilizando están abiertos.

9. Habilite las mejoras de alto rendimiento de TCP. Emita el mandato siguiente:

```
no -p -o rfc1323=1
```

10. Para obtener una fiabilidad y un rendimiento óptimos, vincule cuatro puertos Ethernet de 10 Gb. Utilice la herramienta de la interfaz de gestión del sistema (SMIT) para vincular los puertos utilizando Etherchannel. Durante las pruebas se utilizaron los siguientes valores:

<code>mode</code>	<code>8023ad</code>	
<code>auto_recovery</code>	<code>yes</code>	Habilitar la recuperación automática tras la migración tras error.
<code>backup_adapter</code>	<code>NONE</code>	Adaptador utilizado cuando falla todo el canal.
<code>hash_mode</code>	<code>src_dst_port</code>	Determina cómo se elige el adaptador saliente.
<code>interval</code>	<code>long</code>	Determina el valor de intervalo para IEEE.
<code>mode</code>	<code>8023ad</code>	Modalidad de 802.3ad
<code>netaddr</code>	<code>0</code>	Modalidad de funcionamiento de EtherChannel
<code>noloss_failover</code>	<code>yes</code>	Dirección para el ping
<code>num_retries</code>	<code>3</code>	Habilitar migración tras error sin pérdidas tras anomalía del ping
<code>retry_time</code>	<code>1</code>	Veces que reintentar el ping antes de considerarlo un error
<code>use_alt_addr</code>	<code>no</code>	Tiempo de espera (en segundos) entre pings
<code>use_jumbo_frame</code>	<code>no</code>	Habilitar dirección EtherChannel alternativa
		Habilitar tramas de gran tamaño de Gigabit Ethernet

11. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 1. Si los valores `ulimit` no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 1. Valores de los límites de usuario (`ulimit`)



Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	ulimit -Hc
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	ulimit -Hd
Tamaño de archivo máximo	fsize	Ilimitado	ulimit -Hf
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Linux

Complete los pasos siguientes para instalar Linux x86\_64 en el sistema servidor.

### Antes de empezar

El sistema operativo se instalará en los discos duros internos. Configure los discos duros internos utilizando una matriz de hardware de RAID 1. Por ejemplo, si está configurando un sistema pequeño, los dos discos internos de 300 GB se duplican en RAID 1 de modo que aparece disponible un único disco de 300 GB para el instalador del sistema operativo.

### Procedimiento

1. Instale Red Hat Enterprise Linux Versión 7.1 o posterior, de acuerdo con las instrucciones del fabricante. Obtenga un DVD arrancable que contiene Red Hat Enterprise Linux Versión 7.1 e inicie el sistema desde el DVD. Consulte las siguientes directrices para ver las opciones de instalación. Si un elemento no se menciona en la lista siguiente, deje la selección predeterminada.
  - a. Después de iniciar el DVD, elija Instalar o actualizar un sistema existente en el menú.
  - b. En la pantalla de bienvenida, seleccione Probar este soporte e instalar Red Hat Enterprise Linux 7.1.
  - c. Seleccione las preferencias de idioma y teclado.
  - d. Seleccione la ubicación para establecer el huso horario correcto.
  - e. Seleccione Selección de software y, a continuación, en la siguiente pantalla, seleccione Servidor con GUI.
  - f. Desde la página de resumen de la instalación, pulse Destino de instalación y verifique los elementos siguientes:
    - El disco local de 300 GB se ha seleccionado como destino de instalación.
    - En Otras opciones de almacenamiento, Configurar particionamiento automáticamente está seleccionada.

Pulse Terminado.

g. Pulse Empezar instalación. Una vez iniciada la instalación, establezca la contraseña raíz para la cuenta de usuario root.

Una vez que se haya completado la instalación, reinicie el sistema e inicie una sesión como el usuario root. Emita el mandato df para verificar el particionamiento básico. Por ejemplo, en un sistema de prueba, el particionamiento inicial ha generado el resultado siguiente:

```
[root@tvapp02]# df -h
Filesystem                Size  Used Avail Use% Mounted on
/dev/mapper/rhel-root     50G   3.0G   48G   6% /
devtmpfs                  32G    0    32G   0% /dev
tmpfs                     32G   92K   32G   1% /dev/shm
tmpfs                     32G   8.8M   32G   1% /run
tmpfs                     32G    0    32G   0% /sys/fs/cgroup
/dev/mapper/rhel-home    220G   37M   220G   1% /home
/dev/sda1                 497M  124M   373M  25% /boot
```

2. Configure los valores de TCP/IP según las instrucciones de instalación del sistema operativo.

Para obtener un rendimiento y fiabilidad óptimos, considere la posibilidad de vincular varios puertos de red. Esto se puede conseguir creando la conexión de red del protocolo de control de agregación de enlaces (LACP), que agregar varios puertos subordinados a una sola conexión lógica. El método preferido es utilizar una modalidad de vínculo de 802.3ad, un valor de miimon de 100 y un valor de xmit\_hash\_policy de layer3+4.

Restricción: Para utilizar una conexión de red LACP, debe disponer de un conmutador de red que admita LACP.

Para obtener instrucciones adicionales sobre cómo configurar conexiones de red vinculadas con Red Hat Enterprise Linux Versión 7, consulte Crear una interfaz de acoplamiento de canal.

3. Abra el archivo `/etc/hosts` y complete las siguientes acciones:

- o Actualice el archivo para incluir la dirección IP y el nombre de host para el servidor. Por ejemplo:

```
192.0.2.7 server.yourdomain.com server
```

- o Verifique que el archivo contiene una entrada para localhost con una dirección de 127.0.0.1. Por ejemplo:

```
127.0.0.1 localhost
```

4. Instale los componentes que son necesarios para la instalación de servidor. Complete los pasos siguientes para crear un repositorio Yellowdog Updater Modified (YUM) e instale los paquetes de requisitos previos.

- a. Monte el DVD de instalación de Red Hat Enterprise Linux en el directorio del sistema. Por ejemplo, para montarlo en el directorio `/mnt`, emita el siguiente mandato:

```
mount -t iso9660 -o ro /dev/cdrom /mnt
```

- b. Verifique que el DVD se ha montado emitiendo el mandato `mount`. Debería ver una salida similar al ejemplo siguiente:

```
/dev/sr0 on /mnt type iso9660
```

- c. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

Si el directorio `repos.d` no existe, créelo.

- d. Liste el contenido de directorio:

```
ls rhel-source.repo
```

- e. Cambie el nombre del archivo repo original emitiendo el mandato `mv`. Por ejemplo:

```
mv rhel-source.repo rhel-source.repo.orig
```

- f. Cree un nuevo archivo repo utilizando un editor de texto. Por ejemplo, para utilizar el editor `vi`, emita el siguiente mandato:

```
vi rhel71_dvd.repo
```

- g. Añada las líneas siguientes al nuevo archivo repo. El parámetro `baseurl` especifica el punto de montaje del directorio:

```
[rhel71_dvd]
name=DVD Redhat Enterprise Linux 7.1
baseurl=file:///mnt
enabled=1
gpgcheck=0
```

- h. Instale el paquete de requisito previo `ksh.x86_64`, emitiendo el mandato `yum`. Por ejemplo:

```
yum install ksh.x86_64
```

Excepción: No necesita instalar las bibliotecas `compat-libstdc++-33-3.2.3-69.el6.i686` y `libstdc++.i686` para Red Hat Enterprise Linux Versión 7.1.

5. Cuando se completa la instalación de software, puede restaurar los valores de repositorio YUM originales completando los pasos siguientes:

- a. Desmonte el DVD de instalación de Red Hat Enterprise Linux emitiendo el siguiente mandato:

```
umount /mnt
```

- b. Cambie al directorio de repositorio YUM emitiendo el siguiente mandato:

```
cd /etc/yum/repos.d
```

- c. Cambie el nombre del archivo repo que ha creado:

```
mv rhel71_dvd.repo rhel71_dvd.repo.orig
```

- d. Cambie el nombre del archivo original al nombre original:

```
mv rhel-source.repo.orig rhel-source.repo
```

6. Determine si son necesarios cambios de parámetro de kernel. Realice los pasos siguientes:

- a. Utilice el mandato `sysctl -a` para listar los valores de parámetro.

- b. Analice los resultados utilizando las directrices en Tabla 1 para determinar si es necesario algún cambio.

c. Si se necesitan cambios, establezca los parámetros en el archivo /etc/sysctl.conf. Los cambios de archivo se aplican cuando se inicia el sistema.

Consejo: Ajuste automáticamente los valores de parámetros de kernel y elimine la necesidad de actualizaciones manuales en estos valores. En Linux, el software de base de datos DB2 ajusta automáticamente los valores del parámetro de kernel de comunicación entre procesos (IPC) a los valores preferidos. Para obtener más información sobre los valores de parámetros de kernel, busque los parámetros de kernel de Linux en IBM DB2 versión 11.1 Knowledge Center.

Tabla 1. Valores óptimos del parámetro de kernel Linux

Parámetro	Descripción
kernel.shmni	El número máximo de segmentos.
kernel.shmmax	El tamaño máximo de un segmento de memoria compartida (bytes).  Este parámetro debe establecerse antes de iniciar automáticamente el servidor IBM Spectrum Protect durante el arranque del sistema.
kernel.shmall	La asignación máxima de páginas de memoria compartida (páginas).
kernel.sem  Hay cuatro valores para el parámetro kernel.sem.	(SEMMSL) El número máximo de semáforos por matriz.  (SEMMNS) El número máximo de semáforos por sistema.  (SEMOPM) El número máximo de operaciones por llamada a semáforo.  (SEMMNI) El número máximo de matrices.
kernel.msgmni	El número máximo de colas de mensajes a nivel de sistema.
kernel.msgmax	Tamaño máximo de los mensajes (bytes).
kernel.msgmnb	El tamaño máximo predeterminado de colas (bytes).
kernel.randomize_va_space	El parámetro kernel.randomize_va_space configura el uso del ASLR de memoria para el kernel. Inhabilite ASLR, porque puede provocar errores para el software de DB2. Para obtener más detalles sobre Linux ASLR y DB2, consulte la nota técnica 1365583.
vm.swappiness	El parámetro vm.swappiness define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.
vm.overcommit_memory	El parámetro vm.overcommit_memory influye en la cantidad de memoria virtual que permite asignar el kernel. Para obtener más información sobre los parámetros del kernel, consulte Información del producto DB2.

7. Abra puertos de cortafuegos para comunicarse con el servidor. Realice los pasos siguientes:

a. Determine la zona utilizada por la interfaz de red. De forma predeterminada, la zona es pública.

Emita el mandato siguiente:

```
# firewall-cmd --get-active-zones
public
  interfaces: ens4f0
```

b. Para utilizar la dirección de puerto predeterminada para las comunicaciones con el servidor, abra el puerto TCP/IP 1500 en el cortafuegos de Linux.

Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=1500/tcp --permanent
```

Si desea utilizar un valor distinto del predeterminado, puede especificar un número en el rango 1024 - 32767. Si abre un puerto distinto del predeterminado, tendrá que especificar ese puerto cuando ejecute el script de configuración.

- c. Si piensa utilizar este sistema como concentrador, abra el puerto 11090, que es el puerto predeterminado para las comunicaciones seguras (https).  
Emita el mandato siguiente:

```
firewall-cmd --zone=public --add-port=11090/tcp --permanent
```

- d. Vuelva a cargar las definiciones de cortafuegos para que los cambios entren en vigor.  
Emita el mandato siguiente:

```
firewall-cmd --reload
```

8. Verifique que los límites de recursos de proceso de usuario, también conocidos como *ulimits*, se han establecido de acuerdo con las directrices en Tabla 2. Si los valores ulimit no se establecen correctamente, es posible que experimente inestabilidad del servidor o un fallo en la respuesta del servidor.

Tabla 2. Valores de los límites de usuario (ulimit)

Tipo de límite de usuario	Valor	Valor	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	core	Ilimitado	ulimit -Hc
Tamaño máximo de un segmento de datos para un proceso	datos	Ilimitado	ulimit -Hd
Tamaño de archivo máximo	fsize	Ilimitado	ulimit -Hf
Número máximo de archivos abiertos	nofile	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	cpu	Ilimitado	ulimit -Ht
Número máximo de procesos de usuario	nproc	16384	ulimit -Hu

Si necesita modificar los valores de límite de usuario, siga las instrucciones que encontrará en la documentación para el sistema operativo.

## Instalación en sistemas Windows

Instalar Microsoft Windows Server 2012 Standard Edition en el sistema del servidor y preparar el sistema para la instalación y configuración del servidor IBM Spectrum Protect.

### Procedimiento

1. Instale Microsoft Windows Server 2012 R2 Standard Edition, de acuerdo con las instrucciones del fabricante.
2. Cambie las políticas de control de cuenta Windows completando los pasos siguientes.
  - a. Abra el editor de política de seguridad local ejecutando secpol.msc.
  - b. Pulse Políticas locales > Opciones de seguridad y asegúrese de que están inhabilitadas las políticas siguientes de control de cuenta de usuario:
    - Modo de aprobación de administrador para la cuenta de administrador integrado
    - Ejecute todos los administradores en Modo de aprobación de administrador
3. Configure los valores de TCP/IP según las instrucciones de instalación para el sistema operativo.
4. Aplique actualizaciones de Windows y habilite las funciones opcionales completando los pasos siguientes:
  - a. Aplique las últimas actualizaciones de Windows 2012 R2.
  - b. Instale y habilite la característica de Windows 2012 R2 Microsoft .NET Framework 3.5 de Windows Server Manager.
  - c. Si es necesario, actualice los controladores de dispositivo FC y Ethernet HBA a niveles más nuevos.
  - d. Instale el controlador de E/S de multivía de acceso que es adecuado para el sistema de disco que está utilizando.
5. Abra el puerto TCP/IP predeterminado, 1500, para las comunicaciones con el servidor IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Backup server port 1500"
dir=in action=allow protocol=TCP localport=1500
```

6. En el servidor concentrador de Centro de operaciones, abra el puerto predeterminado para comunicaciones seguras (https) con Centro de operaciones. El número de puerto es 11090. Por ejemplo, emita el siguiente mandato:

```
netsh advfirewall firewall add rule name="Centro de operaciones port 11090"  
dir=in action=allow protocol=TCP localport=11090
```

## Configuración de E/S de la multivía de acceso

---

puede habilitar y configurar varias vías de acceso para el almacenamiento de disco. Utilice la documentación que se proporciona con el hardware para obtener instrucciones detalladas.

- Sistemas AIX  
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.
- Sistemas Linux  
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.
- Sistemas Windows  
Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

## Sistemas AIX

---

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

### Procedimiento

---

1. Determine la dirección de puerto de canal de fibra que debe utilizar para la definición de host en el subsistema de disco. Emita el mandato `lscfg` para cada puerto.

- En sistemas pequeños y medianos, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"
```

- En sistemas grandes, emita los siguientes mandatos:

```
lscfg -vps -l fcs0 | grep "Network Address"  
lscfg -vps -l fcs1 | grep "Network Address"  
lscfg -vps -l fcs2 | grep "Network Address"  
lscfg -vps -l fcs3 | grep "Network Address"
```

2. Asegúrese de que los siguientes conjuntos de archivos AIX están instalados:

- `devices.common.IBM.mpio.rte`
- `devices.fcp.disk.array.rte`
- `devices.fcp.disk.rte`

3. Emita el mandato `cfgmgr` para hacer que AIX vuelva a explorar el hardware y descubrir los discos disponibles. Por ejemplo:

```
cfgmgr
```

4. Para listar los discos disponibles, emita el siguiente mandato:

```
lsdev -Ccdisk
```

Deberá obtener unos resultados parecidos a los siguientes:

```
hdisk0 Available 00-00-00 SAS Disk Drive  
hdisk1 Available 00-00-00 SAS Disk Drive  
hdisk2 Available 01-00-00 SAS Disk Drive  
hdisk3 Available 01-00-00 SAS Disk Drive  
hdisk4 Available 06-01-02 MPIO IBM 2076 FC Disk  
hdisk5 Available 07-01-02 MPIO IBM 2076 FC Disk  
...
```

5. Utilice la salida del mandato `lsdev` para identificar y listar ID de dispositivo para cada dispositivo de disco.

Por ejemplo, un ID de dispositivo podría ser `hdisk4`. Guarde la lista de ID de dispositivo a utilizar cuando crea sistemas de archivos para el servidor IBM Spectrum Protect.

6. Correlacione los ID de dispositivo SCSI para especificar los LUN de disco del sistema de discos listando la información detallada sobre todos los volúmenes físicos del sistema. Emita el mandato siguiente:

```
lspv -u
```

En un sistema IBM® Storwize, la información siguiente es un ejemplo de lo que se muestra para cada dispositivo:

```
hdisk4 00f8cf083fd97327 None active
332136005076300810105780000000000003004214503IBMfcp
```

En el ejemplo, `6005076300810105780000000000030` es el ID de usuario para el volumen, como informa la interfaz de gestión Storwize.

Para verificar el tamaño de disco en megabytes y compararlo con el valor que se lista para el sistema, emita el siguiente mandato:

```
bootinfo -s hdisk4
```

## Sistemas Linux

---

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

### Procedimiento

---

1. Edite el archivo `/etc/multipath.conf` para habilitar las multivías de acceso para los host de Linux. Si el archivo `multipath.conf` no existe, puede crearlo emitiendo el siguiente mandato:

```
mpathconf --enable
```

Los parámetros siguientes se han establecido en `multipath.conf` para realizar pruebas en un sistema IBM Storwize:

```
defaults {
    user_friendly_names no
}

devices {
    device {
        vendor "IBM "
        product "2145"
        path_grouping_policy group_by_prio
        user_friendly_names no
        path_selector "round-robin 0"
        prio "alua"
        path_checker "tur"
        failback "immediate"
        no_path_retry 5
        rr_weight uniform
        rr_min_io_rq "1"
        dev_loss_tmo 120
    }
}
```

2. Establezca la opción de multivía de acceso para iniciarse cuando se inicia el sistema. Emita los mandatos siguientes:

```
systemctl enable multipathd.service
systemctl start multipathd.service
```

3. Para verificar que los discos están visibles para el sistema operativo y gestionados por una multivía de acceso, emita el siguiente mandato:

```
multipath -l
```

4. Asegúrese de que se lista cada uno de los dispositivos y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de ID de dispositivo y tamaño para identificar qué discos se listan.  
Por ejemplo, la salida siguiente muestra que un disco de 2 TB tiene dos grupos de vías de acceso y cuatro vías de acceso activas. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación. Utilice parte del número ID de dispositivo largo (12, en este ejemplo) para buscar el volumen en la interfaz de gestión del sistema de discos.

```
[root@tapsrv01 code]# multipath -l
36005076802810c509800000000000012 dm-43 IBM,2145
size=2.0T features='1 queue_if_no_path' hwhandler='0' wp=rw
|-+- policy='round-robin 0' prio=0 status=active
|  |- 2:0:1:18 sdcw 70:64 active undef running
|  `-- 4:0:0:18 sdgb 131:112 active undef running
`-+- policy='round-robin 0' prio=0 status=enabled
|  |- 1:0:1:18 sdat 66:208 active undef running
|  `-- 3:0:0:18 sddy 128:0 active undef running
```

- a. Si es necesario, corrija las asignaciones de host de LUN de disco y fuerce una reexploración. Por ejemplo:

```
echo "- - -" > /sys/class/scsi_host/host0/scan
echo "- - -" > /sys/class/scsi_host/host1/scan
echo "- - -" > /sys/class/scsi_host/host2/scan
```

También puede reiniciar el sistema para volver a explorar las asignaciones de host de LUN de disco.

- b. Confirme que los discos están ahora disponibles para la E/S de multivía de acceso volviendo a emitir el mandato multipath -l.
5. Utilice la salida de multivía de acceso para identificar y listar los ID de dispositivo para cada dispositivo de disco.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 36005076802810c50980000000000012.

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

## Sistemas Windows

---

Complete los pasos siguientes para habilitar y configurar las multivías de acceso para el almacenamiento de disco.

### Procedimiento

---

1. Asegúrese de que la función de E/S de multivía de acceso está instalada. Si es necesario, instale controladores con varias vías de acceso específicas del proveedor adicionales.
2. Para verificar que los discos están visibles para el sistema operativo y gestionados por una E/S de multivía de acceso, emita el siguiente mandato:

```
c:\program files\IBM\SDDDSM\datapath.exe query device
```

3. Revise la salida de multivía de acceso y asegúrese de que cada dispositivo está listado y de que tiene tantas vías de acceso como esperaba. Puede utilizar la información de serie del dispositivo y el tamaño para identificar qué discos se listan. Por ejemplo, utilizando parte del número de serie del dispositivo largo (34, en este ejemplo), puede buscar el volumen en la interfaz de gestión del sistema de discos. El tamaño de 2 TB confirma que el disco se corresponde con un sistema de archivos de la agrupación de almacenamiento.

```
DEV#: 4 DEVICE NAME: Disk5 Part0 TYPE: 2145 POLICY: OPTIMIZED
SERIAL: 60050763008101057800000000000034 LUN SIZE: 2.0TB
=====
Path# Adapter/Hard Disk State Mode Select Errors
0 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 0 0
1 Scsi Port2 Bus0/Disk5 Part0 OPEN NORMAL 27176 0
2 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 28494 0
3 Scsi Port3 Bus0/Disk5 Part0 OPEN NORMAL 0 0
```

4. Cree una lista de ID de dispositivo de disco mediante los números de serie que se devuelven de la salida de multivía de acceso en el paso anterior.

Por ejemplo, el ID de dispositivo para el disco de 2 TB es 60050763008101057800000000000034

Guarde la lista de ID de dispositivo para utilizarla en el paso siguiente.

5. Para poner los nuevos discos en línea y borrar el atributo de 'sólo lectura', ejecute diskpart.exe con los mandatos siguientes. Repítalo para cada uno de los discos:

```
diskpart
select Disk 1
online disk
attribute disk clear readonly
select Disk 2
online disk
attribute disk clear readonly
< ... >
select Disk 49
online disk
attribute disk clear readonly
exit
```

## Creación del ID de usuario para el servidor

---

Cree el ID de usuario que es propietario de la instancia de servidor de IBM Spectrum Protect. Especifique este ID de usuario cuando cree la instancia de servidor durante la configuración inicial del servidor.

## Acerca de esta tarea

---



Solo puede especificar letras en minúsculas (a-z), números (0-9), y el carácter subrayado ( \_ ) para el ID de usuario. El ID de usuario y nombre de grupo deben cumplir las siguientes normas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.


## Procedimiento

---


1. Utilice mandatos del sistema operativo para crear un ID de usuario.

-   Cree un grupo y un ID de usuario en el directorio de inicio del usuario que es propietario de la instancia de servidor.

Por ejemplo, para crear el ID de usuario `tsminst1` en el grupo `tsmsrvrs` con una contraseña de `tsminst1`, emita los siguientes mandatos desde un ID de usuario de administración:


 **Sistemas operativos AIX**

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

 **Sistemas operativos Linux**

```
groupadd tsmsrvrs
useradd -d /home/tsminst1 -m -g tsmsrvrs -s /bin/bash tsminst1
passwd tsminst1
```

Cierre sesión y, a continuación, inicie sesión en el sistema. Vaya a la cuenta de usuario que ha creado. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

-  **Sistemas operativos Windows** Cree un ID de usuario y, a continuación, añada el nuevo ID al grupo de administradores. Por ejemplo, para crear el ID de usuario `tsminst1`, emita el siguiente mandato:

```
net user tsminst1 * /add
```

Después de crear y verificar una contraseña para el nuevo usuario, añada el ID de usuario al grupo Administradores emitiendo los siguientes mandatos:

```
net localgroup Administrators tsminst1 /add
net localgroup DB2ADMNS tsminst1 /add
```

2. Cierre la sesión con el nuevo ID de usuario.

## Preparación de sistemas de archivos para el servidor

---

Debe completar la configuración del sistema de archivos para el almacenamiento de disco que va a utilizar el servidor.

- Preparación de sistemas de archivos en sistemas AIX  
Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.
- Preparación de sistemas de archivos en sistemas Linux  
Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.
- Preparación de sistemas de archivos en sistemas Windows  
Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas AIX

---

Debe crear grupos de volúmenes, volúmenes lógicos y sistemas de archivos para el servidor utilizando el gestor de volúmenes lógicos de AIX.

## Procedimiento

---



1. Aumente la profundidad de cola y el tamaño de transferencia máximo para todos los discos *hdiskX* disponibles. Emita los siguientes mandatos para cada disco:

```
chdev -l hdisk4 -a max_transfer=0x100000
chdev -l hdisk4 -a queue_depth=32
chdev -l hdisk4 -a reserve_policy=no_reserve
chdev -l hdisk4 -a algorithm=round_robin
```

No ejecute estos mandatos para discos internos del sistema operativo, por ejemplo, *hdisk0*.

2. Cree grupos de volúmenes para la base de datos, registro activo, registro de archivado, copia de seguridad de base de datos y agrupación de almacenamiento de IBM Spectrum Protect. Emita el mandato `mkvg`, especificando los ID de dispositivo para discos correspondientes que ha identificado previamente.

Por ejemplo, si los nombres de dispositivo *hdisk4*, *hdisk5* y *hdisk6* corresponden a discos de base de datos, inclúyalos en el grupo de volúmenes de base de datos y, así, sucesivamente.

Tamaño del sistema: Los siguientes mandatos se basan en la configuración del sistema mediano. Para sistemas pequeños y grandes, debe ajustar la sintaxis como sea necesario.

```
mkvg -S -y tsmdb hdisk2 hdisk3 hdisk4
mkvg -S -y tsmactlog hdisk5
mkvg -S -y tsmarchlog hdisk6
mkvg -S -y tsmdbback hdisk7 hdisk8 hdisk9 hdisk10
mkvg -S -y tsmstgpool hdisk11 hdisk12 hdisk13 hdisk14 ... hdisk49
```

3. Determine los nombres de volumen físico y el número de particiones físicas libre para utilizarlos cuando cree volúmenes lógicos. Emita `lsvg` para cada grupo de volúmenes que ha creado en el paso anterior.

Por ejemplo:

```
lsvg -p tsmdb
```

La salida es similar a la siguiente. La columna *FREE PPs* representa las particiones físicas libres:

```
tsmdb:
PV_NAME  PV STATE  TOTAL PPs  FREE PPs  FREE DISTRIBUTION
hdisk4   active    1631      1631     327..326..326..326..326
hdisk5   active    1631      1631     327..326..326..326..326
hdisk6   active    1631      1631     327..326..326..326..326
```

4. Cree volúmenes lógicos en cada grupo de volúmenes utilizando el mandato `mklv`. El tamaño de volumen, el grupo de volúmenes y los nombres de dispositivo varían, en función del tamaño del sistema y de las variaciones en la configuración de disco.

Por ejemplo, para crear los volúmenes para la base de datos de IBM Spectrum Protect en un sistema mediano, emita los mandatos siguientes:

```
mklv -y tsmdb00 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk2
mklv -y tsmdb01 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk3
mklv -y tsmdb02 -t jfs2 -u 1 -x 1631 tsmdb 1631 hdisk4
```

5. De formato a los sistemas de archivo en cada volumen lógico utilizando el mandato `crfs`.

Por ejemplo, para formatear sistemas de archivos para la base de datos en un sistema mediano, emita los mandatos siguientes:

```
crfs -v jfs2 -d tsmdb00 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace00 -A yes
crfs -v jfs2 -d tsmdb01 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace01 -A yes
crfs -v jfs2 -d tsmdb02 -p rw -a logname=INLINE -a options=rbrw
-a agblksize=4096 -m /tsminst1/TSMdbspace02 -A yes
```

6. Monte todos los sistemas de archivo recién creados emitiendo el siguiente mandato:

```
mount -a
```

7. Liste todos los sistemas de archivos emitiendo el mandato `df`. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.

El ejemplo siguiente de la salida del mandato muestra que la cantidad de espacio utilizado es normalmente un 1%:

```
tapsrv07> df -g /tsminst1/*
Filesystem  GB blocks  Free    %Used  Iused  %Iused  Mounted on
/dev/tsmact00  195.12   194.59   1%     4      1%     /tsminst1/TSMalog
```

8. Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios del servidor.

## Preparación de sistemas de archivos en sistemas Linux

Debe formatear los sistemas de archivos ext4 o xfs en cada uno de los LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

## Procedimiento

---

1. Utilizando la lista de ID de dispositivo que ha generado antes, emita el mandato mkfs para crear y dar formato a un sistema de archivos para cada dispositivo LUN de almacenamiento. Especifique el ID de dispositivo en el mandato. Consulte los ejemplos siguientes. Para la base de datos, formatee los sistemas de archivos ext4:

```
mkfs -t ext4 -T largefile -m 2 /dev/mapper/36005076802810c50980000000000012
```

Para las LUN de agrupación de almacenamiento, formatee los sistemas de archivos xfs:

```
mkfs -t xfs /dev/mapper/3600507630081010578000000000002c3
```

Puede emitir el mandato mkfs hasta 50 veces, dependiendo de cuántos dispositivos diferentes tiene.

2. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato mkdir para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación.

Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
mkdir /tsminst1
```

Repita el mandato mkdir para cada sistema de archivos.

3. Añada una entrada en el archivo /etc/fstab para cada sistema de archivos para que los sistemas de archivos se monten automáticamente cuando se inicia el servidor.  
Por ejemplo:

```
/dev/mapper/36005076802810c50980000000000012 /tsminst1/TSMdbspace00 ext4 defaults 0 0
```

4. Monte los sistemas de archivos que ha añadido al archivo /etc/fstab emitiendo el mandato mount -a.
5. Liste todos los sistemas de archivos emitiendo el mandato df. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Además, verifique el espacio disponible.  
El ejemplo siguiente en un sistema IBM® Storwize muestra que la cantidad de espacio utilizado normalmente es un 1%:

```
[root@tapsrv04 ~]# df -h /tsminst1/*
Filesystem                                Size  Used Avail Use% Mounted on
/dev/mapper/36005076300810105780000000000003 134G  188M 132G   1%  /tsminst1/TSMalog
```

6. Verifique que el ID de usuario que ha creado en Creación del ID de usuario para el servidor tiene acceso de lectura y escritura en los directorios del servidor IBM Spectrum Protect.

## Preparación de sistemas de archivos en sistemas Windows

---

Debe formatear sistemas de archivos NTFS (New Technology File System) en cada una de las LUN de disco que va a utilizar el servidor IBM Spectrum Protect.

## Procedimiento

---

1. Cree directorios de punto de montaje para sistemas de archivos.

Emita el mandato md para cada directorio que debe crear. Utilice los valores de directorio que ha registrado en las hojas de trabajo de planificación. Por ejemplo, para crear el directorio de instancia de servidor utilizando el valor predeterminado, emita el mandato siguiente

```
md c:\tsminst1
```

Repita el mandato md para cada sistema de archivos.

2. Cree un volumen para cada LUN de disco que se correlaciona a un directorio bajo el directorio de instancia de servidor utilizando el gestor de volúmenes de Windows.

Vaya a Gestor de servidores > Servicios de archivo y almacenamiento y complete los pasos siguientes para cada disco que corresponde a la correlación de LUN que se ha creado en el paso anterior:

- a. Ponga el disco en línea.
- b. Inicialice el disco en el tipo básico GPT, que es el valor predeterminado.
- c. Crear un volumen simple que ocupa todo el espacio en el disco. Dé formato al sistema de archivos utilizando NTFS y asignando una etiqueta que coincida con la finalidad del volumen, como TSMfile00. No asigna el nuevo volumen a la letra

de unidad. En su lugar, correlacione el volumen a un directorio bajo el directorio de instancia, como C:\tsminst1\TSMfile00.

Consejo: Determine la etiqueta de volumen y las etiquetas de correlación de directorio en función del tamaño del disco del que se informa.

3. Verifique que los sistemas de archivos están montados en el LUN correcto y el punto de montaje correcto. Liste todos los sistemas de archivos emitiendo el mandato mountvol y, a continuación, revise la salida. Por ejemplo:

```
\\?\Volume{8ffb9678-3216-474c-a021-20e420816a92}\  
C:\tsminst1\TSMdbspace00\  

```

4. Una vez se ha completado la configuración de disco, reinicie el sistema.

## Qué hacer a continuación

---

Puede confirmar la cantidad de espacio libre para cada volumen utilizando Windows Explorer.

## Instalación del servidor y Centro de operaciones

---

Utilice el asistente gráfico de IBM® Installation Manager para instalar los componentes.

- Instalación en sistemas AIX y Linux  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.
- Instalación en sistemas Windows  
Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

## Instalación en sistemas AIX y Linux

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

## Antes de empezar

---

Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

---

1.  Sistemas operativos AIX Verifique que los archivos RPM necesarios están instalados en el sistema.

Consulte Instalación de archivos RPM de requisitos previos para el asistente gráfico para obtener más detalles.


2. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042992.
3. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
4. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

5. Extraiga el paquete emitiendo el siguiente mandato:

```
./nombre_paquete.bin
```

donde *package\_name* es el nombre del archivo descargado.

6.  Sistemas operativos AIX Asegúrese de que el mandato siguiente está habilitado, de forma que los asistentes funcionen correctamente:

```
lsuser
```

De manera predeterminada, el mandato está habilitado.

7. Cambie al directorio en el que colocó el archivo ejecutable.
8. Inicie el asistente de instalación emitiendo el mandato siguiente:

```
./install.sh
```

Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.
- Instalación de archivos RPM de requisitos previos para el asistente gráfico  
Los archivos RPM son necesarios para el asistente gráfico Gestor de instalación de IBM.

## Instalación en sistemas Windows

---

Instalar el servidor IBM Spectrum Protect y Centro de operaciones en el mismo sistema.

### Antes de empezar

---

Asegúrese de que se cumplen los siguientes requisitos previos:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
- Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

### Procedimiento

---

1. Antes de descargar el paquete de instalación, verifique que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para los requisitos de espacio, consulte el documento de descarga en nota técnica 4042993.
2. Vaya a Passport Advantage y descargue el archivo de paquete en un directorio vacío de su elección.
3. Cambie al directorio en el que colocó el archivo ejecutable.
4. Efectúe doble pulsación en el archivo ejecutable para extraerlo al directorio actual.
5. En el directorio donde se han extraído los archivos de instalación, inicie el asistente de instalación efectuando una doble pulsación en el archivo install.bat. Cuando seleccione los paquetes a instalar, elija el servidor y Centro de operaciones.

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros del Gestor de instalación de IBM®.

Para ver archivos de registro de instalación desde la herramienta de Installation Manager, pulse Archivo > Ver registro. Para recopilar estos archivos de registro desde la herramienta Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

- Tras instalar el servidor y antes de personalizarlo para su uso, vaya a Sitio de soporte de IBM Spectrum Protect. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Configuración del servidor y el Centro de operaciones

---

Después de instalar los componentes, complete la configuración del servidor de IBM Spectrum Protect y el Centro de operaciones.

- Configuración de la instancia de servidor  
Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.
- Instalación del cliente de archivado y copia de seguridad  
Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?
- Configuración de opciones para el servidor  
Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

- Conceptos sobre la seguridad  
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- Configuración de Centro de operaciones  
Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.
- Registro de la licencia de producto  
Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.
- Definición de las reglas de retención de datos para su empresa  
Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.
- Definición de planificaciones para actividades de mantenimiento del servidor  
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.
- Definición de planificaciones de cliente  
Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

## Configuración de la instancia de servidor

Utilice el asistente de configuración de instancia de servidor IBM Spectrum Protect para completar la configuración inicial del servidor.

### Antes de empezar

Asegúrese de que se cumplen los siguientes requisitos:

 Sistemas operativos AIX  Sistemas operativos Linux

- El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Windows. Además, debe estar ejecutando un servidor de sistema X Windows en su escritorio.
- El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo sshd\_config en el directorio de /etc/ssh/. También, asegúrese de que el servicio de daemon SSH tiene derechos de acceso para conectarse al sistema utilizando el valor *localhost*.
- Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
- Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.




 Sistemas operativos Windows Verifique que el servicio de registro remoto se ha iniciado completando los pasos siguientes:



1. Pulse Inicio > Herramientas administrativas > Servicios. En la ventana Servicios, seleccione Registro remoto. Si no se ha iniciado, pulse Inicio.
2. Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
  - a. Pulse Inicio > Panel de control > Cortafuegos de Windows.
  - b. Seleccione Configuración avanzada.
  - c. Seleccione Reglas de entrada.
  - d. Seleccione Nueva regla.
  - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones para redes de dominio y privadas.
3. Configure el control de cuenta de usuario accediendo a las opciones de política de seguridad local y completando los siguientes pasos.
  - a. Pulse Inicio > Herramientas administrativas > Política de seguridad local. Expanda Políticas locales > Opciones de seguridad.
  - b. Si no se ha habilitado, habilite la cuenta de administrador incorporada seleccionando Cuentas: Estado de cuenta de administrador > Habilitar > Aceptar.
  - c. Si aún no se ha inhabilitado, inhabilite el control de cuenta de usuario para todos los administradores de Windows seleccionando Control de cuenta de usuario: Ejecutar todos los administradores en modo de aprobación de administrador > Inhabilitar > Aceptar .
  - d. Si aún no se ha inhabilitado, inhabilite el Control de cuenta de usuario para la cuenta de administrador incorporada seleccionando Control de cuenta de usuario: Modo de aprobación de administrador para la cuenta de administrador incorporada > Inhabilitar > Aceptar.
4. Si ha cambiado cualquier valor en los pasos anteriores, reinicie el servidor antes de continuar con el asistente de configuración.


### Acerca de esta tarea

El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Procedimiento

1. Inicie la versión local del asistente.
  -   Abra el programa dsmsicfgx en el directorio /opt/tivoli/tsm/server/bin. Este asistente sólo puede ejecutarse como usuario root.
  -  Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración.
2. Siga las instrucciones para completar la configuración. Utilice la información que ha registrado en Planificación de hojas de trabajo al configurar el sistema IBM Spectrum Protect para especificar directorios y opciones en el asistente.

  En la ventana Información de servidor, establezca el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia cuando se arranca el sistema.

 Utilizando el asistente de configuración, el servidor se configura para iniciarse de forma automática cuando se reinicia.

## Instalación del cliente de archivado y copia de seguridad

Se recomienda instalar el cliente de archivado y copia de seguridad de IBM Spectrum Protect en el sistema servidor para que el cliente de línea de mandatos administrativos y el planificador estén disponibles?

### Procedimiento

Para instalar el cliente de archivado y copia de seguridad, siga las instrucciones de instalación para el sistema operativo.

- Instalación de los clientes de archivado y copia de seguridad de UNIX y Linux
- Instalación del cliente de archivado y copia de seguridad de Windows

## Configuración de opciones para el servidor

Revise el archivo de opciones de servidor que está instalado con el servidor IBM Spectrum Protect para verificar que se han establecido los valores correctos para el sistema.

### Procedimiento

1. Vaya al directorio de instancia de servidor y abra el archivo dsmserv.opt.
2. Revise los valores de la tabla siguiente y verifique los valores de opciones de servidor, en base al tamaño del sistema.

Opción de servidor	Valor
ACTIVELOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración
ACTIVELOGSIZE	131072
ARCHLOGCOMPRESS	No
ARCHLOGDIRECTORY	Vía de acceso de directorio especificada durante la configuración
COMMMETHOD	TCP/IP
COMMTIMEOUT	3600
DEVCONFIG	devconf.dat
EXPINTERVAL	0
IDLETIMEOUT	60
MAXSESSIONS	500
NUMOPENVOLSALLOWED	20
TCPADMINPORT	1500
TCPPORT	1500
VOLUMEHISTORY	volhist.dat

Actualice los valores de opción de servidor si es necesario, para que coincidan con los valores de la tabla. Para realizar actualizaciones, cierre el archivo dsmserv.opt y utilice el mandato SETOPT desde la interfaz de línea de mandatos de administración para establecer las opciones.

Por ejemplo, para actualizar la opción IDLETIMEOUT a 60, emita el siguiente mandato:

```
setopt idletimeout 60
```

3. Para configurar comunicaciones seguras para el servidor, clientes y Centro de operaciones, verifique las opciones de la tabla siguiente.

Opción de servidor	Todos los tamaños del sistema
SSLDISABLELEGACYTLS	YES
SSLFIPSMODE	NO
SSLTCPPOINT	Especifique el número de puerto SSL. La unidad de comunicación TCP/IP del servidor espera solicitudes en este puerto para sesiones con SSL activada del cliente.
SSLTCPADMINPORT	Especifique la dirección del puerto en la que el servidor esperará las solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.
SSLTLS12	YES

Si alguno de los valores de opción debe actualizarse, edite el archivo dsmserv.opt utilizando las siguientes directrices:

- Elimine el asterisco del principio de la línea para habilitar una opción.
- En cada línea, especifique solo una opción y el valor especificado para la opción.
- Si se produce una opción en varias entradas del archivo, el servidor utiliza la última entrada.

Guarde los cambios y cierre el archivo. Si edita el archivo dsmserv.opt directamente, tendrá que reiniciar el servidor para que se apliquen los cambios.

## Conceptos sobre la seguridad

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

### Seguridad de la capa de transporte

Puede utilizar el protocolo de Capa de sockets seguros (SSL) o de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 que utiliza cualquier servidor IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo que esté firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

### Niveles de autorización

Con cada servidor de IBM Spectrum Protect, hay diferentes niveles de autoridad administrativa disponibles que determinan las tareas que un administrador puede realizar.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos, eliminarlos y bloquearlos y desbloquearlos desde el servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. Un ID usuario no root no puede realizar copias de seguridad de los datos del nodo de forma predeterminada. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

## Contraseñas

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña al acceder al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días.  El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña durante este periodo, deberá cambiarla la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

## Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente de IBM Spectrum Protect, los clientes administrativos y los servidores, y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos de cliente	<ul style="list-style-type: none"> <li>• REGISTER NODE</li> <li>• UPDATE NODE</li> </ul>
Administradores	<ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul>
Servidores	<ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul>

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar con una versión anterior, una vez que se han autenticado con la V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:




- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en cada sistema.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplique el nivel de seguridad más elevado para la comunicación con el servidor IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores estén utilizando la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

- Configuración de comunicaciones seguras con Seguridad de la capa de transporte  
Para cifrar los datos y proteger las comunicaciones de su entorno, se habilita la capa de sockets seguros (SSL) o la seguridad de la capa de transporte (TLS) en el servidor IBM Spectrum Protect y el cliente del archivo de copia de seguridad. Se utiliza un certificado SSL para verificar las solicitudes de comunicación entre el servidor y el cliente.

#### Tareas relacionadas:

 Protección de las comunicaciones

## Configuración de Centro de operaciones

---

Después de instalar el Centro de operaciones, complete los siguientes pasos de configuración para iniciar la gestión del entorno de almacenamiento.

### Antes de empezar

---

Cuando se conecte a Centro de operaciones por primera vez, debe proporcionar la siguiente información:

- La información de conexión para el servidor que desea designar como servidor concentrador.
- Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor

### Procedimiento

---

1. Designe el servidor concentrador. En un navegador web, introduzca la siguiente dirección:

```
https://hostname:secure_port/oc
```

donde:

- *nombre\_host* representa el nombre del sistema donde está instalado Centro de operaciones
- *puerto\_seguro* representa el número de puerto que utiliza Centro de operaciones para una comunicación HTTPS en ese sistema

Por ejemplo, si el nombre de host es tsm.storage.mylocation.com y está utilizando el puerto seguro predeterminado para Centro de operaciones, que es 11090, la dirección es:

```
https://tsm.storage.mylocation.com:11090/oc
```

Al iniciar sesión en Centro de operaciones por primera vez, un asistente le guiará a través de la configuración inicial para establecer un nuevo administrador con la autoridad del sistema en el servidor.

2. Establezca comunicaciones seguras entre Centro de operaciones y el servidor concentrador configurando el protocolo de la capa de sockets seguros (SSL).

Siga las instrucciones que encontrará en Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

3. Opcional: Para recibir un informe de correo electrónico diario que resuma el estado del sistema, configure los valores de correo electrónico en Centro de operaciones.

Siga las instrucciones que encontrará en Seguimiento del estado del sistema mediante informes de correo electrónico.

- Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador

Para proteger las comunicaciones entre Centro de operaciones y el servidor concentrador, añada el certificado de seguridad de la capa de transporte (TLS) del servidor concentrador al archivo de almacén de confianza de Centro de operaciones.

## Registro de la licencia de producto

---

Para registrar la licencia para el producto IBM Spectrum Protect, utilice el mandato REGISTER LICENSE.

### Acerca de esta tarea


---

Las licencias se almacenan en archivos de certificados de inscripción, que contienen información de licencias para el producto. Los archivos de certificado de inscripción se encuentran en el soporte de instalación y se colocan en el servidor durante la instalación. Al registrar el producto, las licencias se almacenan en un archivo NODELOCK en el directorio actual.

### Procedimiento

---

Registre una licencia especificando el nombre del archivo de certificado de inscripción que contiene la licencia. Para utilizar el creador de mandato del Centro de operaciones para esta tarea, realice los pasos siguientes.


1. Abra el Centro de operaciones.
2. Abra el creador de mandatos del Centro de operaciones pasando el cursor por encima del icono de configuración  y pulsando Creador de mandatos.
3. Emita el mandato REGISTER LICENSE. Por ejemplo, para registrar una licencia de base de IBM Spectrum Protect, emita el siguiente mandato:

```
register license file=tsmbasic.lic
```

### Qué hacer a continuación

---

Guarde el soporte de instalación que contiene los archivos de certificados de inscripción. Es posible que tenga que registrar la licencia de nuevo si, por ejemplo, se produce una de las condiciones siguientes:

- El servidor se ha trasladado a otro sistema.
- El archivo NODELOCK está dañado. El servidor almacena información de licencia en el archivo NODELOCK, que está en el directorio desde el cual se ha iniciado el servidor.
-  Sistemas operativos Linux Si cambia el chip del procesador que está asociado al servidor en el cual está instalado el servidor.

## Definición de las reglas de retención de datos para su empresa

---

Después de crear una agrupación de almacenamiento de contenedores de directorio para deduplicación de datos, actualice la política de servidor predeterminada para utilizar la nueva agrupación de almacenamiento. El asistente Añadir agrupación de almacenamiento abre la página Servicios en el Centro de operaciones para completar esta tarea.

### Procedimiento

---

1. En la página Servicios del Centro de operaciones, seleccione el dominio STANDARD y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas. La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.
3. Pulse el conmutador Configurar y realice los cambios siguientes:
  - Cambie el destino de copia de seguridad para la clase de gestión STANDARD a la agrupación de almacenamiento de contenedores de directorio.
  - Cambie el valor de la columna de copias de seguridad a Sin límite.
  - Cambie el periodo de retención. Establezca la columna para conservar copias de seguridad adicionales en 30 días o más, en función de los requisitos empresariales.
4. Guarde los cambios y haga clic de nuevo en el conmutador Configurar para que el conjunto de políticas ya no se pueda editar.
5. Activar el conjunto de políticas pulsando Activar.

## Definición de planificaciones para actividades de mantenimiento del servidor

---

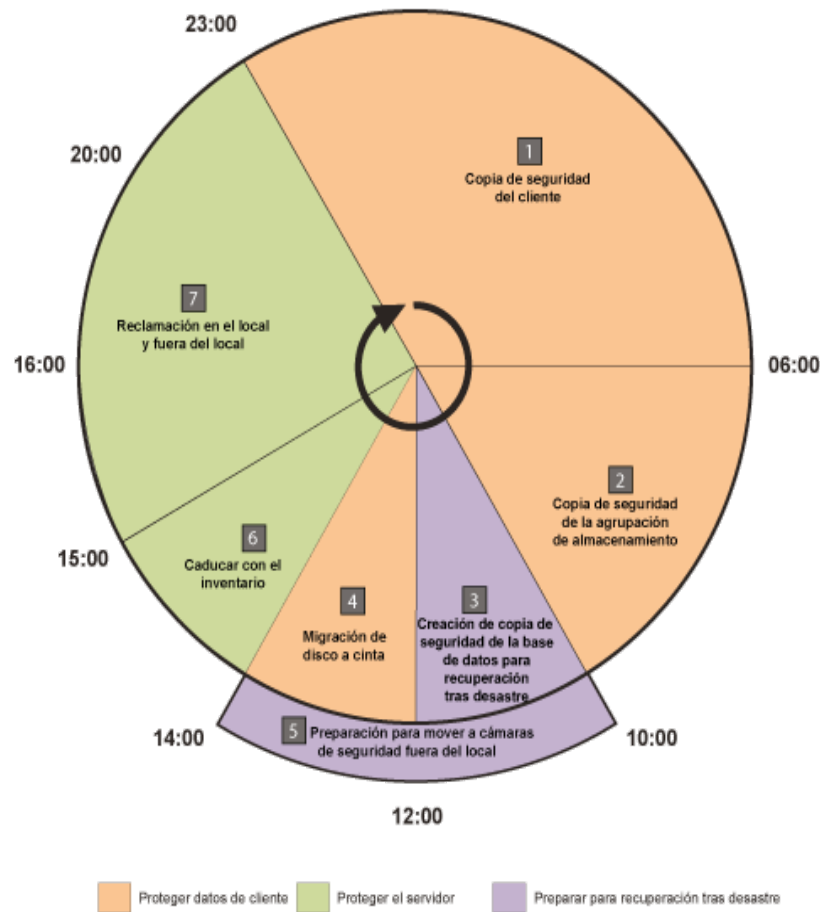
Cree planificaciones para cada operación de mantenimiento de servidor utilizando el mandato DEFINE SCHEDULE en el generador de mandatos de Centro de operaciones.

### Acerca de esta tarea

---

Planifique operaciones de mantenimiento de servidor para ejecutar después de operaciones de copia de seguridad de cliente. Puede controlar la temporización de planificaciones estableciendo la hora de inicio en combinación con la duración para cada operación.

La siguiente figura proporciona un ejemplo de cómo planificar operaciones de mantenimiento. Figura 1. Planificación diaria de operaciones de servidor para una solución de cinta



La tabla siguiente muestra cómo puede planificar procesos de mantenimiento de servidor en combinación con la planificación de copia de seguridad de cliente para una solución de cinta.

Operación	Planificación
Copia de seguridad del cliente	Se inicia a las 11 PM.
Copia de seguridad de agrupaciones de almacenamiento	Se inicia a las 6 AM.
Proceso para archivos de recuperación tras desastre y de base de datos	<ul style="list-style-type: none"> <li>La operación de copia de seguridad de base de datos se inicia a las 10 AM, u 11 después de iniciar la operación de copia de seguridad de cliente. Este proceso se ejecuta hasta completarse.</li> <li>La información de configuración de dispositivos y la copia de seguridad del historial de volumen comienza a las 5PM o 7 horas después del inicio de la copia de seguridad de la base de datos.</li> <li>La supresión del historial de volumen comienza a las 8 PM, o 10 horas después del inicio de la operación de copia de seguridad de la base de datos.</li> </ul>
Preparación de archivos para almacenamiento en cámaras de seguridad fuera del local	Se inicia a las 10 AM, a la misma hora que el procesamiento de los archivos de recuperación tras desastre y base de datos.

Operación	Planificación
Migración de disco a cinta	Se inicia a las 12 PM, o 2 horas después del inicio de la operación de copia de seguridad de la base de datos.
Caducidad de inventario	Se inicia a las 2 PM, o 15 horas después del comienzo de la operación de copia de seguridad del cliente. Este proceso se ejecuta hasta completarse.
Reclamación de espacio	Se inicia a las 3 PM, o 16 horas después del comienzo de la operación de copia de seguridad del cliente.

## Procedimiento

Tras configurar la clase de dispositivo para las operaciones de copia de seguridad de base de datos, cree planificaciones para la copia de seguridad de la base de datos y otras operaciones de mantenimiento necesarias utilizando el mandato DEFINE SCHEDULE. En función del tamaño del entorno, es posible que tenga que ajustar las horas de inicio para cada planificación del ejemplo.

1. Defina una clase de dispositivo para la operación de seguridad antes de crear la planificación para copias de seguridad de base de datos. Utilice el mandato DEFINE DEVCLASS para crear una clase de dispositivo que se denomine LTOTAPE:

```
define devclass ltotape devtype=lto library=ltolib
```

2. Establezca la clase de dispositivo para copias de seguridad de base de datos automáticas. Utilice el mandato SET DBRECOVERY para especificar la clase de dispositivo que ha creado para la copia de seguridad de base de datos en el paso anterior. Por ejemplo, si la clase de dispositivo es LTOTAPE, emita el mandato siguiente:

```
set dbrecovery ltotape
```

3. Cree planificaciones para las operaciones de mantenimiento utilizando el mandato DEFINE SCHEDULE. Consulte la tabla siguiente para las operaciones necesarias con ejemplos de los mandatos.

Operación	Mandatos de ejemplo e información adicional
Realice la copia de seguridad de las agrupaciones de almacenamiento.	<p>Cree una planificación para ejecutar el mandato BACKUP STGPOOL. Por ejemplo, emita el siguiente mandato para crear una planificación de copia de seguridad para una agrupación de almacenamiento primario denominada PRIMARY_POOL. La copia de seguridad de la agrupación se realizará en una agrupación de almacenamiento de copias, COPYSTG:</p> <pre>define schedule BACKUPSTGPOOL type=administrative cmd="backup stgpool primary_pool copystg" active=yes starttime=06:00 period=1</pre>
Realizar una copia de seguridad de la base de datos.	<p>Cree una planificación para ejecutar el mandato BACKUP DB. Por ejemplo, emita el mandato siguiente para crear una planificación de copia de seguridad que utiliza la nueva clase de dispositivo:</p> <pre>define schedule DBBACKUP type=admin cmd="backup db devclass=ltotape type=full numstreams=3 wait=yes compress=yes" active=yes desc="Back up the database." startdate=today starttime=10:00:00 duration=45 durunits=minutes</pre>
Replique los nodos.	<p>Opcionalmente, utilice la réplica de nodo para proteger los datos del cliente realizando una copia de seguridad de los datos a un servidor secundario. Para obtener instrucciones, consulte Réplica de datos de cliente en otro servidor. Asegúrese de completar la réplica de nodo antes de iniciar las operaciones de migración.</p>

Operación	Mandatos de ejemplo e información adicional
<p>Migre los datos de disco a cinta a diario.</p>	<p>Cree una planificación para la migración de agrupación de almacenamiento.</p> <p>Por ejemplo, si una agrupación de almacenamiento de disco se denomina DISKPOOL y la siguiente agrupación de almacenamiento es TAPEPOOL, puede planificar la migración de agrupación de almacenamiento emitiendo el siguiente mandato:</p> <pre>define schedule stgpool_migration type=administrative cmd="migrate stgpool diskpool lomig=0" active=yes description="migrate disk storagepool to tapepool" startdate=today starttime=12:00 duration=2 durunits=hours period=1 perunits=days</pre> <p>Para maximizar el rendimiento, puede especificar el número de procesos paralelos que se utilizarán para migrar archivos llevando a cabo los pasos siguientes:</p> <ol style="list-style-type: none"> <li>Para la agrupación de almacenamiento de cinta, asegúrese de que la función de proximidad esté habilitada. Para verificar que la función de proximidad esté habilitada, ejecute el mandato QUERY STGPOOL. Compruebe que se especifica un valor de GROUP, NODE o FILESPACE en el campo COLLOCATE. Si no se especifica un valor de GROUP, NODE o FILESPACE, utilice el mandato UPDATE STGPOOL para especificar COLLOCATE=GROUP, COLLOCATE=NODE o COLLOCATE=FILESPACE, en función de la configuración del sistema.</li> <li>Para la agrupación de almacenamiento de disco, utilice el mandato DEFINE STGPOOL o UPDATE STGPOOL para especificar un valor para el parámetro MIGPROCESS. Por ejemplo, si tiene 12 unidades de cinta, especifique MIGPROCESS=10. De este modo, se utilizan un máximo de 10 unidades de cinta para los procesos de migración. Dos unidades están reservadas para otras tareas, como restauración, copia de seguridad de base de datos y operaciones de copia de seguridad de cliente.</li> </ol>
<p>Prepare archivos para almacenamiento en cámaras de seguridad fuera del local.</p>	<ol style="list-style-type: none"> <li>Mueva los volúmenes de cinta fuera del local siguiendo las instrucciones de Mover soportes de copia de seguridad.</li> <li>Cree el archivo del plan de recuperación tras desastre emitiendo el mandato PREPARE en el servidor de origen: <pre>preparar</pre> </li> <li>Asegúrese de que todos los volúmenes que son necesarios para la recuperación tras desastre se incluyan en el archivo del plan de recuperación. Para obtener más información, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.</li> </ol>
<p>Realice una copia de seguridad de la información de configuración del dispositivo.</p>	<p>Cree una planificación para ejecutar el mandato BACKUP DEVCONFIG:</p> <pre>define schedule DEVCONFIGBKUP type=admin cmd="backup devconfig   filenames=devconfig.dat" active=yes desc="Backup the device   configuration file." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>
<p>Haga una copia de seguridad del historial de volumen.</p>	<p>Cree una planificación para ejecutar el mandato BACKUP VOLHISTORY:</p> <pre>define schedule VOLHISTBKUP type=admin cmd="backup volhistory   filenames=volhist.dat" active=yes desc="Back up the volume   history." startdate=today starttime=17:00:00 duration=45 durunits=minutes</pre>

Operación	Mandatos de ejemplo e información adicional
Elimine versiones más antiguas de copias de seguridad de base de datos que ya no son necesarias.	<p>Cree una planificación para ejecutar el mandato DELETE VOLHISTORY:</p> <pre>define schedule DELVOLHIST type=admin cmd="delete volhistory   type=dbb todate=today-6 totime=now" active=yes desc="Remove   old database backups." startdate=today starttime=20:00:00 duration=45 durunits=minutes</pre>
Elimine objetos que exceden su retención permitida.	<p>Cree una planificación para ejecutar el mandato EXPIRE INVENTORY.</p> <p>Defina el parámetro RESOURCE en función del tamaño del sistema que va a configurar.</p> <p>Por ejemplo, emita el siguiente mandato para crear una planificación que se denomine EXPINVENTORY:</p> <pre>define schedule EXPINVENTORY type=admin cmd="expire inventory   wait=yes resource=8 duration=120" active=yes desc="Remove expired   objects." startdate=today starttime=14:00:00 duration=1 durunits=hours</pre>
Reclame espacio.	<p>Cree una planificación para ejecutar el mandato RECLAIM STGPOOL.</p> <p>Por ejemplo, emita el siguiente mandato para crear una planificación que se denomine RECLAIM:</p> <pre>define schedule RECLAIM type=admin cmd="reclaim stgpool tapepool duration=60" startdate=today starttime=15:00:00 duration=5 durunits=hours</pre> <p>Consejo: Para maximizar el rendimiento, puede especificar el número de procesos paralelos que se utilizarán para reclamar espacio. Actualice la agrupación de almacenamiento en cinta utilizando el mandato UPDATE STGPOOL y especifique un valor para el parámetro RECLAIMPROCESS. Por ejemplo, si tiene 12 unidades de cinta, especifique RECLAIMPROCESS=5. Puesto que se utilizan dos unidades para cada proceso de reclamación, el número total de unidades que se pueden utilizar para la reclamación es 10. Dos unidades se reservan para las operaciones de copia de seguridad.</p>

## Qué hacer a continuación

Después de crear planificaciones para las tareas de mantenimiento de servidor, puede verlas en el Centro de operaciones completando los pasos siguientes:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Servidores.
2. Pulse Mantenimiento.

- Mover soportes de copia de seguridad

Para recuperarse de un desastre, necesita volúmenes de copia de seguridad de base de datos, volúmenes de agrupación de almacenamiento de copias y archivos adicionales. Para estar preparado ante un desastre, debe completar tareas diarias.

### Referencia relacionada:

- [UPDATE STGPOOL \(Actualizar una agrupación de almacenamiento\)](#)
- [DEFINE SCHEDULE \(Definir una planificación para un mandato de administración\)](#)
- [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)

## Definición de planificaciones de cliente

Utilice el Centro de operaciones para crear planificaciones para operaciones de cliente.

### Procedimiento

1. En la barra de menús del Centro de operaciones, pase el cursor por encima de Clientes.

2. Pulse Planificaciones.
3. Pulse +Planificación.
4. Complete los pasos en el asistente Crear planificación. Establezca que las planificaciones de copia de seguridad de cliente se inicien a las 22:00, basándose en las actividades de mantenimiento del servidor que ha planificado en Definición de planificaciones para actividades de mantenimiento del servidor.

## Conexión de dispositivos de cinta para el servidor

---

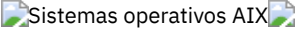
Para que el servidor pueda utilizar un dispositivo de cinta, debe conectar el dispositivo al sistema servidor e instalar el controlador de dispositivo de cinta adecuado

### Acerca de esta tarea

---

Para optimizar el rendimiento del sistema, utilice dispositivos de cinta rápidos y de gran capacidad. Suministre suficientes unidades de cinta para cumplir los requisitos empresariales.

Conecte los dispositivos de cinta a su propio adaptador de bus de host (HBA), no compartidos con otros tipos de dispositivos tales como discos.. Las unidades de cinta de IBM® tienen ciertos requisitos especiales en cuanto a los HBA y los controladores asociados.

-  Sistemas operativos AIX/Sistemas operativos Linux Conectar un dispositivo de biblioteca automática a su dispositivo  
Puede conectar un dispositivo de biblioteca automatizada a su sistema para almacenar datos en cinta.
- Seleccionar un controlador de dispositivo de cinta  
Para utilizar dispositivos de cinta con IBM Spectrum Protect debe instalar el controlador de dispositivo de cinta adecuado.
-  Sistemas operativos AIX/Sistemas operativos Linux Nombres de archivo especiales para dispositivos de cinta  
Se requiere un nombre de archivo especial para que el servidor de IBM Spectrum Protect pueda operar con dispositivos de cinta, de cambiador de medios o de medios extraíbles.
- Instalación y configuración de controladores de dispositivos de cinta  
Para poder utilizar dispositivos de cinta con IBM Spectrum Protect, debe instalar el controlador de dispositivo de cinta correcto.

## Conectar un dispositivo de biblioteca automática a su dispositivo

---

Puede conectar un dispositivo de biblioteca automatizada a su sistema para almacenar datos en cinta.

### Acerca de esta tarea

---

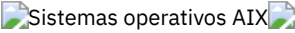
Antes de adjuntar un dispositivo de biblioteca automatizada, tenga en cuenta las siguientes restricciones:

- Los dispositivos conectados deben estar en su propio adaptador de bus de host (HBA).
- Un HBA no se puede compartir con otros tipos de dispositivo como por ejemplo un disco..
- En el caso de HBA de canal de fibra multipuerto, los dispositivos deben estar conectados en su puerto propio. Estos puertos no se pueden compartir con otros tipos de dispositivo.
- Las unidades de cinta de IBM® tienen ciertos requisitos especiales en cuanto a HBA y los controladores asociados. Para obtener más información acerca de los dispositivos, consulte el sitio web sobre su sistema operativo :
  - Dispositivos soportados de IBM Spectrum Protect para AIX
  - Dispositivos soportados de IBM Spectrum Protect para Linux y Windows

### Procedimiento

---

Para utilizar el adaptador de canal de fibra (FC), siga estos pasos:

1. Instale el adaptador FC y los controladores asociados.
  2. Instale los controladores de dispositivo pertinentes para los dispositivos del cambiador de medios.
-  Sistemas operativos AIX/Sistemas operativos Linux Configuración de la modalidad de biblioteca  
Para que el servidor de IBM Spectrum Protect acceda a una biblioteca SCSI, el dispositivo de cinta debe estar en la modalidad adecuada.

#### Conceptos relacionados:

Seleccionar un controlador de dispositivo de cinta

## Seleccionar un controlador de dispositivo de cinta

---

Para utilizar dispositivos de cinta con IBM Spectrum Protect debe instalar el controlador de dispositivo de cinta adecuado.

- Controladores de dispositivos de cinta de IBM  
Hay controladores de dispositivos de cinta IBM® disponibles para la mayoría de dispositivos de cinta etiquetados de IBM.
- Controladores de dispositivos de cinta de IBM Spectrum Protect  
El servidor de IBM Spectrum Protect proporciona controladores de dispositivos de cinta.

**Referencia relacionada:**

Instalación y configuración de controladores de dispositivos de cinta

## Controladores de dispositivos de cinta de IBM

---


Hay controladores de dispositivos de cinta IBM® disponibles para la mayoría de dispositivos de cinta etiquetados de IBM.

Puede descargar controladores de dispositivos de cinta de IBM en el sitio web de Fix Central:

1. Vaya al sitio web de Fix Central: Sitio web de Fix Central.
2. Pulse en Seleccionar producto.
3. Seleccione Sistemas de almacenamiento en el menú Grupo de productos.
4. Seleccione Sistemas de cintas en el menú Almacenamiento del sistema.
5. Seleccione Controladores y software para dispositivos de cinta en el menú Sistemas de cintas.
6. Seleccione Controladores de dispositivo de cinta en el menú Controladores y software para cintas. Además de las unidades de cinta, también tiene acceso a herramientas tales como la IBM Tape Diagnostic Tool (ITDT).
7. Seleccione el sistema operativo en el menú Plataforma.

 Sistemas operativos AIX  Sistemas operativos Windows

Para obtener la lista más actualizada de dispositivos y niveles de sistema operativo soportados por los controladores de dispositivos de cinta de IBM, consulte el sitio web Dispositivos soportados por IBM Spectrum Protect en Dispositivos soportados para AIX y Windows.

 Sistemas operativos Linux

Para obtener la lista más actualizada de dispositivos de cinta y niveles de sistema operativo soportados por los controladores de dispositivos de cinta de IBM, consulte el sitio web Dispositivos soportados por IBM Spectrum Protect en Dispositivos soportados para Linux.

Los controladores de dispositivos de cinta de IBM solo admiten algunos niveles de kernel de Linux. Para obtener información sobre los niveles de kernel soportados, consulte Sitio web de Fix Central.

## Controladores de dispositivos de cinta de IBM Spectrum Protect

---

El servidor de IBM Spectrum Protect proporciona controladores de dispositivos de cinta.

Un controlador de dispositivo de cinta de IBM Spectrum Protect se instala junto con el servidor

 Sistemas operativos AIX

Puede utilizar el controlador de dispositivos de cinta SCSI genérico que proporciona el sistema operativo IBM® AIX para trabajar con dispositivos de cinta que no estén soportados por el controlador de dispositivos IBM Spectrum Protect. Si se utiliza controlador de dispositivo de cinta SCSI genérico de AIX, la clase de dispositivo GENERICTAPE se debe establecer en el tipo de dispositivo que se haya especificado en el mandato DEFINE DEVCLASS.

Para los siguientes dispositivos de cinta, puede elegir si desea instalar el controlador de dispositivo de cinta de IBM Spectrum Protect o el controlador de dispositivo nativo de su sistema operativo:

- ECART
- LTO (no de IBM)

Todas las bibliotecas conectadas a SCSI que contienen unidades de cinta de la lista deben utilizar el controlador del conmutador de IBM Spectrum Protect.

Los controladores de dispositivo de cinta adquiridos de otros proveedores de hardware se pueden utilizar si se asocian a la clase de dispositivo GENERICTAPE. Los controladores de dispositivo genéricos no están admitidos en las clases de dispositivo WORM (write-one read-many).

 Sistemas operativos Linux

Puede utilizar el controlador de dispositivo Passthru IBM Spectrum Protect. Los controladores de dispositivo passthru IBM Spectrum Protect requieren que el controlador de dispositivo de Linux genérico de SCSI (sg) junto con el sistema operativo Linux instalen los




kernels.

Por ejemplo, puede instalar el controlador de dispositivo Passthru IBM Spectrum Protect para los siguientes dispositivos de cinta:

- ECART
- LTO (no de IBM)


Todas las bibliotecas conectadas a SCSI que contengan unidades de cinta que no estén etiquetadas por IBM en la lista también deben utilizar el controlador de dispositivos Passthru de IBM Spectrum Protect.

No puede utilizar el controlador de dispositivo (st) de cinta SCSI genérico que proporciona el sistema operativo Linux. Así pues, el tipo de dispositivo GENERICTAPE no está soportado para el mandato DEFINE DEVCLASS.

 Sistemas operativos Windows Puede seleccionar un controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab en lugar del controlador de dispositivo de IBM Spectrum Protect. El controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab solo se puede utilizar para dispositivos que tengan una etiqueta que no sea IBM y para unidades de cinta que no sean IBM. Para el controlador de dispositivo nativo certificado de Windows Hardware Qualification Lab, puede seleccionar el controlador de dispositivo passthru de SCSI IBM Spectrum Protect o el controlador de dispositivo de cinta nativo de Windows. Si se utiliza el controlador de dispositivo passthru SCSI, la clase de dispositivo definida en el mandato DEFINE DEVCLASS no puede ser GENERICTAPE. Si se utiliza el controlador de dispositivo nativo, la clase de dispositivo debe ser GENERICTAPE.

## Nombres de archivo especiales para dispositivos de cinta


Se requiere un nombre de archivo especial para que el servidor de IBM Spectrum Protect pueda operar con dispositivos de cinta, de cambiador de medios o de medios extraíbles.

 Sistemas operativos AIX

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 1 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a la unidad o biblioteca. Puede utilizar el mandato de sistema operativo SMIT para obtener el nombre de archivo especial de dispositivo. En los ejemplos, *x* especifica un entero, 0 o mayor.

Tabla 1. Ejemplos de dispositivo


Dispositivo	Ejemplo de dispositivo	Nombre de archivo lógico
Unidades de cinta que puede utilizar el controlador de dispositivo de IBM Spectrum Protect	/dev/mtx	mtx
Unidades de cinta que puede utilizar el controlador de dispositivo de cinta de IBM	/dev/rmtx	rmtx
Unidades de cinta que puede utilizar el controlador de dispositivo de cinta genérico de IBM AIX	/dev/rmtx	rmtx
Dispositivos de biblioteca que puede utilizar el controlador de dispositivo de IBM Spectrum Protect	/dev/lbx	lbx
Dispositivos de biblioteca que puede utilizar el controlador de dispositivo de cinta de IBM	/dev/smcx	smcx

 Sistemas operativos Linux

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 2 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a una unidad o biblioteca. En los ejemplos, *x* especifica un entero, 0 o mayor.

Tabla 2. Ejemplos de dispositivo

Dispositivo	Ejemplo de dispositivo	Nombre de archivo lógico
Unidades de cinta que puede utilizar el controlador de dispositivo passthru de IBM Spectrum Protect	/dev/tmscsi/mtx	mtx
Unidades de cinta que puede utilizar el controlador de dispositivo lin_tape de IBM	/dev/IBMtapex	IBMtapex
Dispositivos de biblioteca que puede utilizar el controlador de dispositivo passthru de IBM Spectrum Protect	/dev/tmscsi/lbx	lbx
Dispositivos de biblioteca que puede utilizar el controlador de dispositivo lin_tape de IBM	/dev/IBMchangerx	IBMchangerx

 Sistemas operativos Windows

Cuando se configura un dispositivo correctamente, se devuelve un nombre de archivo lógico. Tabla 3 especifica el nombre del dispositivo, también llamado nombre de archivo especial, que corresponde a una unidad o biblioteca. En los ejemplos, *a*, *b*, *c*, *d* y *x*

especifican un entero, 0 o mayor, donde:

- *a* especifica el ID de destino.
- *b* especifica el LUN.
- *c* especifica el ID de bus SCSI.
- *d* especifica el ID de puerto.




Tabla 3. Ejemplos de dispositivo

Dispositivo	Ejemplo de dispositivo	Nombre dispositivo convertido
Unidades de cinta admitidas por el controlador de dispositivo de IBM Spectrum Protect	<i>mta.b.c.d</i>	<i>mta.b.c.d</i>
Unidades de cinta admitidas por el controlador de dispositivo passthru de IBM Spectrum Protect	<i>mta.b.c.d</i>	<i>mta.b.c.d</i>
Unidades de cinta admitidas por el controlador de dispositivo de IBM	Tapex	<i>mta.b.c.d</i>
Dispositivos de biblioteca admitidos por el controlador de dispositivo de IBM Spectrum Protect	<i>lb.a.b.c.d</i>	<i>lba.b.c.d</i>
Dispositivos de biblioteca admitidos por el controlador de dispositivo passthru de IBM Spectrum Protect	<i>lba.b.c.d</i>	<i>lba.b.c.d</i>
Dispositivos de biblioteca admitidos por el controlador de dispositivo de IBM	Changerx	<i>lba.b.c.d</i>

## Instalación y configuración de controladores de dispositivos de cinta

Para poder utilizar dispositivos de cinta con IBM Spectrum Protect, debe instalar el controlador de dispositivo de cinta correcto.

IBM Spectrum Protect admite todos los dispositivos que están soportados por los controladores de dispositivos de cinta de IBM®. No obstante, IBM Spectrum Protect no admite todos los niveles de sistema operativo que admiten los controladores de dispositivos de cinta de IBM.


- Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM  
Instale y configure un controlador de dispositivo de cinta de IBM para utilizar un dispositivo de cinta de IBM SCSI
-  Sistemas operativos AIX Configuración de controladores de dispositivos de cinta en sistemas AIX  
Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta no IBM en sistemas AIX.
-  Sistemas operativos Linux Configuración de controladores de dispositivos de cinta en sistemas Linux  
Consulte los temas siguientes al instalar y configurar los controladores de dispositivos de cinta en sistemas Linux.
-  Sistemas operativos Windows Configuración de controladores de dispositivos de cinta en sistemas Windows  
Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta y bibliotecas en sistemas Windows.

## Instalación y configuración de controladores de dispositivos de IBM para dispositivos de cinta de IBM

Instale y configure un controlador de dispositivo de cinta de IBM® para utilizar un dispositivo de cinta de IBM SCSI

### Acerca de esta tarea

Para obtener instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*.

 Sistemas operativos AIX Después de completar el procedimiento de instalación en la publicación *IBM Tape Device Drivers Installation and User's Guide*, se emiten mensajes diferentes, dependiendo del controlador de dispositivo que desee instalar. Si está instalando el controlador de dispositivo para una unidad de cinta o de biblioteca de IBM se devolverán los mensajes siguientes:

```
rmtx disponible
```

```
o
```

```
smcx disponible
```


Tome nota del valor de *x*, que asigna el controlador de dispositivo de cinta de IBM. Para determinar el nombre de archivo especial del dispositivo, emita uno de los siguientes mandatos:

- Para unidades de cinta, `ls -l /dev/rmt*`

- Para bibliotecas de cintas, `ls -l /dev/smc*`

Es posible que el nombre de archivo tenga más caracteres al final para indicar características operativas diferentes, pero IBM Spectrum Protect no necesita estos caracteres. Para los controladores de dispositivo de IBM utilice el nombre del archivo base en el parámetro DEVICE del mandato DEFINE PATH para asignar un dispositivo a una unidad (/dev/rmtx) o a una biblioteca (/dev/smcx). Después de instalar el controlador de dispositivo, puede utilizar la herramienta System Management Interface Tool (SMIT) para configurar unidades de cinta y bibliotecas de cintas no IBM. Realice los pasos siguientes:

1. Ejecute el programa SMIT.
2. Pulse en Dispositivos.
3. Pulse Dispositivos de IBM Spectrum Protect.
4. Pulse Dispositivos conectados a la SAN de canal de fibra.
5. Pulse Descubrir dispositivos soportados por IBM Spectrum Protect. Espere a que se complete el proceso de descubrimiento.
6. Vuelva al menú de Dispositivos conectados a la SAN de canal de fibra y pulse Listar atributos de un dispositivo detectado.

 **Sistemas operativos Linux** Después de completar el procedimiento de instalación en la publicación *IBM Tape Device Drivers Installation and User's Guide*, se emiten mensajes diferentes, dependiendo del controlador de dispositivo que desee instalar. Si está instalando el controlador de dispositivo para un dispositivo IBM LTO o 3592, se devuelven los siguientes mensajes:

```
IBMtapex disponible
```


```
o
```

```
IBMChangerx disponible
```

Tome nota del valor de x, que asigna el controlador de dispositivo de cinta de IBM. Para determinar el nombre de archivo especial del dispositivo, emita uno de los siguientes mandatos:

- Para unidades de cinta, `ls -l /dev/IBMtape*`
- Para bibliotecas de cintas, `ls -l /dev/IBMChange*`

Es posible que el nombre de archivo tenga más caracteres al final para indicar características operativas diferentes, pero IBM Spectrum Protect no necesita estos caracteres. Para controladores de dispositivo IBM, utilice el nombre de archivo base en el parámetro DEVICE del mandato DEFINE PATH para asignar un dispositivo a una unidad (/dev/IBMtapex) o a una biblioteca (/dev/IBMChangerx). Restricción: El tipo de dispositivo de esta clase no debe ser GENERICTAPE.

 **Sistemas operativos Windows** Para sistemas operativos Windows, IBM Spectrum Protect proporciona dos controladores de dispositivo.

#### Controlador de dispositivo Passthru

Si el fabricante del dispositivo de cinta proporciona un controlador de dispositivo SCSI, instale el controlador de dispositivo passthru IBM Spectrum Protect passthru



#### Controlador de dispositivo SCSI para dispositivos de cinta

Si el fabricante del dispositivo de cinta no proporciona un controlador de dispositivo SCSI, instale el controlador de dispositivo SCSI IBM Spectrum Protect para dispositivos de cinta. El nombre del archivo de controlador es tsmcsi64.sys.

Para instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*. Después de instalar el controlador de dispositivo de cinta de IBM, el servidor especifica un nombre de archivo especial, TapeX, para las unidades de cinta de IBM, o ChangerY, para los conmutadores de soporte de IBM. Para un controlador de dispositivo SCSI IBM Spectrum Protect o un controlador de dispositivo passthru IBM Spectrum Protect, puede emitir un mandato del sistema operativo Windows, regedit, para verificar el nombre de archivo del archivo especial y el controlador. El servidor IBM Spectrum Protect también proporciona un programa de utilidad para comprobar el dispositivo en el sistema operativo Windows. El programa de utilidad, tsmdlst, se incluye en el paquete de servidor. Para utilizar el programa de utilidad, complete los siguientes pasos:


1. Asegúrese de que la interfaz de programación de aplicaciones (API) del adaptador de bus de host esté instalado
2. Para obtener información de dispositivo del sistema host, escriba:

```
tsmdlst
```

-  **Sistemas operativos AIX**  **Sistemas operativos Linux** Acceso de entrada/salida con dispositivos de cinta IBM La entrada/salida multivía de acceso es una técnica que utiliza distintas vías de acceso para acceder al mismo dispositivo físico, por ejemplo mediante varios adaptadores de bus de host (HBA) o conmutadores. El uso de la técnica multivía de acceso ayuda a asegurarse de que no se produzca un único punto de anomalía.

#### Conceptos relacionados:

Acceso de entrada/salida con dispositivos de cinta IBM

 **Sistemas operativos AIX**





## Configuración de controladores de dispositivos de cinta en sistemas AIX


Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta no IBM® en sistemas AIX.

## Acerca de esta tarea

---

Para obtener instrucciones sobre cómo instalar y configurar controladores de dispositivo de cinta de IBM, consulte *IBM Tape Device Drivers Installation and User's Guide*.

-  **Sistemas operativos AIX** Dispositivos SCSI y de canal de fibra  
Las solicitudes y los menús de definición de dispositivos de IBM Spectrum Protect en SMIT permiten gestionar los dispositivos SCSI y FC (canal de fibra) conectados.
-  **Sistemas operativos AIX** Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores  
Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autocambiadores de bibliotecas que no son IBM.
-  **Sistemas operativos AIX** Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta  
Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autoconmutadores de bibliotecas adquiridas al proveedor.
-  **Sistemas operativos AIX** Configuración de dispositivos conectados a SAN de canal de fibra  
Para configurar un dispositivo conectado a SAN de canal de fibra, complete este procedimiento.

 **Sistemas operativos AIX**

## Dispositivos SCSI y de canal de fibra

---

Las solicitudes y los menús de definición de dispositivos de IBM Spectrum Protect en SMIT permiten gestionar los dispositivos SCSI y FC (canal de fibra) conectados.

El menú principal de IBM Spectrum Protect tiene dos opciones:

### Dispositivos SCSI conectados

Utilice esta opción para configurar dispositivos SCSI que estén conectados a un adaptador SCSI en el host.

### Dispositivos conectados de red de área de almacenamiento (SAN) de canal de fibra

Utilice esta opción para configurar dispositivos que estén conectados a un adaptador FC en el host. Seleccione uno de los siguientes atributos:

#### Lista atributos de un dispositivo descubierto

Lista atributos de un dispositivo conocido en la base de datos ODM actual.

- ID de puerto FC:

Es el ID de puerto FC de 24 bits ID(N(L)\_Puerto o F(L)\_Puerto). Es el identificador de dirección exclusivo en la topología asociada a la que está conectado el dispositivo. En los entornos de conmutador o de tejido, generalmente viene determinado por el conmutador, con los 2 bytes superiores que no sean cero. En un bucle arbitrado privado, es la dirección física del bucle arbitrado (AL\_PA), en la que los 2 bytes superiores tienen el valor cero. Póngase en contacto con los proveedores de FC para saber cómo se asigna una dirección AL\_PA o un ID de puerto.

- ID de LUN correlacionado:

Un sistema de puente de FC a SCSI (denominado también convertidor, direccionador o pasarela). Póngase en contacto con los proveedores de puentes para saber cómo deben correlacionarse los LUN. Es recomendable no cambiar los ID de los LUN correlacionados.

- Nombre WWN:

Nombre de ámbito mundial (WWN) del puerto al que está conectado el dispositivo. Es el identificador exclusivo de 64 bits que asignan los proveedores de componentes FC, tales como puentes o dispositivos FC nativos. Póngase en contacto con los proveedores de FC para saber cuál es el valor de WWN de un puerto.

- ID de producto:

ID de producto del dispositivo. Póngase en contacto con los proveedores de los dispositivos para determinar el ID de producto.

### Detectar dispositivos soportados por IBM Spectrum Protect

Mediante esta opción se descubren los dispositivos de una red SAN FC admitidos por IBM Spectrum Protect y dichos dispositivos pasan a estar disponibles. Si agrega o elimina un dispositivo de un entorno SAN existente, deberá detectar de nuevo los dispositivos mediante esta opción. En primer lugar deben detectarse los dispositivos, de modo que los valores actuales de los atributos de los dispositivos aparezcan en la opción Listar atributos de un dispositivo detectado. Los dispositivos admitidos en


redes SAN FC son unidades de cinta, autocambiadores. El controlador de dispositivo de IBM Spectrum Protect pasa por alto todos los tipos de dispositivo, como por ejemplo, un disco.

Eliminar todos los dispositivos definidos

Mediante esta opción se eliminan todos los dispositivos de IBM Spectrum Protect conectados a la red SAN FC cuyo estado está establecido en `DEFINED` en la base de datos de ODM. En caso necesario, detecte de nuevo los dispositivos mediante la opción `Detectar dispositivos soportados por IBM Spectrum Protect` una vez que haya eliminado todos los dispositivos definidos.

Eliminar un dispositivo

esta opción elimina un único dispositivo de IBM Spectrum Protect conectado a la red SAN FC cuyo estado es `DEFINED` en la base de datos ODM. En caso necesario, detecte de nuevo el dispositivo mediante la opción `Detectar dispositivos soportados por IBM Spectrum Protect` una vez que haya eliminado un dispositivo definido.

 Sistemas operativos AIX

## Configuración de controladores de dispositivo de IBM Spectrum Protect para los autocambiadores

---

Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autocambiadores de bibliotecas que no son IBM.

### Procedimiento


---

Ejecute el programa SMIT para configurar el controlador de dispositivo para cada autocambiador o robot:

1. Seleccione Dispositivos.
2. Seleccione IBM Spectrum ProtectDispositivos.
3. Seleccione Biblioteca/Cambiador de medios.
4. Seleccione Agregar una biblioteca/Cambiador de medios.
5. Seleccione IBM Spectrum Protect-SCSI-LB para cualquier biblioteca admitida por IBM Spectrum Protect.
6. Seleccione el adaptador padre en el que va a conectar el dispositivo. Este número figura con el formato: 00-0X, siendo X la ubicación del número de ranura de la tarjeta adaptadora SCSI.
7. Cuando se le solicite, entre la dirección de conexión (`CONNECTION`) del dispositivo que está instalando. La dirección de conexión es un número de dos dígitos. El primero de ellos es el ID SCSI (el valor que ha anotado en la hoja de trabajo). El segundo es el número de unidad lógica (LUN) SCSI del dispositivo, que suele ser cero a menos que se indique lo contrario. El ID SCSI y el LUN deben estar separados por una coma (,). Por ejemplo, una dirección de conexión de 4, 0 tiene un SCSI ID=4 y un LUN=0.
8. Pulse DO.

Recibirá un mensaje (nombre de archivo lógico) con el formato `lbX disponible`. Tome nota del valor de X, que es un número que asigna el sistema de forma automática. Utilice esta información para completar el campo Nombre de dispositivo en la hoja de trabajo.

Por ejemplo, si el mensaje es `lb0 Available`, el campo Nombre de dispositivo es `/dev/lb0` en la hoja de trabajo. Utilice siempre el prefijo `/dev/` con el nombre proporcionado por SMIT.

 Sistemas operativos AIX

## Configuración de controladores de dispositivo de IBM Spectrum Protect para unidades de cinta

---

Utilice el siguiente procedimiento para configurar controladores de dispositivo de IBM Spectrum Protect para autoconmutadores de bibliotecas adquiridas al proveedor.

### Procedimiento

---

Importante: IBM Spectrum Protect no puede sobrescribir cintas `tar` ni `dd`, pero las cintas `tar` o `dd` pueden sobrescribir cintas de IBM Spectrum Protect.


Restricción: las unidades de cinta sólo pueden compartirse cuando no se ha definido la unidad o cuando no se ha iniciado el servidor. El mandato `MKSYSB` no funciona cuando IBM Spectrum Protect y AIX comparten las mismas unidades. Para utilizar el controlador de dispositivo de cintas nativo del sistema operativo junto con una unidad SCSI, el dispositivo debe configurarse primero para AIX y, a continuación, para IBM Spectrum Protect. Consulte la documentación de AIX relacionada con estos controladores de dispositivo nativos.

Ejecute el programa SMIT para configurar el controlador de dispositivo para cada una de las unidades (incluidas las de la biblioteca) de la forma siguiente:

1. Seleccione Dispositivos.
2. Seleccione IBM Spectrum ProtectDispositivos.
3. Seleccione Unidad de cinta.
4. Seleccione Añadir una unidad de cinta.
5. Seleccione IBM Spectrum Protect-SCSI-MT para cualquier unidad de cinta soportada.
6. Seleccione el adaptador al que va a conectar el dispositivo. Este número figura con el formato: 00-0X, siendo X la ubicación del número de ranura de la tarjeta adaptadora SCSI.
7. Cuando se le solicite, entre la dirección de conexión (CONNECTION) del dispositivo que está instalando. La dirección de conexión es un número de dos dígitos. El primero de ellos es el ID SCSI (el valor que ha anotado en la hoja de trabajo). El segundo es el número de unidad lógica (LUN) SCSI del dispositivo, que suele ser cero a menos que se indique lo contrario. El ID SCSI y el LUN deben estar separados por una coma (,). Por ejemplo, una dirección de conexión de 4, 0 tiene un SCSI ID=4 y un LUN=0.
8. Pulse DO. Recibirá un mensaje:

Si está configurando el controlador de dispositivo para un dispositivo de cinta (que no sea IBM®), recibirá un mensaje (nombre de archivo lógico) con el formato `mtX Disponible`. Tome nota del valor de X, que es un número que asigna el sistema de forma automática. Utilice esta información para completar el campo Nombre de dispositivo en la hoja de trabajo.

Por ejemplo, si el mensaje es `mt0 Available`, el campo Nombre de dispositivo es `/dev/mt0` en la hoja de trabajo. Utilice siempre el prefijo `/dev/` con el nombre proporcionado por SMIT.

 Sistemas operativos AIX

## Configuración de dispositivos conectados a SAN de canal de fibra

---

Para configurar un dispositivo conectado a SAN de canal de fibra, complete este procedimiento.

### Procedimiento

---





1. Ejecute el programa SMIT.
2. Seleccione Dispositivos.
3. Seleccione IBM Spectrum ProtectDispositivos.
4. Seleccione Dispositivos conectados a la SAN de canal de fibra.
5. Seleccione Detectar dispositivos soportados por IBM Spectrum Protect. El proceso de detección puede tardar cierto tiempo.
6. Vuelva al menú Canal de fibra y seleccione Listar atributos de un dispositivo detectado.
7. Anote el identificador de dispositivo de tres caracteres, que utiliza al definir una vía de acceso al dispositivo en IBM Spectrum Protect. Por ejemplo, si una unidad de cintas tiene el identificador `mt2`, especifique `/dev/mt2` como el nombre de dispositivo.

 Sistemas operativos Linux

## Configuración de controladores de dispositivos de cinta en sistemas Linux

---

Consulte los temas siguientes al instalar y configurar los controladores de dispositivos de cinta en sistemas Linux.

-  Sistemas operativos Linux Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas  
Para utilizar el controlador de paso a través de IBM Spectrum Protect Linux, debe llevar a cabo los siguientes pasos.
-  Sistemas operativos Linux Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfc)  
El controlador de dispositivo `zfc` (zSeries Linux Fibre Channel Adapter) es un controlador de adaptador especial en el sistema IBM® zSeries.
-  Sistemas operativos Linux Información sobre los dispositivos SCSI del sistema  
En el archivo `/proc/scsi/scsi` encontrará información acerca de los dispositivos que detecta el sistema. Este archivo contiene una lista de todos los dispositivos SCSI detectados.
-  Sistemas operativos Linux Impedir que las etiquetas de cinta se sobrescriban  
El controlador del dispositivo IBM Spectrum Protect Passthru usa el controlador de dispositivo genérico (`sg`) de Linux SCSI para controlar y operar dispositivos de cinta que están conectados al sistema. Si el controlador de dispositivos de cinta SCSI genérico (`st`) de Linux se carga en el kernel y configura los dispositivos de cinta conectados, pueden surgir conflictos sobre cómo se gestiona un dispositivo puesto que tanto el controlador genérico `sg` como el controlador `st` controlan el mismo dispositivo.

 Sistemas operativos Linux

# Configuración de los controladores de paso a través de IBM Spectrum Protect para dispositivos de cintas y bibliotecas

Para utilizar el controlador de paso a través de IBM Spectrum Protect Linux, debe llevar a cabo los siguientes pasos.

## Procedimiento

1. Verifique que el dispositivo esté conectado a su sistema, que esté encendido y activo.
2. Verifique si el sistema ha detectado correctamente el dispositivo ejecutando este mandato:

```
cat /proc/scsi/scsi
```

3. Asegúrese de que tanto el paquete de controladores de dispositivo IBM Spectrum Protect (tsmscsi) como el paquete del servidor de almacenamiento estén instalados.
4. Hay disponibles dos métodos de configuración del controlador en el paquete de controladores del dispositivo de IBM Spectrum Protect: `autoconf` y `tsmscsi`. Ambos métodos llevan a cabo las tareas siguientes:
  - o Carga del controlador genérico (sg) SCSI de Linux en el kernel.
  - o Creación de los archivos especiales necesarios para el controlador Passthru.
  - o Creación de archivos de información de dispositivo para los dispositivos de cinta (`/dev/tsmscsi/mtinfo`) y las bibliotecas (`/dev/tsmscsi/lbinfo`).
5. Ejecute el método de configuración que prefiera (`autoconf` o `tsmscsi`) para el controlador passthru IBM Spectrum Protect.
  - o Para ejecutar el método de configuración `autoconf`, emita el siguiente mandato:

```
autoconf
```

- o Para ejecutar el método de configuración `tsmscsi`, emita el siguiente mandato:
    - a. Copie los dos archivos de configuración de ejemplo que se encuentran en el directorio de instalación desde `mt.conf.smp` y `lb.conf.smp` a `mt.conf` y `lb.conf`, respectivamente.
    - b. Edite los archivos `mt.conf` y `lb.conf`. Agregue una stanza (como se muestra en el ejemplo al inicio del archivo) para cada destino de SCSI, ID y combinación de LUN. Cada combinación de entradas de LUN, ID y destino de SCSI corresponde a una biblioteca o unidad de cintas que desea configurar. Asegúrese de que los archivos cumplen con estos requisitos:
      - Elimine el ejemplo que figura al principio de los archivos.
      - Debe haber una línea nueva entre cada sección.
      - Debe haber una nueva línea después de la última sección.
      - Asegúrese de que no hay signos de almohadilla (#) en ningún archivo.
    - c. Ejecute el script `tsmscsi` desde el directorio de instalación del controlador de dispositivo.
6. Verifique que el dispositivo está configurado debidamente examinando los archivos de texto correspondientes a los dispositivos de cinta (`/dev/tsmscsi/mtinfo`) y a las bibliotecas (`/dev/tsmscsi/lbinfo`).
  7. Determine los nombres de archivos especiales para las unidades de cinta y bibliotecas:
    - o Para determinar los nombres de los dispositivos de cinta, ejecute el mandato siguiente:

```
> ls /dev/tsmscsi/mt*
```

- o Para determinar los nombres de las bibliotecas, emita el mandato siguiente:

```
> ls /dev/tsmscsi/lb*
```


Esta información le ayuda a identificar los nombres de archivos especiales de `/dev/tsmscsi/mtx` y `/dev/tsmscsi/lbx` a proporcionar al servidor al emitir un mandato `DEFINE PATH`.

## Qué hacer a continuación

Si reinicia el sistema host, debe volver a ejecutar el script `autoconf` o `tsmscsi` para volver a configurar los dispositivos IBM Spectrum Protect. Si reinicia la instancia de servidor IBM Spectrum Protect, no tendrá que volver a configurar los dispositivos. En general, el controlador genérico SCSI de Linux está precargado en el kernel. Para verificar que el controlador se encuentra en el kernel, emita el siguiente mandato:

```
> lsmod | grep sg
```

Si el controlador no está en el kernel, emita el mandato `modprobe sg` para cargar el controlador `sg` en el kernel.

 Sistemas operativos Linux

# Instalación de controladores de dispositivo del adaptador de canal de fibra zSeries Linux (zfcpl)

El controlador de dispositivo zfcpl (zSeries Linux Fibre Channel Adapter) es un controlador de adaptador especial en el sistema IBM® zSeries.


## Acerca de esta tarea

Los controladores de dispositivo de cinta de IBM Spectrum Protect e IBM pueden ejecutarse en las plataformas zSeries con sistemas operativos Linux en entornos de 64 bits, y dan soporte a la mayoría de dispositivos de cinta OEM (original equipment manufacturer) de dispositivos de cinta IBM con interfaces de canal de fibra.

Para obtener más información sobre el controlador zfcpl, consulte el Redpaper de IBM, *Getting Started with zSeries Fibre Channel Protocol*, que está disponible en IBM Redbooks.

## Procedimiento

1. Cargue el módulo qdio.
2. Instale el controlador zfcpl.
3. Correlacione el protocolo de canal de fibra (FCP) y configure el controlador zfcpl.
4. Instale y configure el controlador de dispositivo de cinta de IBM.

 Sistemas operativos Linux

## Información sobre los dispositivos SCSI del sistema

En el archivo `/proc/scsi/scsi` encontrará información acerca de los dispositivos que detecta el sistema. Este archivo contiene una lista de todos los dispositivos SCSI detectados.

Dispone de la información de dispositivos siguiente: el número de host, el número de canal, el ID de SCSI, el número de unidad lógica, el proveedor, el nivel de firmware, el tipo de dispositivo y la modalidad de SCSI. Por ejemplo, si un sistema contiene algunas bibliotecas StorageTek e IBM®, una pasarela de SAN y algunas unidades Quantum DLT, el archivo `/proc/scsi/scsi` tendrá un aspecto similar al siguiente:

```
Attached devices:
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: STK      Model: 9738      Rev: 2003
  Type:  Medium Changer      ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: PATHLIGHT Model: SAN Gateway  Rev: 32aC
  Type:  Unknown            ANSI SCSI revision: 03
Host: scsi2 Channel: 00 Id: 01 Lun: 02
  Vendor: QUANTUM  Model: DLT7000   Rev: 2560
  Type:  Sequential-Access  ANSI SCSI revision: 02
Host: scsi2 Channel: 00 Id: 01 Lun: 04
  Vendor: IBM      Model: 7337      Rev: 1.63
  Type:  Medium Changer      ANSI SCSI revision: 02
```

 Sistemas operativos Linux

## Impedir que las etiquetas de cinta se sobrescriban

El controlador del dispositivo IBM Spectrum Protect Passthru usa el controlador de dispositivo genérico (sg) de Linux SCSI para controlar y operar dispositivos de cinta que están conectados al sistema. Si el controlador de dispositivos de cinta SCSI genérico (st) de Linux se carga en el kernel y configura los dispositivos de cinta conectados, pueden surgir conflictos sobre cómo se gestiona un dispositivo puesto que tanto el controlador genérico sg como el controlador st controlan el mismo dispositivo.

## Acerca de esta tarea

Si el controlador st controla dispositivos utilizados por IBM Spectrum Protect, es posible que las etiquetas de cinta internas de IBM Spectrum Protect se sobregaben y se pierdan datos. Si una aplicación utiliza el controlador st para controlar dispositivos y no se especifica la opción non-rewind, las cintas se rebobinan automáticamente tras finalizar una operación. La operación de rebobinado automático reubica la posición del cabezal de cinta al principio de la cinta. Si la cinta permanece cargada en la unidad, la siguiente



operación de grabación que no sea de IBM Spectrum Protect sobrescribirá la etiqueta de la cinta de IBM Spectrum Protect porque la etiqueta está al principio de la cinta.

Para impedir que se sobrescriban las etiquetas de IBM Spectrum Protect, lo que podría provocar la pérdida de datos, asegúrese de que sólo el controlador Passthru de IBM Spectrum Protect controle los dispositivos utilizados por IBM Spectrum Protect. Elimine el controlador st del kernel o, si el controlador es utilizado por algunas aplicaciones del sistema, suprima los archivos especiales que se corresponden con los dispositivos de IBM Spectrum Protect de modo que el controlador st ya no pueda controlarlos.

Si utiliza el controlador de dispositivo de cinta de IBM para controlar los dispositivos del sistema, puede encontrar los mismos problemas con conflictos en el control de los controladores de dispositivos. Revise la documentación sobre cintas de IBM para determinar cómo resolver este problema y prevenir la pérdida de datos.

#### Eliminar el controlador st

Si no hay ninguna otra aplicación en el sistema que utilice dispositivos st, elimine el controlador st del kernel. Emita el siguiente mandato para descargar el controlador st:

```
rmmod st
```

#### Suprima los archivos especiales de dispositivo que se correspondan con dispositivos de IBM Spectrum Protect

Si hay aplicaciones que requieren el uso del controlador st, suprima los archivos especiales que corresponden a dispositivos de IBM Spectrum Protect. Estos archivos especiales los genera por el controlador st. Cuando se eliminan, el controlador st ya no puede controlar los dispositivos de IBM Spectrum Protect correspondientes. Los nombres de archivos especiales de dispositivo para unidades de cinta aparecen en el directorio /dev/. Sus nombres tienen el formato /dev/[n]st[0-1024][l][m][a].

Enumere los nombres del archivo especial de la unidad st y los nombres del archivo especial del dispositivo IBM Spectrum Protect al usar el mandato ls. Basándose en la salida de las secuencias del dispositivo, puede encontrar dispositivos en la lista de dispositivos st que coincidan con los de la lista de dispositivos de IBM Spectrum Protect. El mandato rm puede utilizarse a continuación para suprimir dispositivos st.

Emita los siguientes mandatos para listar los dispositivos st y de IBM Spectrum Protect:

```
ls -l /dev/*st*
ls -l /dev/tmscsi/mt*
```

Suprima los dispositivos st con el mandato rm:



```
rm /dev/*st*
```

 Sistemas operativos Windows

## Configuración de controladores de dispositivos de cinta en sistemas Windows

---

Revise las instrucciones para instalar y configurar controladores de dispositivo de cinta y bibliotecas en sistemas Windows.

-  **Sistemas operativos Windows** Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta  
Para utilizar el controlador de dispositivo de paso a través de IBM Spectrum Protect Windows para bibliotecas y dispositivos de cinta, debe instalar el controlador y obtener los nombres de dispositivos para que los use el servidor.
-  **Sistemas operativos Windows** Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta  
Si el fabricante de una unidad de cintas o biblioteca de cintas no proporciona un controlador de dispositivos SCSI, debe instalar el controlador de dispositivos IBM Spectrum Protect SCSI.

 Sistemas operativos Windows

## Preparación para utilizar el controlador de paso a través de IBM Spectrum Protect para bibliotecas y dispositivos de cinta

---

Para utilizar el controlador de dispositivo de paso a través de IBM Spectrum Protect Windows para bibliotecas y dispositivos de cinta, debe instalar el controlador y obtener los nombres de dispositivos para que los use el servidor.

### Antes de empezar

---

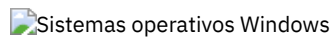
1. Determine si el fabricante del dispositivo de cinta o biblioteca de cintas proporciona un controlador de dispositivo.

2. Si el fabricante proporciona un paquete de controlador de dispositivo, descargue el paquete e instálelo.
3. Configure el controlador de dispositivo SCSI siguiendo las instrucciones del fabricante.

## Procedimiento

---

1. Instale el controlador del dispositivo de paso a través de IBM Spectrum Protect.
2. Obtenga los nombres de dispositivo que el servidor debe utilizar realizando una de las siguientes acciones:
  - En el servidor, ejecute el mandato QUERY SAN. La salida muestra todos los nombres de dispositivo y los números de serie de dispositivo asociados.
  - En el directorio del servidor ejecute el programa de utilidad tsmdlst.exe. La salida muestra todos los nombres de dispositivos, sus números de serie asociados y las ubicaciones de dispositivo asociadas.
  - En el indicador de mandatos del sistema Windows, ejecute el mandato regedit. Desde la salida, obtenga los nombres de archivos de dispositivo en función de las ubicaciones de los dispositivos. La ubicación consta de ID de puerto, ID de bus de SCSI, ID de LUN ID e ID de destino de SCSI. El nombre de archivo de dispositivo de IBM Spectrum Protect tiene un formato mtA.B.C.C para unidades de cinta y lbA.B.C.D para bibliotecas de cinta, donde:
    - A es el ID de destino de SCSI.
    - B es el ID de LUN.
    - C es el ID de bus de SCSI.
    - D es el ID de puerto.



## Configuración del controlador IBM Spectrum Protect SCSI para bibliotecas y dispositivos de cinta

---

Si el fabricante de una unidad de cintas o biblioteca de cintas no proporciona un controlador de dispositivos SCSI, debe instalar el controlador de dispositivos IBM Spectrum Protect SCSI.

### Acerca de esta tarea

---

El nombre de archivo de controlador de dispositivo SCSI de IBM Spectrum Protect es tsm SCSI64.sys.

## Procedimiento

---

1. Localice el dispositivo en la consola del gestor de dispositivos (devmgmt.msc) y selecciónelo. Las unidades de cinta se listan en Unidades de cinta, y los conmutadores de soporte en Conmutadores de soporte.
2. Configure el dispositivo para que lo utilice el controlador de dispositivo tsm SCSI64.sys:
  - a. Pulse con el botón derecho sobre el dispositivo y pulse Actualizar software de controlador.
  - b. Pulse Buscar software de controlador en el equipo.
3. Pulse Elegir en una lista de controladores de dispositivo en mi PC.
4. Pulse Siguiente.
5. Seleccione la opción adecuada:
  - a. Para una unidad de cintas, seleccione IBM Spectrum Protect para unidades de cinta.
  - b. Para un conmutador de soporte, seleccione IBM Spectrum Protect para conmutadores de soporte.
6. Pulse Siguiente.
7. Pulse Cerrar.
8. Compruebe que el dispositivo se ha configurado correctamente para el controlador de dispositivo tsm SCSI64:
  - a. Pulse con el botón derecho sobre el dispositivo y pulse Propiedades.
  - b. Pulse el separador Controlador y Detalles de controlador. La ventana Detalles de controlador muestra el controlador de dispositivo que controla el dispositivo.

## Configuración de bibliotecas para su uso por parte de un servidor

---

Para utilizar una biblioteca o bibliotecas para el almacenamiento de un servidor de IBM Spectrum Protect, primero tiene que configurar los dispositivos en el sistema servidor.

### Antes de empezar

---

1. Conecte los dispositivos al hardware del servidor. Siga las instrucciones que encontrará en Conectar un dispositivo de biblioteca automática a su dispositivo.
2. Seleccione los controladores de dispositivo de cinta. Siga las instrucciones que encontrará en Seleccionar un controlador de dispositivo de cinta.

3. Instale y configure los controladores de dispositivo de cinta. Siga las instrucciones que encontrará en Instalación y configuración de controladores de dispositivos de cinta.
4. Determine los nombres de dispositivo que se necesitan para definir la biblioteca en el servidor. Siga las instrucciones que encontrará en Nombres de archivo especiales para dispositivos de cinta.

## Procedimiento

---

1. Defina la biblioteca y la vía de acceso desde el servidor a la biblioteca. Siga las instrucciones que encontrará en Definición de bibliotecas.
2. Defina las unidades en la biblioteca. Siga las instrucciones que encontrará en Definición de unidades.

Para las bibliotecas SCSI, puede utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca en un solo paso, en lugar de completar los dos pasos 2 y 3. Para utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca, la opción `SANDISCOVERY` debe estar admitida y habilitada.

3. Defina una vía de acceso desde el servidor a cada unidad mediante el mandato `DEFINE PATH`.
4. Defina una clase de dispositivo. Siga las instrucciones que encontrará en Definición de las clases de dispositivo de cinta.

Las clases de dispositivo especifican los formatos de grabación para las unidades y las clasifican según el tipo. Utilice el valor predeterminado, `FORMAT=DRIVE`, como formato de grabación solo si todas las unidades asociadas a la clase de dispositivo pueden leer y grabar en todos los medios.

Por ejemplo, imagine que tiene una mezcla de unidades Ultrium generación 3 y Ultrium generación 4, pero solo tiene medios Ultrium generación 3. Puede especificar `FORMAT=DRIVE` porque tanto las unidades Generación 4 como las unidades Generación 3 pueden leer y grabar en medios de Generación 3. media.

5. Definir una agrupación de almacenamiento con el mandato `DEFINE STGPOOL`.

Tenga en cuenta las siguientes opciones clave para definir agrupaciones de almacenamiento:

- Los volúmenes reutilizables son volúmenes vacíos que están disponibles para el uso. Si especifica un valor para el máximo número de volúmenes reutilizables en la agrupación de almacenamiento, el servidor puede elegir entre los volúmenes reutilizables disponibles en la biblioteca.

Si no permite los volúmenes reutilizables, debe completar el paso adicional de definir explícitamente cada volumen que se utilizará en la agrupación de almacenamiento. Además, especifique el parámetro `MAXSCRATCH=0` al definir la agrupación de almacenamiento para que no se utilicen los volúmenes reutilizables.

- El valor predeterminado de las agrupaciones de almacenamiento primarias es la proximidad por grupo. El valor predeterminado para agrupación de almacenamiento de copias y agrupaciones de datos activos es la desactivación de la proximidad. El servidor utiliza la *proximidad* para mantener todos los archivos que pertenecen a un grupo de nodos cliente, a un solo nodo cliente, a un espacio de archivos de cliente o a un grupo de espacio de archivos de cliente en el mínimo número de volúmenes. Si se desactiva la proximidad para una agrupación de almacenamiento y los clientes comienzan a almacenar datos, no podrá cambiar fácilmente los datos de la agrupación de forma que éstos sigan estando próximos entre sí.

6. Dé de alta y etiquete los volúmenes de la biblioteca. Siga las instrucciones que encontrará en Incorporar volúmenes en una biblioteca automatizada y Etiquetado de volúmenes de cinta.

Asegúrese de que haya suficientes volúmenes disponibles para el servidor. Tenga siempre a mano un número suficiente de volúmenes etiquetados de manera que no le falten cuando realice operaciones importantes, como por ejemplo, la copia de seguridad de los clientes. Etiquete volúmenes reutilizables adicionales para posibles operaciones de recuperación que puedan surgir posteriormente.

Los procedimientos para dar de alta y etiquetar volúmenes son los mismos tanto si la biblioteca contiene unidades de un solo tipo de dispositivo como si son de varios tipos de dispositivo. Puede utilizar el mandato `CHECKIN LIBVOLUME` para dar de alta volúmenes que ya están etiquetados. O, si desea etiquetar y dar de alta volúmenes con un solo paso, emita el mandato `LABEL LIBVOLUME`.

Bibliotecas con varios tipos de dispositivo: Si la biblioteca tiene unidades de varios tipos de dispositivo y ha definido dos bibliotecas en el servidor de IBM Spectrum Protect, las dos bibliotecas definidas representan una biblioteca física. Debe dar de alta los volúmenes de cinta por separado en cada biblioteca definida. Asegúrese de dar de alta los volúmenes en la biblioteca de IBM Spectrum Protect correcta.

## Qué hacer a continuación

---

Compruebe las definiciones de dispositivos para asegurarse de que todo está configurado correctamente. Utilice un mandato `QUERY` para revisar la información sobre cada objeto de almacenamiento.

Al revisar los resultados del mandato `QUERY DRIVE`, verifique que el tipo de dispositivo para la unidad es el esperado. Si no se ha definido una vía de acceso, el tipo de dispositivo de unidad se lista como `UNKNOWN` y si se utiliza la vía de acceso equivocada, se

muestra GENERIC\_TAPE u otro tipo de dispositivo. Este paso es especialmente importante cuando se utilizan medios mezclados.

Opcionalmente, configure la compartición de bibliotecas. Siga las instrucciones que encontrará en Configuración de la compartición de bibliotecas.

- Definición de dispositivos de cinta  
Antes de realizar una copia de seguridad o migrar datos a la cinta, debe definir un dispositivo de cinta en IBM Spectrum Protect.
- Configuración de la compartición de bibliotecas  
Varios servidores de IBM Spectrum Protect pueden compartir dispositivos de almacenamiento por medio de una red de área de almacenamiento (SAN). Se debe configurar un servidor como gestor de biblioteca y los demás servidores como clientes de biblioteca.

**Referencia relacionada:**

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- ➔ PERFORM LIBACTION (Definir o suprimir todas las unidades y las vías de acceso de una biblioteca)

## Definición de dispositivos de cinta

---

Antes de realizar una copia de seguridad o migrar datos a la cinta, debe definir un dispositivo de cinta en IBM Spectrum Protect.

- Definición de bibliotecas y unidades  
Una biblioteca de cintas puede incluir una o más unidades de cinta. Aprenda a definir bibliotecas, unidades y vías de acceso para el servidor IBM Spectrum Protect.
- Definición de las clases de dispositivo de cinta  
Una clase de dispositivo define un conjunto de características que utiliza un conjunto de volúmenes que se pueden crear en una agrupación de almacenamiento. Debe definir una clase de dispositivo para un dispositivo de cinta para asegurarse de que el servidor puede utilizar el dispositivo.

## Definición de bibliotecas y unidades

---

Una biblioteca de cintas puede incluir una o más unidades de cinta. Aprenda a definir bibliotecas, unidades y vías de acceso para el servidor IBM Spectrum Protect.

- Definición de bibliotecas  
Para poder utilizar una unidad, debe definir la biblioteca a la que pertenece.
- Definición de unidades  
Para informar al servidor con respecto a una unidad que puede utilizarse para acceder a los volúmenes de almacenamiento, emita el mandato DEFINE DRIVE, seguido del mandato DEFINE PATH.

## Definición de bibliotecas

---

Para poder utilizar una unidad, debe definir la biblioteca a la que pertenece.

### Procedimiento

---

1. Defina la biblioteca utilizando el mandato DEFINE LIBRARY.


Por ejemplo, si tiene una biblioteca de cintas IBM TS3500, puede definir una biblioteca denominada ROBOTMOUNT con el siguiente mandato:

```
define library robotmount libtype=scsi
```

Si necesita la compartición de biblioteca o el movimiento de datos sin LAN, consulte la siguiente información:

- Configuración de la compartición de bibliotecas
- Configuración del movimiento de datos sin LAN

2. Defina una vía de acceso desde el servidor a la biblioteca mediante el mandato DEFINE PATH. Cuando especifique el parámetro DEVICE, escriba el nombre del archivo especial de dispositivo. El servidor necesita este nombre para comunicarse con las unidades de cinta, el conmutador de soporte y los dispositivos de soporte extraíbles. Para obtener más información sobre los nombres de archivos especiales de dispositivo, consulte Nombres de archivo especiales para dispositivos de cinta.

 Sistemas operativos AIX

```
define path server1 robotmount srctype=server desttype=library
device=/dev/lb0
```

#### Sistemas operativos Linux


```
define path server1 robotmount srctype=server desttype=library
device=/dev/tmsmcsi/lb0
```


#### Sistemas operativos Windows

```
define path server1 robotmount srctype=server desttype=library
device=lb0.0.1.0
```

- **Definición de bibliotecas SCSI en una SAN**  
En el caso de un tipo de biblioteca SCSI en una SAN, el servidor puede hacer el seguimiento del número de serie de la biblioteca. Con el número de serie, el servidor puede confirmar la identidad del dispositivo al definir la vía de acceso o cuando el servidor utilice el dispositivo.

#### Referencia relacionada:

 [DEFINE LIBRARY \(Definir una biblioteca\)](#)

 [DEFINE PATH \(Definir una vía de acceso\)](#)

## Definición de unidades

---

Para informar al servidor con respecto a una unidad que puede utilizarse para acceder a los volúmenes de almacenamiento, emita el mandato DEFINE DRIVE, seguido del mandato DEFINE PATH.

### Antes de empezar

---

Un *objeto de unidad* representa un mecanismo de unidad en una biblioteca que usa soportes de almacenamiento extraíbles. En el caso de dispositivos con varias unidades, incluidas las bibliotecas automatizadas, se debe definir cada unidad por separado y asociarla con una biblioteca. Las definiciones de unidad pueden incluir información como, por ejemplo, la dirección del elemento para las unidades en SCSI, la frecuencia con que se limpia una unidad de cintas y si la unidad está en línea.

IBM Spectrum Protect da soporte a las unidades de cinta que pueden ser autónomas o pueden formar parte de una biblioteca automatizada. El método preferido consiste en configurar la solución de cinta utilizando bibliotecas automatizadas.

### Acerca de esta tarea

---

Al emitir el mandato DEFINE DRIVE, debe proporcionar alguno o todos los datos de la siguiente información:

#### Nombre de biblioteca

El nombre de la biblioteca en la que se encuentra la unidad.

#### Nombre de unidad

El nombre que se ha asignado a la unidad.

#### Número de serie

El número de serie de la unidad. El parámetro de número de serie sólo es válido para las unidades de SCSI. Con el número de serie, el servidor puede confirmar la identidad del dispositivo al definir la vía de acceso o cuando el servidor utilice el dispositivo.

Si lo desea, puede especificar el número de serie. El valor predeterminado consiste en permitir al servidor obtener el número de serie de la propia unidad al definirse la vía de acceso. Si especifica el número de serie, el servidor confirma que el número de serie es correcto al definir la vía de acceso para la unidad. Al definir la vía de acceso, puede establecer el parámetro AUTODETECT=YES para permitir al servidor corregir el número de serie si el número que detecta no coincide con el especificado al definir la unidad. Como práctica recomendada, especifique el parámetro AUTODETECT=YES para actualizar automáticamente el número de serie para la unidad en la base de datos al definir la vía de acceso.

Según las posibilidades de la unidad, es posible que el servidor no pueda detectar automáticamente el número de serie. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo. Consulte el apartado Influencia de los cambios de dispositivo en la SAN.

#### Dirección de elemento

La dirección de elemento de la unidad. El parámetro ELEMENT se aplica solo a las unidades de las bibliotecas SCSI. La dirección de elemento es un número que indica la ubicación física de una unidad en una biblioteca automatizada. El servidor necesita la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. El servidor puede obtener la dirección de elemento desde la unidad al definir la vía de acceso, o puede especificar el número de elemento al definir la

unidad. Como práctica recomendada, especifique el parámetro ELEMENT=AUTODETECT para que el servidor detecte automáticamente el número de elemento cuando se defina la vía de acceso a la unidad.

Según las capacidades de la biblioteca, es posible que el servidor no pueda detectar automáticamente la dirección de elemento. En ese caso, deberá proporcionar la dirección de elemento al definir la unidad, si la biblioteca tiene más de una unidad. Para obtener la dirección de elemento, vaya a [IBM® Support Portal for IBM Spectrum Protect](#).

Consejo: Los controladores de dispositivo de cinta de IBM y los controladores de dispositivo de cinta no IBM generan distintos archivos y formatos de dispositivo:

- Para IBM, los nombres de dispositivos empiezan por rmt seguido de un entero, por ejemplo, /dev/rmt0.
- Para los controladores de dispositivo de cinta de IBM Spectrum Protect, los nombres de controlador de dispositivo de cinta empiezan por mt seguido de un entero, por ejemplo /dev/mt0.

Debe utilizar el archivo de dispositivo correcto cuando defina una vía de acceso.

## Procedimiento

---

1. asigne una unidad a la biblioteca emitiendo el mandato DEFINE DRIVE.
2. Para que el servidor pueda utilizar la unidad, emita el mandato DEFINE PATH.

Para ejemplos sobre la configuración de bibliotecas, vías de acceso y unidades, consulte [Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad](#) y [Ejemplo: Configurar una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad](#).

## Definición de las clases de dispositivo de cinta

---

Una clase de dispositivo define un conjunto de características que utiliza un conjunto de volúmenes que se pueden crear en una agrupación de almacenamiento. Debe definir una clase de dispositivo para un dispositivo de cinta para asegurarse de que el servidor puede utilizar el dispositivo.

## Antes de empezar




---

Debe definir las bibliotecas y unidades en el servidor antes de definir las clases de dispositivo.

## Acerca de esta tarea

---

Para obtener una lista de dispositivos soportados y formatos de clase de dispositivo válidos, consulte el sitio web [Dispositivos soportados de IBM Spectrum Protect para su sistema operativo](#):

-  [Sistemas operativos AIX](#)  [Sistemas operativos Windows](#) [Dispositivos soportados para AIX y Windows](#)
-  [Sistemas operativos Linux](#) [Dispositivos soportados para Linux](#)

Se pueden definir varias clases de dispositivo para cada tipo de dispositivo. Por ejemplo, es posible que necesite especificar distintos atributos para distintas agrupaciones de almacenamiento que utilizan el mismo tipo de unidad de cintas. Es posible que se requieran variaciones que no son específicas para el dispositivo, sino de la forma en que se desea utilizar el dispositivo (por ejemplo, la retención o el límite de montaje).

Directrices:

- Una clase de dispositivo puede asociarse con varias agrupaciones de almacenamiento, pero cada agrupación de almacenamiento puede estar asociada sólo con una clase de dispositivo.
- Las bibliotecas SCSI puede incluir unidades de cinta de más de un tipo de dispositivo. Al definir la clase de dispositivo en este entorno, debe declarar un valor para el parámetro FORMAT.

Para obtener más información, consulte [Mezcla de tipos de dispositivos en una biblioteca](#).

## Procedimiento

---

Para definir una clase de dispositivo, utilice el mandato DEFINE DEVCLASS con el parámetro DEVTYPE, que asigna un tipo de dispositivo a la clase de dispositivo.

## Resultados

---

Si incluye la opción DEVCONFIG del archivo dmserv.opt, los archivos que especifique con esa opción se actualizan automáticamente con los resultados de los mandatos DEFINE DEVCLASS, UPDATE DEVCLASS y DELETE DEVCLASS.

- Definición de las clases de dispositivo LTO  
Para evitar problemas a la hora de combinar distintas generaciones de unidades y medios LTO en una sola biblioteca, revise las restricciones. Revise también las restricciones para el cifrado de unidad LTO.
- Definición de clases de dispositivo 3592  
Las definiciones de clase de dispositivo para 3592, TS1130, TS1140, TS1150 y dispositivos posteriores incluyen parámetros para una mayor velocidad de acceso a los volúmenes y un cifrado de unidad más rápido. Para evitar que se produzcan problemas al mezclar distintas generaciones de 3592 y TS1130 y unidades posteriores de una biblioteca, revise las directrices.

**Referencia relacionada:**

- 🔗 DEFINE DEVCLASS (Definir una clase de dispositivo)
- 🔗 QUERY DEVCLASS (Visualizar información en una o más clases de dispositivo)
- 🔗 UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Definición de las clases de dispositivo LTO

Para evitar problemas a la hora de combinar distintas generaciones de unidades y medios LTO en una sola biblioteca, revise las restricciones. Revise también las restricciones para el cifrado de unidad LTO.

- Combinación de unidades y medios LTO en una biblioteca  
Al combinar diferentes generaciones de unidades y medios LTO, debe tener en cuenta las funcionalidades de lectura-grabación de cada generación. El método preferido consiste en configurar diferentes clases de dispositivo para cada generación de medios.
- Límites de montaje en entornos de medios mixtos LTO  
En una biblioteca con medios mixtos, en la que varias clases de dispositivo hacen referencia a la misma biblioteca, las unidades compatibles se comparten entre las agrupaciones de almacenamiento. Asegúrese de establecer un valor adecuado para el parámetro MOUNTLIMIT en cada una de las clases de dispositivo.
- Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior  
IBM Spectrum Protect admite los tres tipos de cifrado de unidad disponibles con las unidades LTO generación 4 o posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

## Combinación de unidades y medios LTO en una biblioteca

Al combinar diferentes generaciones de unidades y medios LTO, debe tener en cuenta las funcionalidades de lectura-grabación de cada generación. El método preferido consiste en configurar diferentes clases de dispositivo para cada generación de medios.

### Acerca de esta tarea

Si piensa en mezclar distintas generaciones de unidades y medios LTO, revise las siguientes restricciones:

Tabla 1. Funcionalidades de lectura/grabación para distintas generaciones de unidades LTO

Unidades	Medios de la generación 1	Medios de la generación 2	Medios de la generación 3	Medios de la generación 4	Medios de la generación 5	Medios de la generación 6	Medios de la generación 7
Generación 1	Acceso de lectura/escritura	n/d	n/d	n/d	n/d	n/d	n/d
Generación 2	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d	n/d	n/d	n/d
Generación 3	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d	n/d	n/d
Generación 4	n/d	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d	n/d
Generación 5	n/d	n/d	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d
Generación 6	n/d	n/d	n/d	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d

Unidades	Medios de la generación 1	Medios de la generación 2	Medios de la generación 3	Medios de la generación 4	Medios de la generación 5	Medios de la generación 6	Medios de la generación 7
Generación 7	n/d	n/d	n/d	n/d	Acceso de lectura	Acceso de lectura/escritura	Acceso de lectura/escritura

## Ejemplo

Si combina diferentes tipos de unidades y medios, configure diferentes clases de dispositivo: una para cada tipo de medio. Para especificar el tipo de medio, utilice el parámetro `FORMAT` en cada una de las definiciones de clase de dispositivo. (No especifique `FORMAT=DRIVE`.) Por ejemplo, si combina unidades Ultrium generación 5 y Ultrium generación 6, especifique `FORMAT=ULTRIUM5C` (o `ULTRIUM5`) para la clase de dispositivo Ultrium generación 5, y `FORMAT=ULTRIUM6C` (o `ULTRIUM6`) para la clase de dispositivo Ultrium generación 6.

En este ejemplo, ambas clases de dispositivos pueden apuntar a la misma biblioteca con las unidades Ultrium generación 5 y Ultrium generación 6. Las unidades se compartirán entre las dos agrupaciones de almacenamiento. Una agrupación de almacenamiento utilizará exclusivamente la primera clase de dispositivo y el medio Ultrium generación 5. La otra agrupación de almacenamiento utilizará exclusivamente la segunda clase de dispositivo y el medio Ultrium generación 6. Puesto que las dos agrupaciones de almacenamiento comparten una única biblioteca, los medios Ultrium generación 5 pueden montarse en unidades Ultrium generación 6 a medida que vayan estando disponibles durante el procesamiento de puntos de montaje.

Si combina generaciones de soportes de sólo lectura más antiguos con soportes de lectura/escritura más nuevos en una única biblioteca, deberá marcar los soportes de sólo lectura como sólo lectura y extraer todos los soportes reutilizables de sólo lectura. Por ejemplo, si combina unidades y medios Ultrium generación 4 con Ultrium generación 6 en una sola biblioteca, debe marcar los medios de generación 4 como sólo lectura. Además, debe extraer todos los volúmenes reutilizables de generación 4.

## Límites de montaje en entornos de medios mixtos LTO

En una biblioteca con medios mixtos, en la que varias clases de dispositivo hacen referencia a la misma biblioteca, las unidades compatibles se comparten entre las agrupaciones de almacenamiento. Asegúrese de establecer un valor adecuado para el parámetro `MOUNTLIMIT` en cada una de las clases de dispositivo.

Por ejemplo, en una biblioteca de medios mixta que contenga unidades y medios Ultrium Generation 1 y Ultrium Generation 2, por ejemplo, los medios Ultrium Generation 1 pueden montarse en unidades Ultrium Generation 2.

Suponga un ejemplo de una biblioteca mixta que conste de los siguientes medios y unidades:

- Cuatro unidades LTO Ultrium Generation 1 y medios LTO Ultrium Generation 1.
- Cuatro unidades LTO Ultrium Generation 2 y medios LTO Ultrium Generation 2.

Se crearon las clases de dispositivo siguientes:

- Clase de dispositivo de LTO Ultrium Generation 1 `LTO1CLASS`, especificando `FORMAT=ULTRIUMC`
- Clase de dispositivo de LTO Ultrium Generation 2 `LTO2CLASS`, especificando `FORMAT=ULTRIUM2C`

También se crearon las agrupaciones de almacenamiento siguientes:

- Agrupación de almacenamiento LTO Ultrium Generation 1 `LTO1POOL` basada en la clase de dispositivo `LTO1CLASS`.
- Agrupación de almacenamiento LTO Ultrium Generation 2 `LTO2POOL` basada en la clase de dispositivo `LTO2CLASS`.

El número de puntos de montaje disponibles para que utilice cada agrupación de almacenamiento se especifica en la clase de dispositivo utilizando el parámetro `MOUNTLIMIT`. El parámetro `MOUNTLIMIT` de la clase de dispositivo `LTO2CLASS` debe estar establecido en 4 para que coincida con el número de unidades disponibles que solo pueden montar medios LTO2. El parámetro `MOUNTLIMIT` de la clase de dispositivo `LTO1CLASS` debe estar establecido en un valor que sea mayor que el número de unidades disponibles (5 o posiblemente 6) para tener en cuenta que los medios Ultrium Generation 1 pueden montarse en unidades Ultrium Generation 2. El valor óptimo de `MOUNTLIMIT` depende de los patrones de acceso de la carga de trabajo y la agrupación de almacenamiento.

Supervise y ajuste el valor de `MOUNTLIMIT` para adecuarlo a las cargas de trabajo cambiantes. Si `MOUNTLIMIT` para `LTO1POOL` se establece en un valor demasiado alto, es posible que las solicitudes de montaje de `LTO2POOL` se retrasen o fallen, ya que se han utilizado las unidades Ultrium Generation 2 para satisfacer las solicitudes de montaje de medios Ultrium Generation 1. En el peor de los casos, demasiada competencia para las unidades Ultrium Generation 2 puede provocar el siguiente error en los montajes de medios Generation 2:

```
ANR8447E No
hay unidades disponibles en este momento en la biblioteca.
```



Si el valor de MOUNTLIMIT para LTO1POOL no está establecido lo suficientemente alto, se retrasan las solicitudes de montaje de unidades LTO Ultrium Generation 2 que se podrían satisfacer.

Restricción: Se aplican restricciones al combinar unidades Ultrium Generation 1 con unidades Ultrium Generation 2 o Generation 3 debido a la forma en que están asignados los puntos de montaje. Por ejemplo, es posible que aquellos procesos que requieran varios puntos de montaje que incluyan volúmenes tanto Ultrium Generation 1 como Ultrium Generation 2 intenten reservar sólo unidades Ultrium Generation 2 aunque una unidad Ultrium Generation 1 disponible podría satisfacer un montaje. Entre los procesos que se comportan así se incluyen los mandatos MOVE DATA y BACKUP STGPOOL. Estos procesos esperarán hasta que se pueda satisfacer la cantidad necesaria de puntos de montaje con unidades Ultrium Generation 2.

**Referencia relacionada:**

➔ BACKUP STGPOOL (Hacer copia de seguridad de los datos de la agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia)

➔ DEFINE DEVCLASS (Definir una clase de dispositivo)

➔ MOVE DATA (Trasladar archivos a un volumen de agrupación de almacenamiento)

## Habilitación e inhabilitación del cifrado de unidades para unidades de cinta LTO generación 4 o posterior

---

IBM Spectrum Protect admite los tres tipos de cifrado de unidad disponibles con las unidades LTO generación 4 o posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

### Acerca de esta tarea

---

El parámetro DRIVEENCRYPTION del mandato DEFINE DEVCLASS especifica si se permite el cifrado de unidad para unidades IBM y HP LTO generación 4 o posterior, formatos Ultrium 4 y Ultrium 4C. Este parámetro garantiza la compatibilidad de IBM Spectrum Protect con los valores de cifrado de hardware para volúmenes vacíos. No puede utilizar este parámetro para los volúmenes de agrupaciones de almacenamiento que estén llenos o se estén llenando.

IBM Spectrum Protect admite el método de Aplicación de cifrado con unidades IBM y HP LTO-4 o posteriores. Solo IBM LTO-4 o posterior admite los métodos Sistema y Biblioteca. El método de cifrado Biblioteca solo se puede utilizar si el hardware del sistema (por ejemplo IBM TS3500) lo admite.

Restricción: No puede utilizar el cifrado de unidades con medios WORM (grabar una vez leer muchas).

El método de Aplicación se define mediante el hardware. Para utilizar el método de aplicación en el que IBM Spectrum Protect genera y gestiona claves de cifrado, establezca el parámetro DRIVEENCRYPTION en ON. Esta acción habilita el cifrado de datos para volúmenes vacíos. Si el parámetro se establece en ON y el hardware está configurado para otro método de cifrado, las operaciones de copia de seguridad fallan.

### Procedimiento

---

En el ejemplo simplificado siguiente se muestran los pasos que es preciso seguir para habilitar o inhabilitar el cifrado de datos para volúmenes vacíos en una agrupación de almacenamiento:

1. Defina una biblioteca emitiendo el mandato DEFINE LIBRARY:

```
define library 3584 libtype=SCSI
```

2. Defina una clase de dispositivo, LTO\_ENCRYPT, emitiendo el mandato DEFINE DEVCLASS y especificando IBM Spectrum Protect como gestor de claves:

```
define devclass lto_encrypt library=3584 devtype=lto driveencryption=on
```

3. Definir una agrupación de almacenamiento emitiendo el mandato DEFINE STGPOOL:

```
define stgpool lto_encrypt_pool lto_encrypt
```

4. Para inhabilitar el cifrado en volúmenes nuevos, establezca el parámetro DRIVEENCRYPTION con el valor OFF. El valor predeterminado es ALLOW. Se permite el cifrado de unidades de volúmenes vacíos si se ha habilitado otro método de cifrado.

**Conceptos relacionados:**

Métodos de cifrado de cinta

## Definición de clases de dispositivo 3592

---

Las definiciones de clase de dispositivo para 3592, TS1130, TS1140, TS1150 y dispositivos posteriores incluyen parámetros para una mayor velocidad de acceso a los volúmenes y un cifrado de unidad más rápido. Para evitar que se produzcan problemas al mezclar distintas generaciones de 3592 y TS1130 y unidades posteriores de una biblioteca, revise las directrices.

- **Combinación de generaciones de unidades y medios 3592 en una sola biblioteca**  
Para obtener un rendimiento óptimo, no combine generaciones de medios 3592 en una sola biblioteca. Pueden producirse problemas al mezclarse diferentes generaciones de medios. Por ejemplo, puede que IBM Spectrum Protect no sea capaz de leer la etiqueta de un volumen.
- **Control de las velocidades de acceso a datos en volúmenes 3592**  
Puede optimizar la capacidad de almacenamiento y mejorar la velocidad de acceso al crear volúmenes. Al particionar datos en agrupaciones de almacenamiento que tienen volúmenes, puede especificar el porcentaje de capacidad de escala para proporcionar la máxima capacidad de almacenamiento o para proporcionar un acceso rápido al volumen.
- **Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior**  
Con IBM Spectrum Protect, puede utilizar los siguientes tipos de cifrados de unidad con unidades que sean 3592 generación 2 y posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

## Combinación de generaciones de unidades y medios 3592 en una sola biblioteca

Para obtener un rendimiento óptimo, no combine generaciones de medios 3592 en una sola biblioteca. Pueden producirse problemas al mezclarse diferentes generaciones de medios. Por ejemplo, puede que IBM Spectrum Protect no sea capaz de leer la etiqueta de un volumen.

### Acerca de esta tarea

En la tabla siguiente se muestra la interoperatividad de lectura-grabación para las generaciones de unidades.

Unidades	Formato de Generación 1	Formato de Generación 2	Formato de Generación 3	Formato de Generación 4	Formato de Generación 5
Generación 1	Acceso de lectura/escritura	n/d	n/d	n/d	n/d
Generación 2	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d	n/d
Generación 3	Acceso de solo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d	n/d
Generación 4	n/d	Sólo lectura	Acceso de lectura/escritura	Acceso de lectura/escritura	n/d
Generación 5	n/d	n/d	Acceso de lectura	Acceso de lectura/escritura	Acceso de lectura/escritura

Si debe combinar generaciones de unidades en una biblioteca, revise el ejemplo y las restricciones para evitar problemas.

Tabla 1. Combinación de generaciones de unidades

Tipo de biblioteca	Ejemplo y restricciones
--------------------	-------------------------

Tipo de biblioteca	Ejemplo y restricciones
SCSI	<p>Define una nueva agrupación de almacenamiento y clase de dispositivo para la última generación de unidad. Por ejemplo, supongamos que tiene una agrupación de almacenamiento y una clase de dispositivo para 3592-2. La agrupación de almacenamiento contiene todos los medios que se han grabado en formato Generación 2. Supongamos que el valor del parámetro FORMAT en la definición de clase de dispositivo se establece en 3952-2 (no en DRIVE). Añada unidades de Generación 3 a la biblioteca. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la nueva definición de clase de dispositivo para las unidades de generación 3, establezca el valor del parámetro FORMAT en 3592-3 o 3592-3C. No especifique DRIVE.</li> <li>2. En la definición de la agrupación de almacenamiento asociada con las unidades de generación 2, actualice el parámetro MAXSCRATCH a 0, por ejemplo:</li> </ol> <pre data-bbox="537 485 1000 510">update stgpool genpool2 maxscratch=0</pre> <p>Este método permite que ambas generaciones utilicen su formato óptimo y se minimicen los posibles problemas de medios que puedan producirse como consecuencia de combinar generaciones. No obstante, no solucionará todos los problemas de medios. Por ejemplo, pueden darse casos de competencia por los puntos de montaje y que se produzcan anomalías de montaje. (para obtener información sobre cómo completar puntos de montaje en el contexto de unidades y medios 3592, consulte Definición de clases de dispositivo 3592.)</p> <p>Restricción: La siguiente lista describe las restricciones de medios:</p> <ul style="list-style-type: none"> <li>• CHECKIN LIBVOL: El problema radica en la utilización de la opción CHECKLABEL=YES. Si la etiqueta está escrita actualmente en un formato de generación 3 o posterior y especifica la opción CHECKLABEL=YES, las unidades de las generaciones anteriores fallan si utilizan este mandato. Para evitar el problema, especifique CHECKLABEL=BARCODE.</li> <li>• LABEL LIBVOL: Cuando el servidor intenta utilizar unidades de una generación anterior para leer la etiqueta escrita con un formato de generación 3 o posterior, el mandato LABEL LIBVOL falla a menos que se especifique OVERWRITE=YES. Verifique que el soporte que se está etiquetando con OVERWRITE=YES no tiene datos activos.</li> <li>• CHECKOUT LIBVOL: Cuando IBM Spectrum Protect verifica la etiqueta (CHECKLABEL=YES), como un formato de generación 3 o posterior, y lee unidades de generaciones anteriores, el mandato falla. Para evitar este problema, especifique CHECKLABEL=NO.</li> </ul>

**Referencia relacionada:**

- [CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)
- [CHECKOUT LIBVOLUME \(Dar de baja un volumen de almacenamiento de una biblioteca\)](#)
- [LABEL LIBVOLUME \(Etiquetar un volumen de biblioteca\)](#)
- [UPDATE STGPOOL \(Actualizar una agrupación de almacenamiento\)](#)

## Control de las velocidades de acceso a datos en volúmenes 3592

Puede optimizar la capacidad de almacenamiento y mejorar la velocidad de acceso al crear volúmenes. Al particionar datos en agrupaciones de almacenamiento que tienen volúmenes, puede especificar el porcentaje de capacidad de escala para proporcionar la máxima capacidad de almacenamiento o para proporcionar un acceso rápido al volumen.

### Acerca de esta tarea

Para reducir la capacidad de un medio, especifique el parámetro SCALECAPACITY cuando defina la clase de dispositivo utilizando el mandato DEFINE DEVCLASS o cuando actualice la clase de dispositivo utilizando el mandato UPDATE DEVCLASS.

Especifique un valor de porcentaje de 20, 90 o 100. Un valor de 20% proporciona el tiempo de acceso más rápido y un valor de 100% proporciona la mayor capacidad de almacenamiento. Por ejemplo, si especifica una capacidad de escala de 20 para una clase de dispositivo 3592 sin compresión, un volumen 3592 en esa clase de dispositivo almacenaría el 20 por ciento de su capacidad total de 300 GB, cerca de 60 GB.

El valor de la capacidad de escala sólo entra en vigor cuando se graban por primera vez los datos en un volumen. Las actualizaciones de capacidad de escala realizadas en la clase de dispositivo no afectan a los volúmenes que ya tienen datos grabados hasta que el volumen vuelve a estar en estado reutilizable.

**Referencia relacionada:**

- [DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)

## Habilitación e inhabilitación de cifrado de unidad 3592 generación 2 y posterior

---

Con IBM Spectrum Protect, puede utilizar los siguientes tipos de cifrados de unidad con unidades que sean 3592 generación 2 y posterior: Aplicación, Sistema y Biblioteca. Estos métodos se definen mediante el hardware.

### Acerca de esta tarea

---

El parámetro DRIVEENCRYPTION del mandato DEFINE DEVCLASS especifica si se permite el cifrado de unidad para unidades que sean 3592 generación 2 y posterior. Utilice este parámetro para garantizar la compatibilidad de IBM Spectrum Protect con los ajustes de cifrado del hardware para volúmenes vacíos. No puede utilizar este parámetro para los volúmenes de agrupaciones de almacenamiento que estén llenos o se estén llenando.

- Para utilizar el método de aplicación en el que IBM Spectrum Protect genera y gestiona claves de cifrado, establezca el parámetro DRIVEENCRYPTION en ON. De esta forma, se habilita el cifrado de datos para volúmenes vacíos. Si el parámetro se establece en ON y el hardware está configurado para otro método de cifrado, las operaciones de copia de seguridad fallan.
- Para utilizar los métodos de cifrado de biblioteca o de sistema, establezca el parámetro en ALLOW. De esta manera, se especifica que IBM Spectrum Protect no es el gestor de claves del cifrado de unidad, aunque permitirá que el hardware cifre los datos del volumen mediante uno de los otros métodos. La especificación de este parámetro no implica un cifrado automático de los volúmenes. Los datos sólo se pueden cifrar especificando el parámetro ALLOW y configurando el hardware para que utilice uno de estos métodos.

El parámetro DRIVEENCRYPTION es opcional. El valor predeterminado es permitir los métodos de cifrado de biblioteca o de sistema.

### Procedimiento

---

En el siguiente ejemplo simplificado, se muestra cómo cifrar datos para volúmenes vacíos en una agrupación de almacenamiento utilizando IBM Spectrum Protect como gestor de claves:

1. Defina una biblioteca emitiendo el mandato DEFINE LIBRARY. Por ejemplo, emita el siguiente mandato:

```
define library 3584 libtype=SCSI
```

2. Defina una clase de dispositivos, 3592\_ENCRYPT emitiendo el mandato DEFINE DEVCLASS y especificando el valor ON para el parámetro DRIVEENCRYPTION. Por ejemplo, emita el siguiente mandato:

```
define devclass 3592_encrypt library=3584 devtype=3592 driveencryption=on
```

3. Defina una agrupación de almacenamiento. Por ejemplo, emita el siguiente mandato:

```
define stgpool 3592_encrypt_pool 3592_encrypt
```

### Qué hacer a continuación

---

Para inhabilitar cualquier método de cifrado en los volúmenes nuevos, establezca el parámetro DRIVEENCRYPTION en OFF. Si el hardware está configurado para cifrar los datos mediante el método de Biblioteca o el de Sistema y DRIVEENCRYPTION está establecido en OFF, las operaciones de copia de seguridad fallarán.

## Configuración de la compartición de bibliotecas

---

Varios servidores de IBM Spectrum Protect pueden compartir dispositivos de almacenamiento por medio de una red de área de almacenamiento (SAN). Se debe configurar un servidor como gestor de biblioteca y los demás servidores como clientes de biblioteca.

### Antes de empezar

---

Asegúrese de que los sistemas cumplen los requisitos de licencia para la compartición de bibliotecas. Se requiere una autorización para IBM Spectrum Protect for SAN para cada servidor de IBM Spectrum Protect que se configura como cliente de biblioteca o como gestor de biblioteca en un entorno SAN.

### Acerca de esta tarea

---

En el caso de movimiento de datos sin LAN, los sistemas cliente de IBM Spectrum Protect pueden acceder directamente a los dispositivos de almacenamiento definidos en el servidor de IBM Spectrum Protect. Los agentes de almacenamiento instalados y configurados en los sistemas cliente llevan a cabo el traspaso de datos.

Para configurar la compartición de bibliotecas, debe definir un servidor de IBM Spectrum Protect como gestor de biblioteca para la configuración de la biblioteca compartida. A continuación, debe definir otros servidores de IBM Spectrum Protect como clientes de biblioteca que se comunican y solicitan recursos de almacenamiento al gestor de biblioteca. El servidor de gestor de biblioteca debe tener la misma versión o posterior que el servidor o servidores que están definidos como clientes de biblioteca.

## Procedimiento

---

Para completar los pasos siguientes para compartir los recursos de biblioteca en una SAN entre servidores de IBM Spectrum Protect, complete los pasos siguientes:

1. Configurar comunicaciones entre servidores.

Para compartir un dispositivo de almacenamiento en una SAN, defina los servidores entre sí mediante la función de definición cruzada. Cada servidor debe tener un nombre exclusivo.

2. Defina una biblioteca compartida y configure dispositivos de cinta en los sistemas servidor.

Utilice el procedimiento que se describe en Configuración de bibliotecas para su uso por parte de un servidor para definir una biblioteca para utilizarla en el entorno compartido. Modifique el procedimiento para definir la biblioteca como compartida, especificando el parámetro SHARED=YES para el mandato DEFINE LIBRARY.

3. Defina el servidor de gestor de bibliotecas.
4. Defina la biblioteca compartida en el servidor que es la biblioteca.
5. Desde el servidor de gestor de bibliotecas, defina las vías de acceso del cliente de biblioteca a cada unidad a la que puede acceder el cliente de biblioteca. El nombre de dispositivo debe reflejar la forma en que el sistema cliente de biblioteca reconoce el dispositivo de cinta. Se debe definir una vía de acceso desde el gestor de biblioteca a cada una de las unidades de cinta para que el cliente de biblioteca utilice la unidad.



Para evitar problemas, asegúrese de que todas las definiciones de vías de acceso a unidades definidas para el gestor de biblioteca estén definidas también para el cliente de biblioteca.

Por ejemplo, si el gestor de biblioteca define tres unidades de cinta, el cliente de biblioteca también debe definir tres unidades de cinta. Para limitar el número de unidades de cinta que un cliente de biblioteca puede utilizar a la vez, utilice el parámetro MOUNTLIMIT de la clase de dispositivo en el cliente de biblioteca.






6. Defina las clases de dispositivo para la biblioteca compartida.

El método preferido es hacer que los nombres de clase de dispositivo sean iguales en ambos servidores para evitar confusiones al definir varias clases de dispositivo con el mismo tipo de dispositivo y los mismos parámetros de biblioteca. Algunas operaciones, como la copia de seguridad de base de datos, utilizan el nombre de clase de dispositivo para identificar los datos para la copia de seguridad.

Los parámetros de clase de dispositivo especificados en el gestor de biblioteca prevalecen sobre los parámetros especificados para el cliente de biblioteca. Si los nombres de clase de dispositivo son distintos, el gestor de biblioteca utiliza los parámetros especificados en una clase de dispositivo que coincida con el tipo de dispositivo especificado para el cliente de biblioteca.

7. Defina una agrupación de almacenamiento para la biblioteca compartida.
  8. Repita los pasos para configurar otro servidor como un cliente de biblioteca.
-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Compartir biblioteca para servidores AIX y Linux  
Para saber cómo configurar un entorno de compartición de bibliotecas SCSI para servidores que se ejecuten en sistemas AIX o Linux, revise el procedimiento de ejemplo.
  - Ejemplo: compartición de bibliotecas para servidores Windows  
Para conocer cómo configurar un entorno de compartición de bibliotecas para servidores que funcionen en sistemas Windows, revise el procedimiento de ejemplo.

### Referencia relacionada:

-  [DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)
-  [DEFINE LIBRARY \(Definir una biblioteca\)](#)
-  [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)
-  Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: Compartir biblioteca para servidores AIX y Linux

---

Para saber cómo configurar un entorno de compartición de bibliotecas SCSI para servidores que se ejecuten en sistemas AIX o Linux, revise el procedimiento de ejemplo.

## Acerca de esta tarea

---

En este ejemplo, se va a configurar un servidor de gestor de bibliotecas denominado ASTRO y un cliente de biblioteca denominado JUDY. Para ayudar a aclarar donde se realiza cada uno de los pasos, los mandatos van precedidos por el nombre de servidor desde el que se emite el mandato. La mayoría de los mandatos se emiten desde el cliente de biblioteca.

En las bibliotecas SCSI, puede definir la biblioteca especificando el parámetro `libtype=scsi`.

## Procedimiento

---

1. Para configurar ASTRO como el servidor de gestor de bibliotecas, defina una biblioteca de SCSI compartida denominada SANGROUP. Por ejemplo:

```
astro> define library sangroup libtype=scsi shared=yes
```

A continuación, complete el resto de los pasos como se describe en Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad para configurar la biblioteca.

Consejo: Puede utilizar el mandato `PERFORM LIBACTION` para definir unidades y vías de acceso para una biblioteca en un paso.

2. Defina ASTRO como servidor de gestor de bibliotecas emitiendo el mandato `DEFINE SERVER`.


```
judy> define server astro serverpassword=secret hladdress=192.0.2.24  
lladdress=1777 crossdefine=yes
```

3. Defina la biblioteca compartida SANGROUP emitiendo el mandato `DEFINE LIBRARY`. Debe utilizar el nombre del servidor de gestor de bibliotecas en el parámetro `PRIMARYLIBMANAGER` y, después, utilizar `LIBTYPE=SHARED`.

```
judy> define library sangroup libtype=shared primarylibmanager=astro
```

Asegúrese de que el nombre de biblioteca concuerde con el nombre de biblioteca en el gestor de biblioteca.

4. Defina las vías de acceso desde el gestor de biblioteca, ASTRO, a dos unidades de la biblioteca compartida emitiendo el mandato `DEFINE PATH`.

 Sistemas operativos AIX

```
astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/rmt6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/rmt7
```

 Sistemas operativos Linux

```
astro> define path judy drivea srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape6  
astro> define path judy driveb srctype=server desttype=drive  
library=sangroup device=/dev/IBMtape7
```

5. Defina todas las clases de dispositivo que están asociadas a la biblioteca compartida.  Sistemas operativos AIX

```
judy> define devclass tape library=sangroup devtype=lto
```

 Sistemas operativos Linux

```
judy> define devclass tape library=sangroup devtype=lto
```

Los siguientes parámetros de la definición de clase de dispositivo deben ser los mismos en el cliente de biblioteca y el gestor de biblioteca:

- o LIBRARY
- o DRIVEENCRYPTION
- o WORM
- o FORMAT

6. Defina una agrupación de almacenamiento denominada BACKTAPE que utilizará la biblioteca compartida. Emita el mandato `DEFINE STGPOOL`.







```
judy> define stgpool backtape tape maxscratch=50
```

## Qué hacer a continuación

---

Repita el procedimiento para definir más clientes de biblioteca para el gestor de biblioteca.

**Referencia relacionada:**

-  DEFINE DEVCLASS (Definir una clase de dispositivo)
-  DEFINE DRIVE (Definir una unidad en una biblioteca)
-  DEFINE LIBRARY (Definir una biblioteca)
-  DEFINE PATH (Definir una vía de acceso)
-  DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)
-  Sistemas operativos Windows

## Ejemplo: compartición de bibliotecas para servidores Windows

---



Para conocer cómo configurar un entorno de compartición de bibliotecas para servidores que funcionen en sistemas Windows, revise el procedimiento de ejemplo.

### Acerca de esta tarea

---

En este ejemplo, se va a configurar un servidor de gestor de bibliotecas denominado ASTRO y un cliente de biblioteca denominado JUDY.

En las bibliotecas SCSI, puede definir la biblioteca especificando el parámetro `libtype=scsi`.

-  Sistemas operativos Windows Configuración del servidor gestor de bibliotecas  
Debe configurar el servidor gestor de bibliotecas con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN.
-  Sistemas operativos Windows Configuración de los servidores cliente de biblioteca  
Debe configurar uno o varios servidores de cliente de biblioteca con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN..

 Sistemas operativos Windows

## Configuración del servidor gestor de bibliotecas

---

Debe configurar el servidor gestor de bibliotecas con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN.

### Procedimiento

---

El procedimiento siguiente es un ejemplo de cómo configurar un servidor de IBM Spectrum Protect denominado ASTRO como gestor de bibliotecas.

1. Asegúrese de que el servidor gestor de bibliotecas se está ejecutando:
  - a. Inicie Windows Services Management Console (`services.msc`).
  - b. Seleccione el servicio. Por ejemplo, `TSM Server1`.
  - c. Si el servicio no está en ejecución, pulse con el botón derecho del ratón sobre el nombre del servicio y seleccione Iniciar.
2. Obtenga la información de biblioteca y de unidades del dispositivo de biblioteca compartida.
  - a. Ejecute el programa de utilidad `tsmdlst.exe`. Este programa de utilidad se encuentra en el directorio `\Program Files\Tivoli\TSM\server`.
3. Defina una biblioteca de tipo SCSI. Por ejemplo:

```
define library sangroup libtype=scsi shared=yes
```

En este ejemplo se utiliza el valor predeterminado para el número de serie de la biblioteca, es decir, el servidor obtiene el número de serie de la biblioteca en el momento en que se define la vía de acceso. Según las posibilidades de la biblioteca, es posible que el servidor no pueda detectar el número de serie automáticamente. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo.

4. Defina la vía de acceso desde el servidor hasta la biblioteca.

```
define path astro sangroup srctype=server desttype=library  
device=lb0.0.0.2
```

Si no ha especificado el número de serie al definir la biblioteca, el servidor consulta ahora la biblioteca para obtener esta información. Si ha especificado el número de serie al definir la biblioteca, el servidor verifica la información definida y emite un mensaje si hay una discrepancia.

5. Defina las unidades en la biblioteca.

```
define drive sangroup drivea
define drive sangroup driveb
```

En este ejemplo se utiliza el valor predeterminado del número de serie de la unidad, que permite al servidor obtener el número de serie de la propia unidad en el momento en que se define la vía de acceso. Según las posibilidades de la unidad, es posible que el servidor no pueda detectar automáticamente el número de serie. En ese caso, el servidor no registra un número de serie para el dispositivo y no puede confirmar la identidad del dispositivo cuando se define la vía de acceso o cuando el servidor utiliza el dispositivo.

En este ejemplo también se utiliza el valor predeterminado de la dirección de elemento de la unidad, que permite al servidor obtener el número de elemento de la propia unidad en el momento en que se define la vía de acceso.

La dirección de elemento es un número que indica la ubicación física de una unidad en una biblioteca automatizada. El servidor necesita la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Puede hacer que el servidor obtenga el número de elemento de la propia unidad en el momento en que se define la vía de acceso o puede especificar el número de elemento al definir la unidad.

Según las capacidades de la biblioteca, es posible que el servidor no pueda detectar automáticamente la dirección de elemento. En ese caso, deberá proporcionar la dirección de elemento al definir la unidad. Los números de elemento de muchas bibliotecas están disponibles en IBM® Support Portal for IBM Spectrum Protect.

6. Defina la vía de acceso desde el servidor a cada una de las unidades.

```
define path astro drivea srctype=server desttype=drive library=sangroup
device=mt0.1.0.2
define path astro driveb srctype=server desttype=drive library=sangroup
device=mt0.2.0.2
```

Si no ha especificado el número de serie o la dirección de elemento al definir la unidad, el servidor consulta ahora la unidad o biblioteca para obtener esta información.

7. Defina al menos una clase de dispositivo.

```
define devclass tape devtype=dlt library=sangroup
```








8. Dé de alta el inventario de biblioteca. En el ejemplo siguiente se incorporan todos los volúmenes del inventario de la biblioteca como volúmenes reutilizables. El servidor utiliza el nombre que hay en la etiqueta de código de barras como nombre del volumen.

```
checkin libvolume sangroup search=yes status=scratch
checklabel=barcode
```

9. Defina una agrupación de almacenamiento para la biblioteca compartida con un máximo de 50 volúmenes reutilizables.

```
define stgpool backtape tape
description='storage pool for shared sangroup' maxscratch=50
```

#### Referencia relacionada:

-  [CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)
-  [DEFINE DEVCLASS \(Definir una clase de dispositivo\)](#)
-  [DEFINE DRIVE \(Definir una unidad en una biblioteca\)](#)
-  [DEFINE LIBRARY \(Definir una biblioteca\)](#)
-  [DEFINE PATH \(Definir una vía de acceso\)](#)
-  [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)
-  [Sistemas operativos Windows](#)

## Configuración de los servidores cliente de biblioteca

---

Debe configurar uno o varios servidores de cliente de biblioteca con el fin de configurar los servidores de IBM Spectrum Protect para que compartan dispositivos conectados a SAN..

### Antes de empezar

---

Asegúrese de que hay un servidor gestor de biblioteca definido.

### Acerca de esta tarea

---



Debe definir el servidor gestor de biblioteca. Utilice el procedimiento siguiente como ejemplo de cómo configurar un servidor de IBM Spectrum Protect denominado JUDY como cliente de biblioteca.

## Procedimiento

---

1. Asegúrese de que el servidor gestor de biblioteca se está ejecutando:
  - a. Inicie Windows Services Management Console (services.msc).
  - b. Seleccione el servicio. Por ejemplo, TSM Server1.
  - c. Si el servicio no está en ejecución, pulse con el botón derecho del ratón y seleccione Start.
2. Obtenga la información de biblioteca y de unidades del dispositivo de biblioteca compartida.
  - a. Ejecute el programa de utilidad `tsmdlst.exe`. Este programa de utilidad se encuentra en el directorio `\Program Files\Tivoli\TSM\server`.
3. Defina la biblioteca compartida, SANGROUP e identifique el gestor de biblioteca. Asegúrese de que el nombre de biblioteca concuerde con el nombre de biblioteca en el gestor de biblioteca.

```
define library sangroup libtype=shared primarylibmanager=astro
```

4. Defina las vías de acceso desde el servidor cliente de biblioteca hasta cada unidades emitiendo mandatos en el cliente de administración:

```
define path judy drivea srctype=server desttype=drive library=sangroup  
device=mt0.1.0.3  
define path judy driveb srctype=server desttype=drive library=sangroup  
device=mt0.2.0.3
```

5. Defina al menos una clase de dispositivo emitiendo mandatos desde el cliente de biblioteca:

```
define devclass tape devtype=dlt mountretention=1 mountwait=10  
library=sangroup
```

Establezca igual los parámetros para la clase de dispositivo en el cliente de biblioteca que en el gestor de biblioteca. También es recomendable que los nombres de clase de dispositivo sean iguales en ambos servidores, aunque no es obligatorio.

Los parámetros de clase de dispositivo especificados en el servidor gestor de biblioteca prevalecen sobre los especificados para el cliente de biblioteca. Esto es así independientemente de que los nombres de clase de dispositivo sean iguales en ambos servidores. Si los nombres de clase de dispositivo son distintos, el gestor de biblioteca utiliza los parámetros especificados en una clase de dispositivo que coincida con el tipo de dispositivo especificado para el cliente de biblioteca.

Si un cliente de biblioteca requiere un parámetro distinto del que se ha especificado en la clase de dispositivo del gestor de biblioteca (por ejemplo un límite de montaje distinto), siga los pasos siguientes:

- a. Cree una clase de dispositivo adicional en el servidor gestor de biblioteca. Especifique los valores de los parámetros que desea que utilice el cliente de biblioteca.
  - b. Cree una clase de dispositivo en el cliente de biblioteca con el mismo nombre y tipo de dispositivo que la nueva clase de dispositivo que ha creado en el servidor de biblioteca.
6. Defina la agrupación de almacenamiento, BACKTAPE, que utilizará la biblioteca compartida:

```
define stgpool backtape tape  
description='storage pool for shared sangroup' maxscratch=50
```

7. Repita este procedimiento para definir servidores adicionales como clientes de biblioteca.

### Referencia relacionada:

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ DEFINE LIBRARY (Definir una biblioteca)
- ➔ DEFINE PATH (Definir una vía de acceso)
- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Configuración de una jerarquía de agrupaciones de almacenamiento

---

Como parte del proceso de implementación, debe configurar una jerarquía de agrupación de almacenamiento. Configure al menos una agrupación de almacenamiento primario en el disco y una agrupación de almacenamiento primario en la cinta. Asegúrese de que los datos se migren de disco a cinta cada día.

### Antes de empezar

---

1. Asegúrese de revisar la información de Planificación de la jerarquía de agrupaciones de almacenamiento.

2. Asegúrese de que estén especificadas las reglas adecuadas, también conocidas como *políticas*, para realizar la copia de seguridad de los datos de cliente. Siga las instrucciones que encontrará en Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Asegúrese de que esté asignada una política a cada nodo. Para obtener instrucciones sobre cómo asignar una política cuando registra un nodo, consulte Registro de clientes.

## Procedimiento

---

Para configurar una jerarquía de agrupación de almacenamiento, complete los siguientes pasos:

1. Defina una agrupación de almacenamiento primario para el dispositivo de cinta emitiendo el mandato DEFINE STGPOOL.

Por ejemplo, defina una agrupación de almacenamiento primario, TAPE1, con una clase de dispositivo de LTO, y habilite la proximidad de grupo. Establezca el número máximo de volúmenes reutilizables que el servidor puede solicitar para esta agrupación de almacenamiento a 999. Emita el mandato siguiente:

```
define stgpool tape1 lto pooltype=primary collocate=group
maxscratch=999
```

2. Defina las unidades, vías de acceso y bibliotecas para la agrupación de almacenamiento primario en la cinta. Siga las instrucciones de Definición de dispositivos de cinta.
3. Defina una agrupación de almacenamiento primario para el dispositivo de disco emitiendo el mandato DEFINE STGPOOL.

Por ejemplo, defina una agrupación de almacenamiento, DISK1, con una clase de dispositivo de FILE. Asegúrese de que los datos se puedan migrar a la agrupación de almacenamiento de cinta, TAPE1, pero impida la migración automática especificando 100 para el parámetro HIGHMIG y 0 para el parámetro LOWMIG. Impida la reclamación especificando 100 para el parámetro RECLAIM. Habilite la proximidad de nodo. Establezca el número máximo de volúmenes reutilizables que el servidor puede solicitar para esta agrupación de almacenamiento en 9999. Utilice el parámetro MIGPROCESS para especificar el número de procesos de migración. El valor del parámetro MIGPROCESS debe ser igual al número de unidades en la biblioteca menos el número de unidades que se reservan para operaciones de restauración. Emita el mandato siguiente:

```
define stgpool disk1 file pooltype=primary nextstgpool=tape1
highmig=100 lowmig=0 reclaim=100 collocate=node maxscratch=9999 migprocess=5
```

Para obtener más información sobre cómo configurar la migración de disco a cinta, consulte Migración de agrupaciones de almacenamiento de disco.

## Qué hacer a continuación

---

Una jerarquía de agrupación de almacenamiento incluye solo agrupaciones de almacenamiento primario. Después de configurar la jerarquía de agrupación de almacenamiento, complete los pasos siguientes:

1. Cree una agrupación de almacenamiento de copias en un dispositivo de cinta. Para obtener instrucciones, consulte DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial).
2. Realice una copia de seguridad de la agrupación de almacenamiento primario en la agrupación de almacenamiento de copia utilizando el mandato BACKUP STGPOOL. Para obtener instrucciones, consulte BACKUP STGPOOL (Hacer copia de seguridad de los datos de la agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia).
3. Para asegurarse de que los datos se pueden recuperar en un desastre, configure un procedimiento para mover los volúmenes de cinta desde la agrupación de almacenamiento de copia a una ubicación fuera del local. Para obtener instrucciones, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.

### Referencia relacionada:

- [CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)
- [DEFINE STGPOOL \(Definir un volumen en una agrupación de almacenamiento\)](#)

## Protección de aplicaciones, máquinas virtuales y sistemas

---

El servidor protege los datos para los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas.

- Adición de clientes  
Tras la configuración correcta del servidor de IBM Spectrum Protect, instale y configure el software de cliente para empezar a realizar la copia de seguridad de los datos.

## Configuración del movimiento de datos sin LAN


---

Puede configurar el cliente y el servidor de IBM Spectrum Protect de forma que el cliente, a través de un agente de almacenamiento, pueda mover datos directamente al almacenamiento en una SAN. Esta función, denominada movimiento de datos sin LAN, se proporciona en el producto IBM Spectrum Protect for SAN.

## Procedimiento

---

Para configurar el movimiento de datos sin LAN, complete los pasos siguientes. Para obtener información detallada al respecto, consulte la documentación de IBM Spectrum Protect for SAN.

1. Verifique la conexión de red.
2. Establezca comunicaciones entre el cliente, el agente de almacenamiento y el servidor.
3. Instale y configure el software en los sistemas cliente.
4. Configure dispositivos en el servidor a los que pueda acceder el agente de almacenamiento.
5. Configure políticas de IBM Spectrum Protect para el movimiento de datos sin LAN para el cliente.
6. Si utiliza almacenamiento FILE compartido, instale y configure IBM® TotalStorage SAN File System o IBM Spectrum Scale.  
 **Sistemas operativos Windows** Restricción: Si un volumen de IBM Spectrum Scale está formateado por un servidor AIX, el sistema Windows utiliza TCP/IP para transferir datos en lugar de la red de área de almacenamiento.
7. Defina vías de acceso desde el agente de almacenamiento hasta las unidades.
8. Inicie el agente de almacenamiento y verifique la configuración fuera de la LAN.

## Qué hacer a continuación

---

Para ajustar mejor el uso de los recursos de la LAN y la SAN, puede controlar la vía de acceso que siguen las transferencias de datos en el caso de los clientes que disponen de la función de movimiento de datos sin LAN. Controle la vía de acceso utilizando el mandato UPDATE NODE. Para cada cliente, puede seleccionar uno de los valores siguientes para las operaciones de lectura y grabación de datos. Especifique operaciones de lectura de datos utilizando el parámetro DATAREADPATH y operaciones de grabación utilizando el parámetro DATAWRITEPATH. El parámetro es opcional. El valor predeterminado es ANY.

LAN (solo vía de acceso LAN)

Especifique el valor de LAN si se cumple alguna de las siguientes condiciones:

- Si desea hacer copias de seguridad o restaurar una pequeña cantidad de datos.
- El cliente no tiene conectividad SAN.

LANFREE (solo vía de acceso sin LAN)

Especifique el valor LANFREE si el cliente y el servidor están en la misma SAN, y se cumple cualquiera de las siguientes condiciones:

- Si desea hacer copias de seguridad o restaurar una gran cantidad de datos.
- Desea descargar la carga de procesamiento del servidor en el cliente.
- Desea liberar la congestión de LAN.

ANY (cualquier vía de acceso disponible)

Se utiliza una vía de acceso fuera de la LAN si hay alguna disponible. Si no hay ninguna vía de acceso fuera de la LAN disponible, los datos se mueven mediante la LAN.

- Validación de la configuración fuera de la LAN  
Después de configurar un cliente de IBM Spectrum Protect para el movimiento de datos sin LAN, puede verificar la configuración y las definiciones de servidores con el mandato VALIDATE LANFREE.

## Métodos de cifrado de cinta

---

Decidir que método de cifrado utilizar depende de cómo quiera gestionar sus datos.

Es muy importante proteger los datos de cliente, especialmente si son datos confidenciales. Para garantizar la protección de los volúmenes dentro y fuera del local, está disponible la tecnología de cifrado de cinta de IBM.

La tecnología de cinta de IBM da soporte a distintos métodos de cifrado de unidades para los siguientes dispositivos:

- IBM 3592 generación 2 y generación 3
- IBM Linear Tape-Open (LTO) generación 4 y generación 5

Los métodos de cifrado de unidad que puede utilizar con IBM Spectrum Protect se configuran en el nivel del hardware. IBM Spectrum Protect no puede controlar ni cambiar qué método de cifrado se utiliza en la configuración del hardware. Si el hardware está configurado para el método Aplicación, IBM Spectrum Protect puede activar o desactivar el cifrado en función del valor de DRIVEENCRYPTION en la clase de dispositivo.

Para cifrar todos los datos de una determinada biblioteca lógica o para cifrar los datos en más que sólo volúmenes de agrupación de almacenamiento, utilice el método Sistema o Biblioteca. Si el gestor de claves de cifrado está configurado para compartir claves, los métodos Biblioteca y Sistema pueden compartir la clave de cifrado, lo que permite intercambiar los dos métodos. IBM Spectrum Protect no puede compartir o utilizar las claves de cifrado entre el método Aplicación y los métodos Sistema o Biblioteca del cifrado.

Tabla 1. Métodos de cifrado

Método de cifrado	Descripción
Cifrado de aplicación	<p>Con el cifrado gestionado por aplicación, puede crear agrupaciones de almacenamiento dedicado que contengan solo volúmenes cifrados. De esta forma, podrá utilizar jerarquías de agrupaciones de almacenamiento y políticas para gestionar la forma de cifrar los datos.</p> <p>La aplicación, en este caso IBM Spectrum Protect, gestiona las claves de cifrado. IBM Spectrum Protect genera y almacena las claves en la base de datos del servidor. Los datos se cifran durante las operaciones de grabación, cuando la clave de cifrado se pasa del servidor a la unidad. Los datos se descifran para las operaciones de lectura.</p> <p>Para cifrar volúmenes de agrupación de almacenamiento y eliminar parte del procesamiento de cifrado en su sistema, habilite el método Aplicación. Utilice el cifrado gestionado por aplicación solo para volúmenes de agrupaciones de almacenamiento. Otros volúmenes, como las cintas de conjunto de copias de seguridad, los volúmenes de exportación y las copias de seguridad de bases de datos, no se cifran utilizando el método Aplicación.</p> <p>Requisito: Cuando se habilita el cifrado de aplicaciones, preste especial atención para proteger las copias de seguridad de las bases de datos porque las claves de cifrado que se utilizan para cifrar y descifrar datos se almacenan en la base de datos del servidor. Para restaurar los datos, debe tener la copia de seguridad de la base de datos correcta y las claves de cifrado correspondientes para acceder a la información. Asegúrese de hacer una copia de seguridad periódica de la base de datos y de salvaguardar las copias de seguridad para evitar su pérdida o sustracción. Cualquier persona que tenga acceso a la copia de seguridad y la base de datos y a las claves de cifrado tendrá acceso a sus datos.</p>
Cifrado de bibliotecas	<p>Con el cifrado gestionado por la biblioteca, puede controlar qué volúmenes se cifran utilizando sus números de serie. Puede especificar el rango o el conjunto de volúmenes que desea cifrar.</p> <p>Las claves de cifrado se gestionan mediante la biblioteca. Las claves se almacenan en un gestor de claves de cifrado y se proporcionan a la unidad. Si configura el hardware para utilizar el cifrado gestionado por la biblioteca, puede utilizar este método emitiendo el mandato DEFINE DEVCLASS y especificando el parámetro DRIVEENCRYPTION=ALLOW.</p> <p>Restricción: Solo determinadas bibliotecas de IBM dan soporte a IBM LTO-4 y cifrado posterior. Para obtener información detallada al respecto, consulte el apartado Configuración del cifrado de unidades de cinta.</p>
Cifrado de sistemas	<p>El cifrado gestionado por el sistema está disponible solo en el sistema operativo AIX®. El sistema operativo o el controlador de dispositivo gestiona las claves de cifrado que se proporcionan, y que se almacenan en un gestor de claves de cifrado. Si se configura el hardware para utilizar el cifrado de sistemas, puede utilizar este método emitiendo el mandato DEFINE DEVCLASS y especificando el parámetro DRIVEENCRYPTION=ALLOW.</p>



Para determinar si un volumen se cifra y qué método se ha utilizado, emita el mandato QUERY VOLUME y especifique el parámetro FORMAT=DETAILED.

- Configuración del cifrado de unidades de cinta  
Puede utilizar el cifrado de unidades para proteger cintas que contienen datos esenciales o confidenciales, por ejemplo, cintas que contengan información financiera confidencial. El cifrado de unidades puede ser útil al trasladar cintas del entorno de servidor de IBM Spectrum Protect a una ubicación externa o interna.

## Control de las operaciones de control de cintas

---

Las definiciones de clase de dispositivo para cintas incluyen parámetros que permiten controlar las operaciones de almacenamiento.

- Cómo rellena volúmenes IBM Spectrum Protect  
El mandato DEFINE DEVCLASS tiene un parámetro ESTCAPACITY opcional que indica la capacidad estimada de los volúmenes secuenciales asociados a la clase de dispositivo. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado utilizado.
- Especificar la capacidad estimada de los volúmenes de cinta  
IBM Spectrum Protect también utiliza la capacidad estimada para determinar cuándo empezar la reclamación de volúmenes de agrupación de almacenamiento.
- Especificación de formatos de grabación para soportes de cinta  
Puede especificar el formato de grabación utilizado por IBM Spectrum Protect para grabar datos en soportes de cinta. Si tiene previsto combinar generaciones de unidades, o distintos tipos de unidades, en una biblioteca, debe especificar un formato de registro para cada generación de unidad y cada tipo de unidad. De esta forma, el servidor puede diferenciar entre generaciones de unidades y tipos de unidad.
- Asociar objetos de biblioteca con clases de dispositivo  
Una biblioteca contiene las unidades que se pueden utilizar para montar un volumen. Sólo se puede asociar una biblioteca a una clase de dispositivo. Sin embargo, varias clases de dispositivo pueden hacer referencia a la misma biblioteca.
- Control de las operaciones de montaje de medios para dispositivos de cinta  
Utilizando definiciones de clases de dispositivo, puede controlar el número de volúmenes montados, el tiempo que un volumen está montado y el tiempo que el servidor de IBM Spectrum Protect espera a que haya una unidad disponible.
- Operaciones de preferencia  
El servidor puede preferir las operaciones de cliente o servidor en el caso de una operación de prioridad superior cuando se está utilizando un punto de montaje y no hay otros disponibles o cuando se necesita acceder a un volumen específico. Cuando se prefiere una operación, se cancela.
- Influencia de los cambios de dispositivo en la SAN  
El entorno SAN puede modificarse considerablemente debido a los cambios en el dispositivo o en el cableado. La naturaleza dinámica de la SAN puede hacer que las definiciones estáticas fallen o se vuelvan imprevisibles.
-  Sistemas operativos Windows Visualización de la información de dispositivos  
Puede visualizar información sobre los dispositivos conectados al servidor mediante el programa de utilidad de información de dispositivos (tsmdlst).
- Medios de cinta Grabar una vez leer varias  
Los soportes de cinta WORM (Grabar una vez leer varias) ayudan a evitar la supresión accidental o deliberada de datos fundamentales. Sin embargo, IBM Spectrum Protect impone ciertas restricciones y pautas a seguir cuando se utiliza el soporte de tipo Grabar una vez leer varias (WORM).
-  Sistemas operativos Windows Resolución de problemas con dispositivos  
Puede resolver errores que se producen cuando configura o usa dispositivos con IBM Spectrum Protect.

## Cómo rellena volúmenes IBM Spectrum Protect

---

El mandato DEFINE DEVCLASS tiene un parámetro ESTCAPACITY opcional que indica la capacidad estimada de los volúmenes secuenciales asociados a la clase de dispositivo. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado utilizado.

Si no se especifica el parámetro ESTCAPACITY, IBM Spectrum Protect utiliza un valor predeterminado en base al formato de grabación que se ha especificado para la clase de dispositivo utilizando el parámetro FORMAT.

Si especifica una capacidad estimada que excede la capacidad real del volumen de la clase de dispositivo, IBM Spectrum Protect actualiza la capacidad estimada del volumen cuando éste se llena. Cuando IBM Spectrum Protect alcanza el final del volumen, actualiza la capacidad según la cantidad de datos que se han grabado en el volumen.

Puede aceptar la capacidad estimada predeterminada de una clase de dispositivo determinada o especificar explícitamente una capacidad estimada. No es obligatorio que el valor de capacidad estimada sea exacto, pero resulta útil. IBM Spectrum Protect utiliza la capacidad estimada de los volúmenes para determinar la capacidad estimada de una agrupación de almacenamiento y el porcentaje estimado que se utiliza. Puede que desee cambiar la capacidad estimada si se cumple una o las dos condiciones siguientes:

- La capacidad estimada predeterminada es inexacta debido a la compresión de datos.
- Tiene volúmenes de tamaño no estándar.

**Referencia relacionada:**

- DEFINE DEVCLASS (Definir una clase de dispositivo)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Especificar la capacidad estimada de los volúmenes de cinta

---

IBM Spectrum Protect también utiliza la capacidad estimada para determinar cuándo empezar la reclamación de volúmenes de agrupación de almacenamiento.

### Acerca de esta tarea

---

Para las clases de dispositivo de cinta, los valores predeterminados seleccionados por el servidor dependen del formato de grabación que se utiliza para grabar datos en el volumen. Puede aceptar el valor predeterminado para un tipo de dispositivo o especificar un valor.

Para especificar la capacidad estimada para los volúmenes de cinta, utilice el parámetro ESTCAPACITY cuando defina la clase de dispositivo o actualice su definición.

**Referencia relacionada:**

- DEFINE DEVCLASS (Definir una clase de dispositivo)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Especificación de formatos de grabación para soportes de cinta

---

Puede especificar el formato de grabación utilizado por IBM Spectrum Protect para grabar datos en soportes de cinta. Si tiene previsto combinar generaciones de unidades, o distintos tipos de unidades, en una biblioteca, debe especificar un formato de registro para cada generación de unidad y cada tipo de unidad. De esta forma, el servidor puede diferenciar entre generaciones de unidades y tipos de unidad.

### Acerca de esta tarea

---

Para especificar un formato de grabación, utilice el parámetro FORMAT al definir la clase de dispositivo o actualizar su definición.

Si todas las unidades asociadas con esa clase de dispositivo son idénticas, especifique FORMAT=DRIVE. El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen.

Si algunas unidades asociadas con una clase de dispositivo admiten un formato de densidad superior a otras, especifique un formato que sea compatible con todas las unidades.

Si las unidades de una biblioteca SCSI utilizan diferentes tecnologías de cinta (por ejemplo, DLT y LTO Ultrium), especifique un valor único para el parámetro FORMAT en cada definición de clase de dispositivo.

Para ver un ejemplo de configuración, consulte el apartado Ejemplo: Configurar una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad.

El formato de grabación que el servidor utiliza para un volumen se selecciona cuando se graban datos por primera vez en el volumen. La actualización del parámetro FORMAT no afecta a los medios que ya contienen datos hasta que dichos medios vuelven a grabarse desde el principio. Este proceso puede suceder tras reclamar o suprimir un volumen o una vez hayan caducado todos los datos del volumen.

**Referencia relacionada:**

- DEFINE DEVCLASS (Definir una clase de dispositivo)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Asociar objetos de biblioteca con clases de dispositivo

---

Una biblioteca contiene las unidades que se pueden utilizar para montar un volumen. Sólo se puede asociar una biblioteca a una clase de dispositivo. Sin embargo, varias clases de dispositivo pueden hacer referencia a la misma biblioteca.

### Acerca de esta tarea

---

Para asociar una clase de dispositivo a una biblioteca, utilice el parámetro LIBRARY cuando defina una clase de dispositivo o actualice su definición.

**Referencia relacionada:**

- ➡ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➡ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Control de las operaciones de montaje de medios para dispositivos de cinta

---

Utilizando definiciones de clases de dispositivo, puede controlar el número de volúmenes montados, el tiempo que un volumen está montado y el tiempo que el servidor de IBM Spectrum Protect espera a que haya una unidad disponible.

- Control del número de volúmenes montados simultáneamente  
Al establecer un límite de montaje para una clase de dispositivo, debe tener en cuenta el número de dispositivos de almacenamiento conectados al sistema. También debe tener en cuenta si va a utilizar la función de grabación simultánea, si asocia varias clases de dispositivo a una única biblioteca y el número de procesos que se ejecutan al mismo tiempo.
- Control de la cantidad de tiempo que un volumen permanece montado  
Puede controlar la cantidad de tiempo que un volumen permanece montado después de que haya tenido lugar la última actividad de E/S. Si hay un volumen que se utiliza con frecuencia, el rendimiento se puede mejorar estableciendo un período mayor de retención de montaje para evitar las operaciones innecesarias de montaje y desmontaje.
- Control de la cantidad de tiempo que un servidor espera una unidad  
Puede especificar el tiempo máximo, en minutos, que el servidor de IBM Spectrum Protect esperará hasta que haya una unidad disponible para la solicitud de montaje actual.

## Control del número de volúmenes montados simultáneamente

---

Al establecer un límite de montaje para una clase de dispositivo, debe tener en cuenta el número de dispositivos de almacenamiento conectados al sistema. También debe tener en cuenta si va a utilizar la función de grabación simultánea, si asocia varias clases de dispositivo a una única biblioteca y el número de procesos que se ejecutan al mismo tiempo.

### Acerca de esta tarea

---

Al seleccionar un límite de montaje para una clase de dispositivo, tenga en cuenta las siguientes cuestiones:

- ¿Cuántos dispositivos de almacenamiento están conectados al sistema?

No especifique un valor de límite de montaje superior al número de unidades asociadas disponibles que hay en la instalación. Si el servidor intenta montar tantos volúmenes como especifica el límite de montaje y no hay unidades disponibles para el volumen necesario, se produce un error y las sesiones de clientes pueden finalizar. (Esta restricción no se aplica cuando se especifica el parámetro DRIVES.)

Si comparte los recursos de la biblioteca en un SAN entre servidores IBM Spectrum Protect, debe limitar el número de unidades de cinta que un cliente de biblioteca puede utilizar a la vez. Para permitir que varios servidores de cliente de biblioteca utilicen una biblioteca de forma simultánea, especifique el parámetro MOUNTLIMIT al definir o actualizar la clase de dispositivo en el cliente de biblioteca. Para obtener más información sobre cómo configurar el uso compartido de la biblioteca, consulte Configuración de la compartición de bibliotecas.

- ¿Está utilizando la función de grabación simultánea para las agrupaciones de almacenamiento primarias, las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos?

Especifique un valor de límite de montaje que proporcione un número suficiente de puntos de montaje para dar soporte a la grabación simultánea de datos en la agrupación de almacenamiento primaria y en todas las agrupaciones de almacenamiento de copia asociadas y de datos activos.

- ¿Está asociando varias clases de dispositivo a una sola biblioteca?

Una clase de dispositivo asociada con una biblioteca puede utilizar cualquier unidad de la biblioteca que sea compatible con el tipo de dispositivo de esa clase. Puesto que se puede asociar más de una clase de dispositivo a una biblioteca, una misma unidad de la biblioteca podrá ser utilizada por más de una clase de dispositivo. IBM Spectrum Protect garantiza que dos operaciones no puedan utilizar la misma unidad simultáneamente utilizando dos clases de dispositivo diferentes.

- ¿Cuántos procesos de IBM Spectrum Protect quiere ejecutar al mismo tiempo, utilizando dispositivos en esta clase de dispositivo?

IBM Spectrum Protect cancela automáticamente algunos procesos para ejecutar otros procesos de prioridad superior. Si el servidor utiliza todas las unidades disponibles de una clase de dispositivo para realizar los procesos de prioridad superior, los procesos de prioridad inferior deben esperar hasta que queda disponible una unidad. Por ejemplo, IBM Spectrum Protect cancela el proceso para un cliente que realiza la copia de seguridad directamente en cinta si la unidad se necesita para un proceso de migración o de reclamación de cintas del servidor. IBM Spectrum Protect cancela un proceso de reclamación de cintas si la unidad se necesita para una operación de restauración de un cliente. Para obtener más información, consulte Operaciones de preferencia.

Si ocurre con frecuencia que unos procesos cancelan otros procesos, debe plantearse si puede hacer que haya más unidades disponibles para que IBM Spectrum Protect pueda utilizarlas. De lo contrario, revise la planificación de operaciones para reducir la posibilidad de colisiones al intentar obtener unidades.

Esta consideración también se aplica a la función de grabación simultánea. Para que la operación de grabación simultánea sea satisfactoria, debe haber suficientes unidades disponibles.

Para especificar el número máximo de volúmenes que pueden montarse simultáneamente, utilice el parámetro MOUNTLIMIT cuando defina la clase de dispositivo o actualice su definición.

**Referencia relacionada:**

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Control de la cantidad de tiempo que un volumen permanece montado

---

Puede controlar la cantidad de tiempo que un volumen permanece montado después de que haya tenido lugar la última actividad de E/S. Si hay un volumen que se utiliza con frecuencia, el rendimiento se puede mejorar estableciendo un período mayor de retención de montaje para evitar las operaciones innecesarias de montaje y desmontaje.

### Acerca de esta tarea

---

Si las operaciones de montaje se manejan mediante actividades manuales asistidas por el operador, puede que desee especificar un período de retención de montaje más largo. Por ejemplo, si únicamente un operador proporciona soporte para toda la operación de un fin de semana, defina un período de retención de montaje elevado para que no se le solicite al operador que monte volúmenes a cada momento.

Para controlar la cantidad de tiempo que un volumen permanece montado, utilice el parámetro MOUNTRETENTION cuando defina la clase de dispositivo o actualice su definición. Por ejemplo, si el valor de retención de montaje es 60, y el volumen montado permanece desocupado durante 60 minutos, el servidor desmonta el volumen.

Mientras IBM Spectrum Protect tiene un volumen montado, la unidad está asignada a IBM Spectrum Protect y no se puede utilizar para nada más. Si necesita liberar la unidad para otros usos, puede cancelar las operaciones de IBM Spectrum Protect que utilizan la unidad y, a continuación, desmontar el volumen. Por ejemplo, puede cancelar las operaciones de migración o de copia de seguridad del servidor. Para obtener información sobre cómo cancelar los procesos y desmontar volúmenes, consulte Gestión de solicitudes del servidor para los volúmenes.

**Referencia relacionada:**

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Control de la cantidad de tiempo que un servidor espera una unidad

---

Puede especificar el tiempo máximo, en minutos, que el servidor de IBM Spectrum Protect esperará hasta que haya una unidad disponible para la solicitud de montaje actual.

### Acerca de esta tarea

---

Para controlar el tiempo de espera hasta que una unidad esté disponible para una solicitud de montaje, utilice el parámetro MOUNTWAIT cuando defina o actualice una clase de dispositivo.

**Referencia relacionada:**

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)



## Operaciones de preferencia

---

El servidor puede preferir las operaciones de cliente o servidor en el caso de una operación de prioridad superior cuando se está utilizando un punto de montaje y no hay otros disponibles o cuando se necesita acceder a un volumen específico. Cuando se prefiere una operación, se cancela.

Puede utilizar el mandato QUERY MOUNT para ver el estado del volumen para el punto de montaje.

De forma predeterminada, la preferencia está habilitada en el servidor. Para inhabilitar la preferencia, especifique la opción NOPREEMPT en el archivo de opciones del servidor. Si especifica esta opción, el mandato BACKUP DB y los mandatos de exportación e importación son las únicas operaciones que pueden preferir otras operaciones.

- **Preferencia del punto de montaje**  
Si una operación de prioridad alta requiere un punto de montaje que está en una clase de dispositivo específica y todos los puntos de montaje de la clase de dispositivo están en uso, la operación de prioridad alta puede preferir un punto de montaje de una operación de prioridad más baja.
- **Preferencia de acceso a un volumen**  
Si una operación de prioridad alta requiere acceso a un volumen específico y ese volumen está en uso, la operación de prioridad alta puede adelantarse a la operación de prioridad más baja para ese volumen.

### Referencia relacionada:

- [BACKUP DB](#) (Hacer copia de seguridad de la base de datos)
- [QUERY MOUNT](#) (Visualizar información sobre volúmenes de acceso secuencial montados)

## Preferencia del punto de montaje

---

Si una operación de prioridad alta requiere un punto de montaje que está en una clase de dispositivo específica y todos los puntos de montaje de la clase de dispositivo están en uso, la operación de prioridad alta puede preferir un punto de montaje de una operación de prioridad más baja.

Los puntos de montaje pueden adelantarse sólo cuando la clase de dispositivo de la operación preferente y la operación que se está adelantando es la misma.

Las siguientes operaciones de alta prioridad pueden tener preferencia respecto a otras operaciones para un punto de montaje.

- Operaciones de copia de seguridad de base de datos
- Operaciones de recuperación o restauración de HSM iniciadas por clientes
- Operaciones de restauración utilizando un transportador de datos remoto
- Operaciones de exportación
- Operaciones de importación
- Operaciones para generar conjuntos de copias de seguridad

Las operaciones siguientes no pueden anticiparse a otras operaciones ni otras pueden adelantarlas:

- Auditar un volumen
- Restaurar datos de una agrupación de copias o datos activos
- Preparar un archivo de plan de recuperación
- Almacenar datos con un transportador de datos remoto

Las operaciones siguientes se pueden anticipar y aparecen listadas por orden de prioridad, de mayor a menor prioridad. El servidor selecciona la operación de prioridad más baja para adelantarse, por ejemplo, a la identificación de duplicados.

- Replicar nodos
- Hacer copia de seguridad de datos en una agrupación de almacenamiento de copias
- Copiar datos activos a una agrupación de datos activos
- Traspasar datos a un volumen de agrupación de almacenamiento
- Migrar datos de un disco a un soporte secuencial
- Migrar datos de un soporte secuencial a otro soporte secuencial
- Operaciones de recuperación o restauración de HSM inicializadas por clientes
- Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial
- Identificar duplicados

## Preferencia de acceso a un volumen

---

Si una operación de prioridad alta requiere acceso a un volumen específico y ese volumen está en uso, la operación de prioridad alta puede adelantarse a la operación de prioridad más baja para ese volumen.

Por ejemplo, si una solicitud de restauración tiene que acceder a un volumen que está utilizando un proceso de reclamación y hay disponible una unidad, se cancelará el proceso de reclamación.

Las siguientes operaciones de alta prioridad pueden tener preferencia respecto a otras operaciones de acceso a un volumen específico:

- Operaciones de copia de seguridad de base de datos
- Operaciones de recuperación o restauración de HSM iniciadas por clientes
- Operaciones de restauración utilizando un transportador de datos remoto
- Operaciones de exportación
- Operaciones de importación
- Operaciones para generar conjuntos de copias de seguridad

Las operaciones siguientes no pueden anticiparse a otras operaciones ni otras pueden adelantarlas en el orden de preferencia:

- Auditar volumen
- Restaurar datos de una agrupación de copias o datos activos
- Preparar un plan de recuperación
- Almacenar datos con un transportador de datos remoto

Las operaciones siguientes se pueden anticipar y aparecen listadas por orden de prioridad, de mayor a menor prioridad. El servidor selecciona la operación de prioridad más baja para adelantarse, por ejemplo, a la identificación de duplicados.

- Replicar nodos
- Hacer copia de seguridad de datos en una agrupación de almacenamiento de copias
- Copiar datos activos a una agrupación de datos activos
- Traspasar datos a un volumen de agrupación de almacenamiento
- Migrar datos de un disco a un soporte secuencial
- Migrar datos de un soporte secuencial a otro soporte secuencial
- Realizar copia de seguridad, archivado o migración de datos HSM iniciada por el cliente
- Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial
- Identificar duplicados

## Influencia de los cambios de dispositivo en la SAN

---

El entorno SAN puede modificarse considerablemente debido a los cambios en el dispositivo o en el cableado. La naturaleza dinámica de la SAN puede hacer que las definiciones estáticas fallen o se vuelvan imprevisibles.

Los ID de los dispositivos que SAN ha asignado y que conocen el servidor y el agente de almacenamiento se pueden alterar debido a los restablecimientos del bus o a otros cambios de entorno. Por ejemplo, es posible que el servidor conozca un dispositivo X como *rmt0* (en AIX), en base a la especificación de la vía de acceso original al servidor y la configuración original de la LAN. Sin embargo, algunos sucesos de la SAN, por ejemplo, la adición de un nuevo dispositivo Y, hace que el dispositivo X se asigne a *rmt1*. Cuando el servidor intenta acceder al dispositivo X utilizando *rmt0*, falla el acceso o bien accede al dispositivo de destino equivocado. El servidor intenta recuperarse de cambios en dispositivos en la SAN utilizando números de serie de dispositivo para confirmar la identidad de los dispositivos con los que establece contacto.

Al definir una unidad o biblioteca, tiene la opción de especificar el número de serie de ese dispositivo. Si no especifica el número de serie al definir el dispositivo, el servidor obtiene el número de serie al definir la vía de acceso para el dispositivo. En cualquier caso, el servidor tiene el número de serie de dispositivo en su base de datos y se puede utilizar para confirmar la identidad de un dispositivo para las operaciones.

Cuando el servidor utiliza unidades y bibliotecas en una SAN, el servidor intenta verificar que se utiliza el dispositivo correcto. El servidor establece contacto con el dispositivo utilizando el nombre de dispositivo en la vía de acceso que se ha definido para él. A continuación el servidor solicita el número de serie del dispositivo y lo compara con el que está almacenado en la base de datos del servidor para ese dispositivo.


Si el número de serie no coincide, el servidor inicia el proceso de detección en la SAN para intentar localizar el dispositivo con el número de serie coincidente. Si el servidor encuentra el dispositivo con el número de serie coincidente, corrige la definición de la vía de acceso en la base de datos del servidor actualizando el nombre de dispositivo de esa vía de acceso. El servidor emite un mensaje con información sobre el cambio efectuado en el dispositivo. El servidor no utiliza el dispositivo.

Para determinar si los cambios del dispositivo en la SAN afectan al servidor IBM Spectrum Protect, puede revisar el registro de actividad para obtener mensajes. Los siguientes mensajes están relacionados con números de serie:

- De ANR8952 a ANR8958

- De ANR8961 a ANR8968
- De ANR8974 a ANR8975

Restricción: Algunos dispositivos no tienen la posibilidad de informar de los números de serie a aplicaciones tales como el servidor de IBM Spectrum Protect. Si el servidor no puede obtener el número de serie de un dispositivo, el servidor no puede ayudar al sistema a recuperarse de un cambio de ubicación de dispositivo en la SAN.

 Sistemas operativos Windows

## Visualización de la información de dispositivos

---

Puede visualizar información sobre los dispositivos conectados al servidor mediante el programa de utilidad de información de dispositivos (tsmdlst).

### Antes de empezar

---



- Asegúrese de que la API HBA esté instalada. La API HBA es necesaria para ejecutar el programa de utilidad de información de dispositivos.
- Asegúrese de que el controlador de dispositivo de cinta esté instalado y configurado.

### Procedimiento

---

1. Desde un indicador de mandatos, vaya al subdirectorio `server` del directorio de instalación del servidor, por ejemplo, `C:\Program Files\Tivoli\TSM\server`.
2. Ejecute el archivo ejecutable `tsmdlst.exe`.

#### Referencia relacionada:

-  [QUERY SAN \(consultar los dispositivos de SAN\)](#)
-  [tsmdlst \(Visualizar la información sobre los dispositivos\)](#)

## Medios de cinta Grabar una vez leer varias

---

Los soportes de cinta WORM (Grabar una vez leer varias) ayudan a evitar la supresión accidental o deliberada de datos fundamentales. Sin embargo, IBM Spectrum Protect impone ciertas restricciones y pautas a seguir cuando se utiliza el soporte de tipo Grabar una vez leer varias (WORM).

Puede utilizar los siguientes tipos de medios WORM con IBM Spectrum Protect:

- IBM® 3592, todas las generaciones soportadas
- IBM LTO-3 y todas las generaciones soportadas
- HP LTO-3 y todas las generaciones soportadas
- Quantum LTO-3 y todas las generaciones soportadas
- Quantum SDLT 600, Quantum DLT V4 y Quantum DLT S4
- StorageTek VolSafe
- Sony AIT50 y AIT100

Sugerencias:

- Una agrupación de almacenamiento puede componerse de medios WORM o RW, pero no de ambos.
- Para evitar desperdiciar cinta después de una operación de restauración o importación, no utilice cintas WORM para operaciones de exportación o copia de seguridad de base de datos.
- Unidades preparadas para WORM  
Para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben estar habilitadas para WORM. Si se monta un cartucho WORM en una unidad de lectura/escritura (RW), el montaje dará error.
- Incorporación de medios WORM  
El tipo de los medios WORM determina si la etiqueta del medio debe ser leído durante la incorporación.
- Restricciones en los medios WORM  
No puede utilizar los medios WORM preetiquetados con la clase de dispositivo LTO ni ECARTRIDGE.
- Errores de montaje con medios WORM  
Si se cargan medios de cinta WORM en una unidad para un montaje de clase de dispositivo de lectura-grabación (RW), se producirá un error de montaje. De forma similar, si se cargan medios de cinta RW en una unidad para un montaje de clase de dispositivo WORM, el montaje fallará.
- Volver a etiquetar soportes WORM  
No puede volver a etiquetar un cartucho WORM si éste contiene datos. Esto es aplicable a cartuchos Sony AIT WORM, LTO

WORM, SDLT WORM, DLT WORM e IBM 3592. La etiqueta de un volumen VolSafe sólo se puede sobregabar una vez y únicamente si el volumen no contiene datos utilizables, suprimidos o caducados.

- Eliminar volúmenes WORM privados de una biblioteca  
Si lleva a cabo alguna acción en un volumen WORM (por ejemplo, si suprime espacios de archivos) y el servidor no marca el volumen como lleno, el volumen vuelve al estado de reutilizable. Si un volumen WORM no se marca como lleno y se suprime de una agrupación de almacenamiento, el volumen permanecerá privado. Para suprimir un volumen WORM privado de una biblioteca, debe emitir el mandato CHECKOUT LIBVOLUME.
- Creación de volúmenes DLT WORM  
Los volúmenes DLT WORM se pueden convertir desde volúmenes de lectura-grabación (RW).
- Soporte para cintas 3592 WORM cortas y normales  
IBM Spectrum Protect admite cintas 3592 WORM cortas y normales. Para obtener los mejores resultados, defínalas en agrupaciones de almacenamiento distintas.
- Consultar a una clase de dispositivo el valor del parámetro WORM  
Puede determinar el valor del parámetro WORM en una clase de dispositivo utilizando el mandato QUERY DEVCLASS. La salida contiene un campo con la etiqueta WORM y un valor (YES o NO).

## Unidades preparadas para WORM

---

Para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben estar habilitadas para WORM. Si se monta un cartucho WORM en una unidad de lectura/escritura (RW), el montaje dará error.

No obstante, una unidad que admita WORM puede utilizarse como unidad RW si el parámetro WORM de la clase de dispositivo se establece en NO. Cualquier tipo de biblioteca puede tener tanto medios WORM como medios RW si *todas* las unidades admiten WORM. La única excepción a esta regla son las bibliotecas conectadas en red (NAS), en las que no pueden utilizarse medios de cintas WORM.

### Referencia relacionada:

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Incorporación de medios WORM

---

El tipo de los medios WORM determina si la etiqueta del medio debe ser leído durante la incorporación.

Los cambiadores de biblioteca no pueden identificar la diferencia entre los medios de cinta de lectura/escritura (RW) normales y los siguientes tipos de medios de cinta WORM:

- VolSafe
- Sony AIT
- LTO
- SDLT
- DLT

Para determinar el tipo de medio WORM utilizado, hay que cargar un volumen en una unidad. Por lo tanto, al dar de alta uno de estos tipos de volúmenes WORM, debe utilizar la opción CHECKLABEL=YES en el mandato CHECKIN LIBVOLUME.

Si dan soporte para los medios WORM, los cambiadores de biblioteca IBM® 3592 pueden detectar si un volumen es un medio WORM sin cargar el volumen en una unidad. No es necesario especificar CHECKLABEL=YES. Verifique con los proveedores de hardware que sus bibliotecas y unidades 3592 proporcionan el soporte necesario.

### Referencia relacionada:

- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

## Restricciones en los medios WORM

---

No puede utilizar los medios WORM preetiquetados con la clase de dispositivo LTO ni ECARTRIDGE.

No puede utilizar el soporte WORM con IBM Spectrum Protect especificado como gestor de claves de cifrado de unidad para las siguientes unidades:

- IBM® LTO-5, LTO-6, y posterior
- HP LTO-5, LTO-6, y posterior
- Oracle StorageTek T10000B
- Oracle StorageTek T10000C
- Oracle StorageTek T10000D

## Errores de montaje con medios WORM

---

Si se cargan medios de cinta WORM en una unidad para un montaje de clase de dispositivo de lectura-grabación (RW), se producirá un error de montaje. De forma similar, si se cargan medios de cinta RW en una unidad para un montaje de clase de dispositivo WORM, el montaje fallará.

## Volver a etiquetar soportes WORM

---

No puede volver a etiquetar un cartucho WORM si éste contiene datos. Esto es aplicable a cartuchos Sony AIT WORM, LTO WORM, SDLT WORM, DLT WORM e IBM® 3592. La etiqueta de un volumen VolSafe sólo se puede sobregabar una vez y únicamente si el volumen no contiene datos utilizables, suprimidos o caducados.

Emita el mandato LABEL LIBVOLUME una sola vez para los volúmenes VolSafe. Puede proteger la etiqueta contra sobrescritura mediante la opción OVERWRITE=NO del mandato LABEL LIBVOLUME.

### Referencia relacionada:

 LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)

## Eliminar volúmenes WORM privados de una biblioteca

---

Si lleva a cabo alguna acción en un volumen WORM (por ejemplo, si suprime espacios de archivos) y el servidor no marca el volumen como lleno, el volumen vuelve al estado de reutilizable. Si un volumen WORM no se marca como lleno y se suprime de una agrupación de almacenamiento, el volumen permanecerá privado. Para suprimir un volumen WORM privado de una biblioteca, debe emitir el mandato CHECKOUT LIBVOLUME.

### Referencia relacionada:

 CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

## Creación de volúmenes DLT WORM

---

Los volúmenes DLT WORM se pueden convertir desde volúmenes de lectura-grabación (RW).

Si dispone de unidades SDLT-600, DLT-V4 o DLT-S4 y desea habilitarlas para soportes WORM, actualice las unidades utilizando el firmware V30 o posterior disponible de Quantum. También puede utilizar software DLTIce para convertir volúmenes RW sin formatear o volúmenes en blanco en volúmenes WORM.

En bibliotecas SCSI, el servidor de IBM Spectrum Protect crea volúmenes DLT WORM reutilizables de forma automática cuando el servidor no puede localizar ningún volumen WORM reutilizable en el inventario de una biblioteca. El servidor convierte los volúmenes reutilizables RW en blanco o sin formato disponibles o los volúmenes privados RW vacíos en volúmenes WORM reutilizables. El servidor también vuelve a grabar etiquetas sobre volúmenes WORM recién creados utilizando la información de etiqueta sobre los volúmenes RW existentes.

## Soporte para cintas 3592 WORM cortas y normales

---

IBM Spectrum Protect admite cintas 3592 WORM cortas y normales. Para obtener los mejores resultados, defínalas en agrupaciones de almacenamiento distintas.


## Consultar a una clase de dispositivo el valor del parámetro WORM

---

Puede determinar el valor del parámetro WORM en una clase de dispositivo utilizando el mandato QUERY DEVCLASS. La salida contiene un campo con la etiqueta WORM y un valor (YES o NO).

### Referencia relacionada:

 QUERY DEVCLASS (Visualizar información en una o más clases de dispositivo)

 Sistemas operativos Windows

## Resolución de problemas con dispositivos



---

Puede resolver errores que se producen cuando configura o usa dispositivos con IBM Spectrum Protect.

## Acerca de esta tarea

Utilice Tabla 1 para encontrar una solución a un problema relacionado con dispositivos.

Tabla 1. Resolución de problemas de dispositivos

Síntoma	Problema	Solución
Conflictos con otras aplicaciones.	IBM Spectrum Protect requiere una red de área de almacenamiento para compartir dispositivos.	Configure una red de área de almacenamiento. Atención: Puede producirse una pérdida de datos si varios servidores de IBM Spectrum Protect utilizan el mismo dispositivo. Defina o utilice un dispositivo con un solo un servidor de IBM Spectrum Protect.  Sistemas operativos AIX  Sistemas operativos LinuxOtras aplicaciones pueden acceder a los dispositivos IBM Spectrum Protect, utilizando un controlador de cinta SCSI.
El etiquetado falla.	No es posible utilizar un dispositivo para etiquetar volúmenes mientras el servidor utiliza dicho dispositivo para otros procesos.	No puede sobrescribir los volúmenes existentes en una agrupación de almacenamiento.  Debe resolver cualquier problema de hardware antes de etiquetar un volumen.
	Registro de licencia incorrecto o incompleto.	Registre la licencia del soporte de dispositivo que ha adquirido.
Conflictos entre controladores de dispositivo.	IBM Spectrum Protect emite mensajes sobre errores de E/S cuando define o utiliza un dispositivo de acceso secuencial.	Los controladores de dispositivos de Windows y los controladores proporcionados por otras aplicaciones pueden interferir con el controlador de dispositivo de IBM Spectrum Protect si el controlador de IBM Spectrum Protect no se inicia primero. Para comprobar el orden en el que el sistema inicia los controladores de dispositivo, complete los pasos siguientes:  <ol style="list-style-type: none"><li>1. Pulse en Panel de control.</li><li>2. Pulse en Dispositivos. Aparecerá una lista de los controladores de dispositivo y de sus tipos de arranque.</li></ol>
Errores de E/S	Al intentar definir o utilizar un dispositivo de cinta, pueden producirse conflictos en el controlador de dispositivo. Los controladores de dispositivo de Windows y los controladores proporcionados por otras aplicaciones pueden interferir con el controlador de dispositivo de IBM Spectrum Protect si no se inicia primero.	

## Finalización de la implementación

Después de configurar y ejecutar la solución IBM Spectrum Protect, pruebe las operaciones de copia de seguridad y configure la supervisión para asegurarse de que todo se ejecuta sin problemas.

### Procedimiento

1. Pruebe las operaciones de copia de seguridad para verificar que los datos están protegidos del modo que esperaba.

- a. En la página Clientes del Centro de operaciones, seleccione los clientes de los que desea hacer copia de seguridad y pulse Copia de seguridad.
  - b. En la página Servidores de Centro de operaciones, seleccione el servidor para el cual desea realizar la copia de seguridad de la base de datos. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
  - c. Verifique que las operaciones de copia de seguridad se han completado correctamente sin ningún mensaje de aviso o error.  
Consejo: Como alternativa, puede utilizar la interfaz gráfica de usuario del cliente de archivado y copia de seguridad para realizar la copia de seguridad de los datos del cliente y puede hacer una copia de seguridad de la base de datos del servidor emitiendo el mandato BACKUP DB desde una línea de mandatos administrativa.
2. Configure la supervisión de la solución siguiendo las instrucciones de Supervisión de una solución de cinta.

## Supervisión de una solución de cinta

---

Tras implementar una solución basada en cinta de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Al supervisar la solución diariamente y de forma periódica, puede identificar problemas existentes y potenciales. La información que recopila se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

### Acerca de esta tarea

---

El método preferido para supervisar una solución es utilizando Centro de operaciones, que proporciona el estado del sistema detallado y general en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema.

### Procedimiento

---

1. Complete las tareas de supervisión diariamente. Para obtener instrucciones, consulte Lista de comprobación de supervisiones diarias.
2. Complete las tareas de supervisión periódicamente. Para obtener instrucciones, consulte Lista de comprobación de supervisiones periódicas.
3. Verifique que su sistema cumple con los requisitos de licencia. Para obtener instrucciones, consulte Verificación de la conformidad de licencia.
4. Opcional: Configure los informes de correo electrónico del estado del sistema. Para obtener instrucciones, consulte Seguimiento del estado del sistema mediante informes de correo electrónico

## Lista de comprobación de supervisión diaria


---

Para asegurarse de que está completando las tareas de supervisión diarias para la solución IBM Spectrum Protect, revise la lista de comprobación de supervisión diaria.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.








Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.


La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.



Tabla 1. Tareas de supervisión diarias



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>1</b> Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Clientes, seleccione el cliente y pulse Detalles.</li> <li>2. Para diagnosticar un problema, pulse Diagnóstico.</li> </ol>	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>
<p><b>2</b> Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Alertas.</li> <li>2. En la tabla Alertas, seleccione una alerta.</li> <li>3. En el panel Registro de actividad, revise los mensajes. El panel muestra mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.</li> </ol>
<p><b>3</b> Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> <li>1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible.</li> <li>2. Para ver información adicional, pulse el área Servidores.</li> <li>3. Seleccione un servidor en la tabla Servidores y pulse Detalles.</li> </ol>	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione un servidor y pulse Detalles.</li> <li>2. Para actualizar las propiedades de servidor, pulse Propiedades.</li> </ol>



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> <li>o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado.</li> <li>o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor.</li> <li>o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio.</li> <li>o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_nombre_concentrador_IBM-OC.</li> <li>o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio.</li> </ul> </li> </ol>	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas de servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>5</b> Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.</li> </ol>	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione una fila y pulse Detalles.</li> <li>2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad.</li> </ol> <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Servidores.</li> <li>2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad.</li> </ol> <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY DB: <pre>query db f=d</pre> </li> <li>3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.</li> </ol>
<p><b>6</b> Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse Servidores &gt; Mantenimiento.</li> <li>2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial.</li> <li>3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.</li> </ol>	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>7</b> Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> <li>• Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad.</li> <li>• Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.</li> </ul>	<ul style="list-style-type: none"> <li>• Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente.</li> <li>• Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.</li> </ul>
<p><b>8</b> Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<ol style="list-style-type: none"> <li>1. Si se indican problemas en el área Almacenamiento &amp; Disponibilidad de datos, pulse Agrupaciones para ver los detalles: <ul style="list-style-type: none"> <li>◦ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible.</li> <li>◦ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura.</li> </ul> </li> <li>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</li> </ol>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento &amp; Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  El estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Es posible que los dispositivos de cinta tengan un estado de aviso o crítico si las unidades no están disponibles. Una unidad no estará disponible si está fuera de línea, si deja de responder al servidor, o si su vía de acceso está fuera de línea. También puede que un dispositivo de cinta tenga un estado crítico si la biblioteca está fuera de línea. Otras columnas de la tabla Dispositivos de cinta muestran el estado de la robótica, las unidades y las vías de acceso de la biblioteca.</p> <p>Para resolver problemas con unidades de cinta que tengan un estado crítico, sitúe la unidad fuera de línea si necesita utilizarla para otra actividad, como por ejemplo mantenimiento. Para poner una unidad fuera del sitio, complete los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones Almacenamiento, seleccione Dispositivos de cinta.</li> <li>2. Para ver más información sobre una biblioteca de cintas, seleccione una fila y pulse Detalles.</li> <li>3. Para sacar una unidad fuera de línea, seleccione la unidad de cintas y pulse Fuera del sitio.</li> </ol> <p>Para las operaciones de copia de seguridad de cinta, compruebe que haya disponibles suficientes cintas reutilizables. Si no está seguro de si el número de cintas reutilizables es suficiente, abra el cuaderno de detalles para ver el uso de cintas y una estimación de la disponibilidad de cintas reutilizables. Para abrir el cuaderno de detalles, seleccione una biblioteca en la tabla y pulse Detalles.</p>

## Lista de comprobación de supervisión periódica

Para asegurarse de que las operaciones se ejecutan correctamente, complete las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.








Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>. Busque el servidor asociado al cliente.</li> <li>2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>.</li> <li>3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>.</li> <li>4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Para obtener información sobre este mandato, consulte QUERY ACTLOG (Consultar las anotaciones de actividades).</li> <li>5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa.</li> </ol> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Clientes</i>.</li> <li>2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>.</li> <li>3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>.</li> </ol>	<p>Limite el tiempo para las operaciones de copia de seguridad de cliente a 8 - 12 horas. Asegúrese de que las planificaciones de cliente no se solapen con las tareas de mantenimiento del servidor.</p> <p>Para obtener instrucciones sobre cómo reducir el tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento comunes del cliente</i>.</p> <p>Busque cuellos de botella de rendimiento. Para obtener instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Visión general, pase el ratón sobre el icono de configuración y pulse en Creador de mandatos.</li> <li>2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <ul style="list-style-type: none"> <li><code>query option volhistory</code></li> <li><code>query option devconfig</code></li> </ul> </li> <li>3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.</li> </ol> <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determine si hay suficiente espacio disponible en el directorio para la instancia de servidor.</p>	<p>Verifique si hay al menos 50 GB de espacio libre disponible en el directorio para la instancia de servidor. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad.</li> </ul> <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux /home/tsminst1/tsminst1</li> <li>•  Sistemas operativos Windows C:\tsminst1</li> </ul> <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

<b>Tarea</b>	<b>Procedimientos básicos</b>	<b>Procedimientos avanzados y solución de problemas</b>
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Clientes.</li> <li>2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente.</li> <li>3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades.</li> <li>4. En el área Última sesión, visualice la fila Enviado a cliente.</li> </ol>	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p>



Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones.</li> <li>2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles.</li> </ol>	<p>Sugerencias:</p> <ul style="list-style-type: none"> <li>• Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> <li>3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>.</li> </ol> </li> <li>• Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>.</li> <li>• Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> </ol> </li> </ul> <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores de nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que hay disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> <li>• Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.</li> </ul>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervisar y mantener los dispositivos de cinta</p>	<p>Puede supervisar su entorno para ver que no haya errores de hardware en las unidades de cinta ni en las bibliotecas de cintas. Para obtener instrucciones, consulte Supervisión de los mensajes de alerta de cinta sobre errores de hardware.</p> <p>Supervise la compatibilidad de los medios para prevenir errores en las unidades de cinta. Para obtener instrucciones, consulte Prevenir errores causados por la incompatibilidad de los medios.</p> <p>Supervise los mensajes de limpieza de las unidades de cinta. Para obtener instrucciones, consulte Operaciones con cartuchos limpiadores.</p>	
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente no se solapen con las tareas de mantenimiento del servidor. Limite el tiempo para las operaciones de copia de seguridad de cliente a 8 - 12 horas.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes &gt; Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones.</li> <li>2. Seleccione una planificación y pulse Detalles.</li> <li>3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila.</li> <li>4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado.</li> <li>5. Pulse Guardar.</li> </ol>
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento no se solapen con las planificaciones de cliente.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores &gt; Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>El método preferido consiste en asegurarse de que cada tarea de mantenimiento se ejecute hasta el final antes de que se inicie la siguiente tarea de mantenimiento. Ejemplos de tareas de mantenimiento incluyen la caducidad de inventario, la copia de agrupaciones de almacenamiento, la reclamación de espacio y la copia de seguridad de base de datos. Consejo: Si una tarea de mantenimiento está en ejecución durante demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Visión general, pase el ratón sobre el icono de configuración y pulse en Creador de mandatos.</li> <li>2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener información sobre este mandato, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).</li> </ol>

- Supervisión de los mensajes de alerta de cinta sobre errores de hardware  
Los dispositivos de cinta y biblioteca generan mensajes de alerta de cinta para informar de errores de hardware. Estos mensajes ayudan a determinar los problemas que no están relacionados con el servidor de IBM Spectrum Protect.
- Prevenir errores causados por la incompatibilidad de los medios  
Supervisando y resolviendo los problemas de compatibilidad de los medios, puede prevenir errores en una solución basada en cintas de IBM Spectrum Protect. Es posible que una unidad nueva tenga una capacidad limitada de utilizar formatos de medios

que sí están soportados en una versión anterior de la unidad. A menudo, una unidad nueva puede leer pero no grabar en formatos de medios anteriores.

- Operaciones con cartuchos limpiadores

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

## Supervisión de los mensajes de alerta de cinta sobre errores de hardware

---

Los dispositivos de cinta y biblioteca generan mensajes de alerta de cinta para informar de errores de hardware. Estos mensajes ayudan a determinar los problemas que no están relacionados con el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

---

Se crea una página de registro que se puede recuperar en cualquier momento o en un momento específico como, por ejemplo, cuando se desmonta una unidad.

Un mensaje de alerta de cinta puede tener uno de los siguientes niveles de gravedad:

- Informativo (por ejemplo, se ha intentado cargar un tipo de cartucho que no está permitido)
- Aviso (por ejemplo, se prevé un error de hardware)
- Crítico (por ejemplo, hay un problema con la cinta y los datos están en peligro)

De forma predeterminada, los mensajes de alerta de cinta están desactivados.

### Procedimiento

---

- Para habilitar los mensajes de alerta de cinta, emita el mandato SET TAPEALERTMSG y especifique el valor ON: `set tapealertmsg on`
- Para comprobar si los mensajes de alerta de cinta están habilitados, emita el mandato QUERY TAPEALERTMSG: `query tapealertmsg`

## Prevenir errores causados por la incompatibilidad de los medios

---

Supervisando y resolviendo los problemas de compatibilidad de los medios, puede prevenir errores en una solución basada en cintas de IBM Spectrum Protect. Es posible que una unidad nueva tenga una capacidad limitada de utilizar formatos de medios que sí están soportados en una versión anterior de la unidad. A menudo, una unidad nueva puede leer pero no grabar en formatos de medios anteriores.

### Acerca de esta tarea

---

De forma predeterminada, los volúmenes existentes con estado `FILLING` permanecen en ese estado después de una actualización de la unidad. En algunos casos, es posible que desee continuar utilizando una unidad anterior para llenar esos volúmenes. De este modo, puede conservar la posibilidad de lectura/escritura de los volúmenes existentes hasta que sean reclamados. Si opta por actualizar todas las unidades de una biblioteca, verifique que los formatos de los medios están soportados por el nuevo hardware. A menos que tenga pensado utilizar solo los medios más actuales con la nueva unidad, es necesario que sea consciente de los posibles problemas de compatibilidad. Para obtener instrucciones de migración, consulte el apartado Migración de datos a unidades actualizadas.

Para utilizar una nueva unidad con los medios en los que puede leer pero no grabar, emita el mandato `UPDATE VOLUME` para definir el acceso a esos volúmenes como de sólo lectura. De este modo se evitarán errores provocados por la incompatibilidad de lectura/escritura. Por ejemplo, una nueva unidad puede expulsar un medio que esté grabado en un formato que la unidad no admite al cargar el medio en la unidad. O puede que una nueva unidad dé error al emitir el primer mandato de grabar en un formato que la unidad no admite.

Cuando los datos del medio de sólo lectura caduquen y se reclame el volumen, sustitúyalo por un medio que sea totalmente compatible con la nueva unidad. Se pueden generar errores si una unidad nueva no puede calibrar correctamente un volumen grabado al utilizar un formato anterior. Para evitar este problema, asegúrese de que la unidad original esté funcionando correctamente y en los niveles de microcódigo actuales.

## Operaciones con cartuchos limpiadores

---

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

### Supervisión del proceso de limpieza

Si se ha incorporado un cartucho limpiador en una biblioteca y se tiene que limpiar una unidad, el servidor desmonta el volumen de datos y ejecuta la operación de limpieza. Si la operación de limpieza falla o se cancela, o si no hay ningún cartucho limpiador disponible, puede que no se dé cuenta de que la unidad necesita una limpieza. Supervise los mensajes sobre estos problemas de limpieza para asegurarse de que las unidades se limpian cuando es necesario. Si es necesario, emita el mandato CLEAN DRIVE para que el servidor intente la limpieza de nuevo, o cargue manualmente un cartucho limpiador en la unidad.

### Utilización de varios cartuchos limpiadores

El servidor utiliza un cartucho limpiador para el número de limpiezas que especifique al dar de alta el cartucho limpiador. Si incorpora dos o más cartuchos limpiadores, el servidor utilizará sólo uno de los cartuchos hasta alcanzar el número de limpiezas designado para ese cartucho. A continuación, el servidor utiliza el siguiente cartucho limpiador. Si incorpora dos o más cartuchos limpiadores y ejecuta simultáneamente dos o más mandatos CLEAN DRIVE, el servidor utilizará varios cartuchos al mismo tiempo y reducirá las limpiezas restantes en cada cartucho.

### Referencia relacionada:

- ➔ AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- ➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)
- ➔ CLEAN DRIVE (Limpiar una unidad)
- ➔ LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- ➔ QUERY LIBVOLUME (Consultar un volumen de biblioteca)

## Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple con las provisiones del acuerdo de licencia. Verificando la conformidad regularmente, puede realizar un seguimiento de las tendencias en el crecimiento de datos o en el uso de unidades de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

### Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

#### Licencia de capacidad frontal

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

#### Licencia de capacidad de programa de fondo

El modelo de programa de fondo determina los requisitos de licencia basándose en los terabytes de datos que se almacenan en las agrupaciones de almacenamiento primarias y los repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

#### Licencia de PVU

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.

Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.



Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

## Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia.

Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
--------	-------------

Opción	Descripción
<b>Modelo frontal</b>	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
<b>Modelo suplementario</b>	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad de estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
<b>Modelo de PVU</b>	Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de la conformidad con el modelo de licencias de PVU.

## Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

### Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor de SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener el privilegio de sistema para el servidor.
- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

### Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

### Procedimiento

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.  
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

## Resultados

---

Los informes habilitados se envían según los valores especificados.

## Qué hacer a continuación

---

El informe de operaciones general incluye un archivo adjunto. Para obtener información más detallada, expanda las secciones del archivo adjunto.

Si no puede ver la imagen de un informe, puede que esté utilizando un cliente de correo electrónico que convierte HTML a otro formato. Para obtener información sobre las restricciones, consulte la ayuda en línea Centro de operaciones.

## Gestión de operaciones para una solución de cinta

---

Utilice esta información para gestionar las operaciones para una implementación de cinta para un servidor IBM Spectrum Protect.

- **Gestión del Centro de operaciones**  
El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.
- **Gestión de operaciones de cliente**  
Puede resolver errores de cliente, gestionar las actualizaciones de clientes y anular los nodos de cliente que ya no sean necesarios. Para liberar espacio de almacenamiento en el servidor, puede desactivar datos obsoletos almacenados por clientes de aplicación.
- **Gestión del almacenamiento de datos**  
Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.
- **Gestión de dispositivos de cinta**  
Las operaciones rutinarias de cinta incluyen la preparación de volúmenes de cinta para su utilización, controlar cómo y cuándo se reutilizan los volúmenes y asegurarse de que hay suficientes volúmenes disponibles. También debe responder a las solicitudes de operador y gestionar bibliotecas, unidades, discos, vías de acceso y transportadores de datos.
- **Gestión de unidades de cinta**  
Puede consultar, actualizar y suprimir las unidades de cinta. También puede limpiar las unidades de cinta y configurar el cifrado de unidades de cinta y la validación de datos.
- **Protección del servidor IBM Spectrum Protect**  
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- **Detención e inicio del servidor**  
Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.
- **Planificación para actualizar el servidor**  
Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.
- **Preparación para una parada o actualización de sistema**  
Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.
- **Preparación ante desastres y recuperación tras desastres mediante DRM**  
IBM Spectrum Protect proporciona una función de gestor recuperación tras desastre (DRM) para poder recuperar los datos del servidor y del cliente durante un siniestro.

## Gestión del Centro de operaciones

---

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.

## Acerca de esta tarea

---

Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect. Para obtener más información sobre la gestión del Centro de operaciones, consulte Gestión del Centro de operaciones.

## Gestión de operaciones de cliente

---

Puede resolver errores de cliente, gestionar las actualizaciones de clientes y anular los nodos de cliente que ya no sean necesarios. Para liberar espacio de almacenamiento en el servidor, puede desactivar datos obsoletos almacenados por clientes de aplicación.

### Acerca de esta tarea

---

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

Para obtener instrucciones sobre cómo añadir clientes, consulte Protección de aplicaciones, máquinas virtuales y sistemas.

- **Evaluación de errores en registros de errores de cliente**  
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- **Detención y reinicio del aceptador de cliente**  
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- **Restablecimiento de contraseñas**  
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- **Gestión de actualizaciones del cliente**  
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.
- **Poner fuera de servicio un nodo cliente**  
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.
- **Desactivación de datos para liberar espacio de almacenamiento**  
En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

## Evaluación de errores en registros de errores de cliente

---

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

### Antes de empezar

---

Opcionalmente, para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de clientes se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte la publicación Instalación del servicio de gestión de cliente.

### Procedimiento

---

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de clientes se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Detalles.
  3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
  4. Revise los mensajes de registro recuperados.  
Sugerencias:
    - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.

- Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.

- Si servicio de gestión de clientes no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

## Detención y reinicio del aceptador de cliente

---

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

### Acerca de esta tarea

---

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para asegurarse de que las operaciones planificadas se pueden producir en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

### Procedimiento

---

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

AIX y Oracle Solaris

- Para detener el aceptador de cliente, complete los pasos siguientes:
  - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```

- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```


Windows

- Para detener el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.



- c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, complete los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Iniciar y Aceptar.

**Referencia relacionada:**

 Resolución de problemas de planificación del cliente

## Restablecimiento de contraseñas

---

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

### Procedimiento

---

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nodo cliente y *nueva\_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva\_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:

1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nombre del nodo y *nueva\_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.  
Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

## Gestión de actualizaciones del cliente

---

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

### Antes de empezar

---

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de

cliente no se vean afectadas.

2. Verifique los requisitos del sistema para el cliente en Sistemas operativos admitidos para IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad de agente de almacenamiento y cliente de biblioteca con los servidores que se configuran como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

## Procedimiento

Para actualizar el software, siga las instrucciones que se muestran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>• Actualización del cliente de archivado y copia de seguridad</li></ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for VMware</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot for Windows</li></ul>
IBM Spectrum Protect for Databases	<ul style="list-style-type: none"><li>• Actualización de Data Protection for SQL Server</li><li>• Instalación de Data Protection for Oracle</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for DB2</li><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection for SAP for Oracle</li></ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"><li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li><li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server</li></ul>
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"><li>• Instalación y actualización de Data Protection for VMware</li><li>• Instalación de Data Protection for Microsoft Hyper-V</li></ul>

## Poner fuera de servicio un nodo cliente

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor de IBM Spectrum Protect, pero la estación de trabajo ya no se utiliza, puede ponerla fuera de servicio.

### Acerca de esta tarea

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail

- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

## Procedimiento

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
  1. En la página de Centro de operaciones Visión general, pulse Clientes y seleccione el cliente.
  2. Pulse Más > Poner fuera de servicio.
- Para que un nodo cliente quede fuera de servicio utilizando un mandato administrativo, realice una de las siguientes acciones:
  - Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o más espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Qué hacer a continuación

Tenga en cuenta los mensajes de error, que se pueden mostrar en la interfaz de usuario o en la salida de mandatos, inmediatamente después de ejecutar el proceso.

Puede verificar que el nodo de cliente esté fuera de servicio:

1. En la página de Centro de operaciones Visión general, pulse Clientes.
2. En la tabla Clientes, en la columna En riesgo, revise el estado:

- Un estado DECOMMISSIONED especifica que el nodo está fuera de servicio.
- Un valor null especifica que el nodo no está fuera de servicio.
- Un estado PENDING especifica que el nodo se está dejando fuera de servicio, o que el proceso de dejar fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso de invalidación pendiente, emita el mandato siguiente:

```
proceso de consulta
```

3. Revise la salida del mandato:

- Si se proporciona el estado para el proceso de invalidación, el proceso estará en curso. Por ejemplo:

```
proceso de consulta
```

Proceso proceso	Descripción proceso	Estado proceso
----- 3	----- DECOMMISSION NODE	----- Número de objetos de copia de seguridad desactivados para el nodo NODE1: 8 objetos desactivados.

- Si no se proporciona ningún estado para el proceso de invalidación, y si no ha recibido ningún mensaje de error, el proceso estará incompleto. Un proceso puede estar incompleto si los archivos asociados con el nodo no están aún desactivados. Una vez que se desactiven los archivos, ejecute el proceso de invalidación de nuevo.
- Si no se proporciona ningún estado para el proceso de invalidación, y si recibe un mensaje de error, el proceso fallará. Ejecute el proceso de invalidación de nuevo.

**Referencia relacionada:**

- ➔ DECOMMISSION NODE (Poner fuera de servicio un nodo de cliente)
- ➔ DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

## Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar los datos que se almacenan en el servidor de IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

### Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

### Procedimiento

1. En la página Descripción general de Centro de operaciones, pulse Clientes.
2. En la tabla Clientes, seleccione uno o más clientes y pulse Más > Borrar.  
Método de línea de mandatos: Desactive los datos utilizando el mandato DEACTIVATE DATA.

**Referencia relacionada:**

- ➔ DEACTIVATE DATA (Desactivar datos para un nodo de cliente)


## Gestión del almacenamiento de datos

Gestione los datos para la eficiencia y añada dispositivos y soportes compatibles al servidor para almacenar datos de cliente.

- Gestión de la capacidad de inventario  
Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.
- Ajuste de actividades planificadas  
Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

- Optimización de operaciones habilitando la función de proximidad de los archivos de cliente  
La proximidad de los archivos de cliente reduce el número de montajes de volúmenes necesarios cuando los usuarios restauran o recuperan muchos archivos de una agrupación de almacenamiento. Este modo de proximidad reduce la cantidad de tiempo necesario para estas operaciones.

**Referencia relacionada:**

 Tipos de agrupaciones de almacenamiento

## Gestión de la capacidad de inventario

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

### Antes de empezar

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

### Procedimiento

- Para aumentar el espacio de disco para la base de datos, complete los pasos siguientes:
  - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
  - Emita el mandato EXTEND DBSPACE para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.  
Sugerencias:
    - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
    - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
  - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
  - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tabas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.
- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, consulte la información en nota técnica 1683633. Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.
- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo dmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro activo se basa en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB

Valor de la opción <b>ACTIVELOGSize</b>	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de <b>ACTIVELOGSize</b>
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsiz 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
  5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la compresión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción de servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la compresión del registro de archivado de forma inmediata sin detener el servidor.

**Referencia relacionada:**

- 🔗 ACTIVELOGSIZE, opción de servidor
- 🔗 EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- 🔗 SETOPT (Establecer una opción de servidor para actualización dinámica)

## Ajuste de actividades planificadas

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Ajustando la solución, se maximizan los recursos del servidor y se utilizan de forma eficaz distintas funciones disponibles en la solución.

### Procedimiento

1. Supervise el rendimiento de sistema de forma periódica para asegurarse de que las tareas de copia de seguridad y mantenimiento se completan correctamente. Para obtener más información sobre supervisión, consulte Supervisión de una solución de cinta.
2. Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, tal vez tenga que revisar la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
  - El número de clientes aumenta.
  - La cantidad de datos de los que se hace copia de seguridad aumenta.
  - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución tiene problemas de rendimiento. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
  - b. Pulse Detalles.
  - c. Desde la página de Resumen, revise la actividad de Copiado y Replicado para identificar los riesgos.
 Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.
4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:
  - a. Copia de seguridad de la base de datos
  - b. Ejecutar la caducidad para eliminar las copias de seguridad de cliente y las copias de archivo de archivado del almacenamiento de servidor.

**Conceptos relacionados:**

- 🔗 Rendimiento

**Tareas relacionadas:**

- 🔗 Deduplicación de datos (V7.1.1)

# Optimización de operaciones habilitando la función de proximidad de los archivos de cliente

La proximidad de los archivos de cliente reduce el número de montajes de volúmenes necesarios cuando los usuarios restauran o recuperan muchos archivos de una agrupación de almacenamiento. Este modo de proximidad reduce la cantidad de tiempo necesario para estas operaciones.

## Acerca de esta tarea

Con la función de proximidad activada, el servidor intenta conservar todos los archivos en un mínimo de volúmenes de almacenamiento de acceso secuencial. Estos archivos pueden pertenecer a un único nodo de cliente, un grupo de nodos de cliente, un espacio de archivo cliente o a un grupo de espacios de archivo. Puede establecer la función de proximidad para cada agrupación de almacenamiento de acceso secuencial al definir o actualizar la agrupación.

Figura 1 muestra un ejemplo de proximidad por nodo cliente con tres clientes, cada uno con un volumen independiente que contiene los datos del cliente.

Figura 1. Ejemplo de proximidad habilitada por nodo



La Figura 2 muestra un ejemplo de la función de proximidad por grupo de nodos cliente. Se definen tres grupos, y los datos para cada grupo se almacenan en volúmenes independientes.

Figura 2. Ejemplo de proximidad habilitada por asignación de nodos

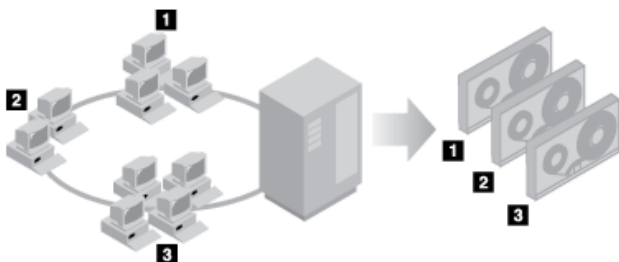
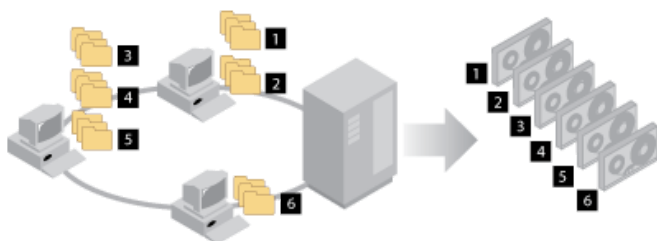


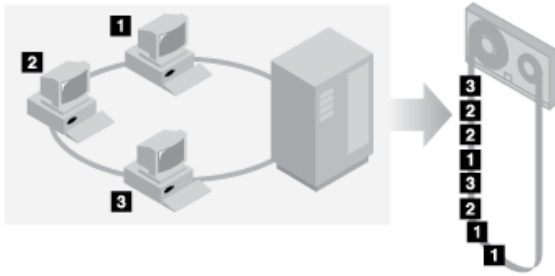
Figura 3 muestra un ejemplo de proximidad por grupo de espacio de archivos. Se definen seis grupos. Cada grupo contiene datos de los espacios de archivos que pertenecen a un único nodo. Los datos para cada grupo se almacenan en un volumen independiente.

Figura 3. Ejemplo de proximidad habilitada por el grupo de asignación del espacio de archivos



Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen antes de seleccionar un nuevo volumen. Este proceso mejora el uso de volúmenes individuales y los archivos de usuario se pueden distribuir en muchos volúmenes. Figura 4 muestra un ejemplo de proximidad que está inhabilitado, con tres clientes que comparten el espacio en un único volumen.

Figura 4. Ejemplo de función de proximidad inhabilitada



Con la proximidad inhabilitada, es posible que se requieran más operaciones de montaje de medios para montar volúmenes cuando los usuarios restauren o recuperen muchos archivos.

La proximidad por grupo es el valor predeterminado del sistema IBM Spectrum Protect para agrupaciones de almacenamiento de acceso secuencial. El valor predeterminado para las agrupaciones de almacenamiento de copias es no proximidad.

- Efectos de la proximidad en las operaciones  
El efecto de la proximidad en los recursos y el rendimiento del sistema depende del tipo de operación que se realice.
- Selección de volúmenes con proximidad habilitada  
La selección del volumen depende de si la proximidad es por grupo, nodo o espacio de archivo.
- Selección de volúmenes con proximidad inhabilitada  
Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen de almacenamiento antes de acceder a otro volumen.
- Valores de proximidad  
Una vez definida una agrupación de almacenamiento, se puede cambiar el valor de la función de proximidad actualizando la agrupación de almacenamiento. La modificación de la agrupación con respecto a la función de proximidad no afecta a los archivos que ya están almacenados en la agrupación.
- Proximidad de agrupaciones de almacenamiento de copias  
En relación con la utilización de la función de proximidad en las agrupaciones de almacenamiento de copia, existen varios aspectos que debe tener en cuenta. La proximidad de agrupaciones de almacenamiento de copia, especialmente por nodo o espacio de archivo, implica más volúmenes parcialmente llenos y actividad de reclamación fuera del local potencialmente innecesaria.
- Planificación y activación de la función de proximidad  
Entender los efectos de la función de proximidad puede ayudar a reducir el número de montajes de medios, aprovechar mejor el espacio en volúmenes secuenciales y mejorar la eficacia de las operaciones de servidor.

## Efectos de la proximidad en las operaciones

El efecto de la proximidad en los recursos y el rendimiento del sistema depende del tipo de operación que se realice.

En la Tabla 1 se resume la incidencia de la proximidad en las operaciones.

Tabla 1. Efecto de la proximidad en las operaciones

Operación	Proximidad habilitada	Proximidad inhabilitada
Copia de seguridad, archivado o migración de archivos de clientes	Más montajes de medios para la función de proximidad de los archivos.	Se requieren menos montajes de medios.
Restauración o recuperación de archivos cliente	Se pueden restaurar o recuperar numerosos archivos más rápidamente debido a que están situados en menos volúmenes.	Pueden necesitarse varios montajes de medios para un único usuario debido a que los archivos pueden estar distribuidos en varios volúmenes.  Pueden almacenarse archivos de más de un usuario en el mismo volumen de almacenamiento de acceso secuencial. Por ejemplo, si dos usuarios intentan recuperar un archivo que reside en el mismo volumen, el segundo usuario se verá obligado a esperar hasta que se hayan recuperado los archivos del primer usuario.



Operación	Proximidad habilitada	Proximidad inhabilitada
Almacenamiento de datos en cinta	El servidor intenta utilizar todos los volúmenes de cinta disponibles para separar los archivos de usuario antes de utilizar todo el espacio disponible en cada volumen de cinta.	El servidor intenta utilizar todo el espacio disponible en cada volumen de cinta antes de que el servidor utilice otro volumen de cinta.
Operaciones de montaje de medios	Se requieren más operaciones de montaje cuando se realizan copias de seguridad, se archivan o se migran los archivos de usuario desde nodos de cliente directamente a volúmenes de acceso secuencial.  Se requieren más operaciones de montaje durante la reclamación y la migración de agrupaciones de almacenamiento.  Se gestionan más volúmenes porque los volúmenes no se utilizan por completo.	Se necesitan más operaciones de montaje durante la restauración y la recuperación de los archivos cliente.
Generación de conjuntos de copias de seguridad	Se dedica menos tiempo a buscar entradas de bases de datos, y se necesitan menos operaciones de montaje.	Se dedica más tiempo a buscar entradas de bases de datos, y se necesitan menos operaciones de montaje.

Cuando se habilita la proximidad para un grupo, un único nodo de cliente o espacio de archivos, un proceso de servidor mueve o copia todos los datos que pertenecen al grupo, el nodo o el espacio de archivos. Por ejemplo, si los datos se aproximan por grupo, todos los datos de todos los nodos que pertenecen al mismo grupo de proximidad se migran en el mismo proceso.

Cuando se aproximan datos, el servidor de IBM Spectrum Protect intentará mantener juntos los archivos en un número mínimo de volúmenes de almacenamiento de acceso secuencial. No obstante, cuando el servidor realice la copia de seguridad de datos a volúmenes en una agrupación de almacenamiento de acceso secuencial, el proceso de copia de seguridad tendrá prioridad sobre los valores de proximidad. Como resultado, el servidor completa la operación de copia de seguridad, pero es posible que no pueda aproximar los datos.

Por ejemplo, supongamos que está aproximando por nodo y que especifica que un nodo puede emplear dos puntos de montaje en el servidor. Supongamos también que los datos cuya copia de seguridad se está realizando desde un nodo, puedan caber fácilmente en un volumen de cinta. Durante la copia de seguridad, el servidor puede montar dos volúmenes de cinta y los datos del nodo se pueden distribuir en dos cintas, en vez de distribuirse en una sola. Si habilita la proximidad, las siguientes operaciones de servidor utilizan un proceso de servidor:

- Mover datos desde volúmenes de acceso aleatorio y de acceso secuencial
- Mover datos de nodo desde volúmenes de acceso secuencial
- Realizar copia de seguridad de una agrupación de almacenamiento de acceso aleatorio o de acceso secuencial.
- Restaurar una agrupación de almacenamiento de acceso secuencial.
- Reclamar espacio en una agrupación de almacenamiento de acceso secuencial o volúmenes fuera del local
- Migrar datos desde una agrupación de almacenamiento de acceso aleatorio

Si migra datos desde una agrupación de almacenamiento de disco de discos de acceso aleatorio a una agrupación de almacenamiento de acceso secuencial, y la proximidad es por nodo o espacio de archivos, los nodos o espacios de archivo se seleccionan automáticamente para la migración en función de la cantidad de datos que se migrarán. El nodo o el espacio de archivos con más cantidad de datos se migra en primer lugar. Si la proximidad es por grupo, todos los nodos de la agrupación de almacenamiento se evalúan en primer lugar para determinar qué nodo tiene más datos. El nodo con más datos se migra el primero junto con todos los datos de todos los nodos pertenecientes a ese grupo de proximidad. Este proceso se realiza, independientemente de cuántos datos se almacenen en los espacios de archivo de los nodos y de si se ha alcanzado el umbral de migración inferior.

Sin embargo, si migra los datos de proximidad desde una agrupación de almacenamiento de acceso secuencial a otra agrupación de almacenamiento de acceso secuencial, el servidor ordena los volúmenes en función de la fecha en la que se accedió al volumen por última vez. El volumen con la fecha de acceso más reciente se migra primero, y el volumen con la última fecha de acceso se migra el último.

Un motivo para realizar la proximidad por grupo es que los nodos cliente individuales no suelen disponer de datos suficientes para llenar volúmenes de cinta de gran capacidad. La proximidad de datos por grupos de nodos puede reducir la capacidad de cinta no utilizada colocando más datos de proximidad en cintas individuales. Además, la proximidad de datos por grupos de espacios de archivos reduce la cinta no utilizada en mayor medida.

Los datos que pertenecen a todos los nodos del mismo grupo de proximidad se migran en el mismo proceso. Por tanto, la proximidad por grupo puede reducir el número de veces que se debe montar un volumen que se va a migrar. La proximidad por grupo también puede minimizar la exploración de bases de datos así como los pases de cinta durante la transferencia de datos de una agrupación de almacenamiento de acceso secuencial a otra.

## Selección de volúmenes con proximidad habilitada

La selección del volumen depende de si la proximidad es por grupo, nodo o espacio de archivo.

La Tabla 1 muestra la forma en que el servidor de IBM Spectrum Protect seleccione el primer volumen cuando la función de proximidad está activada para una agrupación de almacenamiento en el nodo de cliente, el grupo de proximidad y el nivel de espacio de archivos.

Tabla 1. Cómo selecciona volúmenes el servidor si la proximidad está activada

Orden de selección de volúmenes	Cuando la proximidad es por grupo	Cuando la proximidad es por nodo	Cuando la proximidad es por espacio de archivos
1	Un volumen que ya contiene archivos del grupo de proximidad al cual pertenece el cliente	Un volumen que ya contiene archivos del mismo nodo cliente	Un volumen que ya contiene archivos del mismo espacio de archivos de dicho nodo de cliente
2	Un volumen predefinido vacío	Un volumen predefinido vacío	Un volumen predefinido vacío
3	Un volumen reutilizable vacío	Un volumen reutilizable vacío	Un volumen reutilizable vacío
4	El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos	El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos	Un volumen que ya contiene archivos del mismo nodo de cliente
5	No aplicable	No aplicable	El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos

Si el usuario debe continuar almacenando datos en un segundo volumen, utiliza la siguiente selección para adquirir más espacio:

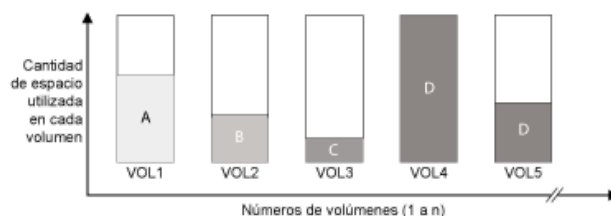
1. Un volumen predefinido vacío
2. Un volumen reutilizable vacío
3. El volumen con la mayor cantidad de espacio libre disponible entre los volúmenes que ya contienen datos
4. Cualquier volumen disponible de la agrupación de almacenamiento

Cuando la proximidad es por nodo de cliente o por espacio de archivos, el servidor intenta proporcionar el mejor uso de los volúmenes individuales y minimizar la mezcla de archivos procedentes de distintos clientes o espacios de archivos en los volúmenes. Esta configuración está representada en Figura 1, que muestra que la selección de volúmenes es *horizontal*, donde se utilizan todos los volúmenes disponibles antes de utilizar todo el espacio disponible de cada volumen que se utiliza. A, B, C y D representan archivos de cuatro nodos cliente distintos.

Sugerencias:

1. Si la proximidad es por nodo y el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos.
2. Si la proximidad es por espacio de archivos y un nodo tiene varios espacios de archivos, el servidor intentará aproximar los datos para los distintos espacios de archivos en distintos volúmenes.

Figura 1. Utilización de todos los volúmenes de almacenamiento de acceso secuencial disponibles con la proximidad habilitada a nivel de espacio de archivos o nodo



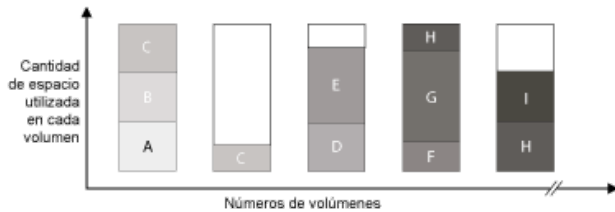
La proximidad puede ser por grupo de espacio de archivos o por grupo de nodos. Cuando la proximidad es por grupo de nodos (grupo de asignación de nodos), el servidor intenta asignar datos desde los nodos que pertenecen al mismo grupo de asignación. Un grupo de proximidad de espacio de archivos utiliza los mismos métodos que un grupo de proximidad de nodos, pero puede utilizar más espacio

por la granularidad de los tamaños de espacio de archivos. Como se muestra en Figura 2, se han asignado datos para los siguientes grupos de nodos:

- El grupo 1 consta de los nodos A, B y C
- El grupo 2 consta de los nodos D y E
- El grupo 3 consta de los nodos F, G, H e I

Siempre que sea posible, el servidor de IBM Spectrum Protect asigna los datos pertenecientes a un grupo de nodos en una sola cinta, tal como se ve representado en el Grupo 2 de la figura. Los datos de un mismo nodo también se pueden distribuir en varias cintas asociadas a un grupo (Grupo 1 y 2). Si los nodos del grupo de proximidad tienen varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos.

Figura 2. Utilización de todos los volúmenes de almacenamiento de acceso secuencial disponibles con la proximidad habilitada a nivel de grupo



Normalmente, el servidor de IBM Spectrum Protect siempre graba los datos en el volumen de llenado actual para la operación que se está ejecutando. Sin embargo, es posible que en ocasiones detecte más de un volumen de relleno en una agrupación de almacenamiento de proximidad. Puede tener más de un volumen de llenado en una asignación de almacenamiento de proximidad si diferentes procesos de servidor o sesiones de cliente intentan almacenar datos en la agrupación de proximidad al mismo tiempo. En esta situación, IBM Spectrum Protect asigna un volumen para cada proceso o sesión que necesita un volumen, de manera que ambas operaciones se completan lo más rápido posible.

## Selección de volúmenes con proximidad inhabilitada

Si la función de proximidad está desactivada, el servidor intenta utilizar todo el espacio disponible en cada volumen de almacenamiento antes de acceder a otro volumen.

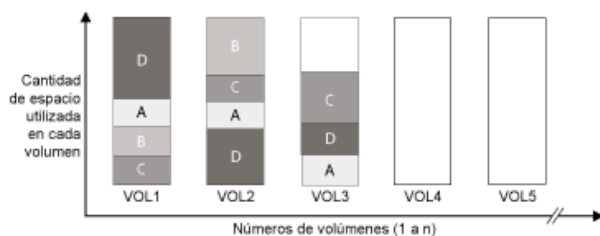
Si almacena archivos de cliente en una agrupación de almacenamiento de acceso secuencial cuando la función de proximidad está inhabilitada, el servidor selecciona un volumen utilizando el siguiente orden de selección:

1. Un volumen secuencial que tenga espacio disponible y que se haya utilizado anteriormente (se selecciona primero el volumen que más datos tiene)
2. Un volumen vacío

Cuando el servidor debe continuar almacenando datos en un segundo volumen, intenta seleccionar un volumen vacío. Si no existe ningún volumen vacío, el servidor intenta seleccionar cualquier volumen disponible que quede en la agrupación de almacenamiento.

Figura 1 muestra que el uso del volumen es vertical cuando la función de proximidad está inhabilitada. En este ejemplo, se utilizan menos volúmenes porque el servidor intenta utilizar todo el espacio disponible mezclando los archivos de clientes en los volúmenes individuales. A, B, C y D representan archivos de cuatro nodos cliente distintos.

Figura 1. Utilización de todo el espacio disponible en volúmenes de acceso secuencial con función de proximidad inhabilitada



## Valores de proximidad

Una vez definida una agrupación de almacenamiento, se puede cambiar el valor de la función de proximidad actualizando la agrupación de almacenamiento. La modificación de la agrupación con respecto a la función de proximidad no afecta a los archivos que ya están almacenados en la agrupación.

Por ejemplo, si la proximidad está desactivada para una agrupación de almacenamiento y la activa, a partir de ese momento se asignan los archivos de cliente que estén almacenados en la agrupación. Los archivos previamente almacenados en la agrupación de almacenamiento no se mueven para asignarse. Cuando se reclamen los volúmenes, los datos de la agrupación tienden a estar más próximos. También puede utilizar los mandatos MOVE DATA o MOVE NODEDATA para mover datos a nuevos volúmenes para incrementar la proximidad. Mover datos a nuevos volúmenes provoca un incremento del tiempo de procesamiento y la actividad de montaje de volúmenes.

Consejo: Se puede producir una espera de montaje o tardar más de lo habitual si la proximidad por espacio de archivo está habilitada y un nodo tiene un volumen que contiene múltiples espacios de archivos. Si un volumen es seleccionable para recibir datos, IBM Spectrum Protect espera a dicho volumen.

## Proximidad de agrupaciones de almacenamiento de copias

En relación con la utilización de la función de proximidad en las agrupaciones de almacenamiento de copia, existen varios aspectos que debe tener en cuenta. La proximidad de agrupaciones de almacenamiento de copia, especialmente por nodo o espacio de archivo, implica más volúmenes parcialmente llenos y actividad de reclamación fuera del local potencialmente innecesaria.

Las agrupaciones de almacenamiento primario tienen un rol de recuperación diferente del de las agrupaciones de almacenamiento de copia. Normalmente, se utilizan las agrupaciones de almacenamiento primario para recuperar datos a los clientes directamente. En caso de desastre, cuando se pierde el servidor y los clientes, puede utilizar volúmenes de agrupación de almacenamiento de copia fuera del sitio para recuperar las agrupaciones de almacenamiento primario. Los tipos de escenarios de recuperación pueden ayudarle a determinar si utilizar la función de proximidad en las agrupaciones de almacenamiento de copia.

La asignación generalmente resulta en el llenado parcial de volúmenes cuando se asigna por nodo o por espacio de archivos. Sin embargo, los volúmenes parcialmente llenos son menos frecuentes cuando aproxima por grupo. Los volúmenes parcialmente llenos se pueden aceptar para agrupaciones de almacenamiento primarias puesto que los volúmenes permanecen disponibles y se pueden llenar durante el siguiente proceso de migración. Sin embargo, los volúmenes parcialmente llenos pueden ser inaceptables para las agrupaciones de almacenamiento de copia cuyos volúmenes de agrupación de almacenamiento se llevan fuera del local de forma inmediata. Si utiliza la función de proximidad para agrupaciones de almacenamiento de copia, debe tomar las siguientes decisiones:

- Mover fuera del sitio más volúmenes parcialmente llenos y aumentar la actividad de reclamación cuando se disminuye o se alcanza el umbral de reclamación.
- Dejar en el local esos volúmenes parcialmente llenos hasta que se llenen y asumir el riesgo de no tener ninguna copia fuera del local de los datos de esos volúmenes.
- Si va a aproximar por grupo para utilizar la máxima capacidad posible de cinta.

Cuando la función de proximidad está inhabilitada para una agrupación de almacenamiento de copia, normalmente solo quedan unos pocos volúmenes parcialmente llenos una vez realizada la copia de seguridad de la agrupación de almacenamiento de copia.

Considere sus opciones detenidamente antes de utilizar la función de proximidad para las agrupaciones de almacenamiento de copia, y si utilizar o no la grabación simultánea. Si no utiliza la grabación simultánea y utiliza la función de proximidad para sus agrupaciones de almacenamiento primario, es posible que desee inhabilitar la función de proximidad para las agrupaciones de almacenamiento de copia. La proximidad de agrupaciones de almacenamiento de copia es recomendable si tiene pocos clientes y cada uno de ellos tiene grandes cantidades de datos de copia de seguridad incremental a diario. Para la proximidad con la grabación simultánea, debe asegurarse de que los parámetros de proximidad sean idénticos para las agrupaciones de almacenamiento primario y las agrupaciones de almacenamiento de copia.

## Planificación y activación de la función de proximidad

Entender los efectos de la función de proximidad puede ayudar a reducir el número de montajes de medios, aprovechar mejor el espacio en volúmenes secuenciales y mejorar la eficacia de las operaciones de servidor.

### Acerca de esta tarea

En la Tabla 1 se enumeran las cuatro opciones de proximidad que puede especificar en los mandatos DEFINE STGPOOL y UPDATE STGPOOL. La tabla muestra los efectos de la proximidad en los datos pertenecientes a los nodos que son miembros de grupos de proximidad y nodos que no son miembros de ningún grupo de proximidad.

Tabla 1. Opciones de proximidad y efectos sobre los datos de los nodos

Opción de proximidad	Si un nodo no está definido como miembro de un grupo de proximidad	Si un nodo está definido como miembro de un grupo de proximidad
No	Los datos del nodo no se colocan juntos.	Los datos del nodo no se colocan juntos.

Opción de proximidad	Si un nodo no está definido como miembro de un grupo de proximidad	Si un nodo está definido como miembro de un grupo de proximidad
<b>Grupo</b>	El servidor almacena los datos del nodo en el menor número posible de volúmenes de la agrupación de almacenamiento.	El servidor almacena los datos del nodo y otros nodos que pertenecen al mismo grupo de proximidad en el menor número posible de volúmenes.
<b>Nodo</b>	El servidor almacena los datos del nodo en el menor número posible de volúmenes.	El servidor almacena los datos del nodo en el menor número posible de volúmenes.
<b>Espacio de archivos</b>	El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento.	El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento.

Tabla 2. Opciones del grupo de proximidad y efectos sobre los datos de espacio de archivos

Opción de proximidad	Si el espacio de archivos no está definido como miembro de un grupo de proximidad	Si el espacio de archivos está definido como miembro de un grupo de proximidad
<b>No</b>	Los datos del espacio de archivos no se colocan juntos.	Los datos del espacio de archivos no se colocan juntos.
<b>Grupo</b>	El servidor almacena los datos del espacio de archivos en el menor número posible de volúmenes de la agrupación de almacenamiento.	El servidor almacena los datos del espacio de archivos y otros espacios de archivos que pertenecen al mismo grupo de proximidad en el menor número posible de volúmenes.
<b>Nodo</b>	El servidor almacena los datos del nodo en el menor número posible de volúmenes.	El servidor almacena los datos del nodo en el menor número posible de volúmenes.
<b>Espacio de archivos</b>	El servidor almacena los datos del espacio de archivos del nodo en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento.	El servidor almacena los datos del espacio de archivos en el menor número posible de volúmenes. Si un nodo tiene varios espacios de archivos, el servidor almacenará los datos de los diversos espacios de archivos en diferentes volúmenes de la agrupación de almacenamiento.

## Procedimiento

Para determinar si colocar y cómo los datos, complete los siguientes pasos:

- Determine cómo organizar los datos, si por nodo de cliente, grupo de nodos de cliente o espacio de archivos. Para colocar por grupo, decida cómo agrupar los nodos:
  - Si la finalidad es la de ahorrar espacio, tal vez desee agrupar los nodos pequeños juntos para utilizar mejor las cintas.
  - Si la finalidad es la de agilizar las restauraciones de cliente, agrupe los nodos juntos de forma que completen las menores cintas posible. Al agrupar nodos, los datos de cada nodo se distribuyen en dos o más cintas y así se pueden montar más cintas simultáneamente durante una operación de restauración sin consulta multisesión.
  - Si el objetivo es departamentalizar los datos, puede agrupar los nodos por departamento.
- Para colocar los grupos, complete los siguientes pasos:
  - Defina los grupos de proximidad con el mandato DEFINE COLLOGROUP.
  - Agregar nodos de cliente a los grupos de proximidad con el mandato DEFINE COLLOCMEMBER.

Los mandatos de consulta siguientes están disponibles para ayudarle a aproximar grupos:

QUERY COLLOGROUP

Muestra los grupos de proximidad definidos en el servidor.

QUERY NODE

Muestra el grupo de proximidad, si lo hay, al cual pertenece el nodo.

QUERY NODEDATA

Muestra información sobre los datos para uno o más nodos en una agrupación de almacenamiento de acceso secuencial.

QUERY STGPOOL

Muestra información sobre la ubicación de los datos de cliente en una agrupación de almacenamiento de acceso secuencial, así como de la cantidad de espacio que ocupa un nodo en un volumen.

También puede utilizar los scripts de servidor IBM Spectrum Protect o scripts de Perl para visualizar información que puede ser útil para definir los grupos de proximidad.

3. Especifique cómo colocar los datos en una agrupación de almacenamiento emitiendo el mandato DEFINE STGPOOL o UPDATE STGPOOL y especificando el parámetro COLLOCATE.

## Qué hacer a continuación

---

Recomendación: Para reducir el número de montajes de medios, utilice el espacio en volúmenes secuenciales de forma más eficiente, y habilite la proximidad, complete los pasos siguientes:

- Defina una jerarquía de agrupación de almacenamiento y una política que requiera que los archivos con copia de seguridad, archivados o gestionados por espacio se almacenen inicialmente en agrupaciones de almacenamiento en disco.

Cuando se migran los archivos de una agrupación de almacenamiento de disco, el servidor intenta migrar todos los archivos pertenecientes al nodo de cliente o al grupo de proximidad que utiliza más espacio en disco en la agrupación de almacenamiento. Este proceso funciona bien con la opción de proximidad ya que el servidor intenta colocar todos los archivos de un determinado cliente en el mismo volumen de almacenamiento de acceso secuencial.

- Utilice volúmenes reutilizables para agrupaciones de almacenamiento de acceso secuencial para permitir al servidor seleccionar nuevos volúmenes para la proximidad.
- Especifique la opción de cliente COLLOCATEBYFILESPEC para limitar el número de cintas en las que se deben grabar los objetos asociados con una especificación de archivo. Esta opción de proximidad hace que la función de proximidad del servidor sea más eficaz; no anula la función de proximidad del espacio de archivos ni la del nodo.

## Gestión de dispositivos de cinta

---

Las operaciones rutinarias de cinta incluyen la preparación de volúmenes de cinta para su utilización, controlar cómo y cuándo se reutilizan los volúmenes y asegurarse de que hay suficientes volúmenes disponibles. También debe responder a las solicitudes de operador y gestionar bibliotecas, unidades, discos, vías de acceso y transportadores de datos.

- Preparación de medios extraíbles  
Debe preparar los medios extraíbles antes de utilizarlos para almacenar datos. Las tareas de preparación típicas incluyen el etiquetado y el dar de alta volúmenes.
- Gestión del inventario de volúmenes  
Puede gestionar el inventario de volúmenes controlando el acceso del servidor a los volúmenes, reutilizando las cintas y reutilizando los volúmenes que se utilizan para las operaciones de copia de seguridad de la base de datos y las operaciones de exportación. También puede gestionar el inventario manteniendo un suministro de volúmenes reutilizables.
- Volúmenes grabados parcialmente  
Los volúmenes grabados parcialmente son siempre volúmenes privados, incluso si su estado era reutilizable antes de que el servidor los montara. El servidor realiza el seguimiento del estado original de los volúmenes reutilizables y les devuelve al estado reutilizable cuando están vacíos.
- Operaciones con bibliotecas compartidas  
Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI bibliotecas. La biblioteca física se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas. Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas de IBM Spectrum Protect.
- Gestión de solicitudes del servidor para los volúmenes  
IBM Spectrum Protect muestra solicitudes y mensajes de estado a todos los clientes administrativos de línea de mandato que se han iniciado en modalidad de consola. Estos mensajes de solicitud a menudo tienen un límite de tiempo. Las operaciones satisfactorias de servidor deben completarse dentro del límite de tiempo que se ha especificado; de lo contrario, la operación supera el tiempo de espera.

## Preparación de medios extraíbles

---

Debe preparar los medios extraíbles antes de utilizarlos para almacenar datos. Las tareas de preparación típicas incluyen el etiquetado y el dar de alta volúmenes.

### Acerca de esta tarea

---

Cuando IBM Spectrum Protect accede a un volumen de medios extraíbles, verifica el nombre de volumen en la cabecera de la etiqueta para asegurarse de que se ha accedido al volumen correcto.

Los volúmenes de cinta deben estar etiquetados antes de que el servidor pueda utilizarlos.

## Procedimiento

---

Para preparar un volumen para su uso, complete los pasos siguientes:

1. Etiquete el volumen emitiendo el mandato LABEL LIBVOLUME.
2. En el caso de bibliotecas automatizadas, compruebe el volumen de la biblioteca. Para obtener instrucciones, consulte Incorporar volúmenes en una biblioteca automatizada, Recomendación: Si utiliza el mandato LABEL LIBVOLUME con unidades de una biblioteca automatizada, puede etiquetar los volúmenes y darlos de alta en un solo mandato.
3. Si la agrupación de almacenamiento no puede contener los volúmenes reutilizables (MAXSCRATCH=0), identifique el volumen en IBM Spectrum Protect por nombre para que se pueda acceder al volumen más tarde.

Si la agrupación de almacenamiento puede contener volúmenes reutilizables (MAXSCRATCH se establece en un valor distinto de cero), omita este paso.

- Etiquetado de volúmenes de cinta  
Debe etiquetar los volúmenes de cinta antes de que el servidor pueda utilizarlos.
- Incorporar volúmenes en una biblioteca automatizada  
Puede dar de alta un volumen en una biblioteca automatizada utilizando el mandato CHECKIN LIBVOLUME.

## Etiquetado de volúmenes de cinta

---

Debe etiquetar los volúmenes de cinta antes de que el servidor pueda utilizarlos.

### Acerca de esta tarea

---

En el caso de las bibliotecas automatizadas, se le pedirá que inserte el volumen en la ranura de entrada/salida de la biblioteca. Si no hay disponible ninguna estación de entrada/salida (E/S) conveniente, inserte el volumen en una ranura vacía. Puede etiquetar los volúmenes cuando los incorpore o antes de incorporarlos.

### Procedimiento

---

Para etiquetar volúmenes de cinta antes de incorporarlos, lleve a cabo los pasos siguientes:

1. Etiquete los volúmenes de cinta emitiendo el mandato LABEL LIBVOLUME. Por ejemplo, para denominar un volumen de biblioteca VOLUME1 en una biblioteca denominada LIBRARY 1, emita el siguiente mandato:

```
label libvolume library1 volume1
```

Requisito: Debe haber al menos una unidad disponible. La unidad no la puede utilizar otro proceso de IBM Spectrum Protect. Si una unidad está desocupada, se considera que no está disponible.

2. Para sobrescribir una etiqueta existente, especifique el parámetro `OVERWRITE=YES`. De forma predeterminada, el mandato LABEL LIBVOLUME no graba encima de la etiqueta existente.
- Etiquetado de volúmenes en una SCSI biblioteca  
Puede etiquetar los volúmenes individualmente o bien utilizar IBM Spectrum Protect para buscar volúmenes en la biblioteca y etiquetar los volúmenes encontrados.

#### Tareas relacionadas:

Etiquetado de nuevos volúmenes utilizando AUTOLABEL

#### Referencia relacionada:

[LABEL LIBVOLUME](#) (Etiquetar un volumen de biblioteca)

## Incorporar volúmenes en una biblioteca automatizada

---

Puede dar de alta un volumen en una biblioteca automatizada utilizando el mandato CHECKIN LIBVOLUME.

### Antes de empezar

---

Para etiquetar automáticamente cintas antes de darlas de alta, emita el mandato DEFINE LIBRARY y especifique el parámetro AUTOLABEL=YES. Utilizando el parámetro AUTOLABEL, se elimina la necesidad de preetiquetar un conjunto de cintas.

### Acerca de esta tarea

---

Los volúmenes que el servidor utiliza para cualquier fin debe tener un nombre exclusivo. Este requisito es válido para todos los volúmenes, tanto si se utilizan para las agrupaciones de almacenamiento como si se emplean para operaciones como una copia de



seguridad o exportación de base de datos. El requisito se aplica también a los volúmenes que residen en distintas bibliotecas pero que utiliza el mismo servidor.

Sugerencias:

- No utilice una única biblioteca para los volúmenes que tienen etiquetas de código de barras y volúmenes que no tienen etiquetas de código de barras. La exploración de código de barras puede tardar mucho tiempo para volúmenes no etiquetados.
- El servidor acepta sólo cintas que están etiquetadas con etiquetas estándares IBM®.
- Todos los volúmenes que tienen un código de barras que empieza por `CLN` se trata como una cinta de limpieza.
- Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

## Procedimiento

---

1. Para dar de alta un volumen de almacenamiento en una biblioteca, emita el mandato `CHECKIN LIBVOLUME`.  
Consejo: El mandato siempre se ejecuta como un proceso en segundo plano. Espere a que finalice el proceso `CHECKIN LIBVOLUME` procesando antes de definir volúmenes, o el proceso de definición fallará. Puede ahorrar tiempo si da de alta volúmenes como parte de la operación de etiquetado.
  2. Dé un nombre a la biblioteca y especifique si el volumen es uno privado o reutilizable. En función de si utiliza volúmenes reutilizables o privados, realice uno de los pasos siguientes:
    - Si utiliza únicamente volúmenes reutilizables, compruebe que haya disponibles suficientes volúmenes reutilizables. Por ejemplo, puede necesitar etiquetar más volúmenes. A medida que se utilizan los volúmenes, también puede tener que aumentar el número de volúmenes reutilizables permitidos en la agrupación de almacenamiento definida para esta biblioteca.
    - Si desea utilizar volúmenes privados además o en lugar de volúmenes reutilizables en la biblioteca, defina volúmenes en la agrupación de almacenamiento utilizando el mandato `DEFINE VOLUME`. Debe etiquetar y dar de alta los volúmenes que defina.
- Incorporar un volumen en una biblioteca SCSI  
Puede dar de alta un volumen emitiendo el mandato `CHECKIN LIBVOLUME` y especificando el parámetro `SEARCH=NO`. IBM Spectrum Protect solicita que el operador de montaje cargue el volumen en el puerto de entrada/salida de la biblioteca.
  - Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca  
Cuando tenga muchos volúmenes para dar de alta y desee evitar emitir un mandato `CHECKIN LIBVOLUME` para cada volumen, puede buscar los nuevos volúmenes en las ranuras de almacenamiento. El servidor ha detectado volúmenes que todavía no se han añadido al inventario de volúmenes.
  - Incorporación de volúmenes desde los puertos de entrada/salida de la biblioteca  
Puede buscar volúmenes etiquetados en todas las ranuras de puertos de entrada/salida en masa y el servidor puede darlos de alta automáticamente.
  - Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas  
Puede ahorrar tiempo al dar de alta volúmenes en las bibliotecas que tengan lectores de códigos de barras utilizando los caracteres de las etiquetas del código de barras como nombres para los volúmenes.
  - Incorporación de volúmenes utilizando un lector de códigos de barras  
Puede ahorrar tiempo al dar de alta volúmenes utilizando un lector de códigos de barras, si la biblioteca tiene uno.
  - Comprobación de volúmenes en una biblioteca completa con intercambio  
Si no hay ranuras vacías disponibles en la biblioteca cuando dé de alta los volúmenes, la operación de registro fallará a menos que se habilite *intercambio*. Si habilita el intercambio y la biblioteca está llena, el servidor seleccionará un volumen para expulsar y, a continuación, da de alta el volumen que ha solicitado.
  -  Sistemas operativos Windows Volúmenes privados y volúmenes reutilizables  
Para optimizar el almacenamiento en cinta, revise la información sobre los volúmenes privados y los volúmenes reutilizables. Utilice los volúmenes privados y los volúmenes reutilizables adecuadamente.
  -  Sistemas operativos Windows Direcciones de elementos para las ranuras de almacenamiento de biblioteca  
Una dirección de elemento es un número que indica la ubicación física de una unidad o ranura de almacenamiento de una biblioteca automatizada.

### Tareas relacionadas:

Etiquetado de volúmenes de cinta

## Incorporar un volumen en una biblioteca SCSI

---

Puede dar de alta un volumen emitiendo el mandato `CHECKIN LIBVOLUME` y especificando el parámetro `SEARCH=NO`. IBM Spectrum Protect solicita que el operador de montaje cargue el volumen en el puerto de entrada/salida de la biblioteca.

## Procedimiento

---

1. Emita el mandato `CHECKIN LIBVOLUME`.



Por ejemplo, para dar de alta el volumen VOL001, introduzca el mandato siguiente:

```
checkin libvolume tapelib vol001 search=no status=scratch
```

2. Responda a la solicitud del servidor.

- Si la biblioteca tiene un puerto de entrada/salida, se le solicitará que inserte una cinta en el puerto de entrada/salida.
- Si la biblioteca no tiene un puerto de entrada/salida, se le solicitará que inserte una cinta en una de las ranuras de la biblioteca. Las direcciones de elementos identifican estas ranuras. Por ejemplo, el servidor detecta que la primera ranura vacía está en la dirección de elemento 5. Se devuelve el siguiente mensaje:

```
ANR8306I 001: Inserte el volumen 8MM VOL001 R/W en la ranura con la dirección de elemento 5 de la biblioteca TAPELIB en no más de 60 minutos; emita 'REPLY' junto con el identificador de solicitud cuando esté preparado.
```

Si no sabe la ubicación de la dirección de elemento 5 en la biblioteca, consulte la hoja de trabajo del dispositivo. Para encontrar la hoja de trabajo, revise la documentación de la biblioteca. Tras insertar el volumen tal como se le ha solicitado, responda al mensaje desde un cliente administrativo de IBM Spectrum Protect. Emita el mandato REPLY, seguido del número de solicitud (el número que aparece el principio de la solicitud de montaje). Por ejemplo:

```
reply 1
```

Consejo: Las direcciones de elementos a veces se numeran empezando por un número distinto de 1. Consulte la hoja de trabajo para estar seguro. Si no se lista ninguna hoja de trabajo para su dispositivo en IBM® Support Portal for IBM Spectrum Protect, consulte la documentación de la biblioteca.

Si especifica un tiempo de espera de 0 utilizando el parámetro opcional WAITTIME en el mandato CHECKIN LIBVOLUME, no es necesario el mandato REPLY. El tiempo de espera predeterminado es de 60 minutos.

## Incorporación de volúmenes desde las ranuras de almacenamiento de la biblioteca

---

Cuando tenga muchos volúmenes para dar de alta y desee evitar emitir un mandato CHECKIN LIBVOLUME para cada volumen, puede buscar los nuevos volúmenes en las ranuras de almacenamiento. El servidor ha detectado volúmenes que todavía no se han añadido al inventario de volúmenes.

### Procedimiento

---

1. Abra la biblioteca y coloque los nuevos volúmenes en ranuras no utilizadas. Por ejemplo, para un dispositivo SCSI, abra la puerta de acceso de la biblioteca, coloque todos los nuevos volúmenes en ranuras no utilizadas, y cierre la puerta.
2. Si los volúmenes no están etiquetados, utilice el mandato LABEL LIBVOLUME para etiquetar el volumen.
3. Emita el mandato CHECKIN LIBVOLUME con el parámetro SEARCH=YES.

#### Referencia relacionada:

[CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)

## Incorporación de volúmenes desde los puertos de entrada/salida de la biblioteca

---

Puede buscar volúmenes etiquetados en todas las ranuras de puertos de entrada/salida en masa y el servidor puede darlos de alta automáticamente.

### Antes de empezar

---

Emita el mandato LABEL LIBVOLUME para etiquetar volúmenes que no estén etiquetados.

### Acerca de esta tarea

---

Para bibliotecas SCSI, el servidor explora todos los puertos de entrada/salida de la biblioteca buscando volúmenes. Si encuentra un volumen que contiene una etiqueta de volumen válida, se le da de alta automáticamente.

### Procedimiento

---

Emita el mandato CHECKIN LIBVOLUME y especifique el parámetro SEARCH=BULK.

- Para cargar una cinta en una unidad y leer la etiqueta, especifique el parámetro CHECKLABEL=YES. Una vez que el servidor ha leído la etiqueta, desplaza la cinta de la unidad a una ranura de almacenamiento.
- Para que el servidor utilice el lector de códigos de barras para verificar las etiquetas externas de las cintas, especifique el parámetro CHECKLABEL=BARCODE. Cuando está habilitada la lectura de códigos de barras, el servidor lee la etiqueta y desplaza la cinta desde el puerto de entrada/salida a una ranura de almacenamiento.

## Incorporación de volúmenes utilizando los lectores de código de barras de las bibliotecas

---

Puede ahorrar tiempo al dar de alta volúmenes en las bibliotecas que tengan lectores de códigos de barras utilizando los caracteres de las etiquetas del código de barras como nombres para los volúmenes.

### Acerca de esta tarea

---

El servidor lee las etiquetas de código de barras y utiliza la información para grabar las etiquetas de los medios internos. En el caso de los volúmenes que no tienen etiquetas de código de barras, el servidor monta los volúmenes en una unidad e intenta leer la etiqueta interna grabada.

### Procedimiento

---

Emita el mandato CHECKIN LIBVOLUME con el parámetro CHECKLABEL=BARCODE. Por ejemplo, para utilizar un lector de códigos de barras para buscar en una biblioteca denominada TAPELIB y dar de alta una cinta reutilizable, emita el mandato siguiente:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

## Incorporación de volúmenes utilizando un lector de códigos de barras

---

Puede ahorrar tiempo al dar de alta volúmenes utilizando un lector de códigos de barras, si la biblioteca tiene uno.

### Acerca de esta tarea

---

Cuando dé de alta un volumen, puede especificar si las etiquetas de los medios se leen durante el proceso de incorporación. Si la comprobación de etiquetas está activada, IBM Spectrum Protect monta cada volumen para leer la etiqueta interna y sólo da de alta un volumen si está correctamente etiquetado. La comprobación de etiquetas puede impedir futuros errores cuando se utilizan los volúmenes de las agrupaciones de almacenamiento, pero también aumenta el tiempo de proceso en el registro.

Si un volumen no tiene etiqueta de código de barras, IBM Spectrum Protect monta los volúmenes en una unidad e intenta leer la etiqueta registrada.

### Procedimiento

---

Para dar de volúmenes utilizando un lector de códigos de barras, emita el mandato CHECKIN LIBVOLUME y especifique CHECKLABEL=BARCODE. Por ejemplo, para utilizar el lector de códigos de barras para dar de alta todos los volúmenes como volúmenes reutilizables en una biblioteca denominada TAPELIB, emita el siguiente mandato:

```
checkin libvolume tapelib search=yes status=scratch checklabel=barcode
```

#### Tareas relacionadas:

Preparación de medios extraíbles

#### Referencia relacionada:

[CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)

## Comprobación de volúmenes en una biblioteca completa con intercambio

---

Si no hay ranuras vacías disponibles en la biblioteca cuando dé de alta los volúmenes, la operación de registro fallará a menos que se habilite *intercambio*. Si habilita el intercambio y la biblioteca está llena, el servidor seleccionará un volumen para expulsar y, a continuación, da de alta el volumen que ha solicitado.

### Acerca de esta tarea

---

El servidor selecciona el volumen de expulsión comprobando primero cualquier volumen reutilizable disponible y, a continuación, para el volumen que está montado con menor frecuencia. El servidor expulsa el volumen que se selecciona para la operación de intercambio

de la biblioteca y sustituye el volumen expulsado por el volumen que se está incorporando.

## Procedimiento

Para intercambiar volúmenes si una ranura de biblioteca vacía no está disponible para dar de alta un volumen, emita el mandato CHECKIN LIBVOLUME y especifique el parámetro SWAP=YES. Por ejemplo, al dar de alta un volumen que se denomina VOL1 en una biblioteca que se denomina AUTO y especifica el intercambio, emita el siguiente mandato:

```
checkin libvolume auto voll swap=yes
```

### Tareas relacionadas:

Gestión de una biblioteca completa con una ubicación de desbordamiento

### Referencia relacionada:

➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

## Volúmenes privados y volúmenes reutilizables

Para optimizar el almacenamiento en cinta, revise la información sobre los volúmenes privados y los volúmenes reutilizables. Utilice los volúmenes privados y los volúmenes reutilizables adecuadamente.

Los volúmenes privados no se pueden sobrescribir cuando se solicita un montaje reutilizable. No se puede dar de alta un volumen con estado reutilizable cuando dicho volumen lo utiliza una agrupación de almacenamiento, para exportar datos, para hacer una copia de seguridad de una base de datos o hacer la copia en un volumen de conjunto de copias de seguridad.

Los volúmenes grabados parcialmente siempre son privados. Los volúmenes tienen un estado de cero o privado, pero cuando IBM Spectrum Protect almacena datos en ellos, su estado pasará a ser privado.

Tabla 1. Usos de los volúmenes privados y los volúmenes reutilizables

Tipo de volumen	Cuándo debe utilizarse
Volúmenes privados	Utilice volúmenes privados para regular los volúmenes utilizados por agrupaciones de almacenamiento individuales y para controlar manualmente los volúmenes. Para definir volúmenes privados, emita el mandato DEFINE VOLUME. Para restauraciones de bases de datos, volcados de memoria o cargas, o para las operaciones de importación, debe especificar volúmenes privados.
Volúmenes reutilizables	En algunos casos, puede simplificar la gestión de volúmenes utilizando volúmenes reutilizables. Puede utilizar volúmenes reutilizables en las siguientes circunstancias: <ul style="list-style-type: none"><li>• Cuando no sea necesario definir cada volumen de agrupación de almacenamiento.</li><li>• Cuando desee aprovechar la automatización de dispositivos robot.</li><li>• Cuando distintas agrupaciones de almacenamiento comparten una biblioteca automatizada y las agrupaciones de almacenamiento pueden adquirir volúmenes de forma dinámica desde los volúmenes reutilizables de la biblioteca. Los volúmenes no tiene que estar preasignados en las agrupaciones de almacenamiento.</li></ul>

### Tareas relacionadas:

Cambiar el estado de un volumen de una biblioteca automatizada

### Referencia relacionada:

➔ CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

➔ DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

## Direcciones de elementos para las ranuras de almacenamiento de biblioteca

Una dirección de elemento es un número que indica la ubicación física de una unidad o ranura de almacenamiento de una biblioteca automatizada.

Si una biblioteca tiene puertos de entrada/salida, puede añadir y eliminar medios utilizando los puertos. Si no existe ningún puerto de entrada/salida, debe cargar cintas en las ranuras de almacenamiento.

Si carga cintas en las ranuras de almacenamiento, debe responder a las solicitudes de montaje que identifican las ranuras de almacenamiento con direcciones de elementos. Si especifica un tiempo de espera de 0 en los mandatos CHECKIN LIBVOLUME o LABEL LIBVOLUME, no es necesario que responda a una solicitud de montaje.

Para direcciones de elemento, consulte la documentación del fabricante del dispositivo o vaya a IBM® Support Portal for IBM Spectrum Protect y busque direcciones de elemento.

**Referencia relacionada:**

[CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)

[LABEL LIBVOLUME \(Etiquetar un volumen de biblioteca\)](#)

## Gestión del inventario de volúmenes



---

Puede gestionar el inventario de volúmenes controlando el acceso del servidor a los volúmenes, reutilizando las cintas y reutilizando los volúmenes que se utilizan para las operaciones de copia de seguridad de la base de datos y las operaciones de exportación. También puede gestionar el inventario manteniendo un suministro de volúmenes reutilizables.

### Acerca de esta tarea

---

Cada volumen que utiliza un servidor debe tener un nombre exclusivo, tanto si los volúmenes se utilizan para las agrupaciones de almacenamiento como si se utilizan para operaciones tales como la copia de seguridad o la exportación de una base de datos. Los volúmenes que residen en distintas bibliotecas pero que utiliza el mismo servidor también tienen que tener un nombre exclusivo.

- **Control de acceso a volúmenes**  
Puede utilizar distintos métodos para controlar el acceso a los volúmenes.
- **Reutilización de cintas**  
Para asegurarse un suministro adecuado de cintas, puede caducar archivos antiguos, reclamar volúmenes y suprimir volúmenes que alcanzan el final de su vida. También puede mantener un suministro de volúmenes reutilizables.
- **Mantenimiento de un suministro de volúmenes reutilizables**  
Debe establecer el número máximo de volúmenes reutilizables para una agrupación de almacenamiento lo suficientemente grande para el uso estimado.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux** **Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM**  
En el caso de las bibliotecas que contienen medios WORM (Write Once Read Many), puede impedir que se cancelen transacciones de almacenamiento de datos manteniendo un suministro de volúmenes privados nuevos o reutilizables en la biblioteca. La cancelación de transacciones puede hacer que se pierdan medios WORM.
- **Gestión del inventario de volumen en bibliotecas automatizadas**  
El servidor de IBM Spectrum Protect utiliza un inventario de volúmenes de biblioteca para realizar el seguimiento de los volúmenes reutilizables y privados disponibles en una biblioteca automatizada. Debe asegurarse de que el inventario es coherente con los volúmenes que están físicamente en la biblioteca.

## Control de acceso a volúmenes

---

Puede utilizar distintos métodos para controlar el acceso a los volúmenes.

### Procedimiento

---

Para controlar el acceso a los volúmenes, realice cualquiera de las siguientes acciones:

- Para impedir que el servidor monte un volumen, emita el mandato UPDATE VOLUME y especifique el parámetro ACCESS=UNAVAILABLE.
- Para convertir a los volúmenes en no disponibles y enviarlos a otro lugar para su protección, utilice una agrupación de almacenamiento de copias o una agrupación de almacenamiento de datos activos.
- Puede hacer copia de seguridad de las agrupaciones de almacenamiento primarias en una agrupación de almacenamiento de copias y después enviar los volúmenes de la agrupación de almacenamiento de copias fuera del local.
- Puede copiar versiones activas de los datos de copia de seguridad de cliente en agrupaciones de almacenamiento de datos activos y, a continuación, enviar los volúmenes a otro lugar.
- Puede hacer el seguimiento de los volúmenes de agrupación de almacenamiento de copias y los volúmenes de agrupación de datos activos cambiando la modalidad de acceso a fuera del local y actualizando el histórico de volúmenes para identificar su ubicación.

**Referencia relacionada:**

➔ UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

## Reutilización de cintas

---

Para asegurarse un suministro adecuado de cintas, puede caducar archivos antiguos, reclamar volúmenes y suprimir volúmenes que alcanzan el final de su vida. También puede mantener un suministro de volúmenes reutilizables.

### Acerca de esta tarea

---

A lo largo del tiempo, los medios envejecen, y es posible que no necesite algunos de los datos de copia de seguridad almacenados en ellos. Puede definir políticas de servidor para determinar cuántas versiones de copia de seguridad se retienen y cuánto tiempo se retienen. Puede utilizar el proceso de caducidad para suprimir archivos que ya no necesite. Puede guardar los datos que necesite en los medios. Cuando ya no los necesite, puede reclamar y reutilizar los medios.

### Procedimiento

---

1. Suprima los datos de clientes no necesarios ejecutando regularmente el proceso de caducidad. El proceso de caducidad suprime los datos que ya no son válidos porque superan las especificaciones de retención de la política o porque los usuarios o los administradores han suprimido las versiones activas de los datos.
2. Reutilice los volúmenes de las agrupaciones de almacenamiento ejecutando el proceso de reclamación.

El proceso de reclamación consolida todos los datos sin caducar traspasándolos de un gran número de volúmenes a un número menor de volúmenes. A continuación, es posible devolver los medios a la agrupación de almacenamiento y reutilizarlos.

3. Puede reutilizar volúmenes que contengan copias de seguridad de bases de datos obsoletas o datos exportados que ya no sean necesarios suprimiendo el historial de volumen.

Para que el servidor pueda reutilizar volúmenes de los que se realiza un seguimiento en el historial de volumen, debe suprimir la información de volúmenes del archivo de historial de volumen emitiendo el mandato DELETE VOLHISTORY.

Consejo: Si el servidor utiliza la función gestor recuperación tras desastre (DRM), la información del volumen se suprime automáticamente durante el proceso del mandato MOVE DRMEDIA.

4. Determine cuándo alcanzan los volúmenes de cinta el final de su vida. Puede utilizar el servidor para visualizar las estadísticas acerca de los volúmenes, incluidos el número de operaciones de grabación completadas en el medio y el número de errores de grabación. Los volúmenes privados y los volúmenes reutilizables muestran los siguientes datos estadísticos:

#### Volúmenes privados

Para los medios inicialmente definidos como volúmenes privados, el servidor mantiene estos datos estadísticos, incluso aunque se reclame el volumen. Puede comparar la información con el número de operaciones y errores de grabación recomendado por el fabricante.

#### Volúmenes reutilizables

Para los medios inicialmente definidos como volúmenes reutilizables, el servidor sobrescribe estos datos estadísticos cada vez que se reclamen los volúmenes.

5. Reclame cualquier dato válido de los volúmenes que alcanzan el final de su vida. Si los volúmenes están en bibliotecas automatizadas, delos de baja del inventario de volúmenes. Suprima los volúmenes privados de la base de datos con el mandato DELETE VOLUME.
6. Asegúrese de que los volúmenes estén disponibles para la rotación de cintas de modo que la agrupación de almacenamiento no se quede sin espacio. Puede utilizar el Centro de operaciones para supervisar la disponibilidad de los volúmenes reutilizables. Asegúrese de que el número de volúmenes reutilizables sea lo suficientemente grande como para satisfacer la demanda. Para obtener más información, consulte Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM.  
medios WORM: Las unidades WORM (una sola grabación, varias lecturas) pueden desperdiciar medios si el servidor cancela transacciones por no encontrarse los volúmenes disponibles para completar la operación de copia seguridad. Una vez que el servidor grabe en los volúmenes WORM, el estado de los volúmenes no se puede reutilizar, incluso aunque se hayan cancelado las transacciones (por ejemplo, si se cancela una copia de seguridad debido a la falta de medios en el dispositivo). Para minimizar los medios WORM desperdiciados, realice las acciones siguientes:
  - a. Asegúrese de que el número máximo de volúmenes reutilizables para la agrupación de almacenamiento es, como mínimo, equivalente al número de ranuras de almacenamiento de la biblioteca.
  - b. Dé de alta suficientes volúmenes en el inventario de volúmenes del dispositivo para la carga prevista.

Si la mayoría de operaciones de copia de seguridad son para archivos pequeños, el control del tamaño de las transacciones puede afectar a la forma como se utilizan los discos WORM. Las transacciones más pequeñas significa que se desperdicia menos

espacio cuando una transacción como una operación de copia de seguridad debe ser cancelada. El tamaño de transacción lo controlan una opción de servidor, TXNGROUPMAX, y una opción de cliente, TXNBYTELIMIT.

**Tareas relacionadas:**

Migración de datos a unidades actualizadas  
Gestión de solicitudes del servidor para los volúmenes

**Referencia relacionada:**

- 🔗 DELETE VOLHISTORY (Suprimir información histórica de volúmenes secuencial)
- 🔗 DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)
- 🔗 EXPIRE INVENTORY (Iniciar manualmente el proceso de caducidad de inventario)
- 🔗 Opción Txnbytelimit
- 🔗 TXNGROUPMAX, opción de servidor

## Mantenimiento de un suministro de volúmenes reutilizables

---

Debe establecer el número máximo de volúmenes reutilizables para una agrupación de almacenamiento lo suficientemente grande para el uso estimado.

### Acerca de esta tarea

---

En el momento de definir una agrupación de almacenamiento, debe especificarse el número máximo de volúmenes reutilizables que puede utilizar la misma. El servidor solicita automáticamente un volumen reutilizable cuando es necesario. Si el número de volúmenes reutilizables que el servidor está utilizando para la agrupación de almacenamiento sobrepasa el máximo especificado, es posible que la agrupación de almacenamiento se quede sin espacio.

### Procedimiento

---

Cuando una agrupación de almacenamiento necesita más que el número máximo de volúmenes reutilizables, puede seguir una o ambas de las acciones siguientes:

1. Aumentar el número máximo de volúmenes reutilizables emitiendo el mandato UPDATE STGPOOL y especificando el parámetro MAXSCRATCH.
2. Consiga volúmenes disponibles para su reutilización ejecutando el proceso de caducidad y el de reclamación a fin de consolidar los datos en menos volúmenes.
  - a. Emita el mandato EXPIRE INVENTORY para ejecutar el proceso de caducidad.  
Consejo: De forma predeterminada este proceso se ejecuta cada día automáticamente. También puede especificar la opción de servidor EXPINTERVAL en el archivo de opciones del servidor, dsmserv.opt, para ejecutar el proceso de caducidad automáticamente. Si el valor es 0 significa que debe utilizar el mandato EXPIRE INVENTORY para ejecutar el proceso de caducidad.
  - b. Emita el mandato RECLAIM STGPOOL para ejecutar el proceso de reclamación.  
Consejo: También puede especificar umbrales de reclamación cuando defina la agrupación de almacenamiento utilizando el mandato DEFINE STGPOOL y especificando el parámetro RECLAIMPROCESS.

### Qué hacer a continuación

---

Si necesita más volúmenes para futuras operaciones de copia de seguridad, etiquete más volúmenes reutilizables utilizando el mandato LABEL LIBVOLUME.

**Tareas relacionadas:**

Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada

**Referencia relacionada:**

- 🔗 EXPIRE INVENTORY (Iniciar manualmente el proceso de caducidad de inventario)
- 🔗 LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)
- 🔗 RECLAIM STGPOOL (Reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial)
- 🔗 UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

## Mantenimiento de un suministro de volúmenes en una biblioteca que contiene los medios WORM

---

En el caso de las bibliotecas que contienen medios WORM (Write Once Read Many), puede impedir que se cancelen transacciones de almacenamiento de datos manteniendo un suministro de volúmenes privados nuevos o reutilizables en la biblioteca. La cancelación de transacciones puede hacer que se pierdan medios WORM.

## Acerca de esta tarea

---

IBM Spectrum Protect cancela una transacción si los volúmenes, ya sean privados o reutilizables, no están disponibles para completar la operación de almacenamiento de datos. Una vez que IBM Spectrum Protect empieza una transacción y graba en un volumen WORM, el espacio grabado del volumen no puede volverse a utilizar aunque se cancele la transacción.

Por ejemplo, si tiene volúmenes WORM que tienen 2,6 GB cada uno de ellos y un cliente empieza a hacer copia de seguridad de un archivo de 12 GB. Si IBM Spectrum Protect no puede adquirir un quinto volumen reutilizable después de que cuatro volúmenes estén llenos, IBM Spectrum Protect cancela la operación de copia de seguridad. Los cuatro volúmenes que IBM Spectrum Protect ya ha llenado no se pueden volver a utilizar.

Para minimizar la cancelación de transacciones, debe disponer de suficientes volúmenes disponibles en la biblioteca para gestionar operaciones de cliente esperadas como, por ejemplo, copias de seguridad.

## Procedimiento

---

1. Asegúrese de que la agrupación de almacenamiento asociada con la biblioteca tenga suficientes volúmenes reutilizables. Emita el mandato UPDATE STGPOOL y especifique el parámetro MAXSCRATCH.
2. Para gestionar la carga esperada, dé de alta un número suficiente de volúmenes privados o reutilizables en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME.
3. Para controlar el tamaño de la transacción, especifique la opción de servidor TXNGROUPMAX y la opción de cliente TXNBYTELIMIT. Si los clientes tienden a almacenar archivos pequeños, el control del tamaño de las transacciones puede afectar al uso de los volúmenes WORM. Las transacciones más pequeñas desperdician menos espacio cuando se debe cancelar una transacción como una copia de seguridad.

### Referencia relacionada:

- [CHECKIN LIBVOLUME \(Dar de alta un volumen de almacenamiento en una biblioteca\)](#)
- [UPDATE STGPOOL \(Actualizar una agrupación de almacenamiento\)](#)
- [Opción Txnbytelimit](#)
- [TXNGROUPMAX, opción de servidor](#)

## Gestión del inventario de volumen en bibliotecas automatizadas

---

El servidor de IBM Spectrum Protect utiliza un inventario de volúmenes de biblioteca para realizar el seguimiento de los volúmenes reutilizables y privados disponibles en una biblioteca automatizada. Debe asegurarse de que el inventario es coherente con los volúmenes que están físicamente en la biblioteca.

El inventario de volúmenes de biblioteca es independiente del inventario de volúmenes de cada agrupación de almacenamiento. Para añadir un volumen a un inventario de volúmenes de biblioteca, incorpore un volumen a dicha biblioteca de IBM Spectrum Protect.

Una lista de los volúmenes en el inventario de volúmenes de la biblioteca puede no ser idéntica a una lista de volúmenes en el inventario de agrupación de almacenamiento del dispositivo. Por ejemplo, puede dar de alta volúmenes reutilizables a la biblioteca pero no puede definirlos en una agrupación de almacenamiento. Si no se seleccionan volúmenes reutilizables para las operaciones de copia de seguridad, puede definir los volúmenes privados en una agrupación de almacenamiento pero no puede darlos de alta en el inventario de volúmenes para el dispositivo.

Para garantizar que el inventario de volúmenes de la biblioteca del servidor sea exacto, debe dar de baja los volúmenes para eliminarlos físicamente de una biblioteca SCSI. Cuando se da de baja un volumen que utiliza una agrupación de almacenamiento, el volumen permanece en la agrupación de almacenamiento. Si debe montar el volumen cuando se ha extraído, se mostrará un mensaje en la consola del operador de montaje con una solicitud para dar de alta el volumen. Si la operación de dar de alta no es correcta, el servidor marcará el volumen como no disponible.

Cuando un volumen está en el inventario de volúmenes de biblioteca, puede cambiar su estado de reutilizable a privado.

Para comprobar si el inventario de volumen para la biblioteca del servidor es coherente con los volúmenes que se encuentran físicamente en la biblioteca, puede auditar la biblioteca. El inventario puede volverse inexacto si los volúmenes se mueven dentro y fuera de la biblioteca sin informar al servidor utilizando las operaciones de dar de alta o de dar de baja volúmenes.

- Cambiar el estado de un volumen de una biblioteca automatizada  
Puede cambiar el estado de un volumen de privado a reutilizable o de reutilizable a privado.
- Eliminación de volúmenes de una biblioteca automatizada  
Puede eliminar volúmenes de una biblioteca automatizada si ha exportado los datos a un volumen y desea importar los datos a otro sistema. También es posible que desee eliminar volúmenes para crear espacio para nuevos volúmenes.
- Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada  
Al definir una agrupación de almacenamiento asociada con una biblioteca automatizada, puede especificarse un número máximo

de volúmenes reutilizables que sea igual a la capacidad física de la biblioteca. Si el servidor utiliza un número mayor de volúmenes reutilizables para la agrupación de almacenamiento, debe asegurarse de que hay suficientes volúmenes disponibles.

- **Gestión de una biblioteca completa con una ubicación de desbordamiento**  
Como aumenta la demanda de almacenamiento, el número de volúmenes que necesita para una agrupación de almacenamiento puede superar la capacidad física de una biblioteca automatizada. Para crear espacio disponible para nuevos volúmenes y para supervisar los volúmenes existentes, puede definir una ubicación de desbordamiento para una agrupación de almacenamiento.
- **Auditoría de inventarios de volúmenes en una biblioteca**  
Puede auditar una biblioteca automatizada para asegurarse de que el inventario de volúmenes de biblioteca es coherente con los volúmenes que están físicamente en la biblioteca. Es posible que desee auditar una biblioteca si el inventario de volúmenes de biblioteca se ha distorsionado debido al traspaso manual de volúmenes en la biblioteca o a problemas con la base de datos.

**Tareas relacionadas:**

Incorporar volúmenes en una biblioteca automatizada

**Referencia relacionada:**

[AUDIT LIBRARY](#) (Inventarios de volúmenes de auditoría en una biblioteca automatizada)

## Cambiar el estado de un volumen de una biblioteca automatizada

---

Puede cambiar el estado de un volumen de privado a reutilizable o de reutilizable a privado.

### Procedimiento

---

Para cambiar el estado de un volumen, emita el mandato UPDATE LIBVOLUME. Por ejemplo, para cambiar el estado de un volumen que se denomina VOL1 a un volumen privado, emita el siguiente mandato:

```
update libvolume lib1 vol1 status=private
```

Restricciones:

- No puede cambiar el estado de un volumen de privado a reutilizable si el volumen pertenece a una agrupación de almacenamiento o se define en el archivo histórico de volúmenes.
- Los volúmenes privados deben ser volúmenes definidos por el administrador, ya sea sin datos o con datos no válidos. No pueden ser volúmenes grabados parcialmente que contienen datos activos. Las estadísticas de los volúmenes se pierden cuando se modifican los estados de los volúmenes.

## Eliminación de volúmenes de una biblioteca automatizada

---

Puede eliminar volúmenes de una biblioteca automatizada si ha exportado los datos a un volumen y desea importar los datos a otro sistema. También es posible que desee eliminar volúmenes para crear espacio para nuevos volúmenes.

### Acerca de esta tarea

---

De forma predeterminada, el servidor monta el volumen que se extrae y verifica la etiqueta interna. Una vez comprobada la etiqueta, el servidor elimina el volumen del inventario de volúmenes de la biblioteca y, seguidamente, lo traslada al puerto de entrada/salida o a la estación de E/S de la biblioteca que convenga. Si la biblioteca no tiene un puerto de entrada/salida, el servidor solicita que el operador de montaje elimine el volumen de una ranura o dispositivo dentro de la biblioteca.

### Procedimiento

---

- Para eliminar un volumen de una biblioteca automatizada, emita el mandato CHECKOUT LIBVOLUME.
- Para las bibliotecas automatizadas con varios puertos de entrada/salida, emita el mandato CHECKOUT LIBVOLUME y especifique el parámetro REMOVE=BULK. El servidor expulsa el volumen al siguiente puerto de entrada/salida disponible.

### Qué hacer a continuación

---

Si da de baja un volumen definido en una agrupación de almacenamiento y el servidor debe acceder más tarde al volumen, el servidor requiere que se dé de alta el volumen. Para devolver volúmenes a una biblioteca, emita el mandato CHECKIN LIBVOLUME.

**Referencia relacionada:**

[CHECKIN LIBVOLUME](#) (Dar de alta un volumen de almacenamiento en una biblioteca)

[CHECKOUT LIBVOLUME](#) (Dar de baja un volumen de almacenamiento de una biblioteca)



# Mantenimiento de un suministro de volúmenes reutilizables en una biblioteca automatizada

---

Al definir una agrupación de almacenamiento asociada con una biblioteca automatizada, puede especificarse un número máximo de volúmenes reutilizables que sea igual a la capacidad física de la biblioteca. Si el servidor utiliza un número mayor de volúmenes reutilizables para la agrupación de almacenamiento, debe asegurarse de que hay suficientes volúmenes disponibles.

## Procedimiento

---

Si el número de volúmenes reutilizables que el servidor está utilizando para la agrupación de almacenamiento sobrepasa el número que se especifica en la definición de la agrupación de almacenamiento, lleve a cabo los pasos siguientes:

1. Puede añadir volúmenes reutilizables a la biblioteca emitiendo el mandato CHECKIN LIBVOLUME.  
Consejo: Puede que tenga que utilizar una ubicación suplementaria para sacar volúmenes de la biblioteca y dejar sitio para los volúmenes reutilizables. Para obtener más información, consulte Gestión de una biblioteca completa con una ubicación de desbordamiento.
2. Aumentar el número máximo de volúmenes reutilizables que se pueden añadir a una agrupación de almacenamiento emitiendo el mandato UPDATE STGPOOL y especificando el parámetro MAXSCRATCH.

## Qué hacer a continuación

---

Es posible que necesite más volúmenes para futuras operaciones de recuperación, de modo que tenga en cuenta etiquetar y apartar volúmenes reutilizables adicionales.

### Tareas relacionadas:

Mantenimiento de un suministro de volúmenes reutilizables

# Gestión de una biblioteca completa con una ubicación de desbordamiento

---

Como aumenta la demanda de almacenamiento, el número de volúmenes que necesita para una agrupación de almacenamiento puede superar la capacidad física de una biblioteca automatizada. Para crear espacio disponible para nuevos volúmenes y para supervisar los volúmenes existentes, puede definir una ubicación de desbordamiento para una agrupación de almacenamiento.

## Acerca de esta tarea

---

El servidor realiza un seguimiento de los volúmenes que se mueven al área de desbordamiento y hace que las ranuras de almacenamiento estén disponibles para nuevos volúmenes.

## Procedimiento

---

1. Cree una ubicación de desbordamiento de un volumen. Defina o actualice la agrupación de almacenamiento asociada con la biblioteca automatizada emitiendo el mandato DEFINE STGPOOL o UPDATE STGPOOL y especificando el parámetro OVFLLOCATION. Por ejemplo, para crear una ubicación de desbordamiento denominada ROOM2948 para una agrupación de almacenamiento denominada ARCHIVEPOOL, emita el siguiente mandato:  

```
update stgpool archivepool ovflocation=Room2948
```
2. Cuando necesite crear espacio en la biblioteca para los volúmenes reutilizables, mueva volúmenes completos a la ubicación de desbordamiento emitiendo el mandato MOVE MEDIA. Por ejemplo, para mover todos los volúmenes completos de la agrupación de almacenamiento especificada fuera de la biblioteca, emita el siguiente mandato:  

```
move media * stgpool=archivepool
```
3. Dé de alta los volúmenes reutilizables según sea necesario.  
Restricción: Si un volumen tiene una entrada en el archivo histórico de volúmenes, no puede darlo de alta como volumen reutilizable. Para obtener más información, consulte Incorporar volúmenes en una biblioteca automatizada.
4. Identifique las cintas reutilizables vacías de la ubicación de desbordamiento emitiendo el mandato QUERY MEDIA. Por ejemplo, emita el siguiente mandato:  

```
query media * stg=* whereovflocation=Room2948 wherestatus=empty
```
5. Si el servidor solicita volúmenes adicionales, localice y dé de alta los volúmenes desde la ubicación de desbordamiento.

Para buscar volúmenes en una ubicación de desbordamiento, emita el mandato QUERY MEDIA. También puede utilizar el mandato QUERY MEDIA para generar mandatos para dar de alta volúmenes.

Por ejemplo, para listar los volúmenes de la ubicación de desbordamiento y a la vez generar los mandatos para dar de alta esos volúmenes en la biblioteca, emita un mandato parecido al del siguiente ejemplo:

```
query media format=cmd stgpool=archivepool whereovflocation=Room2948
cmd="checkin libvol autolib &vol status=private"
cmdfilename="\storage\move\media\checkin.vols"
```

Sugerencias:

- Las solicitudes de montaje del servidor incluyen la ubicación de los volúmenes.
- Para especificar el número de días que deben transcurrir hasta que los volúmenes sean elegibles para su procesamiento, emita el mandato UPDATE STGPOOL y especifique el parámetro REUSEDELAY.
- El archivo que contiene los mandatos generados se puede ejecutar utilizando el mandato MACRO de IBM Spectrum Protect.

**Referencia relacionada:**

- 🔗 MOVE MEDIA (Trasladar medios de agrupación de almacenamiento de acceso secuencial)
- 🔗 QUERY MEDIA (Consultar un medio de agrupación de almacenamiento de acceso secuencial)
- 🔗 UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

## Auditoría de inventarios de volúmenes en una biblioteca

---

Puede auditar una biblioteca automatizada para asegurarse de que el inventario de volúmenes de biblioteca es coherente con los volúmenes que están físicamente en la biblioteca. Es posible que desee auditar una biblioteca si el inventario de volúmenes de biblioteca se ha distorsionado debido al traspaso manual de volúmenes en la biblioteca o a problemas con la base de datos.

### Procedimiento

---

1. Asegúrese de que no haya volúmenes montados en las unidades de biblioteca. Si hay algún volumen montado en estado IDLE, emita el mandato DISMOUNT VOLUME para desmontarlo.
2. Audite el inventario de volumen emitiendo el mandato AUDIT LIBRARY. Realice una de las siguientes acciones:
  - Si la biblioteca tiene un lector de códigos de barras, puede ahorrar tiempo utilizando el lector de códigos de barras para identificar volúmenes. Por ejemplo, para auditar la biblioteca TAPELIB mediante su lector de códigos de barras, emita el siguiente mandato:

```
audit library tapelib checklabel=barcode
```

- Si la biblioteca no tiene un lector de códigos de barras, emita el mandato AUDIT LIBRARY sin especificar CHECKLABEL=BARCODE. El servidor monta cada volumen para verificar la etiqueta. Una vez verificada la etiqueta, el servidor finaliza la auditoría de los volúmenes restantes.

### Resultados

---

El servidor suprime los volúmenes ausentes del inventario y actualiza las ubicaciones de los volúmenes que se han movido desde la última auditoría.

Restricción: El servidor no puede agregar volúmenes nuevos al inventario durante una operación de auditoría.

**Tareas relacionadas:**

Etiquetado de volúmenes de cinta

**Referencia relacionada:**

- 🔗 AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- 🔗 DISMOUNT VOLUME (Desmontar un volumen por nombre de volumen)

## Volúmenes grabados parcialmente

---

Los volúmenes grabados parcialmente son siempre volúmenes privados, incluso si su estado era reutilizable antes de que el servidor los montara. El servidor realiza el seguimiento del estado original de los volúmenes reutilizables y les devuelve al estado reutilizable cuando están vacíos.

Excepto los volúmenes en las bibliotecas automatizadas, el servidor no reconoce un volumen reutilizable hasta que el volumen no está montado. A continuación, el estado del volumen cambia a privado y el volumen se define automáticamente como componente de la agrupación de almacenamiento para la que se ha efectuado la solicitud de montaje.

**Tareas relacionadas:**

Cambiar el estado de un volumen de una biblioteca automatizada

## Operaciones con bibliotecas compartidas

Las bibliotecas compartidas son bibliotecas lógicas que están representadas físicamente por SCSI bibliotecas. La biblioteca física se controla mediante el servidor de IBM Spectrum Protect que está configurado como gestor de bibliotecas. Los servidores de IBM Spectrum Protect que utilizan el tipo de biblioteca SHARED son clientes de biblioteca en el servidor de gestión de bibliotecas de IBM Spectrum Protect.

El cliente de biblioteca se pone en contacto con el gestor de bibliotecas cuando este se inicia y el dispositivo de almacenamiento se inicializa, o después de definir un gestor de bibliotecas para un cliente de biblioteca. El cliente de biblioteca confirma que el servidor contactado es el gestor de bibliotecas para el dispositivo de biblioteca especificado. El cliente de biblioteca también compara con el gestor de bibliotecas las definiciones de unidades para comprobar que son coherentes. El cliente de biblioteca se pone en contacto con el gestor de biblioteca para cada una de las operaciones siguientes:

**Montaje de un volumen**

Un cliente de biblioteca envía una solicitud al gestor de biblioteca para acceder a un volumen en el dispositivo de biblioteca compartida. Para un volumen reutilizable, el cliente de biblioteca no especifica un nombre de volumen. Si el gestor de bibliotecas no puede acceder al volumen solicitado, o si los volúmenes reutilizables no están disponibles, el gestor de bibliotecas deniega la solicitud de montaje. Si la operación de montaje es correcta, el gestor de bibliotecas devuelve el nombre de la unidad en el que está montado el volumen.

**Liberación de un volumen**

Cuando un cliente de biblioteca ya no necesita acceder a un volumen, notifica al gestor de bibliotecas que el volumen se puede retornar a volumen reutilizable. La base de datos del gestor de bibliotecas se actualiza con la nueva ubicación del volumen, que es ahora el inventario del servidor de biblioteca. El volumen se suprime del inventario de volumen del cliente de biblioteca.

En la Tabla 1 se muestra la interacción entre los clientes de biblioteca y el gestor de bibliotecas al procesar las operaciones de IBM Spectrum Protect.

Tabla 1. Cómo procesan los servidores habilitados para SAN las operaciones de IBM Spectrum Protect

<b>Operación (mandato)</b>	<b>Gestor de bibliotecas</b>	<b>Cliente de biblioteca</b>
Consultar volúmenes de biblioteca  (QUERY LIBVOLUME)	Muestra los volúmenes dados de alta en la biblioteca. En el caso de volúmenes privados, también se muestra el servidor propietario.	No aplicable.
Dar de alta y de baja volúmenes de biblioteca  (CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME)	Envía los mandatos al dispositivo de biblioteca.	No aplicable.  Cuando se requiere una operación de dar de alta a causa de una operación de restauración de un cliente, se envía una solicitud al servidor del gestor de bibliotecas.
Trasladar medios y trasladar medios de DRM  (MOVE MEDIA, MOVE DRMEDIA)	Válido sólo para los volúmenes que utiliza el servidor del gestor de bibliotecas.	Solicita que el servidor del gestor de bibliotecas complete la operación. Genera un proceso de baja en el servidor gestor de bibliotecas.
Auditar inventario de biblioteca  (AUDIT LIBRARY)	Sincroniza el inventario con el dispositivo de biblioteca.	Sincroniza el inventario con el servidor del gestor de bibliotecas.

<b>Operación (mandato)</b>	<b>Gestor de bibliotecas</b>	<b>Cliente de biblioteca</b>
Etiquetar un volumen de biblioteca  (LABEL LIBVOLUME)	Etiqueta y da de alta los volúmenes.	No aplicable.
Desmontar un volumen  (DISMOUNT VOLUME)	Envía la solicitud al dispositivo de biblioteca.	Solicita que el servidor del gestor de bibliotecas complete la operación.
Consultar un volumen  (QUERY VOLUME)	Comprueba si el volumen es propiedad del cliente de biblioteca solicitante y comprueba si el volumen está en el dispositivo de biblioteca.	Solicita que el servidor del gestor de bibliotecas complete la operación.

## Gestión de solicitudes del servidor para los volúmenes

IBM Spectrum Protect muestra solicitudes y mensajes de estado a todos los clientes administrativos de línea de mandato que se han iniciado en modalidad de consola. Estos mensajes de solicitud a menudo tienen un límite de tiempo. Las operaciones satisfactorias de servidor deben completarse dentro del límite de tiempo que se ha especificado; de lo contrario, la operación supera el tiempo de espera.

### Acerca de esta tarea

En las bibliotecas automatizadas, utilice los mandatos CHECKIN LIBVOLUME y LABEL LIBVOLUME para insertar cartuchos en ranuras. Si se especifica un valor para el parámetro WAITTIME, se muestra un mensaje de respuesta. Si el valor del parámetro es 0, no hace falta respuesta alguna. Cuando emite el mandato CHECKOUT LIBVOLUME, debe insertar cartuchos en las ranuras y, en todos los casos, se muestra un mensaje de respuesta.

### Procedimiento

La tabla siguiente proporciona información acerca de cómo manejar diferentes tareas de soportes del servidor.

<b>Tarea</b>	<b>Detalles</b>
Utilizar el cliente administrativo para mensajes de montaje	El servidor envía mensajes de estado de la solicitud de montaje a la consola del servidor y a todos los clientes administrativos de línea de mandatos en modalidad de montaje o de consola.  Para iniciar un cliente administrativo de línea de mandatos en modalidad de montaje, emita el mandato dsmadm -mountmode en el cliente administrativo de línea de mandatos.
Recibir mensajes sobre las bibliotecas automatizadas	Puede ver mensajes de montaje y mensajes de error sobre las bibliotecas automatizadas en los clientes administrativos de línea de mandatos en modalidad de montaje o de consola. Los mensajes de montaje se envían a la biblioteca y no a un operador. La información relativa a problemas con la biblioteca se envían a la cola de mensajes de montaje.
Obtenga información acerca de las solicitudes de operador pendientes	Para obtener información acerca de las solicitudes de operador pendientes, utilice el mandato QUERY REQUEST o consulte la cola de mensajes de montaje de un cliente administrativo de línea de mandatos iniciado en modalidad de montaje. Cuando emita el mandato QUERY REQUEST, el servidor muestra las acciones solicitadas y la cantidad de tiempo que queda antes de que las solicitudes superen el tiempo de espera.

Tarea	Detalles
Responder a las solicitudes de operador	<p>Si el servidor requiere una respuesta explícita al completarse una solicitud de montaje, utilice el mandato REPLY.</p> <p>El parámetro <i>número_solicitud</i> especifica el número de identificación de solicitud que indica al servidor cuál de las operaciones de operador pendientes se ha completado. Este número de tres dígitos se visualiza siempre como parte del mensaje de solicitud.</p>
Cancelar una solicitud de operador	<p>Para cancelar una solicitud de montaje para una biblioteca, emita el mandato CANCEL REQUEST. Para la mayoría de las solicitudes asociadas con las bibliotecas SCSI automatizadas, un operador debe completar una acción de hardware o del sistema para cancelar el montaje solicitado. En este tipo de solicitudes, el servidor no acepta el mandato CANCEL REQUEST.</p> <p>El mandato CANCEL REQUEST debe incluir el número de identificación de la solicitud. Este número está incluido en el mensaje de solicitud.</p> <p>Si desea marcar el volumen solicitado como UNAVAILABLE, emita el mandato CANCEL REQUEST y especifique el parámetro PERMANENT. Si especifica el parámetro PERMANENT, el servidor no intentará montar el volumen solicitado de nuevo. Esto es útil si, por ejemplo, el volumen está en un sitio remoto o si no está disponible.</p>
Responder a una solicitud para dar de alta el volumen	<p>Si el servidor no encuentra un volumen determinado que debe montarse en una biblioteca automatizada, el servidor pide que el operador dé de alta el volumen.</p> <p>Si el volumen solicitado está disponible, colóquelo en la biblioteca y efectúe el alta. Para obtener más información, consulte Incorporar volúmenes en una biblioteca automatizada.</p> <p>Si el volumen solicitado no está disponible, actualice la modalidad de acceso del volumen emitiendo el mandato UPDATE VOLUME y especificando el parámetro ACCESS=UNAVAILABLE. A continuación, cancele la solicitud de alta utilizando el mandato CANCEL REQUEST. No cancele el proceso de cliente que ha originado la solicitud. Utilice el mandato QUERY REQUEST para obtener el ID de la solicitud que desea cancelar.</p> <p>Si no responde a la solicitud de dar de alta desde el servidor dentro del periodo de espera de montaje especificado para la clase de dispositivo para la agrupación de almacenamiento, el servidor marcará el volumen como no disponible.</p>
Determinar qué volúmenes se montan	<p>Para generar un informe de todos los volúmenes montados actualmente para que los utilice el servidor, emita el mandato QUERY MOUNT. El informe muestra los volúmenes que están montados, las unidades que acceden a ellos y si los volúmenes están en uso.</p>
Desmontar volúmenes desocupados	<p>Cuando un volumen está desocupado, el servidor lo mantiene montado durante un periodo de tiempo especificado por el parámetro de retención de montaje para la clase de dispositivo. El uso de un valor de retención de montaje puede reducir el tiempo de acceso cuando los volúmenes se utilizan reiteradamente.</p> <p>Para desmontar un volumen desocupado desde la unidad donde está montado, emita el mandato DISMOUNT VOLUME.</p> <p>Para obtener información sobre definición de tiempos de retención de montaje, consulte el apartado Control de la cantidad de tiempo que un volumen permanece montado.</p>

**Referencia relacionada:**

[QUERY REQUEST](#) (Consultar una o más solicitudes de montaje pendientes)

## Gestión de unidades de cinta

Puede consultar, actualizar y suprimir las unidades de cinta. También puede limpiar las unidades de cinta y configurar el cifrado de unidades de cinta y la validación de datos.

- Actualización de unidades  
Puede cambiar los atributos de una definición de unidad para coger una unidad externa y reconfigurarla.

- Validación de datos durante operaciones de lectura/escritura en cinta  
Para validar datos e identificar los datos dañados, puede utilizar una característica que se llama protección de bloques lógicos. Si utiliza la protección de bloques lógicos, IBM Spectrum Protect inserta un valor de comprobación de redundancia cíclica (CRC) al final de cada bloque lógico de datos cuando se graba en cinta.
- Limpieza de unidades de cinta  
Puede utilizar el servidor para gestionar la limpieza de las unidades de cinta. El servidor puede controlar la limpieza de las unidades de cinta en bibliotecas SCSI.
- Sustitución de unidades de cinta  
Si sustituye una unidad en una biblioteca de cintas definida en IBM Spectrum Protect, debe suprimir las definiciones de unidad y vía de acceso de la unidad antigua y definir la nueva unidad y vía de acceso.

## Actualización de unidades

Puede cambiar los atributos de una definición de unidad para coger una unidad externa y reconfigurarla.

### Acerca de esta tarea

Puede cambiar los siguientes atributos de una unidad.

- La dirección de elemento, si la unidad está en una SCSI
- La frecuencia de limpieza
- El estado de la unidad: en línea o fuera de línea


Restricción: Si una unidad se está utilizando, no se puede cambiar el número de elemento ni el nombre de dispositivo. Para obtener instrucciones sobre cómo externalizar unidades, consulte Poner las unidades de cinta fuera de línea.

Si un volumen está montado en la unidad pero el volumen está desocupado, se puede desmontar explícitamente. Para obtener instrucciones sobre cómo desmontar volúmenes desocupados, consulte Gestión de solicitudes del servidor para los volúmenes.

### Procedimiento

- Cambie la dirección de elemento de una unidad emitiendo el mandato UPDATE DRIVE. Por ejemplo, en una biblioteca denominada AUTO, cambie la dirección de elemento DRIVE3 a 119 emitiendo el mandato siguiente:


```
update drive auto drive3 element=119
```

- Cambie el nombre de dispositivo de una unidad emitiendo el mandato UPDATE PATH. Por ejemplo, para cambiar el nombre de dispositivo de una unidad denominada DRIVE3, emita el mandato siguiente:  Sistemas operativos AIX

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/rmt0
```

 Sistemas operativos Linux



```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=/dev/IBMtape0
```

 Sistemas operativos Windows

```
update path server1 drive3 srctype=server desttype=drive library=scsilib
device=mt3.0.0.0
```

- Poner las unidades de cinta fuera de línea  
Puede poner una unidad de cinta fuera de línea mientras se está utilizando. Por ejemplo, puede poner una unidad de cinta fuera de línea para completar el mantenimiento.

#### Referencia relacionada:

-  [UPDATE DRIVE \(Actualizar una unidad\)](#)
-  [UPDATE PATH \(Cambiar una vía de acceso\)](#)

## Validación de datos durante operaciones de lectura/escritura en cinta

Para validar datos e identificar los datos dañados, puede utilizar una característica que se llama protección de bloques lógicos. Si utiliza la protección de bloques lógicos, IBM Spectrum Protect inserta un valor de comprobación de redundancia cíclica (CRC) al final de cada bloque lógico de datos cuando se graba en cinta.

Con la protección de bloques lógicos, puede identificar los errores que se producen cuando se graban los datos en cinta y durante la transferencia de datos de la unidad de cinta a IBM Spectrum Protect a través de la red de área de almacenamiento. Las unidades que

dan soporte a la protección de bloques lógicos validan datos durante las operaciones de lectura y grabación. El servidor de IBM Spectrum Protect valida los datos durante las operaciones de lectura.

Si falla la validación por la unidad durante las operaciones de grabación, la anomalía puede indicar que los datos se han dañado durante la transferencia a cinta. En este caso, el servidor de IBM Spectrum Protect da error en la operación de grabación. Debe reiniciar la operación para continuar. Si falla la validación por la unidad durante las operaciones de lectura, la anomalía puede indicar que el soporte de cinta está dañado. Si falla la validación por el servidor de IBM Spectrum Protect durante las operaciones de lectura, la anomalía puede indicar que los datos se ha dañado durante la transferencia desde la unidad de cinta, y el servidor vuelve a intentar la operación. Si la validación falla constantemente, el servidor de IBM Spectrum Protect emite un mensaje de error que indica problemas de hardware o de conexión.

Si la protección de bloques lógicos está inhabilitada en una unidad de cinta o la unidad no admite la protección de bloques lógicos, el servidor de IBM Spectrum Protect podrá leer los datos protegidos. Sin embargo, los datos no se validan.

La protección de bloques lógicos es superior a la validación de CRC que puede especificar al definir o actualizar una agrupación de almacenamiento. Cuando especifica la validación de CRC para una agrupación de almacenamiento, los datos solo se validarán durante operaciones de auditoría de volumen. Los errores se identifican después de grabar los datos en cinta.

Restricciones:

- No puede utilizar la protección de bloques lógicos para datos secuenciales tales como conjuntos de copias de seguridad y copias de seguridad de bases de datos.
- La comprobación CRC afecta al rendimiento porque se necesita más utilización de procesador en el cliente y en el servidor para calcular y comparar valores CRC.
- Para un volumen reutilizable, si especifica la protección de bloque lógico para operaciones de lectura/escritura (LBPROTECT=READWRITE), no cambie el valor del parámetro en cualquier momento después de grabar los datos en el volumen. No se admite cambiar el valor del parámetro durante la vida del volumen en el servidor IBM Spectrum Protect.
- Unidades que dan soporte a la protección de bloques lógicos  
La protección de bloques lógicos solo está disponible para tipos de dispositivo ECARTRIDGE, 3592 y LTO. Las unidades 3592 compatibles incluyen IBM TS1130, TS1140 y generaciones posteriores. Las unidades LTO preparadas incluyen IBM LTO-5 y unidades LTO-6 soportadas. Las unidades Oracle StorageTek compatibles incluyen unidades con el formato T10000C y T10000D.
- Habilitación e inhabilitación de la protección de bloques lógicos  
Puede especificar la protección de bloques lógicos para operaciones de lectura y grabación, o sólo para operaciones de grabación. También puede inhabilitar la protección de bloques lógicos. De forma predeterminada, la protección de bloques lógicos está inhabilitada debido a efectos de rendimiento resultado de la comprobación de redundancia cíclica (CRC) en el servidor y en la unidad de cinta.
- Operaciones de lectura/escritura en volúmenes con protección de bloques lógicos  
Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen.
- Gestión de agrupaciones de almacenamiento en una biblioteca de cintas  
Para mezclar datos protegidos y no protegidos en una biblioteca, debe crear clases de dispositivo y distintas agrupaciones de almacenamiento para separar los datos. Si una clase de dispositivo está asociada a datos protegidos, puede especificar la protección de bloques lógicos para operaciones de lectura y grabación o solo para operaciones de grabación.

## Unidades que dan soporte a la protección de bloques lógicos

La protección de bloques lógicos solo está disponible para tipos de dispositivo ECARTRIDGE, 3592 y LTO. Las unidades 3592 compatibles incluyen IBM TS1130, TS1140 y generaciones posteriores. Las unidades LTO preparadas incluyen IBM LTO-5 y unidades LTO-6 soportadas. Las unidades Oracle StorageTek compatibles incluyen unidades con el formato T10000C y T10000D.

La siguiente tabla muestra los soportes y los formatos que se pueden utilizar con unidades que admitan la protección de bloques lógicos.

Unidad	Medio de cinta	Formatos de unidad
IBM TS1130	3592 Generación 2	3592-3 y 3592-3C
IBM TS1140	3592 Generación 2	Generación 2: 3592-3 y 3592-3C
	3592 Generación 3	Generación 3: 3592-4 y 3592-4C
IBM TS1150	3592 Generación 3	Generación 4: 3592-5 y 3592-5C
	3592 Generación 4	
IBM LTO-5	LTO-5	Ultrium 5 y Ultrium 5C

Unidad	Medio de cinta	Formatos de unidad
IBM LTO-6	LTO-6	Ultrium 6 y Ultrium 6C
	LTO-5	Ultrium 5 y Ultrium 5C
IBM LTO-7	LTO-7	Ultrium 7 y Ultrium 7C
	LTO-6	Ultrium 6 y Ultrium 6C
Oracle T10000C	Oracle StorageTek T10000 T2	T10000C y T10000C-C
Oracle T10000D	Oracle StorageTek T10000 T2	T10000D y T10000D-C

Sugerencias:

- Para habilitar la protección de bloques lógicos para un volumen de cinta y después reutilizar el volumen para hacer una copia de seguridad de los datos, debe habilitar la protección de bloques lógicos para esa clase de dispositivo y para la unidad.
- Si tiene una unidad 3592, LTO, u Oracle StorageTek que no permite protección de bloques lógicos, puede actualizar la unidad con firmware que proporcione protección de bloques lógicos.

La protección de bloques lógicos está disponible para unidades que estén en SCSI bibliotecas. Para obtener la información más actual sobre el soporte para la protección de bloques lógicos, consulte la nota técnica 1568108.

Para utilizar la protección de bloques lógicos para operaciones de grabación, todas las unidades de la biblioteca deben admitir este tipo de protección. Si una unidad no permite la protección de bloques lógicos, no se montarán los volúmenes que tengan acceso de lectura y grabación. No obstante, el servidor puede utilizar la unidad para montar volúmenes que tengan acceso de sólo lectura. El servidor de IBM Spectrum Protect lee y valida los datos protegidos si la protección de bloques lógicos está habilitada para las operaciones de lectura/escritura.

## Habilitación e inhabilitación de la protección de bloques lógicos

Puede especificar la protección de bloques lógicos para operaciones de lectura y grabación, o sólo para operaciones de grabación. También puede inhabilitar la protección de bloques lógicos. De forma predeterminada, la protección de bloques lógicos está inhabilitada debido a efectos de rendimiento resultado de la comprobación de redundancia cíclica (CRC) en el servidor y en la unidad de cinta.

### Acerca de esta tarea

Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen. Si cambia el valor de la protección de bloques lógicos, el cambio solo se aplica a los volúmenes vacíos. Los volúmenes que ya están llenos o los que se están llenando mantienen su estado de protección de bloques lógicos hasta que están vacíos y listos para ser llenados de nuevo. Por ejemplo, si inhabilita la protección de bloques lógicos y el servidor selecciona un volumen que está asociado con una clase de dispositivo que tiene protección de bloques lógicos, el servidor sigue grabando datos protegidos en el volumen.

Restricción: La protección de bloques lógicos solo está disponible para ciertos tipos de dispositivo. Para obtener más información, consulte Unidades que dan soporte a la protección de bloques lógicos.

### Procedimiento

1. Para habilitar la protección de bloques lógicos para tipos de dispositivo 3592, LTO y ECARTRIDGE, emita el mandato DEFINE DEVCLASS o UPDATE DEVCLASS y especifique el parámetro LBPROTECT. Por ejemplo, para especificar la protección de bloques lógicos durante las operaciones de lectura y escritura para una clase de dispositivo 3592 denominada 3592\_lbprotect, emita el mandato siguiente:

```
define devclass 3592_lbprotect library=3594 lbprotect=readwrite
```

Sugerencias:

- Si actualiza el valor del parámetro LBPROTECT de NO a READWRITE o WRITEONLY y el servidor selecciona un volumen de relleno sin protección de bloque lógico para las operaciones de grabación, el servidor emite un mensaje cada vez que se monta el volumen. El mensaje indica que los datos se grabarán en el volumen sin protección de bloque lógico. Para evitar que aparezca este mensaje o para que IBM Spectrum Protect solo grabe datos sin protección de bloque lógico, actualice el acceso de los volúmenes de relleno sin protección de bloque lógico a de solo lectura.
- Para mejorar el rendimiento, no especifique el parámetro CRCDATA en el mandato DEFINE STGPOOL ni en el mandato UPDATE STGPOOL.
- Cuando se validan los datos durante las operaciones de lectura, tanto por parte de la unidad como del servidor de IBM Spectrum Protect, puede ralentizar el rendimiento del servidor durante las operaciones de restauración y recuperación. Para reducir el tiempo necesario para las operaciones de restauración y recuperación, cambie el valor del parámetro



LBPROTECT de READWRITE a WRITEONLY. Una vez restaurados o recuperados los datos, puede restablecer el parámetro LBPROTECT en READWRITE.

2. Para inhabilitar la protección de bloques lógicos, emita el mandato DEFINE DEVCLASS o el mandato UPDATE DEVCLASS y especifique el parámetro LBPROTECT=NO.

Restricción: Si la protección de bloques lógicos está inhabilitada, el servidor no graba en una cinta vacía con protección de bloques lógicos. No obstante, si se selecciona un volumen de relleno con protección de bloques lógicos, el servidor sigue grabando en el volumen con protección de bloques lógicos. Para impedir que el servidor grabe en cintas con protección de bloques lógicos, cambie el acceso de los volúmenes de relleno con protección de bloques lógicos a de sólo lectura. Cuando se leen los datos, la unidad o el servidor no comprueban los resultados de la CRC.

Si se produce un siniestro y el sitio de recuperación tras desastre no tiene unidades que admitan protección de bloques lógicos, debe especificar el parámetro LBPROTECT=NO. Si las unidades de cinta se utilizan para operaciones de grabación, deberá cambiar el acceso de volumen para los volúmenes con datos protegidos a "sólo lectura" para impedir que el servidor utilice los volúmenes.

Si el servidor debe habilitar la protección de bloques lógicos, el servidor emite un mensaje de error indicando que la unidad no admite protección de bloques lógicos.

## Qué hacer a continuación

---

Para determinar si un volumen tiene protección de bloques lógicos, emita el mandato QUERY VOLUME y revise el valor del campo Logical Block Protection.

### Referencia relacionada:

- ➔ DEFINE DEVCLASS (Definir una clase de dispositivo)
- ➔ DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)
- ➔ QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)
- ➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

## Operaciones de lectura/escritura en volúmenes con protección de bloques lógicos

---

Las operaciones de lectura/escritura para vaciar o llenar volúmenes dependen de si dichos volúmenes tienen protección de bloques lógicos. Los bloques de datos protegidos y no protegidos no se pueden mezclar en el mismo volumen.

Si utiliza el mandato UPDATE DEVCLASS para cambiar el valor de la protección de bloques lógicos, el cambio solo se aplica a los volúmenes vacíos. Los volúmenes que ya están llenos o los que se están llenando mantienen su estado de protección de bloques lógicos hasta que están vacíos y listos para ser llenados de nuevo.

Por ejemplo, supongamos que cambia el valor del parámetro LBPROTECT de READWRITE a NO. Si el servidor selecciona un volumen que está asociado con la clase de dispositivo que tiene la protección de bloques lógicos, el servidor sigue grabando datos protegidos en el volumen.

Sugerencias:

- Si una unidad no admite la protección de bloques lógicos, no se pueden montar los volúmenes con protección de bloques lógicos para las operaciones de grabación. Para evitar que el servidor monte volúmenes protegidos para operaciones de grabación, cambie el acceso del volumen a sólo lectura. Además, inhabilite la protección de bloques lógicos para impedir que el servidor habilite la función en la unidad de cintas.
- Si una unidad no admite la protección de bloques lógicos, y la protección de bloques lógicos se inhabilita, el servidor lee los datos de los volúmenes protegidos. No obstante, ni servidor ni la unidad de cintas validan los datos.

### Referencia relacionada:

- ➔ QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)
- ➔ UPDATE DEVCLASS (Actualizar una clase de dispositivo)

## Gestión de agrupaciones de almacenamiento en una biblioteca de cintas

---

Para mezclar datos protegidos y no protegidos en una biblioteca, debe crear clases de dispositivo y distintas agrupaciones de almacenamiento para separar los datos. Si una clase de dispositivo está asociada a datos protegidos, puede especificar la protección de bloques lógicos para operaciones de lectura y grabación o solo para operaciones de grabación.

Para definir clases de dispositivos y agrupaciones de almacenamiento para una biblioteca TS3500 que tiene unidades LTO-5, para datos protegidos y no protegidos, puede emitir una serie de mandatos como se muestra en el ejemplo siguiente:

```
define library 3584 libtype=scsi
define devclass lbprotect library=3584 devicetype=lto lbprotect=readwrite
define devclass normal library=3584 devicetype=lto lbprotect=no
define stgpool lbprotect_pool lbprotect maxscratch=10
define stgpool normal_pool normal maxscratch=10
```

**Referencia relacionada:**

- DEFINE DEVCLASS (Definir una clase de dispositivo)
- DEFINE LIBRARY (Definir una biblioteca)
- DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

## Limpeza de unidades de cinta

---

Puede utilizar el servidor para gestionar la limpieza de las unidades de cinta. El servidor puede controlar la limpieza de las unidades de cinta en bibliotecas SCSI.

### Acerca de esta tarea

---

Debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones para poder limpiar unidades de cinta. Para las bibliotecas automatizadas, puede automatizar la limpieza especificando la frecuencia de las operaciones de limpieza y comprobando que haya un cartucho limpiador en el inventario de volúmenes de la biblioteca. IBM Spectrum Protect monta el cartucho limpiador tal y como se especifica. Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades controladas por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

Consejo: Si una biblioteca de cintas automatizada admite la limpieza de las unidades de la biblioteca, asegúrese de que la característica está habilitada.

Puede prevenir el desgaste prematuro de los cabezales de lectura/escritura de las unidades utilizando las funciones de limpieza de biblioteca que proporciona el fabricante del dispositivo.

Las unidades y las bibliotecas de fabricantes distintos se distinguen entre sí en la forma de gestionar los cartuchos limpiadores y en cómo informan de la presencia de un cartucho limpiador en una unidad. Es posible que el controlador de dispositivo no pueda abrir la unidad que contiene el cartucho limpiador. Los códigos de detección y de error que emiten los dispositivos para la limpieza de unidades son variados. La limpieza de unidades de la biblioteca normalmente es desconocida para las aplicaciones. Así pues, es posible que IBM Spectrum Protect no siempre detecte los cartuchos limpiadores en las unidades y puede que no sea capaz de determinar cuando empieza la limpieza.

Algunos dispositivos necesitan un cierto tiempo de inactividad entre solicitudes de montaje para iniciar la limpieza de unidades. Sin embargo, IBM Spectrum Protect intenta minimizar el tiempo de inactividad para una unidad. Esto puede suponer que se impida el buen funcionamiento de la limpieza de unidades de la biblioteca. Si esto sucediera, intente utilizar IBM Spectrum Protect para controlar la limpieza de unidades. Puede establecer la frecuencia de forma que coincida con las recomendaciones de limpieza del fabricante.

- Métodos para limpiar unidades de cinta  
Con el tiempo, los cabezales de lectura de las cintas pueden ensuciarse, lo que puede hacer que fallen las operaciones de lectura y grabación. Para evitar estos problemas, habilite la limpieza de cintas. Puede habilitar la limpieza de cintas de la unidad o desde IBM Spectrum Protect.
- Configuración del servidor para la limpieza de unidades en una biblioteca automatizada  
Al configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, puede especificar la frecuencia con la que desea que se limpien las unidades.
- Resolución de errores relacionados con la limpieza de unidades  
Al mover cartuchos dentro de una biblioteca, puede que coloque un cartucho de datos donde debería ir un cartucho limpiador. Revise el proceso que ha completado el servidor y los mensajes que se han emitido para resolver el problema.

## Métodos para limpiar unidades de cinta

---

Con el tiempo, los cabezales de lectura de las cintas pueden ensuciarse, lo que puede hacer que fallen las operaciones de lectura y grabación. Para evitar estos problemas, habilite la limpieza de cintas. Puede habilitar la limpieza de cintas de la unidad o desde IBM Spectrum Protect.

Puede elegir utilizar el método de limpieza de unidades de biblioteca o el método de limpieza de unidades de IBM Spectrum Protect, pero no ambos. Algunas bibliotecas SCSI proporcionan la limpieza automática de las unidades. Seleccione el método de limpieza de

unidades de biblioteca si está disponible. Si no está disponible o da problemas, utilice IBM Spectrum Protect para controlar la limpieza de unidades de biblioteca.

#### Método de limpieza de unidades de biblioteca

El método de limpieza de unidades de biblioteca proporciona varias ventajas para las bibliotecas de cintas automatizadas que utilizan esta función.

- Reduce la carga sobre el administrador de IBM Spectrum Protect de gestionar físicamente la limpieza de los cartuchos.
- Mejora las tasas de uso del cartucho de limpieza. La mayoría de bibliotecas de cintas hacen un seguimiento del número de veces que se pueden limpiar las unidades basándose en los indicadores de hardware. IBM Spectrum Protect utiliza un recuento bruto.
- Reduce las limpiezas innecesarias. Las unidades de cinta modernas no se tienen que limpiar a intervalos fijos, pueden detectar y solicitar cuándo necesitan una limpieza.

Los fabricantes que proporcionan un método de limpieza de unidades de biblioteca, recomiendan utilizarlo para evitar un desgaste prematuro de los cabezales de lectura/escritura de las unidades. Las unidades y las bibliotecas de fabricantes distintos se distinguen entre sí en la forma de gestionar los cartuchos limpiadores y en cómo informan de la presencia de un cartucho limpiador en una unidad. Es posible que el controlador de dispositivo no pueda abrir la unidad que contiene el cartucho limpiador. Los códigos de detección y de error que emiten los dispositivos para la limpieza de unidades son variados. La limpieza de unidades de biblioteca normalmente es transparente para todas las aplicaciones. No obstante, es posible que IBM Spectrum Protect no siempre detecte los cartuchos limpiadores en las unidades y puede que no sea capaz de determinar cuando empieza la limpieza.

#### Método de limpieza de unidades de IBM Spectrum Protect

Algunos dispositivos necesitan un cierto tiempo de inactividad entre solicitudes de montaje para iniciar la limpieza de unidades. Sin embargo, IBM Spectrum Protect intenta minimizar el tiempo de inactividad para una unidad. Esto puede suponer que se impida el buen funcionamiento de la limpieza de unidades de la biblioteca. Si esto sucediera, intente utilizar IBM Spectrum Protect para controlar la limpieza de unidades. Establezca la frecuencia de forma que coincida con las recomendaciones de limpieza del fabricante.

Si IBM Spectrum Protect controla el proceso de limpieza de unidades, inhabilite la función de limpieza de unidades de biblioteca para evitar problemas. Si la función de limpieza de unidades de biblioteca está habilitada, algunos dispositivos mueven automáticamente cualquier cartucho limpiador que encuentren en la biblioteca a ranuras de la biblioteca dedicados a cartuchos limpiadores. No podrá dar de alta un cartucho limpiador en el inventario de biblioteca de IBM Spectrum Protect hasta que inhabilite la función de limpieza de unidades de biblioteca.

Para habilitar la limpieza desde la unidad, siga las instrucciones proporcionadas por el fabricante de la misma. Para habilitar la limpieza utilizando IBM Spectrum Protect, consulte Configuración del servidor para la limpieza de unidades en una biblioteca automatizada.

## Configuración del servidor para la limpieza de unidades en una biblioteca automatizada

---

Al configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, puede especificar la frecuencia con la que desea que se limpien las unidades.

### Antes de empezar

---

Determine la frecuencia con la que se debe limpiar la unidad. Este paso es necesario para que pueda especificar el valor adecuado para el parámetro CLEANFREQUENCY en el mandato DEFINE DRIVE o UPDATE DRIVE. Por ejemplo, para limpiar una unidad tras procesar 100 GB de datos en la misma, tendría que especificar CLEANFREQUENCY=100.




Para obtener directrices sobre la frecuencia de limpieza, consulte la documentación del fabricante de la unidad. Si la documentación proporciona directrices para la frecuencia de limpieza en términos de horas de uso, puede convertir el valor en un valor en gigabytes completando los pasos siguientes :

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor de gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.

Puede especificar un valor para el parámetro CLEANFREQUENCY o especificar ASNEEDED para limpiar la unidad según sea necesario. Restricciones:

1. Para unidades IBM® 3592, debe especificar un valor numérico para el parámetro CLEANFREQUENCY. Si utiliza la frecuencia de limpieza que se indica en la documentación del producto, no limpiará las unidades más de la cuenta.

2. El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Para determinar si una unidad admite esta función, consulte la información de su sistema operativo.

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos soportados para AIX y Windows
-  Sistemas operativos Linux Dispositivos soportados para Linux

En la nota técnica, pulse en el nombre de la unidad para ver la información detallada. SI el valor ASNEEDED no está soportado, especifique el número de gigabytes.

## Procedimiento

---

Para configurar la limpieza de unidades controlada por el servidor en una biblioteca automatizada, complete los pasos siguientes:

Defina o actualice las unidades en la biblioteca utilizando el parámetro CLEANFREQUENCY en el mandato DEFINE DRIVE o UPDATE DRIVE. Por ejemplo, para limpiar una unidad denominada DRIVE1 tras procesar 100 GB de datos, emita el mandato siguiente:

```
update drive autolib1 drive1 cleanfrequency=100
```

## Resultados

---

Una vez que el cartucho limpiador esté dado de alta, el servidor montará el cartucho limpiador en una unidad cuando ésta necesite limpieza. El servidor utiliza ese cartucho para el número de limpiezas especificado. Para obtener más información, consulte Operaciones con cartuchos limpiadores.



## Qué hacer a continuación

---

Incorpore el cartucho limpiador en el inventario de volúmenes de biblioteca siguiendo las instrucciones que encontrará en Incorporar un cartucho limpiador en una biblioteca.

- Incorporar un cartucho limpiador en una biblioteca  
Para habilitar la limpieza automática de unidades de cinta, debe incorporar un cartucho limpiador en el inventario de volúmenes de la biblioteca automatizada.
- Operaciones con cartuchos limpiadores  
Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

### Referencia relacionada:

-  DEFINE DRIVE (Definir una unidad en una biblioteca)
-  UPDATE DRIVE (Actualizar una unidad)

## Incorporar un cartucho limpiador en una biblioteca

---

Para habilitar la limpieza automática de unidades de cinta, debe incorporar un cartucho limpiador en el inventario de volúmenes de la biblioteca automatizada.

## Acerca de esta tarea

---

Al incorporar un cartucho limpiador a una biblioteca, asegúrese de que está correctamente identificado en el servidor como cartucho limpiador. Asegúrese de que el cartucho limpiador no se encuentre en una ranura que pueda detectar un proceso de búsqueda. Si se producen errores o retrasos de 15 minutos o más, puede ser indicativo de que hay un cartucho limpiador mal colocado.

El método preferido es dar de alta los cartuchos limpiadores individualmente. Si tiene que dar de alta cartuchos de datos y cartuchos limpiadores, ponga los cartuchos de datos en la biblioteca e incorpórelos antes. A continuación incorpore el cartucho limpiador a la biblioteca.

## Procedimiento

---

Para incorporar un cartucho limpiador a una biblioteca, emita el mandato CHECKIN LIBVOLUME. Por ejemplo, para dar de alta un cartucho limpiador denominado AUTOLIB1, emita el mandato siguiente:

```
checkin libvolume autolib1 cleanv status=cleaner cleanings=10  
checklabel=no
```

El servidor solicita que el cartucho se coloque en el puerto de entrada/salida o en una ranura específica.

### Referencia relacionada:

-  CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)

## Operaciones con cartuchos limpiadores

---

Para garantizar que las unidades de cinta se limpian cuando es necesario, y para evitar problemas con el almacenamiento en cinta, siga las directrices siguientes.

### Supervisión del proceso de limpieza

Si se ha incorporado un cartucho limpiador en una biblioteca y se tiene que limpiar una unidad, el servidor desmonta el volumen de datos y ejecuta la operación de limpieza. Si la operación de limpieza falla o se cancela, o si no hay ningún cartucho limpiador disponible, puede que no se dé cuenta de que la unidad necesita una limpieza. Supervise los mensajes sobre estos problemas de limpieza para asegurarse de que las unidades se limpian cuando es necesario. Si es necesario, emita el mandato CLEAN DRIVE para que el servidor intente la limpieza de nuevo, o cargue manualmente un cartucho limpiador en la unidad.

### Utilización de varios cartuchos limpiadores

El servidor utiliza un cartucho limpiador para el número de limpiezas que especifique al dar de alta el cartucho limpiador. Si incorpora dos o más cartuchos limpiadores, el servidor utilizará sólo uno de los cartuchos hasta alcanzar el número de limpiezas designado para ese cartucho. A continuación, el servidor utiliza el siguiente cartucho limpiador. Si incorpora dos o más cartuchos limpiadores y ejecuta simultáneamente dos o más mandatos CLEAN DRIVE, el servidor utilizará varios cartuchos al mismo tiempo y reducirá las limpiezas restantes en cada cartucho.

### Referencia relacionada:

- [AUDIT LIBRARY](#) (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- [CHECKIN LIBVOLUME](#) (Dar de alta un volumen de almacenamiento en una biblioteca)
- [CLEAN DRIVE](#) (Limpiar una unidad)
- [LABEL LIBVOLUME](#) (Etiquetar un volumen de biblioteca)
- [QUERY LIBVOLUME](#) (Consultar un volumen de biblioteca)

## Resolución de errores relacionados con la limpieza de unidades

---

Al mover cartuchos dentro de una biblioteca, puede que coloque un cartucho de datos donde debería ir un cartucho limpiador. Revise el proceso que ha completado el servidor y los mensajes que se han emitido para resolver el problema.

Cuando una unidad necesita una limpieza, el servidor carga el cartucho que en su base de datos se indica como cartucho limpiador en la unidad. A continuación, la unidad pasa al estado READY y IBM Spectrum Protect detecta que el cartucho es un cartucho de datos. El servidor completa los pasos siguientes:

1. El servidor intenta leer la etiqueta de la cinta interna del cartucho de datos.
2. El servidor expulsa el cartucho de la unidad y lo mueve a la ranura inicial del cartucho limpiador dentro de la biblioteca. Si la operación de expulsión falla, el servidor marca la unidad como fuera de línea y emite un mensaje indicando que el cartucho todavía se encuentra en la unidad.
3. El servidor extrae el cartucho limpiador para evitar seleccionarlo para otra solicitud de limpieza de la unidad. El cartucho limpiador permanece en la biblioteca pero ya no aparece en el inventario de biblioteca de IBM Spectrum Protect.
4. Utilizando la etiqueta de cinta interna, el servidor comprueba el nombre del volumen en el inventario de biblioteca actual, los volúmenes de agrupación de almacenamiento y el archivo de historial de volúmenes.
  - Si el nombre del volumen no se encuentra en el inventario de la biblioteca, puede que se haya dado de alta un cartucho de datos como cartucho limpiador por error. Una vez extraído el volumen, no tiene que hacer nada más.
  - Si el nombre del volumen se encuentra en el inventario de la biblioteca, el servidor emite mensajes de que se requiere una intervención manual y una auditoría de biblioteca. Para resolver este problema, siga las instrucciones de Auditoría de inventarios de volúmenes en una biblioteca.

## Sustitución de unidades de cinta

---

Si sustituye una unidad en una biblioteca de cintas definida en IBM Spectrum Protect, debe suprimir las definiciones de unidad y vía de acceso de la unidad antigua y definir la nueva unidad y vía de acceso.

La sustitución de definiciones de unidad y vía de acceso es necesaria aunque esté intercambiando una unidad por otra del mismo tipo, utilizando la misma dirección lógica y dirección física, el mismo ID de SCSI y el mismo número de puerto. Los nombres de alias de dispositivo se pueden cambiar cuando se cambian las conexiones de las unidades.

Si la unidad nueva es una actualización que da soporte a un nuevo formato de medios, es posible que también tenga que definir una nueva biblioteca lógica, clase de dispositivo y agrupación de almacenamiento. Los procedimientos para configurar una política para una nueva unidad en una biblioteca de múltiples unidades varían según los tipos de unidades y medios que haya en la biblioteca.

- Suprimir unidades de cinta  
Puede suprimir unidades de cinta de una biblioteca. Por ejemplo, puede suprimir una unidad que ya no utilice o que desee sustituir.
- Sustitución de las unidades con otras del mismo tipo  
Para añadir una unidad que admita los mismos formatos de medios que la unidad a la que sustituye, debe definir una unidad y una vía de acceso nuevas.
- Migración de datos a unidades actualizadas  
Su actualiza todas las unidades de cinta de una biblioteca, puede conservar las definiciones de política existente para migrar y caducar los datos existentes, y puede utilizar las nuevas unidades para almacenar datos.

## Suprimir unidades de cinta

Puede suprimir unidades de cinta de una biblioteca. Por ejemplo, puede suprimir una unidad que ya no utilice o que desee sustituir.

### Procedimiento



1. Detenga el servidor de IBM Spectrum Protect y cierre el sistema operativo.
2. Extraiga la unidad antigua y siga las instrucciones del fabricante para instalar la unidad nueva.
3. Reinicie el sistema operativo y el servidor de IBM Spectrum Protect.
4. Suprima la vía de acceso desde el servidor a la unidad. Por ejemplo, para suprimir una vía de acceso de SERVER1 a LIB1, emita el mandato siguiente:

```
delete path server1 lib1 srctype=server desttype=drive
```

5. Suprima la definición de la unidad. Por ejemplo, emita el siguiente mandato para suprimir una unidad denominada DLT1 de un dispositivo de biblioteca denominado LIB1:

```
delete drive lib1 dlt1
```

#### Referencia relacionada:

-  [DELETE DRIVE \(Suprimir una unidad de una biblioteca\)](#)
-  [DELETE PATH \(suprimir una vía de acceso\)](#)

## Sustitución de las unidades con otras del mismo tipo

Para añadir una unidad que admita los mismos formatos de medios que la unidad a la que sustituye, debe definir una unidad y una vía de acceso nuevas.

### Acerca de esta tarea


Si una biblioteca sólo incluye un modelo de unidad y desea sustituir una unidad, debe sustituir la unidad por la misma unidad de modelo. Si una biblioteca incluye modelos mixtos de unidades y usted desea sustituir una unidad, puede sustituir el modelo por cualquier unidad de modelo que exista en la biblioteca.

### Procedimiento

1. Suprima la vía de acceso y las definiciones de unidad de la unidad antigua. Por ejemplo, para suprimir una unidad denominada DRIVE1 de una biblioteca denominada LIB1, emita el mandato siguiente:

```
delete path server2 drive1 srctype=server desttype=drive library=lib1
delete drive lib1 drive1
```

2. Apague la biblioteca, elimine la unidad original, sustitúyala por la nueva unidad y encienda la biblioteca.
3. Actualice el sistema host para asegurarse de que el sistema detecta la nueva unidad.
4. Defina la unidad y la vía de acceso nuevas. Por ejemplo, para definir una nueva unidad, DRIVE2, y una vía de acceso a ella desde SERVER2, si utiliza un controlador de dispositivo IBM Spectrum Protect, escriba los siguientes mandatos:

 Sistemas operativos AIX

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/mt0
```

 Sistemas operativos Linux


```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=/dev/tmscsi/mt0
```


 Sistemas operativos Windows

```
define drive lib1 drive2
define path server2 drive2 srctype=server desttype=drive library=lib1
device=mt3.0.0.1
```

Consejo: Puede utilizar las definiciones de biblioteca, clase de dispositivo y agrupación de almacenamiento existentes.

**Referencia relacionada:**

 DELETE DRIVE (Suprimir una unidad de una biblioteca)

 DELETE PATH (suprimir una vía de acceso)

## Migración de datos a unidades actualizadas

---

Su actualiza todas las unidades de cinta de una biblioteca, puede conservar las definiciones de política existente para migrar y caducar los datos existentes, y puede utilizar las nuevas unidades para almacenar datos.

### Antes de empezar

---

En el ejemplo siguiente se presupone que ya dispone de una agrupación de almacenamiento primario para una clase de dispositivo DISK denominada POOL1.

### Procedimiento

---

1. Para migrar los datos a una agrupación de almacenamiento que se haya creado para las nuevas unidades, especifique el parámetro NEXTSTGPOOL. Por ejemplo, para migrar datos de una agrupación de almacenamiento existente, POOL1, a la nueva agrupación de almacenamiento, POOL2, emita el mandato siguiente:


```
update stgpool pool1 nextstgpool=pool2
```

2. Actualice las definiciones de clase de gestión existentes para almacenar datos en la agrupación de almacenamiento DISK utilizando el mandato UPDATE MGMTCLASS.

**Referencia relacionada:**

 DEFINE STGPOOL (Definir un volumen en una agrupación de almacenamiento)

 UPDATE MGMTCLASS (Actualizar una clase de gestión)

 UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

## Protección del servidor IBM Spectrum Protect

---

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- Gestión de administradores  
Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.
- Cambio de los requisitos de contraseña  
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- Protección del servidor en el sistema  
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

## Gestión de administradores

---

Un administrador que tiene autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas tareas, se le debe otorgar autorización asignándole uno o más niveles de autorización.

### Procedimiento

---

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	<p>Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:</p> <ol style="list-style-type: none"> <li>Registre el administrador y especifique Pa\$#\$twO como contraseña ejecutando el siguiente mandato:           <pre>register admin admin1 Pa\$#\$twO</pre> </li> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:           <pre>grant authority admin1 classes=system</pre> </li> </ol>
Cambie los permisos del administrador.	<p>Cambie el nivel de autorización de un administrador, ADMIN1.</p> <ul style="list-style-type: none"> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador:           <pre>grant authority admin1 classes=system</pre> </li> <li>Emita el siguiente mandato para revocar la autoridad del sistema del administrador:           <pre>revoke authority admin1 classes=system</pre> </li> </ul>
Elimine administradores.	<p>Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect:</p> <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	<p>Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.</p>

**Conceptos relacionados:**

Planificación de los roles de administración

## Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

### Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

### Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</li> <li>Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</li> </ol> <p>El valor predeterminado en la instalación es 0.</p>



Tarea	Procedimiento
Establezca una longitud mínima para las contraseñas.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>Establezca el número de caracteres en el campo Longitud de contraseña mínima.</li> </ol>
Establezca el periodo de caducidad para las contraseñas.	<ol style="list-style-type: none"> <li>En la página Servidores del Centro de operaciones, seleccione el servidor.</li> <li>Pulse Detalles y, a continuación, pulse el separador Propiedades.</li> <li>Establecer el número de días en el campo Caducidad común de la contraseña.</li> </ol>
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben especificar una contraseña para acceder al servidor.</p> <p>Puede inhabilitar la autenticación de contraseña sólo para las contraseñas que se autentican en el servidor (LOCAL). Al inhabilitar la autenticación de contraseña, se aumenta el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como el método de autenticación predeterminado, emita el siguiente mandato:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para autenticarse en el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

## Protección del servidor en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

### Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios para la base de datos del servidor y la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor  
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

## Detención e inicio del servidor

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

### Antes de empezar

Debe tener el privilegio de operador o sistema para detener e iniciar el servidor de IBM Spectrum Protect.

- Detención del servidor  
Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de

datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

- Inicio del servidor para tareas de mantenimiento o reconfiguración

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento.

Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Detención del servidor

---

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

### Acerca de esta tarea

---

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

### Procedimiento

---

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si los procesos o las sesiones de nodo de cliente están en curso completando los pasos siguientes:

- a. En la página *Visión general* del Centro de operaciones, vea el área *Actividad* para conocer el número total de procesos y sesiones que están activos actualmente. Si los números difieren de forma significativa de los números normales que se visualizan durante la rutina de gestión de almacenamiento diaria, vea otros indicadores de estado del Centro de operaciones para comprobar si hay un problema.

- b. Vea el gráfico en el área *Actividad* para comparar la cantidad de tráfico de red durante los periodos siguientes:

- El periodo actual, es decir, el periodo de 24 horas más reciente
- El periodo anterior, es decir, 24 horas antes del periodo actual

Si el gráfico del periodo anterior representa la cantidad de tráfico esperada, las diferencias significativas en el gráfico del periodo actual pueden indicar que hay un problema.

- c. En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*. Si el servidor no está registrado como servidor concentrador o de radio en el Centro de operaciones, obtenga información sobre los procesos utilizando mandatos administrativos. Emita el mandato QUERY PROCESS para consultar procesos y obtener información sobre sesiones emitiendo el mandato QUERY SESSION.

3. Espere hasta que las sesiones de nodo cliente se completen o cancélelas. Para cancelar los procesos y las sesiones, realice los pasos siguientes:

- En la página *Servidores*, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse *Detalles*.
- Pulse el separador *Tareas activas* y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
- Pulse *Cancelar*.

- Si el servidor no está registrado como un servidor concentrador o de radio en el Centro de operaciones, cancele las sesiones utilizando mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancelar procesos utilizando el mandato CANCEL PROCESS.

Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje.

Dependiendo del entorno del sistema, esto puede tardar varios minutos.

4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

## Inicio del servidor para tareas de mantenimiento o reconfiguración

---

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o

reconfiguración.

## Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

## Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo sobre cómo iniciar el servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.




## Qué hacer a continuación

---

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
  -  Sistemas operativos AIX Inicio de la instancia de servidor
  -  Sistemas operativos Linux Inicio de la instancia de servidor
  -  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

## Planificación para actualizar el servidor

---

Cuando un fixpack o arreglo temporal queda disponible, puede actualizar el servidor de IBM Spectrum Protect para sacar provecho de las mejoras del producto. Los servidores y los clientes se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

## Acerca de esta tarea

---

Siga estas directrices:

- El método preferido es actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

## Procedimiento

---

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.




Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.

3. Asegúrese de que la versión a la que actualiza el servidor sea compatible con otros componentes, como agentes de almacenamiento y clientes de biblioteca. Consulte nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

## Qué hacer a continuación

---

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

### Información relacionada:

 Proceso de actualización y migración: preguntas más frecuentes

## Preparación para una parada o actualización de sistema

---

Prepare IBM Spectrum Protect para mantener el sistema en un estado coherente durante un corte eléctrico planificado o una actualización del sistema.

### Acerca de esta tarea

---

Asegúrese de planificar actividades regularmente para gestionar, proteger y mantener el servidor. Para obtener información acerca de la planificación actividades como la copia de seguridad de la base de datos, la copia de seguridad del archivo de configuración de dispositivo, y la copia de seguridad del historial de volumen, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

### Procedimiento

---

1. Cancele los procesos y las sesiones que están en curso completando los pasos siguientes:
  - a. En el Centro de operaciones, en la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
  - b. Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
  - c. Pulse Cancelar.

2. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

Consejo: Puede emitir el mandato HALT desde el Centro de operaciones pasando el cursor por encima del icono Valores y pulsando en Creador de mandatos. A continuación, seleccione el servidor, escriba `halt` y pulse Intro.

### Referencia relacionada:

 HALT (Concluir el servidor)

## Preparación ante desastres y recuperación tras desastres mediante DRM

---

IBM Spectrum Protect proporciona una función de gestor recuperación tras desastre (DRM) para poder recuperar los datos del servidor y del cliente durante un siniestro.

DRM realiza el seguimiento del movimiento de los medios fuera del sitio y registra esa información en la base de datos de IBM Spectrum Protect. DRM consolida los planes, los scripts y cualquier otra información de un archivo de plan que sea necesaria para recuperar el servidor de IBM Spectrum Protect cuando se produce un siniestro o una parada no prevista del sistema.

Restricción: DRM solo está disponible en el producto IBM Spectrum Protect Extended Edition.

- Archivo del plan de recuperación tras desastre  
El archivo del plan de recuperación tras desastre contiene la información que se necesita para recuperar un servidor de IBM Spectrum Protect al punto en el tiempo de la última operación de copia de seguridad de la base de datos antes de crear el plan.
- Recuperación de datos de cliente y servidor utilizando DRM  
Utilice la función gestor recuperación tras desastre (DRM) para recuperar el servidor de IBM Spectrum Protect y los datos de cliente cuando se produzca un siniestro.

- Ejecución de obtenciones de detalles de recuperación tras desastre  
Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.
- Restauración de la base de datos  
Si tiene habilitada la función gestor recuperación tras desastre (DRM) y ha seguido el procedimiento para prepararse ante un desastre, puede restaurar la base de datos después de que se produzca un desastre. Si no tiene configurado DRM, todavía podrá restaurar la base de datos, siempre que tenga los archivos de copia de seguridad necesarios.

## Archivo del plan de recuperación tras desastre

El archivo del plan de recuperación tras desastre contiene la información que se necesita para recuperar un servidor de IBM Spectrum Protect al punto en el tiempo de la última operación de copia de seguridad de la base de datos antes de crear el plan.

El plan se organiza en secciones, que puede separar en diversos archivos. Cada sección tiene una sentencia de inicio y una sentencia de finalización.

Tabla 1. Secciones del archivo del plan de recuperación tras desastre

Sección	Información de la sección
SERVER.REQUIREMENTS	Identifica los requisitos de almacenamiento de la base de datos y del registro de recuperación para el servidor.
RECOVERY.INSTRUCTIONS.GENERAL	Identifica las instrucciones específicas del sitio que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.GENERAL. En las instrucciones se incluye la estrategia de recuperación, los nombres de contacto clave, una visión general de las aplicaciones clave de las que este servidor hace copia de seguridad y otras instrucciones de recuperación relevantes.
RECOVERY.INSTRUCTIONS.OFFSITE	Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.OFFSITE. En las instrucciones se describe el nombre y la ubicación de la caja fuerte externa y cómo ponerse en contacto con el administrador de la caja fuerte (por ejemplo, un nombre y un número de teléfono) .
RECOVERY.INSTRUCTIONS.INSTALL	Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.INSTALL. En las instrucciones se describe cómo reconstruir el servidor base y se proporciona la ubicación de las copias de seguridad de la imagen del sistema.
RECOVERY.INSTRUCTIONS.DATABASE	Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.DATABASE. En las instrucciones se describe cómo preparar la recuperación de la base de datos. Por ejemplo, puede especificar instrucciones sobre cómo inicializar o cargar los volúmenes de copia de seguridad de una biblioteca automatizada. No se proporciona ningún ejemplo de esta sección.
RECOVERY.INSTRUCTIONS.STGPOOL	Contiene instrucciones que el administrador introduce en el archivo que se identifica mediante el prefijo RECOVERY.INSTRUCTIONS.STGPOOL. En las instrucciones se incluyen los nombres de sus aplicaciones de software y los nombres de las agrupaciones de almacenamiento de copias que contienen las copias de seguridad de estas aplicaciones. No se proporciona ningún ejemplo de esta sección.

Sección	Información de la sección
RECOVERY.VOLUMES.REQUIRED	Proporciona una lista de volúmenes de copia de seguridad de base de datos y volúmenes de agrupación de almacenamiento de copias necesarios para recuperar el servidor. Se incluye un volumen de copia de seguridad de la base de datos incluye si forma parte de la serie más reciente de copia de seguridad de la base de datos. Un volumen de la agrupación de almacenamiento de copia se incluye si no está vacío y no está marcado como destruido.
RECOVERY.DEVICES.REQUIRED	Proporciona detalles sobre los dispositivos necesarios para leer los volúmenes de copia de seguridad.
RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE	Contiene un script con los mandatos necesarios para recuperar el servidor.
RECOVERY.SCRIPT.NORMAL.MODE	Contiene un script con los mandatos necesarios para restaurar las agrupaciones de almacenamiento primarias del servidor.
DB.STORAGEPATHS	Identifica los directorios de la base de datos de IBM Spectrum Protect.
LICENSE.REGISTRATION	Contiene una macro para registrar licencias de su servidor.
COPYSTGPOOL.VOLUMES.AVAILABLE	Contiene una macro para marcar los volúmenes de agrupación de almacenamiento de copias que se han movido fuera del sitio y después se han devuelto al sitio. Puede utilizar la información como guía y ejecutar los mandatos administrativos. Como alternativa, puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
COPYSTGPOOL.VOLUMES.DESTROYED	Contiene una macro para marcar los volúmenes de agrupación de almacenamiento de copias como no disponibles si los volúmenes estaban en el local en el momento de producirse el siniestro. Se considera que estos volúmenes están fuera del local y, por consiguiente, no han sido destruidos en un siniestro. Puede utilizar la información como guía y emitir los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.DESTROYED	Contiene una macro para marcar los volúmenes de agrupación de almacenamiento primario como destruidos si los volúmenes estaban en el sitio en el momento de producirse el siniestro. Puede utilizar la información como guía y ejecutar los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
PRIMARY.VOLUMES.REPLACEMENT	Contiene una macro para identificar los volúmenes de agrupación de almacenamiento primaria de sustitución. Puede utilizar la información como guía y ejecutar los mandatos administrativos desde una línea de mandatos o puede copiar, modificar y ejecutar la macro en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
STGPOOLS.RESTORE	Contiene una macro para restaurar las agrupaciones de almacenamiento primarias. Puede utilizar la sección como guía y ejecutar los mandatos administrativos desde una línea de mandatos. También puede copiarla, modificarla y ejecutarla en un archivo. Esta macro la inicia el script RECOVERY.SCRIPT.NORMAL.MODE.

Sección	Información de la sección
VOLUME.HISTORY.FILE	Contiene una copia de la información histórica de volúmenes en el momento de la creación del plan de recuperación. El programa de utilidad DSMSERV RESTORE DB utiliza el archivo de historial de volumen para determinar qué volúmenes son necesarios para restaurar la base de datos. El archivo de historial de volumen se utiliza por el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DEVICE.CONFIGURATION.FILE	Contiene una copia de la información de configuración de dispositivos del servidor en el momento de la creación del plan de recuperación. El programa de utilidad DSMSERV RESTORE DB utiliza el archivo de configuración del dispositivo para leer los volúmenes de copia de seguridad de la base de datos. El archivo de configuración de dispositivo es utilizado por el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
DSMSERV.OPT.FILE	Contiene una copia del archivo de opciones del servidor. Esta sección la utiliza el script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE.
LICENSE.INFORMATION	Contiene una copia del resultado de la auditoría de licencias más reciente y los términos del sistema de licencias del servidor.
MACHINE.GENERAL.INFORMATION	Proporciona información para la máquina servidor, como su ubicación, que es necesaria para recrear la máquina del servidor. Esta sección se incluye en el archivo del plan si la información de máquina se ha guardado en la base de datos utilizando el mandato DEFINE MACHINE y especificando el parámetro ADSMSERVER=YES.
MACHINE.RECOVERY.INSTRUCTIONS	Proporciona las instrucciones de recuperación sobre la máquina del servidor. Esta sección se incluye en el archivo del plan si las instrucciones de recuperación de la máquina se han guardado en la base de datos.
MACHINE.RECOVERY.CHARACTERISTICS	Proporciona las características de hardware y software para la máquina del servidor. Esta sección se incluye en el archivo del plan si las características de la máquina se han guardado en la base de datos.
MACHINE.RECOVERY.MEDIA	Proporciona información sobre los medios necesarios para recrear la máquina que contiene el servidor. Esta sección se incluye en el archivo del plan si la información de medios de recuperación se ha guardado en la base de datos y se ha asociado a la máquina que contiene el servidor.

## Recuperación de datos de cliente y servidor utilizando DRM

Utilice la función gestor recuperación tras desastre (DRM) para recuperar el servidor de IBM Spectrum Protect y los datos de cliente cuando se produzca un siniestro.

### Antes de empezar

IBM Spectrum Protect está configurado para utilizar el protocolo SSL (capa de sockets seguros) para la autenticación de cliente/servidor. Al iniciar el servidor, se crea un archivo de certificado digital cert.kdb como parte del proceso. Este archivo incluye la clave pública del servidor, que permite al cliente cifrar datos. El archivo de certificado digital no se puede almacenar en la base de datos de servidor porque Global Security Kit (GSKit) requiere un archivo distinto en un determinado formato.

La clave de cifrado maestra está almacenada en una base de datos clave nueva gestionada por GSKit, dsmkeydb.kdb. Si el servidor ya tiene una clave de cifrado maestra, esta se migra del archivo dsmserv.pwd file a la base de datos clave, dsmkeydb.kdb. Conserve las copias de seguridad de los archivos dsmkeydb.kdb y dsmkeydb.sth. Puede configurar el mandato BACKUP DB para realizar la copia de seguridad de la clave de cifrado maestra o bien realizar usted mismo una copia de seguridad de los archivos dsmkeydb.kdb y dsmkeydb.sth de forma manual.

1. Conserve copias de seguridad de los archivos cert.kdb, cert.sth, y cert256.arm.

2. Si se han perdido o dañado tanto los archivos de certificado originales como las copias, genere nuevos archivos de certificado.

## Procedimiento

---

1. Obtenga el último plan de recuperación.
2. Revise los pasos de recuperación que se describen en la sección RECOVERY.INSTRUCTIONS.GENERAL del plan.
3. Separe las secciones del archivo de plan en archivos individuales para obtener instrucciones generales preliminares, scripts de recuperación de servidor de IBM Spectrum Protect e instrucciones de recuperación de cliente.
4. Recupere todos los volúmenes de recuperación necesarios (enumerados en el plan) de la caja fuerte.
5. Revise el archivo de configuración de dispositivos para asegurarse de que la configuración de hardware en el local de recuperación sea la misma que la del local original. Si hay diferencias, deben actualizarse en el archivo de configuración de dispositivos. Los siguientes cambios de configuración de ejemplo requieren actualizaciones para la información de configuración:
  - o Diferentes nombres de dispositivo.
  - o Para bibliotecas automatizadas, el requisito de colocar manualmente los volúmenes de copia de seguridad de la base de datos en la biblioteca automatizada y actualizar la información de configuración para identificar el elemento en la biblioteca. Esto permite al servidor localizar los volúmenes de copia de seguridad de la base de datos necesarios.
6. Configure hardware de sustitución para el servidor de IBM Spectrum Protect, incluyendo la instalación del sistema operativo y del release base de IBM Spectrum Protect.
7. Ejecute los scripts de recuperación del servidor de IBM Spectrum Protect desde el plan de recuperación. Las secciones RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE y RECOVERY.SCRIPT.NORMAL.MODE contienen archivos de mandatos ejecutables que se pueden utilizar para dirigir la recuperación del servidor de IBM Spectrum Protect llamando a otros archivos de mandatos que se hayan generado en el plan. El script RECOVERY.SCRIPT.DISASTER.RECOVERY.MODE recupera el servidor al punto en que los clientes pueden iniciar restauraciones directamente desde los volúmenes de agrupaciones de almacenamiento de copias.
8. Restablezca las agrupaciones de almacenamiento primarias con el script RECOVERY.SCRIPT.NORMAL.MODE.
9. Inicie las operaciones de restauración de clientes por orden de mayor prioridad, según definido en su planificación de alto nivel.

## Qué hacer a continuación

---

El servidor IBM Spectrum Protect ya se puede utilizar para operaciones de servidor normales. Asegúrese de planificar todas las operaciones necesarias. Para obtener instrucciones, consulte Definición de planificaciones para actividades de mantenimiento del servidor y Planificación de copia de seguridad y operaciones de archivado.

### Tareas relacionadas:

- 🔗 Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedor de directorios

### Referencia relacionada:

- 🔗 PREPARE (Crear un archivo de plan de recuperación)

## Ejecución de obtenciones de detalles de recuperación tras desastre

---

Planifique las obtenciones de detalles de recuperación tras desastre para prepararse para las auditorías que certifican la recuperabilidad del servidor de IBM Spectrum Protect y garantizar que los datos pueden restaurarse y las operaciones pueden reanudarse tras una parada. Las obtenciones de detalles le ayudan a garantizar que los datos se podrán restaurar y que se retomarán las operaciones antes de que se produzca una situación crítica.

## Antes de empezar

---

Complete las siguientes tareas:

- Planifique actividades regularmente para gestionar, proteger y mantener el servidor. Para obtener más información sobre actividades planificadas, consulte Definición de planificaciones para actividades de mantenimiento del servidor. Asegúrese de planificar las siguientes tareas:
  - o Realizar una copia de seguridad de la base de datos.
  - o Mover medios fuera del local.
  - o Realizar copia de seguridad del archivo de configuración de dispositivo, el archivo de historial de volumen y el archivo de opciones del servidor dsmserv.opt.
  - o **Opcional:** Emitir el mandato PREPARE para crear el archivo del plan de recuperación tras desastre.

Consejo:

Cuando emite el mandato PREPARE, la función IBM Spectrum Protect gestor recuperación tras desastre (DRM) crea una copia del archivo del plan de recuperación tras desastre.

Puede gestionar la recuperación tras desastre fuera del local sin utilizar DRM, sin embargo, DRM ayuda a consolidar planes, scripts y otra información necesaria durante la recuperación tras desastre.



Cree múltiples copias del plan para conservarlo. Por ejemplo, mantenga copias en formato de impresión, en una unidad flash USB, en espacio de disco que se encuentra fuera del local o en un servidor remoto. El archivo del plan de recuperación tras desastre se mueve fuera del local a diario con las cintas. Para obtener más información sobre DRM, consulte Preparación ante desastres y recuperación tras desastres mediante DRM.

- Configure los siguientes recursos en el sitio de recuperación tras desastre:
  1. Un servidor IBM Spectrum Protect de recuperación. El servidor en el sitio de recuperación de desastres debe estar en el mismo nivel que el servidor en el sitio de producción.
  2. Una biblioteca de cintas para almacenar los medios que se envían desde el sitio de producción. Para obtener más información sobre ubicaciones de recuperación fuera del local, consulte Almacenamiento de datos fuera del local.
  3. >Espacio de almacenamiento de disco para la base de datos, el registro de archivado, los registros activos y las agrupaciones de almacenamiento.
  4. Clientes para probar operaciones de restauración.

## Acerca de esta tarea

---

Pruebe el plan de recuperación tras desastre y la recuperabilidad del servidor IBM Spectrum Protect con frecuencia, en un entorno similar al entorno de producción.

## Procedimiento

---

1. Asegúrese de que las cintas estén disponibles en el local. Emita el mandato QUERY LIBVOLUME para identificar volúmenes que se dan de alta en una biblioteca automatizada.
2. Realice una copia de seguridad de la base de datos a las cintas en el local completando los pasos siguientes:
  - a. En la página Servidores del Centro de operaciones, seleccione el servidor cuya base de datos desea hacer una copia de seguridad.
  - b. Pulse Copia de seguridad y siga las instrucciones de la ventana Copia de seguridad de la base de datos.
3. Copie los archivos siguientes en el directorio de inicio del servidor en el local de recuperación:
  - Archivo del plan de recuperación tras desastre
  - Archivo de historial de volumen
  - Archivo de configuración de dispositivo
  - Opcional: archivo de opciones de servidor dmserv.opt
4. Traslade la cinta a la ubicación de recuperación fuera del local.
5. Restablezca la base de datos de servidor utilizando el programa de utilidad DSMSERV RESTORE DB en el servidor de recuperación. Para obtener más información sobre la restauración de la base de datos de servidor, consulte Restauración de la base de datos.
6. Emita el mandato UPDATE VOLUME y especifique el parámetro ACCESS=DESTROYED para indicar que debe restaurarse un volumen entero.
7. En el servidor de recuperación, restaure los volúmenes de agrupación de almacenamiento utilizando el mandato RESTORE STGPOOL.

## Qué hacer a continuación

---

Asegúrese de poder acceder a los datos de la biblioteca auditando un volumen de cinta en la agrupación de almacenamiento restaurada para verificar que los datos sean coherentes. Emita el mandato AUDIT VOLUME para auditar un volumen de cinta. Para acelerar el rendimiento, audite solo los datos restaurados.

### Tareas relacionadas:

Auditoría de inventarios de volúmenes en una biblioteca

### Referencia relacionada:

- [AUDIT VOLUME](#) (Verificar información de base de datos para un volumen de agrupación de almacenamiento)
- [DSMSERV RESTORE DB](#) (Restaurar la base de datos)
- [RESTORE STGPOOL](#) (Restaurar datos de agrupación de almacenamiento)

## Restauración de la base de datos

---

Si tiene habilitada la función gestor recuperación tras desastre (DRM) y ha seguido el procedimiento para prepararse ante un desastre, puede restaurar la base de datos después de que se produzca un desastre. Si no tiene configurado DRM, todavía podrá restaurar la base de datos, siempre que tenga los archivos de copia de seguridad necesarios.

## Antes de empezar

---

Si los directorios de la base de datos y el registro de recuperación se han perdido, vuelva a crearlos antes de ejecutar el programa de utilidad del servidor DSMSERV RESTORE DB.

## Acerca de esta tarea

---

Puede restaurar la base de datos al estado más actual o a un punto en el tiempo especificado. Para recuperar la base de datos al instante en que se ha perdido la base de datos, recupérela a su estado actual.

Restricciones:

- Para restaurar la base de datos a la versión más reciente, debe ubicar el directorio de registro de archivado. Si no puede ubicar el directorio, puede restaurar la base de datos sólo en un momento específico.
- No puede utilizar el protocolo SSL (Secure Sockets Layer) para las operaciones de restauración de la base de datos.
- Si el nivel de release de la copia de seguridad de base de datos es diferente del nivel de release del servidor que se está restaurando, no puede restaurar la base de datos del servidor. Por ejemplo, si está utilizando un servidor de la Versión 8.1 e intenta restaurar una base de datos de la Versión 7.1, se produce un error.

## Procedimiento

---

Utilice el programa de utilidad del servidor DSMSERV RESTORE DB para restaurar la base de datos. En función de la versión de la base de datos que desee restaurar, elija uno de los siguientes métodos:

- Restaure una base de datos a su versión más reciente. Por ejemplo, utilice este mandato:

```
dsmserv restore db
```

- Restaure una base de datos a un momento específico. Por ejemplo, para restaurar la base de datos a una serie de copias de seguridad que se ha creado el 19 de abril de 2017, utilice el siguiente mandato:

```
dsmserv restore db todate=04/19/2017
```

**Referencia relacionada:**

[DSMSERV RESTORE DB \(Restaurar la base de datos\)](#)

## Documentación de la solución de servidor en archivos PDF

---

Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

Los siguientes archivos PDF precompilados están disponibles para soluciones de protección de datos de IBM Spectrum Protect:

- Introducción a Soluciones de protección de datos
- Guía de soluciones de disco de sitio único
- Guía de soluciones de disco multisitio
- Guía de soluciones de cintas

Para obtener más archivos PDF compilados de la documentación del servidor, consulte la lista completa.

## Servidores de IBM Spectrum Protect

---

Los servidores de IBM Spectrum Protect almacenan y gestionan datos de copia de seguridad, archivado y gestionados por espacio para clientes de archivado y copia de seguridad y otros componentes de IBM Spectrum Protect y IBM Spectrum Protect Snapshot.

- **Novedades**  
Obtenga información sobre las nuevas características y actualizaciones en IBM Spectrum Protect versión 8.1.
- **Instalación y actualización**  
Puede instalar o actualizar componentes individuales o múltiples en la red de la empresa. Hay documentación de soluciones disponible para ayudarle a seleccionar una solución adecuada, basándose en las necesidades de negocio y, a continuación, instalar, configurar, supervisar y operar dicha solución.
- **Configuración y gestión**  
Para completar las tareas de configuración del servidor, revise la documentación disponible.
- **Mandatos, opciones y programas de utilidad del servidor**  
Utilice mandatos para administrar y configurar el servidor, opciones para personalizar el servidor y programas de utilizar para realizar tareas especiales cuando el servidor no se está ejecutando.
- **Documentación de servidor en archivos PDF**  
Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

## Novedades

---

Obtenga información sobre las nuevas características y actualizaciones en IBM Spectrum Protect versión 8.1.

Consejo: Para ver vídeos sobre las nuevas características y actualizaciones, consulte la biblioteca de vídeo.  
 Para obtener más información sobre las nuevas características y actualizaciones, siga los enlaces de la tabla.

Release	Nuevas características y actualizaciones
V8.1.2	<p>Servidor</p> <ul style="list-style-type: none"> <li>• Copia de seguridad de los datos en Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube</li> <li>• Cifrado de datos de cliente en una agrupación de almacenamiento de contenedores de directorio</li> <li>• Copia de seguridad de un servidor de archivos NAS en una agrupación de almacenamiento de contenedores de directorio</li> <li>• Instalación de IBM Spectrum Protect en el sistema operativo Linux en sistemas Power Systems (little endian)</li> <li>• Proteja su entorno de almacenamiento con un protocolo de seguridad mejorado</li> <li>• Optimización de la seguridad con la clave de cifrado maestra generada automáticamente</li> <li>• Actualice el servidor de IBM Spectrum Protect a la V8.1.2 antes de actualizar los clientes</li> <li>• Configuración de un entorno de almacenamiento utilizando la Guía de soluciones de cintas</li> <li>• Planificación de actualizaciones automáticas para la copia de seguridad y restauración de clientes</li> <li>• Opciones, mandatos y parámetros del servidor en desuso y sin mantenimiento</li> </ul> <p>Centro de operaciones            Actualizaciones del Centro de operaciones</p>
V8.1.1	<p>Servidor</p> <ul style="list-style-type: none"> <li>• Instale IBM Spectrum Protect en el sistema operativo Linux on Power Systems (little endian)</li> <li>• Instale IBM Spectrum Protect en el sistema operativo Microsoft Windows Server 2016</li> <li>• Utilice la biblioteca de Quantum Scalar i6</li> <li>• Revise los problemas resueltos</li> </ul> <p>Centro de operaciones</p> <ul style="list-style-type: none"> <li>• Revise los problemas resueltos</li> </ul>
V8.1	<p>Servidor</p> <ul style="list-style-type: none"> <li>• Conozca IBM Spectrum Protect</li> <li>• Protección de comunicaciones mediante el protocolo TLS 1.2</li> <li>• Conversión de una agrupación de almacenamiento de cinta en una agrupación de almacenamiento de contenedores</li> <li>• Actualización de software para el gestor de la base de datos del servidor</li> <li>• El mandato REGISTER NODE ya no crea un ID de usuario de administración de forma predeterminada</li> <li>• Optimización de la autenticación de usuario en una base de datos de Active Directory</li> <li>• Aumento en la flexibilidad al proteger y reclamar volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor</li> <li>• Sistemas operativos soportados</li> <li>• Supervisión del sistema sin utilizar SNMP</li> </ul> <p>Centro de operaciones            Actualizaciones del Centro de operaciones</p>

- Actualizaciones del Centro de operaciones  
 Hay nuevas características disponibles en IBM Spectrum Protect Operations Center Versión 8.1.2. Con Centro de operaciones actualizado, puede realizar una copia de seguridad de los datos en el almacenamiento en la nube de Microsoft Azure y aprovechar la aplicación de una seguridad mejorada.
- Actualizaciones de servidor IBM Spectrum Protect  
 Hay características nuevas y otros cambios disponibles en el servidor IBM Spectrum Protect Versión 8.1.2.
- Notas del release para componentes de la versión 8.1 del servidor  
 Las notas del release están disponibles para los componentes de V8.1.
- Archivos léame para componentes de la versión 8.1 del servidor  
 Los archivos léame para los fixpacks de la Versión 8.1 están publicados en el sitio web de soporte de software de IBM. Pueden existir actualizaciones disponibles para los componentes del servidor, incluyendo el propio servidor, el soporte de dispositivos y el Centro de operaciones.

**Información relacionada:**

## Actualizaciones del Centro de operaciones

---

Hay nuevas características disponibles en IBM Spectrum Protect Operations Center Versión 8.1.2. Con Centro de operaciones actualizado, puede realizar una copia de seguridad de los datos en el almacenamiento en la nube de Microsoft Azure y aprovechar la aplicación de una seguridad mejorada.

Se han realizado las siguientes mejoras en Centro de operaciones:

- Puede utilizar el asistente Añadir agrupación de almacenamiento para crear agrupaciones de almacenamiento de contenedores de nube que utilicen Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube, para hacer la copia de seguridad de los datos.
- Ahora Centro de operaciones proporciona seguridad mejorada aplicando el uso del cifrado Transport Layer Security (TLS) 1.2 para la comunicación entre Centro de operaciones y el servidor concentrador.

Para obtener más información sobre estas mejoras, consulte la ayuda de Centro de operaciones.

## Actualizaciones de servidor IBM Spectrum Protect

---

Hay características nuevas y otros cambios disponibles en el servidor IBM Spectrum Protect Versión 8.1.2.

- Copia de seguridad de los datos en Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube  
Con IBM Spectrum Protect Versión 8.1.2, puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube, para hacer copia de seguridad y restaurar datos.
- Cifrado de datos de cliente en una agrupación de almacenamiento de contenedores de directorio  
IBM Spectrum Protect Versión 8.1.2 ofrece protección mejorada para los datos del cliente. Si ha utilizado una versión anterior de IBM Spectrum Protect para escribir datos de cliente en una agrupación de almacenamiento de contenedores de directorio, puede cifrar los datos de cliente existentes en la agrupación de almacenamiento. También puede habilitar el cifrado de los nuevos datos del cliente antes de que se graben en la agrupación de almacenamiento.
- Copia de seguridad de un servidor de archivos NAS en una agrupación de almacenamiento de contenedores de directorio  
Con IBM Spectrum Protect Versión 8.1.2, puede hacer copia de seguridad de un sistema de archivos perteneciente a un servidor de archivos de almacenamiento conectado a red (NAS) en una agrupación de almacenamiento de contenedor de directorio. Mediante las agrupaciones de almacenamiento de contenedor de directorio, puede reducir el coste del hardware de almacenamiento, mejorar el rendimiento del servidor y mejorar la seguridad.
- Instalación de IBM Spectrum Protect en el sistema operativo Linux en sistemas Power Systems (little endian)  
Puede instalar IBM Spectrum Protect Versión 8.1.2 en el sistema operativo Linux on Power Systems (little endian). Se incorporó soporte limitado para este sistema operativo en la V8.1.1, y se incorpora soporte completo en la V8.1.2. Después de instalar y configurar el servidor V8.1.2 en Linux on Power Systems (little endian), puede hacer copia de seguridad de sus datos en dispositivos de disco, en almacenamiento de objetos en la nube y en dispositivos de cinta.
- Proteja su entorno de almacenamiento con un protocolo de seguridad mejorado  
IBM Spectrum Protect Versión 8.1.2 proporciona un protocolo de seguridad mejorado.
- Optimización de la seguridad con la clave de cifrado maestra generada automáticamente  
A partir de IBM Spectrum Protect Versión 8.1.2, se genera automáticamente una clave de cifrado maestra cuando se inicia el servidor si la clave de cifrado maestra no existía anteriormente.
- Configuración de un entorno de almacenamiento utilizando la Guía de soluciones de cintas  
El conjunto de documentación se ha actualizado para incluir la *Guía de soluciones de cintas de IBM Spectrum Protect*. Siguiendo las instrucciones de la guía, puede configurar una solución de cinta que optimice el almacenamiento y la recuperación ante siniestro, garantizando una copia segura de los datos en una ubicación externa.
- Planificación de actualizaciones automáticas para la copia de seguridad y restauración de clientes  
Con IBM Spectrum Protect Versión 8.1.2, Puede planificar el despliegue de actualizaciones de software en sistemas que ya tienen instalado el cliente de copia de seguridad y archivado.
- Actualice el servidor de IBM Spectrum Protect a la V8.1.2 antes de actualizar los clientes  
Actualice los servidores de IBM Spectrum Protect a la versión 8.1.2 antes de actualizar los clientes de archivado y copia de seguridad.
- Opciones, mandatos y parámetros del servidor en desuso y sin mantenimiento  
Algunas opciones, mandatos y parámetros del servidor han quedado en desuso o ya no están disponibles a partir de IBM Spectrum Protect Versión 8.1.2. El comportamiento de algunos parámetros y opciones ha cambiado.

## Copia de seguridad de los datos en Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube

---

Con IBM Spectrum Protect Versión 8.1.2, puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar Microsoft Azure, un sistema de almacenamiento de objetos basado en la nube, para hacer copia de seguridad y restaurar datos.

Mediante la configuración de agrupaciones de almacenamiento de contenedores de nube para utilizar Azure, puede simplificar la gestión de almacenamiento y proteger los datos utilizando el cifrado.

**Tareas relacionadas:**

Preparación para Azure

Configuración de una agrupación de almacenamiento de contenedor de nube

**Referencia relacionada:**

DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedor de nube)

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de nube)

## Cifrado de datos de cliente en una agrupación de almacenamiento de contenedores de directorio

---

IBM Spectrum Protect Versión 8.1.2 ofrece protección mejorada para los datos del cliente. Si ha utilizado una versión anterior de IBM Spectrum Protect para escribir datos de cliente en una agrupación de almacenamiento de contenedores de directorio, puede cifrar los datos de cliente existentes en la agrupación de almacenamiento. También puede habilitar el cifrado de los nuevos datos del cliente antes de que se graben en la agrupación de almacenamiento.

Para habilitar el cifrado para una agrupación de almacenamiento de contenedor de directorio existente, emita el mandato UPDATE STGPOOL y especifique ENCRYPT=YES. Para habilitar el cifrado para una nueva agrupación de almacenamiento de contenedor de directorio, defina la agrupación de almacenamiento mediante el mandato DEFINE STGPOOL y especifique ENCRYPT=YES.

**Tareas relacionadas:**

Configuración de una agrupación de almacenamiento de contenedor de directorios para almacenamiento de datos

**Referencia relacionada:**

DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio)

UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de directorio)

## Copia de seguridad de un servidor de archivos NAS en una agrupación de almacenamiento de contenedores de directorio

---

Con IBM Spectrum Protect Versión 8.1.2, puede hacer copia de seguridad de un sistema de archivos perteneciente a un servidor de archivos de almacenamiento conectado a red (NAS) en una agrupación de almacenamiento de contenedor de directorio. Mediante las agrupaciones de almacenamiento de contenedor de directorio, puede reducir el coste del hardware de almacenamiento, mejorar el rendimiento del servidor y mejorar la seguridad.

Las agrupaciones de almacenamiento de contenedor de directorio ofrecen las siguientes ventajas:

- Puede habilitar la deduplicación de datos en línea para eliminar datos duplicados cuando se graban en una agrupación de almacenamiento. De este modo, puede reducir la necesidad de reorganización fuera de línea, mejorar el rendimiento del servidor y reducir los costes.
- Puede habilitar la compresión en línea para reducir la cantidad de espacio que ocupan los datos.
- Puede habilitar el cifrado de datos del cliente antes de que se graben en la agrupación de almacenamiento.
- Puede proteger los datos mediante el mandato PROTECT STGPOOL. Puede almacenar una copia de los datos en otra agrupación de almacenamiento de contenedor de directorio en un servidor de réplica de destino o en cinta en una agrupación de almacenamiento de copia de contenedor. Para restaurar datos dañados, puede ejecutar el mandato REPAIR STGPOOL.


**Tareas relacionadas:**

Protección de los servidores de archivos NAS

**Referencia relacionada:**

DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio)

REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

 Sistemas operativos Linux

## Instalación de IBM Spectrum Protect en el sistema operativo Linux en sistemas Power Systems (little endian)

---

Puede instalar IBM Spectrum Protect Versión 8.1.2 en el sistema operativo Linux on Power Systems (little endian). Se incorporó soporte limitado para este sistema operativo en la V8.1.1, y se incorpora soporte completo en la V8.1.2. Después de instalar y configurar el

servidor V8.1.2 en Linux on Power Systems (little endian), puede hacer copia de seguridad de sus datos en dispositivos de disco, en almacenamiento de objetos en la nube y en dispositivos de cinta.

Los paquetes de instalación incluyen el servidor y la licencia, las herramientas de controladores de dispositivos, el Centro de operaciones y el agente de almacenamiento. Se aplican las restricciones siguientes:

- No puede configurar un entorno en clúster.
- No puede utilizar el mandato QUERY SAN ni la opción de servidor SANDISCOVERY para detectar dispositivos en una red de área de almacenamiento cuando los dispositivos están conectados a una tarjeta adaptadora de bus de host(HBA) configurada utilizando el método de virtualización por identificador de puerto de nodo (NPIV).
- No puede optimizar la transferencia de datos a servidores remotos mediante la habilitación de la tecnología Aspera Fast Adaptive Protocol (FASP).
- No puede configurar bibliotecas de software de sistema de cartuchos automatizados (ACSLs).

**Tareas relacionadas:**

Linux: Instalación del servidor

**Referencia relacionada:**

Linux: Requisitos mínimos del servidor Linux on Power Systems™ (little endian)

## Proteja su entorno de almacenamiento con un protocolo de seguridad mejorado

---

IBM Spectrum Protect Versión 8.1.2 proporciona un protocolo de seguridad mejorado.

Para proteger su entorno de almacenamiento de amenazas de seguridad, IBM Spectrum Protect tiene un protocolo de seguridad mejorado que utiliza Seguridad de la capa de transporte (TLS) 1.2 para cifrar todas las comunicaciones entre el servidor, el agente de almacenamiento y los clientes. Un nuevo parámetro SESSIONSECURITY determina si un administrador, nodo o servidor debe utilizar los valores más seguros para comunicarse con un servidor de IBM Spectrum Protect. Los servidores, clientes y agentes de almacenamiento de IBM Spectrum Protect que utilicen V8.12 o software posterior se configurarán automáticamente para que se comuniquen entre sí mediante SSL. Los certificados se distribuyen automáticamente.

Para ver una descripción detallada del parámetro SESSIONSECURITY parameter, consulte los temas para registrar y actualizar ID de administrador, nodos y servidores. Para obtener la información más reciente acerca de las actualizaciones de seguridad de V8.1.2, consulte la nota técnica 2004844.

**Referencia relacionada:**

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

REGISTER ADMIN (Registrar un ID de administrador)

REGISTER NODE (Registrar un nodo)

UPDATE ADMIN (Actualizar un administrador)

UPDATE NODE (Actualizar atributos del nodo)

UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)

**Información relacionada:**

Qué debería saber sobre seguridad antes de actualizar el servidor (AIX)

Qué debería saber sobre seguridad antes de actualizar el servidor (Linux)

Qué debería saber sobre seguridad antes de actualizar el servidor (Windows)

Conceptos sobre la seguridad

## Optimización de la seguridad con la clave de cifrado maestra generada automáticamente

---

A partir de IBM Spectrum Protect Versión 8.1.2, se genera automáticamente una clave de cifrado maestra cuando se inicia el servidor si la clave de cifrado maestra no existía anteriormente.

La clave de cifrado maestra recién generada se almacena en una nueva base de datos de claves, dsmkeydb.kdb. Si el servidor tiene una clave de cifrado maestra existente, la clave se migra del archivo dsmserv.pwd a la nueva base de datos de claves. La generación automática de la clave de cifrado maestra y su almacenamiento en la nueva base de datos de claves se han diseñado para mejorar la seguridad del sistema. Los certificados del servidor se siguen almacenando en la base de datos de claves cert.kdb y se accede a los mismos mediante el archivo stash cert.sth.

Debe proteger ambas bases de datos de claves (cert.kdb y dsmkeydb.kdb) y los archivos stash (cert.sth y dsmkeydb.sth) que proporcionan acceso a cada una de las bases de datos de claves. De forma predeterminada, el mandato BACKUP DB protege la clave de cifrado maestra, pero debe recordar la contraseña de la copia de seguridad de la base para restaurar la base de datos. El archivo

dmserv.pwd del servidor de IBM Spectrum Protect, que se ha utilizado para almacenar la clave de cifrado maestra en releases anteriores, ya no se utiliza.

**Referencia relacionada:**

BACKUP DB (copia de seguridad de la base de datos)

**Información relacionada:**

Recuperación de datos utilizando DRM

## Configuración de un entorno de almacenamiento utilizando la Guía de soluciones de cintas


---

El conjunto de documentación se ha actualizado para incluir la *Guía de soluciones de cintas de IBM Spectrum Protect*. Siguiendo las instrucciones de la guía, puede configurar una solución de cinta que optimice el almacenamiento y la recuperación ante siniestro, garantizando una copia segura de los datos en una ubicación externa.

La guía contiene instrucciones para realizar las siguientes tareas:

- Planificar e implementar una solución de protección de datos que utilice uno o varios dispositivos de almacenamiento en cinta para hacer copia de seguridad de los datos
- Supervisar una solución de cinta de IBM Spectrum Protect
- Gestionar dispositivos de cinta y unidades de cintas
- Recuperar datos después de que se produzca un siniestro o una interrupción no planificada

**Información relacionada:**

 Guía de soluciones de cintas (PDF)

Visión general de las soluciones de cintas

Planificación, implementación, supervisión y gestión de una solución de cintas

## Planificación de actualizaciones automáticas para la copia de seguridad y restauración de clientes

---

Con IBM Spectrum Protect Versión 8.1.2, Puede planificar el despliegue de actualizaciones de software en sistemas que ya tienen instalado el cliente de copia de seguridad y archivado.

Puede utilizar mandatos del servidor de IBM Spectrum Protect para planificar actualizaciones para uno o varios clientes de copia de seguridad y archivado. Las actualizaciones pueden ser fixpacks o releases nuevos. Esta característica estaba disponible en releases anteriores de IBM Spectrum Protect, pero ahora dispone de un procedimiento mejorado para V8.1.2.

Para obtener más información sobre cómo desplegar automáticamente las actualizaciones de cliente desde el servidor, consulte los documentos siguientes:

- Para servidores de IBM Spectrum Protect V8.1.2 o posteriores, consulte la nota técnica 2004596.
- Para servidores de IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la nota técnica 1673299.

## Actualice el servidor de IBM Spectrum Protect a la V8.1.2 antes de actualizar los clientes

---

Actualice los servidores de IBM Spectrum Protect a la versión 8.1.2 antes de actualizar los clientes de archivado y copia de seguridad.

Si no actualiza primero los servidores, es posible que la comunicación entre servidores y clientes se interrumpa.

**Información relacionada:**

Qué debería saber sobre seguridad antes de actualizar el servidor (AIX)

Qué debería saber sobre seguridad antes de actualizar el servidor (Linux)

Qué debería saber sobre seguridad antes de actualizar el servidor (Windows)

## Opciones, mandatos y parámetros del servidor en desuso y sin mantenimiento

---

Algunas opciones, mandatos y parámetros del servidor han quedado en desuso o ya no están disponibles a partir de IBM Spectrum Protect Versión 8.1.2. El comportamiento de algunos parámetros y opciones ha cambiado.

Debido a los cambios en los protocolos de seguridad, se han realizado las siguientes actualizaciones en el producto:

- Dos parámetros relacionados con SSL, VALIDATEPROTOCOL y SSLREQUIRED, han quedado en desuso y se ignoran. Estos parámetros se han sustituido por el parámetro SESSIONSECURITY.
- Cuatro opciones del servidor relacionadas con SSL, USETLS12, SSLTLS12, SSLHIDELEGACY, and SSLDISABLELEGACYTLS, ya no están disponibles.
- El comportamiento del parámetro SSL en los mandatos DEFINE SERVER y UPDATE SERVER ha cambiado. Ahora se utiliza SSL para cifrar ciertas comunicaciones con el servidor, incluso si se especifica SSL=NO.
- El comportamiento de las opciones TCPSPORT y TCPADMINPORT ha cambiado. Ahora el número de puerto que se especifica en la opción TCPSPORT o TCPADMINPORT escucha y acepta sesiones habilitadas tanto para TCP/IP como para SSL. Ya no es necesario especificar la opción SSLTCPSPORT o SSLTCPADMINPORT para permitir sesiones habilitadas para SSL desde el cliente.
- Los mandatos SET AUTHENTICATION, SET REGISTRATION, DELETE KEYRING, QUERY SSLKEYRINGPW y SET SSLKEYRINGPW ya no están disponibles.

**Referencia relacionada:**

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)

## Notas del release para componentes de la versión 8.1 del servidor

---

Las notas del release están disponibles para los componentes de V8.1.

- Notas del release para el servidor de IBM Spectrum Protect versión 8.1  
El servidor de IBM Spectrum Protect 8.1 está disponible. Incluye información de compatibilidad, instalación y otros temas de iniciación.
- Notas del release para Centro de operaciones versión 8.1  
El Centro de operaciones es una interfaz basada en web que puede utilizar para gestionar el entorno de IBM Spectrum Protect. Las notas del release le proporcionan acceso al anuncio del producto, problemas conocidos, requisitos del sistema, instrucciones de instalación y actualizaciones.
- Notas del release del soporte de dispositivos de IBM Spectrum Protect versión 8.1  
El soporte de dispositivos de IBM Spectrum Protect para V8.1 está disponible. Incluye problemas de compatibilidad, instalación y otros temas de iniciación.

## Notas del release para el servidor de IBM Spectrum Protect versión 8.1

---

El servidor de IBM Spectrum Protect 8.1 está disponible. Incluye información de compatibilidad, instalación y otros temas de iniciación.

### Contenido

---

- Descripción
- Anuncio
- Compatibilidad con versiones anteriores
- Requisitos del sistema
- Instalación y actualización de IBM Spectrum Protect
- Actualizaciones, limitaciones y problemas conocidos

### Descripción

---

IBM Spectrum Protect proporciona características de gestión de espacios, archivado y copia de seguridad automatizadas, planificadas centralmente y gestionadas mediante políticas para servidores de archivos, estaciones de trabajo, máquinas virtuales y aplicaciones.

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR resueltos, consulte la publicación APAR arreglados en el servidor de IBM Spectrum Protect, versión 8.1.

### Anuncio

---

El anuncio de la familia de productos de IBM Spectrum Protect V8.1 incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto



- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

## Compatibilidad con versiones anteriores

---

Para ver la compatibilidad con versiones anteriores, consulte la publicación Compatibilidad de cliente y servidor de IBM Spectrum Protect y consideraciones de actualización.

## Requisitos del sistema

---

Para ver la información de requisitos del sistema, consulte la publicación Sistemas operativos compatibles con IBM Spectrum Protect.

## Instalación y actualización de IBM Spectrum Protect

---

Para obtener instrucciones de instalación del servidor, consulte el procedimiento correspondiente a su sistema operativo:

IBM AIX

Instalación del servidor

Linux

Instalación del servidor

Microsoft Windows

Instalación del servidor

Para obtener instrucciones de actualización, consulte el apartado Actualización a V8.1.

## Actualizaciones, limitaciones y problemas conocidos

---

Las actualizaciones describen nueva información del producto o nuevas características del producto que pasan a estar disponibles después del lanzamiento del producto. Las actualizaciones, limitaciones y problemas conocidos están documentados en forma de notas técnicas en la base de conocimiento de soporte de IBM® Support Portal. Pueden encontrarse soluciones o métodos alternativos para los problemas conocidos buscando en la base de conocimiento.

Actualizaciones

### **El mandato REGISTER NODE ya no crea un ID de usuario de administración de forma predeterminada**

A partir de IBM Spectrum Protect V8.1, el mandato REGISTER NODE no crea automáticamente un ID de usuario de administración que coincide con el nombre de nodo. Este producto puede afectar al proceso de registro de nodos de cliente, incluidos, entre otros, los nodos del cliente de archivado y copia de seguridad de IBM Spectrum Protect. En algunos casos, puede que tenga que crear un ID de usuario de administración especificando el parámetro USERID en el mandato REGISTER NODE. Para obtener información sobre los tipos de clientes afectados, consulte la nota técnica 7048963.

Para buscar las últimas actualizaciones, consulte la publicación Actualizaciones para IBM Spectrum Protect V8.1.

Limitaciones y problemas conocidos

En el momento de la publicación, no existían limitaciones ni problemas conocidos.

Para buscar las limitaciones y problemas conocidos más recientes, que podrían incluir elementos adicionales, consulte Limitaciones y problemas conocidos de IBM Spectrum Protect V8.1.

## Notas del release para Centro de operaciones versión 8.1

---

El Centro de operaciones es una interfaz basada en web que puede utilizar para gestionar el entorno de IBM Spectrum Protect. Las notas del release le proporcionan acceso al anuncio del producto, problemas conocidos, requisitos del sistema, instrucciones de instalación y actualizaciones.

## Contenido

---

- Descripción
- Anuncio
- Compatibilidad con el servidor de IBM Spectrum Protect
- Requisitos del sistema
- Instalación o actualización del Centro de operaciones
- Actualizaciones, limitaciones y problemas conocidos

## Descripción

---

Puede utilizar el Centro de operaciones para realizar las acciones siguientes:

- Identificar problemas potenciales con el entorno de IBM Spectrum Protect
- Supervisar aspectos clave del entorno de almacenamiento: alertas, clientes, servidores, políticas, agrupaciones de almacenamiento y dispositivos de almacenamiento
- Registrar clientes
- Añadir servidores a supervisar
- Realizar copias de seguridad de clientes, bases de datos de servidor y agrupaciones de almacenamiento
- Iniciar la reclamación y la migración de la agrupación de almacenamiento
- Asignar alertas a para administradores y cerrar alertas
- Ver y cancelar procesos de servidor y sesiones de cliente
- Cambiar los valores del dispositivo de almacenamiento, el cliente, el servidor y la agrupación de almacenamiento
- Crear y gestionar planificaciones de cliente y ver planificaciones de administración
- Convertir agrupaciones de almacenamiento primario en agrupaciones de almacenamiento de contenedores
- Copiar datos de las agrupaciones de almacenamiento de contenedores de directorio en la cinta
- Configurar réplica
- Modificar valores de política
- Dejar fuera de servicio a los clientes y desactivar los datos
- Crear informes de correo electrónico
- Ver el uso de la capacidad frontal y de fondo para supervisar la conformidad con las licencias
- Emitir mandatos a servidores de IBM Spectrum Protect

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR arreglados, consulte la publicación APAR arreglados en el centro de operaciones de IBM Spectrum Protect versión 8.1.

## Anuncio

---

El Centro de operaciones forma parte de la familia de productos de IBM Spectrum Protect V8.1. El anuncio de estos productos incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto
- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

## Compatibilidad con el servidor de IBM Spectrum Protect

---

Para obtener información sobre la compatibilidad, consulte la publicación Compatibilidad del centro de operaciones y el servidor de IBM Spectrum Protect.

## Requisitos del sistema

---

Para obtener los requisitos del sistema, consulte la publicación Requisitos de hardware y software del centro de operaciones de IBM Spectrum Protect.

## Instalación o actualización del Centro de operaciones

---

Para obtener instrucciones de instalación, o actualizar una versión existente del Centro de operaciones, consulte Instalación y actualización del Centro de operaciones.

## Actualizaciones, limitaciones y problemas conocidos

---

Las actualizaciones describen nueva información del producto o nuevas características del producto que pasan a estar disponibles después del lanzamiento del producto. Las actualizaciones, limitaciones y problemas conocidos están documentados en forma de notas técnicas en la base de conocimiento de soporte de IBM® Support Portal. Pueden encontrarse soluciones o métodos alternativos para los problemas conocidos buscando en la base de conocimiento.

### Actualizaciones

Para obtener la lista de actualizaciones más reciente, consulte Resultados de búsqueda de actualizaciones de Centro de operaciones V8.1.

### Limitaciones y problemas conocidos

- Para obtener una lista de limitaciones y problemas conocidos, consulte Limitaciones y problemas conocidos con Centro de operaciones V8.1.
- Para buscar problemas adicionales que puedan pasar a ser problemas conocidos después del lanzamiento del producto, consulte Resultados de búsqueda de problemas conocidos con Centro de operaciones V8.1.

## Notas del release del soporte de dispositivos de IBM Spectrum Protect versión 8.1

---

El soporte de dispositivos de IBM Spectrum Protect para V8.1 está disponible. Incluye problemas de compatibilidad, instalación y otros temas de iniciación.

### Contenido

---

- Descripción
- Anuncio
- Dispositivos compatibles
- Requisitos de controladores de dispositivos
- Información de bibliotecas
- Actualizaciones, limitaciones y problemas conocidos

### Descripción

---

Este documento incluye información sobre controladores de dispositivos de IBM Spectrum Protect V8.1.

Un informe autorizado de análisis de programa (APAR) es una solicitud para que se corrija un defecto en un release compatible de un programa proporcionado por IBM. Para obtener una lista de los APAR resueltos, consulte la publicación APAR arreglados en el controlador de dispositivo de IBM Spectrum Protect versión 8.1.

### Anuncio

---

El soporte de dispositivos de IBM Spectrum Protect para V8.1 se anuncia como parte del anuncio de los productos de la familia de IBM Spectrum Protect. El anuncio de estos productos incluye la información siguiente:

- Descripción detallada del producto, incluidas las descripciones de las nuevas funciones
- Declaración de posicionamiento del producto
- Información sobre compatibilidad internacional

Para buscar el anuncio de producto, realice los pasos siguientes:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Buscar, especifique el identificador de producto (PID) correspondiente a su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Tipo de información, seleccione Cartas de anuncio y pulse Buscar.
4. En la lista Buscar en, seleccione Número de producto.
5. Opcional: en el panel Refinar la búsqueda de la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Ordenar por, seleccione Más nuevos primero.

## Dispositivos admitidos

---

Para obtener información sobre los dispositivos y el hardware compatibles con sistemas IBM AIX y Microsoft Windows, consulte el apartado Dispositivos compatibles con AIX y Windows.

Para obtener información sobre el hardware y dispositivos con soporte para sistemas Linux, consulte Dispositivos compatibles con Linux.

## Requisitos de controladores de dispositivos

---

### Requisitos del adaptador de bus de host

Para obtener mejores resultados, conecte las unidades de cinta y las bibliotecas de cinta al sistema con un adaptador de bus de host exclusivo. No comparta el adaptador de bus de host con otro tipo de dispositivo, como DISK o CD.

### El número máximo de dispositivos soportados por los controladores de dispositivo de IBM Spectrum Protect

Para obtener información sobre el número máximo de dispositivos que los controladores de dispositivos de IBM Spectrum Protect pueden admitir en cada sistema operativo, consulte la nota técnica 1364225.

### Soporte de dispositivos SAS (SCSI de conexión en serie)

Los dispositivos SAS pueden utilizarse en algunos sistemas operativos y arquitecturas. Para obtener información sobre los sistemas operativos y las arquitecturas para los dispositivos SAS, consulte la nota técnica 1396706.

### Ejecución del controlador de paso a través de IBM Spectrum Protect con un ID de usuario no root en sistemas operativos Linux

Para obtener información sobre cómo permitir que un usuario no root utilice dispositivos con el controlador de paso a través de IBM Spectrum Protect en Linux, consulte la nota técnica 1321130. Utilice la opción `-g` o la opción `-a` del programa de utilidad `autoconf` del dispositivo para garantizar que los usuarios que no sean root puedan utilizar dispositivos que estén configurados con el controlador de paso a través de IBM Spectrum Protect. Utilice la opción `-g` para añadir permisos de lectura y escritura para grupos en archivos de dispositivos del controlador genérico SCSI (sg). Utilice la opción `-a` para añadir permisos de lectura y escritura para todos los usuarios en archivos de dispositivos del controlador genérico SCSI (sg).

## Información de bibliotecas

---

- Es necesario disponer de IBM Spectrum Protect Extended Edition para una biblioteca con más de cuatro unidades o más de 48 ranuras de almacenamiento.
- Es posible que las direcciones de elementos de las ranuras de almacenamiento no se correspondan directamente con los números de ranura de almacenamiento. Esto es importante porque el servidor de IBM Spectrum Protect siempre hace referencia a las ranuras de almacenamiento por direcciones de elementos, no según los números de las ranuras de almacenamiento. Consulte la página de configuración de bibliotecas para conocer las direcciones de elementos.
- Para una biblioteca con varias unidades, se necesita una dirección de elemento de la unidad para los mandatos `DEFINE` y `UPDATE DRIVE`. No obstante, cuando la biblioteca indica los números de serie de la unidad, puede especificar `ELEMENT=AUTODETECT` y no es necesario conocer la dirección de elemento.
- Para el procedimiento de configuración independiente del cambiador automático y de cada unidad de la biblioteca, consulte Configuración y gestión de dispositivos de almacenamiento.

## Actualizaciones, limitaciones y problemas conocidos

---

### Actualizaciones

Algunos dispositivos que eran compatibles con releases anteriores de IBM Spectrum Protect ya no lo son en el servidor de IBM Spectrum Protect V8.1. Para obtener la lista más reciente de dispositivos soportados, consulte los enlaces siguientes:

- Dispositivos compatibles con AIX y Windows
- Dispositivos compatibles con Linux

Para buscar las actualizaciones, limitaciones y problemas conocidos más recientes, que podrían incluir elementos adicionales, consulte Actualizaciones, limitaciones y problemas conocidos del soporte de dispositivos de IBM Spectrum Protect V8.1.

## Archivos léame para componentes de la versión 8.1 del servidor

---

Los archivos léame para los fixpacks de la Versión 8.1 están publicados en el sitio web de soporte de software de IBM. Pueden existir actualizaciones disponibles para los componentes del servidor, incluyendo el propio servidor, el soporte de dispositivos y el Centro de operaciones.

Visualizar archivo léame de fixpack del servidor de IBM Spectrum Protect V8.1

## Instalación y actualización

- Implementación de una solución IBM Spectrum Protect  
Si está desplegando un nuevo entorno de servidor IBM Spectrum Protect, plantéese implementar la configuración más adecuada.
- Instalación y actualización del servidor  
El servidor de IBM Spectrum Protect proporciona servicios de copia de seguridad, archivado y gestión de espacio a clientes. Puede instalar o actualizar servidores individuales o múltiples en la red de la empresa.
- Instalación y actualización del Centro de operaciones  
Centro de operaciones es la interfaz basada en web para gestionar el entorno de almacenamiento.

## Implementación de una solución IBM Spectrum Protect

Si está desplegando un nuevo entorno de servidor IBM Spectrum Protect, plantéese implementar la configuración más adecuada.

Hay documentación de soluciones IBM Spectrum Protect disponible para ayudarle a seleccionar una solución adecuada, basándose en las necesidades de negocio y, a continuación, instalar, configurar, supervisar y operar dicha solución.

Para obtener detalles, consulte Selección de una solución IBM Spectrum Protect.

## Disponibilidad de las características por sistema operativo

La mayoría de las características de IBM Spectrum Protect están disponibles en todos los sistemas operativos que reciben soporte para el servidor.

En la tabla siguiente, una marca de selección indica que una característica está disponible.

Tabla 1. Disponibilidad de las características de IBM Spectrum Protect por sistema operativo

Característica	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (little endian)	Microsoft Windows
Tecnología Aspera Fast Adaptive Secure Protocol (FASP): Optimización de la transferencia de datos a un servidor remoto.		☑			
Almacenamiento en la nube mediante la tecnología Amazon Simple Storage Service (Amazon S3).	☑	☑		☑	☑
Almacenamiento en la nube mediante la tecnología IBM Cloud Object Storage.	☑	☑		☑	☑
Almacenamiento en la nube mediante la tecnología IBM SoftLayer (IBM Bluemix).	☑	☑		☑	☑
Almacenamiento en la nube mediante la tecnología Microsoft Azure.	☑	☑		☑	☑
Almacenamiento en la nube mediante la tecnología OpenStack Swift.	☑	☑		☑	☑

Característica	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (little endian)	Microsoft Windows
<p>Deduplicación de datos:</p> <p>Utilización de la <i>deduplicación de datos en línea</i> para eliminar datos duplicados cuando los datos se graban en una agrupación de almacenamiento del contenedor de directorio o en una agrupación de almacenamiento de contenedor en la nube. Mediante la deduplicación de datos en línea, se reduce la necesidad de realizar una reorganización fuera de línea y se puede mejorar el rendimiento del servidor y reducir el coste del hardware de almacenamiento.</p>	✓	✓	✓	✓	✓
<p>Deduplicación de datos:</p> <p>Utilización de la <i>deduplicación de datos postproceso</i> para eliminar los datos duplicados de las agrupaciones de almacenamiento de disco de acceso secuencial. Esta opción puede aumentar los tiempos de proceso debido a que el servidor debe identificar los datos y luego eliminarlos de la agrupación de almacenamiento.</p>	✓	✓	✓	✓	✓
<p>Gestor de recuperación ante siniestro (DRM):</p> <p>Preparación de un plan para recuperar los datos del servidor y del cliente en caso de que se produzca un siniestro.</p>	✓	✓	✓	✓	✓
<p>Compresión de datos en línea:</p> <p>Compresión de los datos a medida que se graban en una agrupación de almacenamiento de contenedor en la nube o de contenedor de directorio para reducir la cantidad de espacio que ocupan los datos.</p>	✓	✓	✓	✓	✓
<p>Autenticación con Lightweight Directory Access Protocol (LDAP):</p> <p>Autenticación de los usuarios ante una base de datos de Active Directory en un servidor LDAP.</p>	✓	✓	✓	✓	✓
<p>Réplica de nodos:</p> <p>Copia incremental de los datos pertenecientes a nodos de cliente de copia de seguridad y archivado de un servidor en otro.</p>	✓	✓	✓	✓	✓
<p>Centro de operaciones:</p> <p>Supervisión y gestión del entorno de almacenamiento mediante Centro de operaciones, una interfaz de usuario basada en la web.</p>	✓	✓	✓	✓	✓

Característica	IBM® AIX	Linux x86_64	Linux on System z	Linux on Power Systems (little endian)	Microsoft Windows
<b>Protección de agrupaciones de almacenamiento de contenedor de directorio:</b> Protección de los datos de las agrupaciones de almacenamiento de contenedor de directorio mediante el mandato PROTECT STGPOOL. Puede almacenar una copia de los datos en otra agrupación de almacenamiento de contenedor de directorio en un servidor de réplica de destino o almacenar una copia en cinta en una agrupación de almacenamiento de copia de contenedor del mismo servidor.	✓	✓	✓	✓	✓
<b>Cifrado de agrupación de almacenamiento:</b> Cifrado de los datos de las agrupaciones de almacenamiento de contenedor de nube.	✓	✓		✓	✓
<b>Cifrado de agrupación de almacenamiento:</b> Cifrado de los datos de las agrupaciones de almacenamiento de contenedor de directorio.	✓	✓	✓	✓	✓
<b>Almacenamiento en cinta:</b> Almacenamiento de los datos en cinta, lo que proporciona una opción flexible y asequible para la conservación de datos a largo plazo.	✓	✓	✓	✓	✓
<b>Protocolo Transport Layer Security (TLS) 1.2:</b> Protección de comunicaciones mediante el protocolo TLS 1.2	✓	✓	✓	✓	✓

## Instalación y actualización del servidor

El servidor de IBM Spectrum Protect proporciona servicios de copia de seguridad, archivado y gestión de espacio a clientes. Puede instalar o actualizar servidores individuales o múltiples en la red de la empresa.

- Instalación del servidor en sistemas AIX
- Instalación del servidor en sistemas Linux
- Instalación del servidor en sistemas Windows
- Actualización del servidor

## AIX: Instalación del servidor

La instalación del servidor incluye la planificación, instalación y configuración inicial.



- AIX
- AIX: Planificación para instalar el servidor  
 Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- AIX: Instalación de los componentes de servidor  
 Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- AIX: Primeros pasos tras instalar IBM Spectrum Protect  
 Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.
- AIX: Instalación de un fixpack de servidor de IBM Spectrum Protect  
 Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

- AIX: Revertir de la versión 8.1.2 a un servidor anterior  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- AIX: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- AIX: Desinstalar IBM Spectrum Protect  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## AIX: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.


- AIX: Qué debe saber primero  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- AIX: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor  
Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.
- AIX: Planificación de rendimiento óptimo  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  Sistemas operativos AIX AIX: Requisitos de sistema mínimos para sistemas AIX  
Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo AIX, en un sistema sin deduplicación de datos, revise los requisitos de hardware y software.
-  Sistemas operativos AIX AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema  
Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.2, con algunas limitaciones.
- AIX: IBM Installation Manager  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- AIX: Hojas de trabajo para planificar detalles para el servidor  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- AIX: Planificación de la capacidad  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.
- AIX: Prácticas más adecuadas de denominación del servidor  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- AIX: Directorios de instalación  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

## AIX: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 Sistemas operativos AIX Restricción: Puede instalar y ejecutar el servidor de la versión 8.1.2 en un sistema que ya tenga DB2 instalado, tanto si DB2 se ha instalado de forma independiente como si se ha instalado como parte de otra aplicación, con algunas restricciones. Para conocer más detalles, consulte el tema sobre compatibilidad con otros productos DB2.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.2 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.



Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## AIX: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor

---

Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.

### Acerca de esta tarea

---

Las mejoras de seguridad en V8.1.2 y posterior han aplicado parámetros de seguridad más estrictos. Para garantizar que no se interrumpa la comunicación entre servidores y clientes al instalar o actualizar el software IBM Spectrum Protect a V8.1.2, siga el procedimiento.

### Procedimiento

---

1. Instale o actualice los servidores IBM Spectrum Protect a 8.1.2 o posterior.
2. Instale o actualice los clientes de copia de seguridad y archivado. Si desea más información, consulte *Instalación y configuración de clientes*.  
Para obtener información sobre la planificación del despliegue de actualizaciones de clientes desde el servidor, consulte los siguientes documentos:
  - Para servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.
  - Para servidores IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la nota técnica 1673299.
3. Configure las opciones para clientes de copia de seguridad y archivado. Para obtener más información, consulte *Actualización del servidor de IBM Spectrum Protect e IBM Spectrum Protect Client*.

## AIX: Planificación de rendimiento óptimo

---

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.


### Procedimiento

---



1. Revise AIX: Qué debe saber primero.
2. Revise cada una de las siguientes subsecciones.
  - AIX: Planificación del hardware del servidor y el sistema operativo  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de discos de base de datos del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de discos de registro de recuperación del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - AIX: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.
  - AIX: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
  - AIX: Planificación del tipo correcto de tecnología de almacenamiento  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
  - AIX: Aplicación de prácticas recomendadas para la instalación del servidor  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

## AIX: Planificación del hardware del servidor y el sistema operativo

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul>	<p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p> <p> Sistemas operativos AIX Restricción: No utilice Active Memory Expansion (AME). Al utilizar AME, el software de IBM DB2 utiliza páginas de 4 KB en lugar de páginas de 64 KB. Cada página de 4 KB debe descomprimirse al acceder a ella, y comprimirse cuando no sea necesaria. Cuando se produce la compresión o la descompresión, DB2 y el servidor esperan para acceder a la página, lo que degrada el rendimiento del servidor.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p>
<p>¿Están configurados los discos para un rendimiento óptimo?</p>	<p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿El servidor tiene suficiente memoria?	<p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p>	<p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul>
¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente?	<p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>	<p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?	<p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul>
¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect?	<p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. La siguiente lista identifica el sistema de archivos preferido:</p> <p> Sistemas operativos</p> <ul style="list-style-type: none"> <li>• AIX Utilice el sistema de archivos JFS2 con la opción rbrw.</li> </ul>	<p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>
¿Tiene pensado configurar suficiente espacio de paginación?	<p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos AIX Utilice un mínimo de 32 GB de espacio de paginación o el 50% de su RAM, el valor que sea mayor.</p>	

## AIX: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Se encuentra la base de datos en discos rápidos de baja latencia?	<p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p>	Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.
¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento?	<p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>	
Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?	<p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>	
Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?	Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.	El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p>	<p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <code>DB2_PARALLEL_IO</code> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <code>DB2_PARALLEL_IO</code>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <code>DB2_PARALLEL_IO</code>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>	<p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>	
<p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>	<p>La profundidad de cola predeterminada suele ser demasiado baja.</p>	<p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>

## AIX: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos?	Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.	La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.
¿Se encuentran los registros en discos con memoria caché de escritura no volátil?	La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.	
¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?	Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.  Registro activo El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.  Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.  Registro de archivos El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo.	<ul style="list-style-type: none"> <li>Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>
¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?	El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.	Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.  Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande.
Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?	Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro. <ul style="list-style-type: none"> <li>Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>Utilice la duplicación en el hardware del sistema de disco.</li> </ul>	Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.  Para obtener más información, consulte Configuración y ajuste del registro de recuperación.

## AIX: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p>	<p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$	<p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>	<p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul>	<p>Requisitos de memoria</p>



Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>	<p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p>	<p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>	<p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>	<p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p>	<p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>	<p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p>
<p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>	<p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>	<ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha asignado suficiente espacio de almacenamiento para la base de datos?	<p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>	
¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?	<p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol>	Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?	<p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p>	<p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad?	<p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>	<ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>
¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?	<p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>	<p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?	<p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>	Para obtener más información, consulte la opción de cliente enablededup.
¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?	<p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>	
¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?	<p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul>	

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha seleccionado el tipo apropiado de almacenamiento local?	<p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul>	

## AIX: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo?	<p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p>	Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.
¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?	Utilice más memoria caché para un mejor rendimiento.	
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?	Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.	Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario.
Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?	<p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>	<p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>
Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?	Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.	Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?</p>	<p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p>	<p>Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.</p>
<p>En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?</p>	<p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>	<p>Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.</p>
<p>¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?</p>	<p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>	<p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul>

## AIX: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento

Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

<b>Tipo de tecnología de almacenamiento</b>	<b>Base de datos</b>	<b>Registro activo</b>	<b>Registro de archivado y registro de migración tras error de archivado</b>	<b>Agrupaciones de almacenamiento</b>
<b>Unidad de estado sólido (SSD)</b>	<p>Coloque la base de datos en SSD en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>	<p>Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>
<p><b>Disco de alto rendimiento con las siguientes características:</b></p> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.</p>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.</p>	<p>Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.</p>	<p>Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.</p>



Tipo de tecnología de almacenamiento	Base de datos	Registro activo	Registro de archivado y registro de migración tras error de archivado	Agrupaciones de almacenamiento
<b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>• Disco de 10.000 rpm</li> <li>• Interfaz Fibre Channel o SAS</li> </ul>	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.	Utilice disco de rendimiento medio o alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.
<b>SATA, almac. adjunto de red</b>	No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.	No utilice este almacenamiento para el registro activo.	El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.	Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>• Los datos se leen con poca frecuencia.</li> </ul>
<b>Cinta y cinta virtual</b>				Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.

## AIX: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

Práctica recomendada	Más información
----------------------	-----------------

<b>Práctica recomendada</b>	<b>Más información</b>
<p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p>	<p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>
<p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>
<p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>	<p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>
<p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>	<p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>
<p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>	<p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>

Práctica recomendada	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores.	<p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p>
Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.	<p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>○ Ajuste de la planificación para las operaciones diarias</li> <li>○ Lista de comprobación para la configuración de servidor</li> </ul>
Supervise las operaciones de forma constante.	<p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento. Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>

## AIX: Requisitos de sistema mínimos para sistemas AIX

Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo AIX, en un sistema sin deduplicación de datos, revise los requisitos de hardware y software.

### Requisitos de software y de hardware de la instalación del servidor de IBM Spectrum Protect

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado AIX: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Hardware	Un sistema POWER5 o posterior (64 bits)

Tipo de hardware	Requisitos de hardware
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección AIX: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes son los requisitos mínimos de memoria del sistema para servidores con bases de datos hasta 500 GB, con ingestión diaria de no más de 200 GB al día:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>


## Requisitos de software

Tabla 2 describe los requisitos de software mínimos necesarios para un servidor en un sistema AIX.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
------------------	--------------------------------

Tipo de software	Requisitos mínimos de software
Sistema operativo	<p>AIX 6.1 ejecutándose en un entorno de kernel de 64 bits con los siguientes requisitos adicionales:</p> <ul style="list-style-type: none"> <li>• AIX 6.1 TL 7 y SP6.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 12.1.0.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 12.1.0.1. El conjunto de archivos se incluye en el paquete de fixpack de junio de 2008 de los componentes del entorno de tiempo de ejecución C++ de IBM® para AIX.</li> </ul> <p>AIX 7.1 en un entorno de kernel de 64 bits.</p> <ul style="list-style-type: none"> <li>• AIX 7.1 TL 4 y SP2.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 12.1.0.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 12.1.0.1. El conjunto de archivos se incluye en el paquete de fixpack de junio de 2008 de los componentes del entorno de tiempo de ejecución C++ de IBM para AIX.</li> </ul> <p>AIX 7.2 que se ejecuta en un entorno de kernel de 64 bits.</p> <ul style="list-style-type: none"> <li>• AIX 7.2 TL 0 y SP2.</li> <li>• Nivel de tiempo de ejecución C++ mínimo con los conjuntos de archivos xLC.rte 13.1.3.1 posterior. El conjunto de archivos se actualiza automáticamente si el nivel es anterior a 13.1.3.1.</li> </ul> <p>Para ver las últimas recomendaciones sobre los niveles de mantenimiento de AIX, consulte la nota técnica 21165448</p> <p>Para utilizar el recurso N_Port ID Virtualization (NPIV), asegúrese de que cumple los siguientes requisitos mínimos:</p> <ul style="list-style-type: none"> <li>• Servidor de E/S virtual 2.1.2 o posterior</li> <li>• AIX 7.1 o posterior</li> <li>• Un adaptador HBA compatible con el servidor de E/S virtual y AIX correspondiente</li> </ul>
Protocolo de comunicaciones	Un método de comunicación configurado.
Proceso	Tiene que habilitarse la entrada/salida asíncrona.
Controladores de dispositivo	<p>El controlador de dispositivo IBM Spectrum Protect es necesario para unidades y biblioteca de cintas que no son de IBM. El paquete del controlador de dispositivos IBM Spectrum Protect incluye herramientas del controlador del dispositivo y daemons de ACSLS.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p>
Programa de utilidad gunzip	El programa de utilidad gunzip debe estar disponible en el sistema para poder instalar o actualizar el servidor. Asegúrese de que el programa de utilidad gunzip esté instalado y que la vía de acceso al mismo esté establecida en la variable de entorno PATH.
Otro software	<p>Se necesita el shell Korn (ksh). Configure los puertos de terminación de entrada y salida (IOCP) en el sistema operativo.</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

 Sistemas operativos AIX

## AIX: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.2, con algunas limitaciones.

Para instalar y utilizar otros productos que usen un producto DB2 en el mismo sistema que el servidor de IBM Spectrum Protect, asegúrese de que se cumplan los siguientes criterios:

Tabla 1. Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Criterio	Instrucciones
Nivel de versión	El resto de productos que utilizan un producto DB2 tienen que utilizar la versión 9 de DB2 o una versión posterior. Los productos de DB2 incluyen soporte de encapsulamiento y segregación de productos desde la versión 9. A partir de esta versión, puede ejecutar varias copias de productos de DB2, en diferentes niveles de código, en el mismo sistema. Si desea detalles, consulte la información sobre varias copias de DB2 en Información sobre el producto DB2.
ID de usuario y directorios	Asegúrese de que los ID de usuario, los ID de usuarios delimitados, la ubicación de la instalación, otros directorios y la información relacionada no se compartan en instalaciones de DB2. Las especificaciones deben ser distintas a partir de los ID y ubicaciones utilizados para la instalación y configuración del servidor de IBM Spectrum Protect. Si utilizó el asistente dsmicfgx para configurar el servidor, estos son los valores especificados al ejecutar el asistente. Si utilizó el método de configuración manual, revise los procedimientos utilizados, si fuese necesario, para recordar los valores utilizados en el servidor.
Asignación de recursos	<p>Tenga en cuenta los recursos y las prestaciones del sistema en comparación con los requisitos del servidor de IBM Spectrum Protect y las otras aplicaciones que utilizan el producto de DB2. Para proporcionar recursos suficientes para el resto de aplicaciones DB2, es posible que deba modificar los ajustes del servidor IBM Spectrum Protect para que el servidor utilice menos recursos y memoria del sistema. De manera similar, si las cargas de trabajo de las demás aplicaciones de DB2 compiten con el servidor de IBM Spectrum Protect en cuanto a los recursos de memoria y del procesador, el rendimiento del servidor relacionado con la carga de trabajo de cliente prevista y otras operaciones podría verse afectado negativamente.</p> <p>Para segregación de recursos y proporcionar más capacidades para el ajuste y la asignación del procesador, de la memoria y de otros recursos del sistema para varias aplicaciones, puede utilizar particiones lógicas (LPAR), particiones de carga de trabajo (WPAR) o el soporte de otra estación de trabajo virtual. Por ejemplo, ejecute una aplicación de DB2 en su propio sistema virtualizado.</p>

## AIX: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager
- Oferta de IBM Spectrum Protect

### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es IBM Installation Manager.

#### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.

#### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## AIX: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarle a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

Elemento	Espacio necesario	Número de directorios	Ubicación de los directorios
La base de datos			
Registro activo			
Registro de archivos			
Opcional: duplicado de registro para el registro activo			
Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado)			

Elemento	Nombres e ID de usuario	Ubicación
El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect		
El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia		
El nombre de instancia de la base de datos		
El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor)		
El nombre del servidor; utilice un nombre exclusivo para cada servidor		

## AIX: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- AIX: Estimación de los requisitos de espacio para la base de datos  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

- **AIX: Requisitos de espacio del registro de recuperación**  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.
- **AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación**  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- **AIX: Supresión de archivos de retrotracción de instalación**  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## AIX: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- **AIX: Estimación de los requisitos de espacio de base de datos en función del número de archivos**  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- **AIX: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento**  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- **AIX: El gestor de bases de datos y el espacio temporal**  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## AIX: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.
- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.



En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:

$$500 * 3.5 = 1.7 \text{ TB}$$

## Resultados

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrece acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

Tamaño de la base de datos	Requisito mínimo de espacio temporal
< 500 GB	50 GB
≥ 500 GB y < 1 TB	100 GB
≥ 1 TB y < 1,5 TB	150 GB
≥ 1,5 y < 2 TB	200 GB
≥ 2 y < 3 TB	250 - 300 GB
≥ 3 y < 4 TB	350 - 400 GB

## AIX: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## AIX: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.

- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.
- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## AIX: Requisitos de espacio del registro de recuperación

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- AIX: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- AIX: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- AIX: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## AIX: Espacio del registro activo y archivado

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:

- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.

- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- AIX: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

número de clientes x archivos almacenados durante cada transacción  
x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.

Elemento	Valores de ejemplo	Descripción
Espacio de registro necesario para cada archivo	3053 bytes	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	19,5 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 3,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>3,5 + 16 = 19,5 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	58,5 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p><math>3,5 \times 3 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>10,5 + 48 = 58,5 \text{ GB}</math></p>
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

Elemento	Valores de ejemplo	Descripción
----------	--------------------	-------------

Elemento	Valores de ejemplo		Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	1000	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Sesiones posibles para cada cliente	3	3	El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.
Archivos almacenados durante cada transacción	4096	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3053	3053	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	26,5 GB <sup>1</sup>	51 GB <sup>1</sup>	<p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	79,5 GB <sup>1</sup>	153 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p>		

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
Registro de archivado: Tamaño recomendado	60 GB <sup>1</sup>	Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:  4 GB x 3 = 12 GB  Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:  12 + 48 = 60 GB
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

`300 clientes x 100.000 archivos por cada cliente x 110 bytes = 3,1 GB`

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## AIX: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.



La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día	60 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana	132 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p>		
<p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## AIX: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

### La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

### El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

### El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

### El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que

una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.
Tamaño medio de extensiones	700 KB	700 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.
Extensiones para un determinado archivo	1.198.372 bits	6.135.667 bits	Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.  Se ha utilizado el siguiente cálculo para un objeto de 800 GB: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$  Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	1,7 GB	8,6 GB	El espacio de registro activo estimado necesario para esta transacción.

Elemento	Valores de ejemplo		Descripción
Registro activo: Tamaño total recomendado	66 GB <sup>1</sup>	79,8 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$
Registro de archivado: Tamaño recomendado	198 GB <sup>1</sup>	239,4 GB <sup>1</sup>	<p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.

Elemento	Valores de ejemplo		Descripción
Tamaño medio de extensiones	256 KB	256 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.
Extensiones para un determinado archivo	3.276.800 bits	16.777.216 bits	<p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	4,5 GB	23,4 GB	El tamaño estimado del espacio de registro activo necesario para esta transacción.
Registro activo: Tamaño total recomendado	71,6 GB <sup>1</sup>	109,4 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$

Elemento	Valores de ejemplo		Descripción
Registro de archivado: Tamaño recomendado	214,8 GB <sup>1</sup>	328,2 GB <sup>1</sup>	<p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

## AIX: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## AIX: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## AIX: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## AIX: Supresión de archivos de retroacción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retroacción son tipos de archivos que puede suprimir.

## Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- AIX: Supresión de archivos de retroacción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la

interfaz de usuario de IBM® Installation Manager.

- AIX: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

## AIX: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico


---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.

 Sistemas operativos AIX En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente para iniciar IBM Installation Manager:

```
./IBMIM
```

2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.


## AIX: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos

---



Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos AIX/eclipse/tools

Por ejemplo:

-  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
  -  Sistemas operativos AIX./imcl -c
3. Especifique **P** para seleccionar Preferencias.
4. Especifique **3** para seleccionar Archivos a restaurar.
5. Especifique **D** para Suprimir los Archivos a restaurar.
6. Especifique **A** para Aplicar cambios y volver al menú Preferencias.
7. Especifique **C** para salir del Menú Preferencias.
8. Especifique **X** para Salir de Installation Manager.

## AIX: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.

### Identificador de usuario de la instancia

---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.



## Directorio de inicio del ID de usuario de la instancia

---

El directorio de inicio puede crearse cuando se crea el ID de usuario de la instancia, utilizando la opción (-m) para crear un directorio de inicio si todavía no existe. Dependiendo de la configuración local, el directorio padre podría tener la forma:  
`/home/instance_user_ID`

Por ejemplo: `/home/tsminst1`

El directorio de inicio se utiliza principalmente como contenedor del perfil del ID de usuario y de valores de seguridad.

## Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos tiene que ser el mismo que el identificador de usuario de la instancia en la que ejecuta la instancia del servidor.

Por ejemplo: `tsminst1`

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede crear el directorio de la instancia como subdirectorio del directorio padre para el identificador de usuario de la instancia.  
Por ejemplo: `/home/instance_user_ID/instance_user_ID`

En el siguiente ejemplo se coloca el directorio de la instancia en el directorio padre del identificador de usuario `tsminst1`:  
`/home/tsminst1/tsminst1`

También puede crear el directorio en otra ubicación, por ejemplo: `/tsmserv/tsminst1`

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`
- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre `TSMDB1`, para todas las instancias del servidor. Este nombre no puede modificarse.


## Nombre de servidor

---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato `QUERY SERVER`), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.

Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.

 Sistemas operativos AIX Por ejemplo:

- PAYROLL
- SALES

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos AIX/tsminst1\_archlog

## AIX: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

/opt/tivoli/tsm/server/bin es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es /opt/tivoli/tsm/db2.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## AIX: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Al urukuzar ek software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones


 Sistemas operativos AIX Deje aproximadamente entre 30 y 45 minutos para instalar un servidor V 8.1.2, utilizando esta guía.

- AIX: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- AIX: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- AIX: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## AIX: Obtener el paquete de instalación

---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

 Sistemas operativos AIX

## Antes de empezar

---

Si tiene la intención de descargar los archivos, establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente:

1. Para consultar el valor de tamaño máximo de archivo, emita el mandato siguiente:


```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado siguiendo las instrucciones de la documentación de su sistema operativo.

## Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - o Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - o Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos AIX


- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
- c. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```



- d. Extraiga el paquete emitiendo el siguiente mandato:

```
./package_name.bin
```

donde *nombre\_paquete* es el nombre del archivo descargado, por ejemplo:

 Sistemas operativos AIX

```
8.1.x.000-IBM-SPSRV-AIX.bin
```

3.  Sistemas operativos AIX asegúrese de que el siguiente mandato esté habilitado para que los asistentes de IBM Spectrum Protect funcionen correctamente:
  - o  Sistemas operativos AIX `lsuser`  
De manera predeterminada, el mandato está habilitado.
4. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - o AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - o AIX: Instalación de IBM Spectrum Protect en modalidad de consola
  - o AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa
5. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación


---

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.

## Antes de empezar


---

Realice las acciones siguientes antes de iniciar la instalación:

-  Sistemas operativos AIX Si los siguientes archivos RPM no están instalados en el sistema, debe instalarlos. Para obtener instrucciones, consulte Instalación de archivos RPM para el asistente gráfico.
  - atk-1.12.3-2.aix5.2.ppc.rpm
  - cairo-1.8.8-1.aix5.2.ppc.rpm
  - expat-2.0.1-1.aix5.2.ppc.rpm
  - fontconfig-2.4.2-1.aix5.2.ppc.rpm
  - freetype2-2.3.9-1.aix5.2.ppc.rpm
  - gettext-0.10.40-6.aix5.1.ppc.rpm
  - glib2-2.12.4-2.aix5.2.ppc.rpm
  - gtk2-2.10.6-4.aix5.2.ppc.rpm
  - libjpeg-6b-6.aix5.1.ppc.rpm
  - libpng-1.2.32-2.aix5.2.ppc.rpm
  - libtiff-3.8.2-1.aix5.2.ppc.rpm
  - pango-1.14.5-4.aix5.2.ppc.rpm
  - pixman-0.12.0-3.aix5.2.ppc.rpm
  - xcursor-1.1.7-3.aix5.2.ppc.rpm
  - xft-2.1.6-5.aix5.1.ppc.rpm
  - xrender-0.9.1-3.aix5.2.ppc.rpm
  - zlib-1.2.3-3.aix5.1.ppc.rpm
- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	a. Cambie al directorio donde ha descargado el paquete. b. Inicie el asistente de instalación emitiendo el mandato siguiente:  Sistemas operativos AIX  <code>./install.sh</code>

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.  
  
Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos AIX AIX: Instalación de los archivos RPM de requisito previo para el asistente gráfico  
Antes de poder utilizar el asistente gráfico de IBM Installation Manager para instalar IBM Spectrum Protect, debe asegurarse de que los archivos RPM necesarios estén instalados.

## AIX: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.

### Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:



- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p> <pre>Sistemas operativos AIX  ./install.sh -c</pre> <p>Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique G para generar las respuestas.</p>

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos AIX/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

### Antes de empezar

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


### Procedimiento

1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas. Si está utilizando el archivo install\_response\_sample.xml, añada la contraseña en la línea siguiente del archivo, donde *mypassword* representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```



Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación


Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo update\_response\_sample.xml.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor *archivo\_respuestas* representa la vía de acceso del archivo de respuestas y el nombre del archivo:
  -  Sistemas operativos AIX

```
./install.sh -s -input archivo_respuestas
-acceptLicense
```

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos AIX/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos AIX Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

 Sistemas operativos AIX

## AIX: Instalación de paquetes de idioma del servidor

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.


### Antes de empezar

Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.

- AIX: Idiomas locales del servidor  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- AIX: Configuración de un paquete de idiomas  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.
- AIX: Actualización de un paquete de idiomas  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## AIX: Idiomas locales del servidor

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 Sistemas operativos AIX Este paquete de idioma se instala automáticamente para la siguiente opción de idioma predeterminado para los mensajes y la ayuda del servidor de IBM Spectrum Protect:

-  Sistemas operativos AIX LANGUAGE en\_US

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera. Puede utilizar los idiomas que se muestran:



 Sistemas operativos AIX

Tabla 1. Idiomas del servidor para AIX

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
Chino, simplificado (UTF-8)	ZH_CN
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (UTF-8)	ZH_TW
Chino, tradicional (euc_tw)	zh_TW
Inglés	en_US
Inglés (UTF-8)	EN_US
Francés	fr_FR
Francés (UTF-8)	FR_FR
Alemán	de_DE
Alemán (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT

Idioma	Valor de la opción LANGUAGE
Japonés, EUC	ja_JP
Japonés, PC	Ja_JP
Japonés, UTF8	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Portugués, de Brasil	pt_BR
Portugués, de Brasil (UTF-8)	PT_BR
Ruso	ru_RU
Ruso (UTF-8)	RU_RU
Español	es_ES
Español (UTF-8)	ES_ES



 **Sistemas operativos AIX** Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.

## AIX: Configuración de un paquete de idiomas

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

### Acerca de esta tarea

 **Sistemas operativos AIX** Para definir el soporte para un determinado entorno nacional, realice una de las siguientes tareas:

- Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo:
  -  **Sistemas operativos AIX** Para utilizar el entorno `it_IT`, establezca la opción LANGUAGE en `it_IT`. Consulte AIX: Idiomas locales del servidor.
-  **Sistemas operativos AIX** Si está iniciando el servidor en segundo plano, establezca el entorno variable `LC_ALL` para que coincida con el valor que se establece en el archivo de opciones del servidor. Por ejemplo, para establecer la variable de entorno en italiano, especifique el siguiente valor:

```
exportar LC_ALL=it_IT
```

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## AIX: Actualización de un paquete de idiomas

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.




Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.

## AIX: Primeros pasos tras instalar IBM Spectrum Protect

Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

## Acerca de esta tarea

---

1. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado AIX: Creación del ID de usuario y de directorios para la instancia del servidor.
  2. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
    - Utilice el asistente de configuración, el método preferido. Consulte el apartado AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
    - Configure manualmente la nueva instancia. Consulte el apartado AIX: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
      - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte AIX: Creación de una instancia del servidor.
      - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  Sistemas operativos AIX AIX: Configuración de comunicaciones de servidor y de cliente.
      - c. Emita el mandato DSMSERV FORMAT para formatear la base de datos. Consulte el apartado AIX: Formateo de la base de datos y las anotaciones.
      - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
  3. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
  4. Inicie la instancia del servidor, si todavía no se ha iniciado.
    -  Sistemas operativos AIX Consulte el apartado AIX: Inicio de la instancia de servidor.
  5. Registre su licencia. Consulte el apartado AIX: Registro de licencias.
  6. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
  7. Supervise el servidor. Consulte el apartado AIX: Supervisión del servidor.
- AIX: Creación del ID de usuario y de directorios para la instancia del servidor  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
  - AIX: Configuración del servidor de IBM Spectrum Protect  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
  - AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
  -  Sistemas operativos AIX AIX: Inicio de la instancia de servidor  
Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario root.
  - AIX: Detención del servidor  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
  - AIX: Registro de licencias  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
  - AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
  - AIX: Ejecución de varias instancias de servidor en un solo sistema  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
  - AIX: Supervisión del servidor  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## AIX: Creación del ID de usuario y de directorios para la instancia del servidor

---

Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.

### Antes de empezar

---




Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado AIX: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento

1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.

### Sistemas operativos AIX

 Cree un ID de usuario y un grupo que actuarán como propietarios de la instancia del servidor.

- a. Los siguientes mandatos se pueden ejecutar desde un ID de usuario administrador que vaya a definir el usuario y el grupo. Cree el ID de usuario y el grupo en el directorio de inicio del usuario.

Restricción: El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos ( \_ ). El nombre del ID de usuario y del grupo deben cumplir las siguientes reglas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Cree, por ejemplo, el ID de usuario `tsminst1` en el grupo `tsmsrvrs`. Los siguientes ejemplos muestran cómo crear este ID de usuario y grupo utilizando mandatos del sistema operativo.


### Sistemas operativos AIX

```
mkgroup id=1001 tsmsrvrs
mkuser id=1002 pgrp=tsmsrvrs home=/home/tsminst1 tsminst1
passwd tsminst1
```

Restricción: DB2 no admite la autenticación directa de usuarios del sistema operativo a través de LDAP.

- b. Cierre sesión y, a continuación, inicie sesión en su sistema. Cambie a la cuenta de usuario que acaba de crear. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

2. Cree los directorios necesarios para el servidor.

 Cree directorios vacíos para cada elemento de la tabla y asegúrese de que los directorios son propiedad del nuevo ID de usuario que acaba de crear. Monte el almacenamiento asociado en cada directorio para el registro activo, el registro de archivado y los directorios de bases de datos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El <i>directorio de instancias</i> del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir /tsminst1</code>	
Los directorios de bases de datos	<code>mkdir /tsmdb001</code> <code>mkdir /tsmdb002</code> <code>mkdir /tsmdb003</code> <code>mkdir /tsmdb004</code>	
Directorio de registro de activo	<code>mkdir /tsmlog</code>	
Directorio de registro de archivado	<code>mkdir /tsmarchlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir /tsmlogmirror</code>	
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir /tsmarchlogfailover</code>	

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSEV FORMATT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.

## AIX: Configuración del servidor de IBM Spectrum Protect

---

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

### Acerca de esta tarea

---

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:

- **AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **AIX: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

## AIX: Configuración de IBM Spectrum Protect utilizando el asistente de configuración

---

El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.



### Antes de empezar

---

Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.

### Procedimiento

---


1. Asegúrese de que se cumplen los siguientes requisitos:  Sistemas operativos AIX
  - El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Window. Además, debe estar ejecutando un servidor de sistema X Window en su escritorio.
  - El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. Asegúrese también de que el servicio del daemon de SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
  - Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
  - Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
  -  Sistemas operativos AIX Abra el programa `dsmicfgx` en el directorio `/opt/tivoli/tsm/server/bin`. Este asistente sólo puede ejecutarse como usuario `root`.

Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## AIX: Configuración de la instancia del servidor manualmente

---

Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

- **AIX: Creación de una instancia del servidor**  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.
-  **Sistemas operativos AIX: Configuración de comunicaciones de servidor y de cliente**  
Se crea un archivo de opciones de servidor de ejemplo predeterminado, `dsmerv.opt.smp`, durante la instalación de IBM Spectrum Protect en el directorio `/opt/tivoli/tsm/server/bin`. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.

- AIX: Formateo de la base de datos y las anotaciones  
Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## AIX: Creación de una instancia del servidor


Cree una instancia de IBM Spectrum Protect emitiendo el mandato db2icrt.


### Acerca de esta tarea

Puede tener una o más instancias del servidor en una estación de trabajo.


 **Sistemas operativos AIX** Importante: Antes de ejecutar el mandato db2icrt, verifique los siguientes elementos:

- El directorio padre para el usuario (/home/tsminst1) existe. Si no existe ningún directorio de inicio, debe crearlo. El directorio de instancia almacena los siguientes archivos principales generados por el servidor de IBM Spectrum Protect:
  - El archivo de opciones de servidor dmserv.opt
  - El archivo de la base de datos de la clave del servidor, cert.kdb, y los archivos .arm (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
  - El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
  - El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
  - Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
  - El usuario existe
  - Salida de rastreo (si no está cualificada al completo)
- Existe un archivo de configuración de shell (por ejemplo, .profile) en el directorio de inicio. El usuario root y el ID de usuario de instancia deben tener permiso de escritura para este archivo. Si desea más información, consulte Información sobre el producto DB2. Busque los ajustes de variable de entorno de Linux y UNIX.

 **Sistemas operativos AIX**

1. Inicie sesión utilizando el ID de usuario y cree una instancia de IBM Spectrum Protect. El nombre de la instancia debe coincidir con el del usuario que sea su propietario. Utilice el mandato db2icrt y entre el mandato en una línea.  **Sistemas operativos AIX**

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
nombre_instancia nombre_instancia
```

Por ejemplo, si el ID de usuario de esta instancia es tsminst1, utilice el siguiente mandato para crear la instancia. Escriba el mandato en una línea.  **Sistemas operativos AIX**

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u
tsminst1 tsminst1
```

Recuerde: A partir de este momento, utilice este ID de nuevo usuario al configurar el servidor IBM Spectrum Protect. Cierre la sesión del ID de usuario root e inicie sesión con el nuevo ID de usuario de la instancia.


2. Cambie el directorio predeterminado de la base de datos para que sea la misma que el directorio de instancia del servidor. Si tiene varios servidores, inicie sesión en el ID de la instancia para cada servidor. Emita este mandato:

```
db2 update dbm cfg using dftdbpath directorio_instancia
```

Por ejemplo, si directorio\_instancia es el ID del usuario de la instancia:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Modifique la vía de acceso a biblioteca para utilizar la versión del IBM Global Security Kit (GSKit) que está instalada con el servidor. En los siguientes ejemplos, server\_bin\_directory es un subdirectorio del directorio de instalación del servidor. Por ejemplo, /opt/tivoli/tsm/server/bin.

-  **Sistemas operativos AIX** Emita el siguiente mandato en una sola línea:

```
export LIBPATH=server_bin_directory/dbbkapi:
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```


- Debe actualizar los archivos siguientes para establecer la vía de acceso a biblioteca cuando se inicia DB2 o el servidor:

Ejemplo de shell Korn o bash:

```
directorio_inicio_usuarios_instancia/sqllib/userprofile
```

Ejemplo de C shell:

```
directorio_inicio_usuarios_instancia/sqllib/usercshrc
```


- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/userprofile* (shell Korn o bash). Cada entrada debe estar en una línea. 

```
LIBPATH=server_bin_directory/dbbkapi:  
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```


```
export LIBPATH
```

Recuerde: Las siguientes entradas deben estar en la vía de acceso a biblioteca:

- /usr/local/ibm/gsk8\_64/lib64
- /opt/ibm/lib
- /opt/ibm/lib64
- /usr/lib64

- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/usercshrc* (C shell), en una línea: 


```
setenv LIBPATH server_bin_directory/dbbkapi:  
/usr/opt/ibm/gsk8_64/lib64:$LIBPATH
```

- Verifique los valores de la vía de acceso de la biblioteca y que el GSKit es la versión 8.0.14.43 o posterior. Emita los mandatos siguientes: 

```
echo $LIBPATH  
gsk8capicmd_64 -version  
gsk8ver_64
```

Si la versión de GSKit no es 8.0.14.43 o posterior, debe volver a instalar el servidor de IBM Spectrum Protect. La reinstalación garantiza que esté disponible la versión correcta de GSKit.

4. Cree un archivo de opciones de servidor. Consulte AIX: Configuración de comunicaciones de servidor y de cliente.

 Sistemas operativos AIX

## AIX: Configuración de comunicaciones de servidor y de cliente

---

Se crea un archivo de opciones de servidor de ejemplo predeterminado, *dsmerv.opt.smp*, durante la instalación de IBM Spectrum Protect en el directorio */opt/tivoli/tsm/server/bin*. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.

### Acerca de esta tarea

---

Asegúrese de que dispone de un directorio de instancias del servidor, como */tsminst1*, y copie el archivo de muestra a este directorio. Llame a este nuevo archivo *dsmerv.opt* y edite las opciones. Finalice esta configuración antes de inicializar la base de datos de servidor. Cada entrada de ejemplo o predeterminada del archivo de opciones de muestra es un comentario, una línea que empieza con un asterisco (\*). Las opciones no distinguen entre mayúsculas y minúsculas y se permiten uno o varios espacios en blanco entre las palabras clave y los valores.

Cuando modifique el archivo de opciones, siga estas indicaciones:




- Elimine el asterisco del principio de la línea para activar una opción.
- Puede empezar a especificar las opciones en cualquier columna.
- Escriba sólo una opción por línea. La opción debe ocupar sólo una línea.
- Si realiza varias entradas para una palabra clave, el servidor de IBM Spectrum Protect aplica la última.

Si modifica el archivo de opciones del servidor, deberá volver a arrancar el servidor para que los cambios surtan efecto.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- TCP/IP Versión 4 o Versión 6
- Memoria compartida
- capa de sockets seguros (SSL)

Consejo: Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.

-  Sistemas operativos AIXAIX: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos AIXAIX: Establecimiento de opciones de memoria compartida  
Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.
-  Sistemas operativos AIXAIX: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## AIX: Establecimiento de opciones de TCP/IP

---

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea

---

Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.


```
commmethod          tcpip
tcpport             1500
tcpwindowsize      0
tcpnodelay         yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPORT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.

#### Sistemas operativos AIXTCPWINDOWSIZE

 Sistemas operativos AIXEspecifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Puede especificar un entero de 0 a 2048. Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPORT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## AIX: Establecimiento de opciones de memoria compartida

---

Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.

### Acerca de esta tarea

---


El siguiente ejemplo muestra un valor de memoria compartida:


```
commmethod          sharedmem
shmport            1510
```

En este ejemplo, SHMPORT especifica la dirección de puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Utilice la opción SHMPORT para especificar un puerto TCP/IP diferente. La dirección de puerto predeterminada es 1510.

COMMETHOD se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:

```
commmethod tcpip
commmethod sharedmem
```

 Sistemas operativos AIX El número máximo de sesiones simultáneas de memoria compartida está basado en los recursos del sistema disponibles. Cada sesión de memoria compartida utiliza una región de memoria compartida de hasta 4 MB, y cuatro colas de mensaje IPCS, dependiendo del nivel de cliente IBM Spectrum Protect.

 Sistemas operativos AIX Si el servidor y el cliente no se ejecutan con el mismo ID de usuario, el servidor debe ser un usuario root. De este modo se impide que se produzcan errores de comunicación de memoria compartida.

## AIX: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.

## AIX: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.

Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  Sistemas operativos AIX

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Inicialización de una instancia del servidor

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es */tsminst1*, emita los mandatos siguientes:  Sistemas operativos AIX


```
cd /tsminst1
dsmserv format dbdir=/tsmdb001 activelogsiz=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

 Sistemas operativos AIX Consejo: Si DB2 no se inicia después de emitir el mandato DSMSERV FORMAT, puede que tenga que inhabilitar la opción de montaje NOSUID del sistema de archivos. Si esta opción está establecida en el sistema de archivos que contiene el directorio de propietario de instancia de DB2, o en cualquiera de los sistemas de archivos que contienen la base de datos de DB2 o registros activos, registros de archivos, registros de migración tras error o registros duplicados, la opción debe estar inhabilitada para iniciar el sistema.

Después de inhabilitar la opción NOSUID, vuelva a montar el sistema de archivos y después inicie DB2 emitiendo el siguiente mandato:


**Información relacionada:**

 [DSMSERV FORMAT](#) (Dar formato a la base de datos y a las anotaciones)

## AIX: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos


Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

### Acerca de esta tarea

 **Sistemas operativos AIX** Comenzando con IBM Spectrum Protect V7.1, ya no es necesario establecer la contraseña de API durante una configuración manual del servidor. Si establece la contraseña de API durante el proceso de configuración manual, los intentos para hacer una copia de seguridad de la base de datos pueden fallar.

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos BACKUP DB o RESTORE DB.

**Atención:** Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 **Sistemas operativos AIX** En los siguientes mandatos, sustituya los valores de ejemplo por los valores reales. Los ejemplos utilizan `tsminst1` para el ID de usuario de instancia del servidor, `/tsminst1` para el directorio de instancia del servidor, y `/home/tsminst1` como directorio de inicio de usuarios de instancia del servidor.

1. Establezca la configuración de la variable de entorno de IBM Spectrum Protect para la instancia de la base de datos:

- a. Inicie la sesión utilizando el ID de usuario `tsminst1`.
- b. Cuando el usuario `tsminst1` inicia sesión, asegúrese de que el entorno de DB2 esté debidamente inicializado. El entorno de DB2 se inicializa ejecutando el script `/home/tsminst1/sqllib/db2profile`, que normalmente se ejecuta de forma automática desde el perfil del ID de usuario. Asegúrese de que el archivo `.profile` existe en el directorio de inicio de los usuarios de instancia, por ejemplo `/home/tsminst1/.profile`. Si `.profile` no ejecuta el script `db2profile`, agregue las siguientes líneas:

```
Si [ -f /home/tsminst1/sqllib/db2profile ]; entonces
    . /home/tsminst1/sqllib/db2profile
fi
```

- c. En el archivo `directorio_instancia/sqllib/userprofile`, añada las líneas siguientes:

```
DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
DSMI_DIR=directorio_bin_servidor/dbbkapi
DSMI_LOG=directorio_instancia_servidor
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

donde:

- `directorio_instancia` es el directorio de inicio del usuario de instancia de servidor.
- `directorio_instancia_servidor` es el directorio de instancia de servidor.
- `directorio_bin_servidor` es el directorio bin de servidor. La ubicación predeterminada es `/opt/tivoli/tsm/server/bin`.

En el archivo `directorio_instancia/sqllib/usercshrc`, añada las líneas siguientes:

```
setenv DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
setenv DSMI_DIR=directorio_bin_servidor/dbbkapi
setenv DSMI_LOG=directorio_instancia_servidor
```

2. Cierre la sesión y vuelva a iniciar la sesión como `tsminst1` o emita este mandato:

```
. ~/.profile
```

Consejo: Asegúrese de que especifica un espacio en blanco después del primer carácter de punto (.)

3. Cree el archivo que se denomine `tsmdbmgr.opt` en el directorio `instancia_servidor`, que se encuentra en el directorio `/tsminst1` en este ejemplo, y añada la línea siguiente:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Recuerde: El valor para `SERVERNAME` debe ser coherente en los archivos `tsmdbmgr.opt` y `dsm.sys`.

4. Como usuario root, agregue las siguientes líneas al archivo de configuración IBM Spectrum Protect API `dsm.sys`. De forma predeterminada, el archivo de configuración `dsm.sys` está en la ubicación predeterminada siguiente:

- `directorio_bin_servidor/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod          tcpip
tcpserveraddr localhost
tcpport             1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

donde

- `servername` coincide con el valor de `servername` en el archivo `tsmdbmgr.opt`.
  - `commethod` especifica la API de cliente que se utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Este valor puede ser `tcpip` o `sharedmem`. Para obtener más información sobre la memoria compartida, consulte el paso 5.
  - `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
  - `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmserv.opt`.
  - `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.
  - `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Para asegurarse de que se puede hacer copia de seguridad de la base de datos, este valor debe ser `$$_TSMDBMGR_$$`.
5. Opcional: configura el servidor en el cual realizar la copia de seguridad mediante el uso de una memoria compartida. De esta manera, podría reducir la carga del procesador y mejorar la capacidad. Realice los siguientes pasos:
- a. Revise el archivo `dsmserv.opt`. Si las líneas siguientes no están en el archivo, añádalas:

```
commethod          sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

- b. En el archivo de configuración `dsm.sys`, localice las siguientes líneas:

```
commethod          tcpip
tcpserveraddr localhost
tcpport número_puerto
```

Reemplace las líneas especificadas con las siguientes líneas:

```
commethod          sharedmem
shmport número_puerto
```


donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

## AIX: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor

Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

### Acerca de esta tarea

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.

 Sistemas operativos AIX Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.




Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

## Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos AIX Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancia del servidor. Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `/opt/tivoli/tsm/server/bin`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.

- a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:






```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```

4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.

### Información relacionada:

-  [ALLOWREORGINDEX](#)
-  [ALLOWREORGTABLE](#)
-  [REORGBEGINTIME](#)
-  [REORGDURATION](#)
-  [Sistemas operativos AIX](#)

## AIX: Inicio de la instancia de servidor


---

Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario `root`.

### Antes de empezar

---


Asegúrese de establecer los permisos de acceso y los límites de usuario correctamente.

 Sistemas operativos AIX Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).

### Acerca de esta tarea

---

Al iniciar el servidor utilizando el ID de usuario de la instancia, se simplifica el proceso de configuración y se evitan posibles problemas. Sin embargo, en algunos casos, es posible que sea necesario iniciar el servidor con el ID de usuario `root`. Por ejemplo, es posible que desee utilizar el ID de usuario `root` para garantizar que el servidor pueda acceder a determinados dispositivos. Puede configurar el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia o el ID de usuario `root`.


 Sistemas operativos AIX Si necesita completar un mantenimiento o tareas de reconfiguración, inicie el servidor en la modalidad de mantenimiento.

## Procedimiento

---


Para iniciar el servidor, realice una de las siguientes acciones:


- Inicie el servidor haciendo uso del ID de usuario de la instancia.


 Sistemas operativos AIX Para obtener las instrucciones, consulte Inicio del servidor desde el ID del usuario de la instancia .

- Inicie el servidor utilizando el ID de usuario root.


Para obtener instrucciones sobre cómo autorizar a los ID de usuarios root a iniciar el servidor, consulte Autorización de los ID de usuario root para iniciar el servidor (V7.1.1). Para obtener instrucciones sobre cómo iniciar el servidor utilizando el ID de usuario root, consulte el apartado Inicio del servidor desde el ID de usuario root (V7.1.1).

-  Sistemas operativos AIX Inicie el servidor automáticamente.

 Sistemas operativos AIX Para obtener instrucciones, consulte AIX: Inicio automático de los servidores.

-  Sistemas operativos AIX Inicie el servidor en modalidad de mantenimiento.

Para obtener instrucciones, consulte AIX: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos AIX

## AIX: Comprobación de los derechos de acceso y límites de usuario

Antes de iniciar el servidor, compruebe los derechos de acceso y límites de usuario.

### Acerca de esta tarea

Si no verifica los límites de usuario, conocidos también como *límitesu*, podría experimentar inestabilidad del servidor o una falla del servidor al responder. También debe verificar el límite en todo el sistema para ver el número máximo de archivos abiertos. El límite de todo el sistema debe ser mayor que o equivalente al límite de usuario.

### Procedimiento

1. Compruebe que el ID del usuario de la instancia del servidor tenga autorizaciones para iniciar el servidor.
2. Para la instancia del servidor que piensa iniciar, asegúrese que tiene la autoridad para leer y escribir archivos en el directorio de la instancia del servidor. Compruebe que el archivo `dsmserv.opt` existe en el directorio de la instancia del servidor y de que el archivo incluye parámetros para la instancia del servidor.
3. Si el servidor está conectado a una unidad de cinta, cambiador de recursos o dispositivo de soporte extraíble y piensa iniciar el servidor mediante el uso del ID del usuario de la instancia, otorgue acceso de lectura/escritura al ID de usuario de instancias para esos dispositivos. Para establecer los permisos, realice una de las siguientes acciones:
  - Si el sistema está dedicado a IBM Spectrum Protect y solo el administrador de IBM Spectrum Protect tiene acceso, haga que el archivo especial del dispositivo sea grabable para todos los usuarios. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod +w /dev/rmtX
```

- Si el sistema cuenta con varios usuarios, puede restringir el acceso si hace que el ID de usuario de la instancia de IBM Spectrum Protect sea el propietario de los archivos especiales de dispositivo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod u+w /dev/rmtX
```

- Si se están ejecutando varias instancias de usuario en el mismo sistema, cambie el nombre de grupo, por ejemplo TAPEUSERS, y añada cada ID de usuario de instancia IBM Spectrum Protect a dicho grupo. A continuación cambie la propiedad de los archivos especiales de dispositivo para que pertenezcan al grupo TAPEUSERS y haga que sean grabables para el grupo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod g+w /dev/rmtX
```

4. Compruebe los siguientes límites de usuario con base en los lineamientos de la tabla.

Tabla 1. Valores del límite (no límite) de usuario

Tipo de límite de usuario	Valor recomendado	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	Ilimitada	<code>ilimitado -Hc</code>
Tamaño máximo de un segmento de datos para un proceso	Ilimitada	<code>ulimit -Hd</code>
Tamaño de archivo máximo	Ilimitada	<code>ulimit -Hf</code>
Número máximo de archivos abiertos	65536	<code>ulimit -Hn</code>

Tipo de límite de usuario	Valor recomendado	Mandato del valor de consulta
La cantidad máxima de tiempo del procesador en segundos	Ilimitada	ilimitado -Ht

Para modificar los límites de usuario, siga las instrucciones en la documentación del sistema operativo.

Consejo: Si planea iniciar el servidor automáticamente haciendo uso de un script, puede establecer los límites de usuario en el script.

- Asegúrese de que el límite de usuario de procesos de usuario máximos (el valor de `nproc`) se establece en el valor mínimo sugerido de 16384.

- Para verificar el límite de usuario actual, emita el mandato `ulimit -Hu` utilizando el ID de usuario de instancia. Por ejemplo:


```
[user@Machine ~]$ ulimit -Hu
16384
```

- Si el límite de procesos máximos del usuario no se establece en 16384, establezca el valor en 16384.

 Sistemas operativos AIX Añada la siguiente línea al archivo `/etc/security/limits`:

```
id_usuario_instancia      -      nproc          16384
```

donde `id_usuario_instancia` especifica el ID de usuario de instancia de servidor.

 Sistemas operativos AIX

## AIX: Inicio del servidor con el ID de usuario de la instancia

Para iniciar el servidor desde el ID de usuario de la instancia, inicie sesión con el ID de usuario de la instancia y emita el mandato correspondiente desde el directorio de la instancia del servidor.

### Antes de empezar

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para obtener instrucciones, consulte AIX: Comprobación de los derechos de acceso y límites de usuario.


### Procedimiento

- Inicie sesión en el sistema donde instalado IBM Spectrum Protect utilizando el ID de usuario de instancia para el servidor.
- Si no tiene un perfil de usuario que ejecuta el script de `db2profile`, emita el siguiente mandato:


```
. /home/tsminst1/sqlllib/db2profile
```

Consejo: Para obtener instrucciones sobre cómo actualizar el script de inicio de sesión de ID de usuario para ejecutar el script `db2profile` automáticamente, consulte la documentación de DB2.


- Inicie el servidor emitiendo el siguiente mandato en una línea desde el directorio de instancia del servidor:

 Sistemas operativos AIX


```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPsize=64K
usr/bin/dsmserv
```

 Sistemas operativos AIX Asegúrese de incluir un espacio después de `SHMPsize=64K`. Al iniciar el servidor con este mandato, habilitará páginas de memoria de 64 KB en el servidor. Este valor le ayuda a optimizar el rendimiento del servidor.

Consejo: El mandato se ejecuta en primer plano para que pueda configurar un ID de administrador y conectarlo con la instancia del servidor.

 Sistemas operativos AIX Por ejemplo, si el nombre de la instancia del servidor es `tsminst1` y el directorio de la instancia de servidor es `/tsminst1`, puede iniciar la instancia emitiendo los mandatos siguientes:

```
cd /tsminst1
. ~/sqlllib/db2profile
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPsize=64K
usr/bin/dsmserv
```

 Sistemas operativos AIX


## AIX: Inicio automático de los servidores

Puede configurar el servidor se inicie automáticamente durante el arranque del sistema. Utilice el script `rc.dsmserv`, que se proporciona para este fin.

## Antes de empezar

---


Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente.

 Sistemas operativos AIX Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).

## Acerca de esta tarea

---

El script `rc.dsmserv` se encuentra en el directorio de instalación del servidor, por ejemplo, en el directorio `/opt/tivoli/tsm/server/bin`.

 Sistemas operativos AIX Consejo: Si ha utilizado el asistente de actualización o el asistente de configuración, debería haber elegido iniciar el servidor automáticamente al reiniciar el sistema. Si seleccionó esa opción, se agregó automáticamente una entrada para iniciar el servidor al archivo `/etc/inittab`.

## Procedimiento

---


Si no ha utilizado un asistente para configurar el servidor, añada una entrada al archivo `/etc/inittab` para cada servidor que desee que se inicie automáticamente:

1. Establezca el nivel de ejecución en el valor que corresponde a la modalidad de varios usuarios con la red habilitada. Generalmente, el nivel de ejecución que utilizar es 2, 3, o 5, en función del sistema operativo y de su configuración. Asegúrese de que el nivel de ejecución del archivo `/etc/inittab` coincida con el nivel de ejecución del sistema operativo. Para obtener más información acerca de la modalidad multiusuario y los niveles de ejecución, consulte la documentación del sistema operativo.
2. En el mandato `rc.dsmserv` en el archivo `/etc/inittab`, especifique el ID de usuario de instancia con la opción `-u` y la ubicación del directorio de instancia de servidor con la opción `-i`. Si desea iniciar más de una instancia del servidor automáticamente, agregue una entrada para cada instancia del servidor. Para verificar la sintaxis, consulte la documentación de su sistema operativo. Consejo: Para iniciar automáticamente una instancia de servidor con el ID de usuario raíz, use la opción `-U`.

## Ejemplo

---


Por ejemplo, si el propietario de la instancia es `tsminst1` y el directorio de la instancia del servidor es `/home/tsminst1/tsminst1`, añada la siguiente entrada a `/etc/inittab`, en una línea:

 Sistemas operativos AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
```


En este ejemplo, el ID de proceso es `tsm1`, y el nivel de ejecución es 2.


Si desea ejecutar más de una instancia del servidor, añada una entrada para cada una de las instancias. Por ejemplo, si tiene los ID de propietario `tsminst1` y `tsminst2`, y los directorios de instancia `/home/tsminst1/tsminst1` y `/home/tsminst2/tsminst2`, añada las siguientes entradas a `/etc/inittab`. Cada entrada debe estar en una línea.

 Sistemas operativos AIX

```
tsm1:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst1
-i /home/tsminst1/tsminst1 -q >/dev/console 2>&1
tsm2:2:once:/opt/tivoli/tsm/server/bin/rc.dsmserv -u tsminst2
-i /home/tsminst2/tsminst2 -q >/dev/console 2>&1
```

### Referencia relacionada:

 Script de inicio del servidor: `rc.dsmserv`

 Sistemas operativos AIX

## AIX: Inicio del servidor en modalidad de mantenimiento

---

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

## Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad `DSMSERV` con el parámetro `MAINTENANCE`.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

## Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

## Qué hacer a continuación

---

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## AIX: Detención del servidor

---


Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

## Acerca de esta tarea

---

Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:


```
halt
```

 Sistemas operativos AIX Si no se puede conectar al servidor con un cliente administrativo y desea detener el servidor, debe cancelar el proceso utilizando el mandato kill con el número del ID de proceso (pid). El pid se muestra en la inicialización.

**Importante:** Antes de emitir el mandato kill, asegúrese de que conoce el ID de proceso correcto del servidor IBM Spectrum Protect.

El archivo `dsmserv.v6lock`, en el directorio desde el cual se está ejecutando el servidor, se puede usar para identificar el ID de proceso del proceso que desea detener. Para mostrar el archivo, especifique:

```
cat /instance_dir/dsmserv.v6lock
```

 Sistemas operativos AIX Emita el siguiente mandato para detener el servidor:

```
kill -36 dsmserv_pid
```

donde `dsmserv_pid` es el número de ID del proceso.

## AIX: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

## Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

## Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## AIX: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

## Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

## Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

## Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

## Ejemplo

---

Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:


```
set dbrecovery dbback
```

## AIX: Ejecución de varias instancias de servidor en un solo sistema

---

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.

Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.

 Sistemas operativos AIXEl conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos de AIX: Creación de una instancia del servidor para cada instancia nueva, incluida la creación del nuevo usuario de la instancia.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.

Puede actualizar directamente desde V6.3 a V7.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.2 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

**Tareas relacionadas:**

📄 Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## AIX: Supervisión del servidor

---

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

### Procedimiento

---

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de espacio de las anotaciones activas, pero durante poco tiempo.
  - Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.
- Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tarden más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible. Recuerde: Si el registro de archivado y el registro de archivado de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.

Probablemente observará el siguiente patrón:

- a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
- b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.
- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## AIX: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.2 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.2, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado AIX: Revertir de la versión 8.1.2 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

### Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup devconfig filenames=nombre_archivo
```



donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:



```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7.  Sistemas operativos AIX Conéctese como usuario root.
8. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
9.  Sistemas operativos AIX Cambie al directorio donde situó el archivo ejecutable y complete los pasos siguientes.  
Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.

- a. Cambie los permisos de archivo emitiendo el siguiente mandato:

```
chmod a+x 8.x.x.x-IBM-SPSRV-plataforma.bin
```

donde *plataforma* indica la arquitectura en la que se va a instalar IBM Spectrum Protect.

- b. Emita el siguiente mandato para extraer los archivos de instalación:

```
./8.x.x.x-IBM-SPSRV-plataforma.bin
```

10. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.

Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.

Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

#### Asistente de instalación

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

#### Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect en modalidad de consola

#### Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

AIX: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.



## Resultados

---

Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos AIX/var/ibm/InstallationManager/logs
-  Sistemas operativos AIX AIX: Aplicación de un fixpack a IBM Spectrum Protect V8.1.2 en un entorno de clúster para AIX  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual. Es posible aplicar un fixpack en un entorno en clúster para AIX.

## AIX: Revierta de la versión 8.1.2 a un servidor anterior

---

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

## Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:

- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

## Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.2 al 8.1.1 o del 8.1.2 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.


## Pasos para recuperar la versión anterior del servidor


---

### Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

### Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato:  Sistemas operativos AIX

```
dsmserv removedb tsmdl
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado AIX: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.2. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato:  Sistemas operativos AIX

```
./dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.
7. Restablezca la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - Archivo de configuración de dispositivos
  - Archivo histórico de volúmenes
  - El archivo de opciones de servidor (generalmente dsmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.2, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de

seguridad de la base de datos. Utilice el mandato RESTORE VOLUME.

Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:

```
audit volume nombre_volumen fix=yes
```

11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

---

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.2, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.2.

### Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.2:

- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.2. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

### Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:
  - Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.2.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro REUSEDelay para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.2. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.2, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.2.

## AIX: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect


---

Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.

Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.

Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.

Tabla 1. Mandatos de DB2

Man dato	Descripción	Ejemplo
db2i crt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia.</p> <p>Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p> <p> Sistemas operativos AIX Este programa de utilidad está en el directorio DB2DIR/instance, donde DB2DIR representa la ubicación donde se instala la versión actual del sistema de base de datos de DB2.</p>	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre>/opt/tivoli/ts m/db2/instance / db2icrt -a server -u nombre_instanc ia nombre_instanc ia</pre>
db2s et	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> <pre>db2set</pre>
CAT ALO G DAT ABA SE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	<p>Catalogue la base de datos:</p> <pre>db2 catalog database tsmdb1</pre>
CON NEC T TO DAT ABA SE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	<p>Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:</p> <pre>db2 connect to tsmdb1</pre>

Mandato	Descripción	Ejemplo
GET DAT ABA SE CON FIG URA TIO N	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Muestre la información de configuración para un alias de base de datos:  db2 get db cfg for tsmdb1  Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.  db2 get db config for tsmdb1 show detail
GET DAT ABA SE MAN AGE R CON FIG URA TIO N	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEA LTH SNA PSH OT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsmdb1
GRA NT (Aut oriza cion es de base de dato s)	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser

Man dato	Descripción	Ejemplo
RUN STAT S	<p>Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.</p> <p>Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.</p> <p>Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.</p> <p>Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.</p>	<p>Actualice las estadísticas en una única tabla.</p> <pre>db2 runstats on table SCHEMA_NAME.TA BLE_NAME with distribution and sampled detailed indexes all</pre>
SET SCH EMA	<p>Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2.</p> <p>Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.</p>	<p>Establezca el esquema para IBM Spectrum Protect:</p> <pre>db2 set schema tsmdb1</pre>
STA RT DAT ABA SE MAN AGE R	<p>Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Inicie el gestor de base de datos:</p> <pre>db2start</pre>
STO P DAT ABA SE MAN AGE R	<p>Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.</p> <p>Este mandato no es válido en un cliente.</p> <p>El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.</p> <p>Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.</p>	<p>Detenga el gestor de base de datos:</p> <pre>db2 stop dbm</pre>

## AIX: Desinstalar IBM Spectrum Protect

Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.
- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

### Acerca de esta tarea

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

- AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- AIX: Desinstalación e instalación de IBM Spectrum Protect  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- AIX: Desinstalación de IBM Installation Manager  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.


## Qué hacer a continuación

Consulte AIX: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## AIX: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento




1. Inicie el Installation Manager.  
 Sistemas operativos AIX En el directorio en donde se encuentra instalado Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:  

```
./IBMIM
```
2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.

## AIX: Desinstalación de IBM Spectrum Protect en modalidad de consola

Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.

### Procedimiento

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos AIX/eclipse/tools
 Por ejemplo:
  -  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio herramientas, emita el siguiente mandato:
  -  Sistemas operativos AIX./imcl -c
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique N para Siguiente.
6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
7. Especifique N para Siguiente.
8. Escriba U para Desinstalar.
9. Escriba F para Finalizar.

## AIX: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.

## Antes de empezar

---


Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.


Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


## Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos AIX/eclipse/tools


Por ejemplo:

-  Sistemas operativos AIX/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio herramientas, emita el siguiente mandato, donde `archivo_respuestas` representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

 Sistemas operativos AIX

```
./imcl -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos AIX

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## AIX: Desinstalación e instalación de IBM Spectrum Protect


---

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.

## Acerca de esta tarea


---

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos AIX Realice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:


 Sistemas operativos AIX

```
db2 attach to instance_name
db2 get dbm cfg show detail
db2 detach
```

Mantenga un registro de la ruta de base de datos para cada instancia.

3. Desinstale IBM Spectrum Protect. Consulte el apartado AIX: Desinstalar IBM Spectrum Protect.
4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten las credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estos credenciales utilizando la variable `INSTANCE_CRED`.

Puede encontrar el archivo de instancias en la siguiente ubicación:


-  Sistemas operativos AIX/etc/tivoli/tsm/instanceList.obj

5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado AIX: Instalación de los componentes de servidor.




Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- a. Vuelva a crear las instancias de servidor. Consulte el apartado AIX: Creación de una instancia del servidor.  
Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- b. Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos AIX

```
db2 catalog database tsmdb1
db2 attach to instance_name
db2 update dbm cfg using dftdbpath instance_directory
db2 detach
```

- c.  Sistemas operativos AIX Compruebe que la instancia de servidor se haya creado correctamente. Emita este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```

Si figura TS MDB1 puede iniciar el servidor.

## AIX: Desinstalación de IBM Installation Manager


---

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

### Antes de empezar

---

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.


 Sistemas operativos AIX Para ver los paquetes instalados, emita el mandato siguiente desde una línea de mandatos:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

### Procedimiento

---

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos AIX

1. Abra una línea de mandatos y cambie el directorio a `/var/ibm/InstallationManager/uninstall`.
2. Emita el mandato siguiente:

```
./uninstall
```

Restricción: Debe haber iniciado sesión en el sistema utilizando el ID de usuario `root`.

## Linux: Instalación del servidor

---

La instalación del servidor incluye la planificación, instalación y configuración inicial.



- Linux
- Linux: Planificación para instalar el servidor  
Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- Linux: Instalación de los componentes de servidor  
Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Linux: Primeros pasos tras instalar IBM Spectrum Protect  
Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

- **Linux: Instalación de un fixpack de servidor de IBM Spectrum Protect**  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.
- **Linux: Revierta de la versión 8.1.2 a un servidor anterior**  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- **Linux: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect**  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- **Linux: Desinstalar IBM Spectrum Protect**  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## Linux: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.


- **Linux: Qué debe saber primero**  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- **Linux: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor**  
Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.
- **Linux: Planificación de rendimiento óptimo**  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  **Sistemas operativos LinuxLinux: Requisitos mínimos del sistema para sistemas Linux**  
Para instalar el servidor IBM Spectrum Protect en un sistema Linux, es necesario que tenga un nivel mínimo de hardware y software, incluyendo un método de comunicación y el controlador de dispositivo más actual.
-  **Sistemas operativos LinuxLinux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema**  
Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.2, con algunas limitaciones.
- **Linux: IBM Installation Manager**  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- **Linux: Hojas de trabajo para planificar detalles para el servidor**  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- **Linux: Planificación de la capacidad**  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.
- **Linux: Prácticas más adecuadas de denominación del servidor**  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- **Linux: Directorios de instalación**  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

## Linux: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 **Sistemas operativos LinuxRestricción:** Puede instalar y ejecutar el servidor de la versión 8.1.2 en un sistema que ya tenga DB2 instalado, tanto si DB2 se ha instalado de forma independiente como si se ha instalado como parte de otra aplicación, con algunas restricciones. Para conocer más detalles, consulte el tema sobre compatibilidad con otros productos DB2.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores

preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.2 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Linux: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor

---

Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.

### Acerca de esta tarea

---

Las mejoras de seguridad en V8.12 y posterior han aplicado parámetros de seguridad más estrictos. Para garantizar que no se interrumpa la comunicación entre servidores y clientes al instalar o actualizar el software IBM Spectrum Protect a V8.1.2, siga el procedimiento.

### Procedimiento

---

1. Instale o actualice los servidores IBM Spectrum Protect a 8.1.2 o posterior.
2. Instale o actualice los clientes de copia de seguridad y archivado. Si desea más información, consulte *Instalación y configuración de clientes*.  
Para obtener información sobre la planificación del despliegue de actualizaciones de clientes desde el servidor, consulte los siguientes documentos:
  - Para servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.
  - Para servidores IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la nota técnica 1673299.
3. Configure las opciones para clientes de copia de seguridad y archivado. Para obtener más información, consulte *Actualización del servidor de IBM Spectrum Protect e IBM Spectrum Protect Client*.

## Linux: Planificación de rendimiento óptimo

---

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.

### Procedimiento

---

1. Revise *Linux: Qué debe saber primero*.
2. Revise cada una de las siguientes subsecciones.
  - **Linux: Planificación del hardware del servidor y el sistema operativo**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Linux: Planificación de discos de base de datos del servidor**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Linux: Planificación de discos de registro de recuperación del servidor**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Linux: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios**  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.
  - **Linux: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE**  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
  - **Linux: Planificación del tipo correcto de tecnología de almacenamiento**  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
  - **Linux: Aplicación de prácticas recomendadas para la instalación del servidor**  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM

Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.


## Linux: Planificación del hardware del servidor y el sistema operativo





Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

<b>Pregunta</b>	<b>Tareas, características, opciones o valores</b>	<b>Más información</b>
<p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul>	<p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p>
<p>¿Están configurados los discos para un rendimiento óptimo?</p>	<p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿El servidor tiene suficiente memoria?	<p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p>	<p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul>
¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente?	<p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>	<p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>

<b>Pregunta</b>	<b>Tareas, características, opciones o valores</b>	<b>Más información</b>
<p>¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?</p>	<p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect?</p>	<p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. La siguiente lista identifica el sistema de archivos preferido:</p> <p> Sistemas operativos</p> <ul style="list-style-type: none"> <li>• Linux <ul style="list-style-type: none"> <li>Utilice el sistema de archivos ext3, ext4 o xfs para los datos de la agrupación de almacenamiento, la base de datos y el registro de recuperación. Utilice el siguiente sistema de archivos adecuado para su sistema operativo y nivel: <ul style="list-style-type: none"> <li>◦ Para Red Hat Enterprise Linux x86_64, utilice el sistema de archivos ext3, ext4 o xfs. Si está instalado Red Hat Enterprise Linux 6.4 o posterior, utilice el sistema de archivos ext4 o xfs.</li> <li>◦ En SUSE Linux Enterprise Server y Red Hat Enterprise Linux ppc64, utilice el sistema de archivos ext3 o xfs. Si utilizar xfs en SUSE Linux Enterprise Server 12 requiere kernel predeterminado 3.12.32-33.1.x86_64.rpm o posterior.</li> </ul> </li> </ul> </li> </ul>	<p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Tiene pensado configurar suficiente espacio de paginación?	<p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos Linux Utilice un mínimo de 32 GB de espacio de paginación o el 50% de su RAM, el valor que sea mayor.</p>	
<p> Sistemas operativos Linux</p> <p>¿Tiene pensado ajustar los parámetros de kernel tras la instalación del servidor?</p>	<p> Sistemas operativos Linux</p> <p>Tiene que ajustar los parámetros de kernel.</p>	<p> Sistemas operativos Linux</p> <p>Consulte la información sobre cómo ajustar los parámetros de kernel: Linux: Ajuste de los parámetros de kernel para sistemas Linux</p>

## Linux: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
¿Se encuentra la base de datos en discos rápidos de baja latencia?	<p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p>	<p>Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.</p>



<b>Pregunta</b>	<b>Tareas, características, opciones o valores</b>	<b>Más información</b>
<p>¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento?</p>	<p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>	
<p>Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?</p>	<p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>	
<p>Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?</p>	<p>Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.</p>	<p>El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB.</p>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p>	<p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <code>DB2_PARALLEL_IO</code> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <code>DB2_PARALLEL_IO</code>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <code>DB2_PARALLEL_IO</code>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>	<p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>	
<p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>	<p>La profundidad de cola predeterminada suele ser demasiado baja.</p>	<p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>

## Linux: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos?	Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.	La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.
¿Se encuentran los registros en discos con memoria caché de escritura no volátil?	La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.	
¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?	Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.  Registro activo El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.  Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.  Registro de archivos El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo.	<ul style="list-style-type: none"> <li>• Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>• Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>
¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?	El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.	Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.  Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande.
Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?	Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro. <ul style="list-style-type: none"> <li>• Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>• Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>• Utilice la duplicación en el hardware del sistema de disco.</li> </ul>	Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.  Para obtener más información, consulte Configuración y ajuste del registro de recuperación.

## Linux: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p>	<p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$	<p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>	<p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul>	<p>Requisitos de memoria</p>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>	<p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p>	<p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>	<p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>	<p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p>	<p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>	<p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p>
<p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>	<p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>	<ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha asignado suficiente espacio de almacenamiento para la base de datos?	<p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>	
¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?	<p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol>	Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?</p>	<p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p>	<p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad?</p>	<p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>	<ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>
<p>¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?</p>	<p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>	<p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?	<p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>	Para obtener más información, consulte la opción de cliente enablededup.
¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?	<p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>	
¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?	<p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul>	



Pregunta	Tareas, características, opciones o valores	Más información
¿Ha seleccionado el tipo apropiado de almacenamiento local?	<p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul>	

## Linux: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo?	<p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p>	Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.
¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?	Utilice más memoria caché para un mejor rendimiento.	
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?	Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.	Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario.
Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?	<p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>	<p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>
Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?	Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.	Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.

Pregunta	Tareas, características, opciones o valores	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?	<p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p>	Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.
En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?	<p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>	Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.
¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?	<p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>	<p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul>

## Linux: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento

Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

<b>Tipo de tecnología de almacenamiento</b>	<b>Base de datos</b>	<b>Registro activo</b>	<b>Registro de archivado y registro de migración tras error de archivado</b>	<b>Agrupaciones de almacenamiento</b>
<b>Unidad de estado sólido (SSD)</b>	<p>Coloque la base de datos en SSD en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>	<p>Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>
<p><b>Disco de alto rendimiento con las siguientes características:</b></p> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.</p>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.</p>	<p>Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.</p>	<p>Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.</p>

Tipo de tecnología de almacenamiento	Base de datos	Registro activo	Registro de archivado y registro de migración tras error de archivado	Agrupaciones de almacenamiento
<b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>• Disco de 10.000 rpm</li> <li>• Interfaz Fibre Channel o SAS</li> </ul>	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.	Utilice disco de rendimiento medio o rendimiento alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.
<b>SATA, almac. adjunto de red</b>	No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.	No utilice este almacenamiento para el registro activo.	El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.	Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>• Los datos se leen con poca frecuencia.</li> </ul>
<b>Cinta y cinta virtual</b>				Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.

## Linux: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

Práctica recomendada	Más información
----------------------	-----------------

<b>Práctica recomendada</b>	<b>Más información</b>
<p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p>	<p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>
<p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>
<p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>	<p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>
<p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>	<p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>
<p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>	<p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>

Práctica recomendada	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores.	<p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p>
Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.	<p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>○ Ajuste de la planificación para las operaciones diarias</li> <li>○ Lista de comprobación para la configuración de servidor</li> </ul>
Supervise las operaciones de forma constante.	<p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento. Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>




## Linux: Requisitos mínimos del sistema para sistemas Linux

Para instalar el servidor IBM Spectrum Protect en un sistema Linux, es necesario que tenga un nivel mínimo de hardware y software, incluyendo un método de comunicación y el controlador de dispositivo más actual.

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

El paquete de controladores de dispositivo de IBM Spectrum Protect no contiene un controlador de dispositivos para este sistema operativo porque se utiliza un controlador de dispositivo genérico SCSI. Configure el controlador de dispositivo antes de utilizar el servidor de IBM Spectrum Protect con dispositivos de cinta. El paquete de controladores de IBM Spectrum Protect contiene herramientas de controladores y daemons de ACSLS. Encontrará paquetes de controladores de IBM® en el sitio web de Fix Central.

Los requisitos, dispositivos soportados, paquetes de instalación de cliente y arreglos están disponibles en IBM Support Portal para IBM Spectrum Protect. Tras instalar IBM Spectrum Protect y antes de personalizarlo para su uso, vaya al sitio web y descargue y aplique cualquier arreglo aplicable.

-  Sistemas operativos LinuxLinux: Requisitos mínimos del servidor Linux X86\_64  
Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux X86\_64, revise los requisitos de hardware y software.
-  Sistemas operativos LinuxLinux: Requisitos mínimos del servidor Linux on System z  
Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux en System z, revise los requisitos de hardware y software.
-  Sistemas operativos LinuxLinux: Requisitos mínimos de servidor Linux on Power Systems (little endian)  
Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo Linux on Power Systems (little endian), revise los requisitos de hardware y software.

## Linux: Requisitos mínimos del servidor Linux X86\_64

Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux X86\_64, revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
servidor	Un procesador AMD64 o Intel EMT-64
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos de software mínimos necesarios para un servidor en un sistema Linux X86\_64.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	<p>El servidor IBM Spectrum Protect en Linux X86_64 requiere uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 6.7</li> <li>• Red Hat Enterprise Linux 7, incluyendo actualizaciones</li> <li>• SUSE Linux Enterprise Server 11, Service Pack 4 o posterior</li> <li>• SUSE Linux Enterprise Server 12</li> </ul>



Tipo de software	Requisitos mínimos de software
Bibliotecas	<p>Bibliotecas GNU C, versión 2.3.3-98.38 o posterior, que están instaladas en el sistema IBM Spectrum Protect.</p> <p>Para SUSE Linux Enterprise Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 en la versión 4.3 o posterior (se requieren paquetes de 32 bits y 64 bits)</li> </ul> <p>Para Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (paquetes de 32 y 64 bit necesarios)</li> <li>• numactl.x86_64</li> </ul> <p>Para determinar si SELinux está instalado y en modalidad de imposición, realice una de las siguientes acciones:</p> <ul style="list-style-type: none"> <li>• Examine el archivo <code>/etc/sysconfig/selinux</code>.</li> <li>• Ejecute el mandato del sistema operativo <code>sestatus</code>.</li> <li>• Examine el archivo <code>/var/log/messages</code> para ver avisos de SELinux.</li> </ul> <p>Para inhabilitar SELinux, realice una de las tareas siguientes:</p> <ul style="list-style-type: none"> <li>• Establezca la modalidad permisiva emitiendo el mandato <code>setenforce 0</code> como superusuario.</li> <li>• Modifique el archivo <code>/etc/sysconfig/selinux</code> y reinicie la máquina.</li> </ul>
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con cliente de IBM Spectrum Protect Linux X86_64)</li> </ul>
Proceso	<p>Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.</p>
Controladores de dispositivo	<p>El controlador del dispositivo de paso IBM Spectrum Protect se usa para dispositivos que no sean de IBM®. Utiliza la interfaz de paso SCSI para comunicarse con los dispositivos de cinta y las bibliotecas de cintas. El controlador de dispositivos Linux SCSI Generic (sg) es necesario para los controladores de cintas y las bibliotecas de cintas. El paquete de controladores de dispositivos de IBM Spectrum Protect incluye herramientas de controladores de dispositivos y daemons de ACSLS.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p>
Otro software	<p>Se necesita el shell Korn (ksh). Configure los puertos de terminación de entrada y salida (IOCP) en el sistema operativo.</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Linux: Requisitos mínimos del servidor Linux on System z

Antes de instalar el servidor IBM Spectrum Protect en un sistema operativo Linux en System z, revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware necesarios para IBM Spectrum Protect Linux en el sistema System z. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Servidor	Una partición lógica nativa de 64 bits de IBM® zSeries, IBM System z9, IBM System z10 o IBM zEnterprise System (z114 y z196) o invitado z/VM.
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 512 MB para el directorio /var</li> <li>• 2 GB para el directorio /tmp</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos mínimos de software que se requieren para IBM Spectrum Protect Linux en el sistema System z.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Servidor	<p>El servidor de IBM Spectrum Protect en Linux en System z (arquitectura de s390x 64 bits) requiere uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Red Hat Enterprise Linux 7.1</li> <li>• SUSE Linux Enterprise Server 12</li> </ul>

Tipo de software	Requisitos mínimos de software
Bibliotecas	<p>Una biblioteca GNU C, versión 2.4-31.43.6, está instalada en el sistema IBM Spectrum Protect. Para SUSE Linux Enterprise Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 en la versión 4.3 o posterior (se requieren paquetes de 32 bits y 64 bits)</li> <li>• libxlc-1.2.0.0.151119a.s390x o posterior</li> </ul> <p>Para Hat Enterprise Linux Servers:</p> <ul style="list-style-type: none"> <li>• libaio</li> <li>• libstdc++.so.6 (se necesitan paquetes de 32 bits y 64 bits)</li> <li>• numactl.x86_64</li> <li>• libxlc-1.2.0.0.151119a.s390x o posterior</li> </ul>
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con el cliente de IBM Spectrum Protect Versión 8.1.2 Linux on System z)</li> </ul>
Proceso	Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.
Otro software	<p>Se necesita el shell Korn (ksh). Configure los puertos de terminación de entrada y salida (IOCP) en el sistema operativo.</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Linux: Requisitos mínimos de servidor Linux on Power Systems (little endian)

Antes de instalar un servidor IBM Spectrum Protect en un sistema operativo Linux on Power Systems (little endian), revise los requisitos de hardware y software.

### Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Linux: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Servidor	Un servidor Linux on Power Systems (little endian) en un sistema IBM®, como uno listado en el sitio web de Linux on IBM Power Systems.

Tipo de hardware	Requisitos de hardware
Espacio de disco	<p>El espacio mínimo de disco siguiente:</p> <ul style="list-style-type: none"> <li>• 5 GB para el directorio de instalación</li> <li>• 128 MB en el directorio de inicio para el usuario root.</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Linux: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>


## Requisitos de software

En el apartado Tabla 2 se describen los requisitos mínimos de software necesarios para su sistema.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	El sistema operativo Red Hat Enterprise Linux (RHEL) 7.3 con la arquitectura PPC64LE.
Bibliotecas	Bibliotecas GNU C, Versión 2.4-31.30 y posterior. libaio.so.1 (paquetes de 32 bits y 64 bits).
Protocolo de comunicaciones	<ul style="list-style-type: none"> <li>• TCP/IP Versión 4 o Versión 6, que es estándar con Linux</li> <li>• Protocolo de memoria compartida (con un cliente versión 8.1.2)</li> </ul>
Proceso	Tiene que habilitarse la entrada/salida asíncrona. En los kernels de Linux en el 2.6 o posterior, instale la biblioteca libaio para habilitar la E/S asíncrona.
Otro software	<p>Se necesita el shell Korn (ksh). Configure los puertos de terminación de entrada y salida (IOCP) en el sistema operativo.</p> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

Restricción: Los volúmenes lógicos RAW no están soportados.

 Sistemas operativos Linux

## Linux: Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Puede instalar otros productos que despliegan y utilizan productos DB2 en el mismo sistema que el servidor IBM Spectrum Protect Versión 8.1.2, con algunas limitaciones.

Para instalar y utilizar otros productos que usen un producto DB2 en el mismo sistema que el servidor de IBM Spectrum Protect, asegúrese de que se cumplan los siguientes criterios:

Tabla 1. Compatibilidad del servidor de IBM Spectrum Protect con otros productos DB2 en el sistema

Criterio	Instrucciones
Nivel de versión	El resto de productos que utilizan un producto DB2 tienen que utilizar la versión 9 de DB2 o una versión posterior. Los productos de DB2 incluyen soporte de encapsulamiento y segregación de productos desde la versión 9. A partir de esta versión, puede ejecutar varias copias de productos de DB2, en diferentes niveles de código, en el mismo sistema. Si desea detalles, consulte la información sobre varias copias de DB2 en Información sobre el producto DB2.
ID de usuario y directorios	Asegúrese de que los ID de usuario, los ID de usuarios delimitados, la ubicación de la instalación, otros directorios y la información relacionada no se compartan en instalaciones de DB2. Las especificaciones deben ser distintas a partir de los ID y ubicaciones utilizados para la instalación y configuración del servidor de IBM Spectrum Protect. Si utilizó el asistente dsmlcfx para configurar el servidor, estos son los valores especificados al ejecutar el asistente. Si utilizó el método de configuración manual, revise los procedimientos utilizados, si fuese necesario, para recordar los valores utilizados en el servidor.
Asignación de recursos	<p>Tenga en cuenta los recursos y las prestaciones del sistema en comparación con los requisitos del servidor de IBM Spectrum Protect y las otras aplicaciones que utilizan el producto de DB2. Para proporcionar recursos suficientes para el resto de aplicaciones DB2, es posible que deba modificar los ajustes del servidor IBM Spectrum Protect para que el servidor utilice menos recursos y memoria del sistema. De manera similar, si las cargas de trabajo de las demás aplicaciones de DB2 compiten con el servidor de IBM Spectrum Protect en cuanto a los recursos de memoria y del procesador, el rendimiento del servidor relacionado con la carga de trabajo de cliente prevista y otras operaciones podría verse afectado negativamente.</p> <p>Para segregarse recursos y proporcionar más capacidades para el ajuste y la asignación del procesador, de la memoria y de otros recursos del sistema para varias aplicaciones, puede utilizar particiones lógicas (LPAR), particiones de carga de trabajo (WPAR) o el soporte de otra estación de trabajo virtual. Por ejemplo, ejecute una aplicación de DB2 en su propio sistema virtualizado.</p>

## Linux: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager

- Oferta de IBM Spectrum Protect

#### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es `IBM Installation Manager`.

#### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.

#### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## Linux: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarle a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

Elemento	Espacio necesario	Número de directorios	Ubicación de los directorios
La base de datos			
Registro activo			
Registro de archivos			
Opcional: duplicado de registro para el registro activo			
Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado)			

Elemento	Nombres e ID de usuario	Ubicación
El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect		
El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia		
El nombre de instancia de la base de datos		
El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor)		
El nombre del servidor; utilice un nombre exclusivo para cada servidor		

## Linux: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- Linux: Estimación de los requisitos de espacio para la base de datos  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.
- Linux: Requisitos de espacio del registro de recuperación  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.
- Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- Linux: Supresión de archivos de retrotracción de instalación  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Linux: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- Linux: Estimación de los requisitos de espacio de base de datos en función del número de archivos  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- Linux: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- Linux: El gestor de bases de datos y el espacio temporal  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## Linux: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.

- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.

En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:



$$500 * 3.5 = 1.7 \text{ TB}$$

## Resultados

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrece acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

Tamaño de la base de datos	Requisito mínimo de espacio temporal
< 500 GB	50 GB
≥ 500 GB y < 1 TB	100 GB
≥ 1 TB y < 1,5 TB	150 GB
≥ 1,5 y < 2 TB	200 GB
≥ 2 y < 3 TB	250 - 300 GB
≥ 3 y < 4 TB	350 - 400 GB

## Linux: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## Linux: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.
- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.
- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## Linux: Requisitos de espacio del registro de recuperación

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- Linux: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- Linux: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- Linux: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## Linux: Espacio del registro activo y archivado

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:

- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.
- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- Linux: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

número de clientes x archivos almacenados durante cada transacción  
x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.

Elemento	Valores de ejemplo	Descripción
Espacio de registro necesario para cada archivo	3053 bytes	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	19,5 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p>(300 cliente x 4096 archivos almacenados durante cada transacción x 3053 bytes para cada archivo) ÷ 1.073.741.824 bytes = 3,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p>3,5 + 16 = 19,5 GB</p>
Registro de archivado: Tamaño recomendado	58,5 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p>3,5 x 3 = 10,5 GB</p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p>10,5 + 48 = 58,5 GB</p>
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

Elemento	Valores de ejemplo	Descripción
----------	--------------------	-------------

Elemento	Valores de ejemplo		Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	1000	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Sesiones posibles para cada cliente	3	3	El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.
Archivos almacenados durante cada transacción	4096	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3053	3053	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	26,5 GB <sup>1</sup>	51 GB <sup>1</sup>	<p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	79,5 GB <sup>1</sup>	153 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
Registro de archivado: Tamaño recomendado	60 GB <sup>1</sup>	Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:  $4 \text{ GB} \times 3 = 12 \text{ GB}$  Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:  $12 + 48 = 60 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

`300 clientes x 100.000 archivos por cada cliente x 110 bytes = 3,1 GB`

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## Linux: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.

La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día	60 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana	132 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>



Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Linux: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que

una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.
Tamaño medio de extensiones	700 KB	700 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.
Extensiones para un determinado archivo	1.198.372 bits	6.135.667 bits	Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.  Se ha utilizado el siguiente cálculo para un objeto de 800 GB: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$  Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	1,7 GB	8,6 GB	El espacio de registro activo estimado necesario para esta transacción.

Elemento	Valores de ejemplo		Descripción
Registro activo: Tamaño total recomendado	66 GB <sup>1</sup>	79,8 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$
Registro de archivado: Tamaño recomendado	198 GB <sup>1</sup>	239,4 GB <sup>1</sup>	<p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.

Elemento	Valores de ejemplo		Descripción
Tamaño medio de extensiones	256 KB	256 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.
Extensiones para un determinado archivo	3.276.800 bits	16.777.216 bits	<p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	4,5 GB	23,4 GB	El tamaño estimado del espacio de registro activo necesario para esta transacción.
Registro activo: Tamaño total recomendado	71,6 GB <sup>1</sup>	109,4 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$

Elemento	Valores de ejemplo		Descripción
Registro de archivado: Tamaño recomendado	214,8 GB <sup>1</sup>	328,2 GB <sup>1</sup>	<p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

## Linux: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## Linux: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## Linux: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## Linux: Supresión de archivos de retrotracción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

### Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la

interfaz de usuario de IBM® Installation Manager.

- Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

## Linux: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico


---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.

 Sistemas operativos Linux En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente para iniciar IBM Installation Manager:

```
./IBMIM
```

2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.

## Linux: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos

---



Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Linux/eclipse/tools

Por ejemplo:

-  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
  -  Sistemas operativos Linux./imcl -c
3. Especifique **P** para seleccionar Preferencias.
4. Especifique **3** para seleccionar Archivos a restaurar.
5. Especifique **D** para Suprimir los Archivos a restaurar.
6. Especifique **A** para Aplicar cambios y volver al menú Preferencias.
7. Especifique **C** para salir del Menú Preferencias.
8. Especifique **X** para Salir de Installation Manager.

## Linux: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.

### Identificador de usuario de la instancia

---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.

## Directorio de inicio del ID de usuario de la instancia

---

El directorio de inicio puede crearse cuando se crea el ID de usuario de la instancia, utilizando la opción (-m) para crear un directorio de inicio si todavía no existe. Dependiendo de la configuración local, el directorio padre podría tener la forma:  
`/home/instance_user_ID`

Por ejemplo: `/home/tsminst1`

El directorio de inicio se utiliza principalmente como contenedor del perfil del ID de usuario y de valores de seguridad.

## Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos tiene que ser el mismo que el identificador de usuario de la instancia en la que ejecuta la instancia del servidor.

Por ejemplo: `tsminst1`

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede crear el directorio de la instancia como subdirectorio del directorio padre para el identificador de usuario de la instancia.  
Por ejemplo: `/home/instance_user_ID/instance_user_ID`

En el siguiente ejemplo se coloca el directorio de la instancia en el directorio padre del identificador de usuario `tsminst1`:  
`/home/tsminst1/tsminst1`

También puede crear el directorio en otra ubicación, por ejemplo: `/tsmservr/tsminst1`

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`
- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre `TSMDB1`, para todas las instancias del servidor. Este nombre no puede modificarse.

## Nombre de servidor


---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato `QUERY SERVER`), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.

Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.



 Sistemas operativos Linux Por ejemplo:


- PAYROLL
- SALES

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos Linux/tsminst1\_archlog

## Linux: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

`/opt/tivoli/tsm/server/bin` es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es `/opt/tivoli/tsm/db2`.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## Linux: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Al urukuzar ek software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones


 Sistemas operativos Linux Deje aproximadamente entre 30 y 45 minutos para instalar un servidor V 8.1.2, utilizando esta guía.

- Linux: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- Linux: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- Linux: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## Linux: Obtener el paquete de instalación

---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

 Sistemas operativos Linux

## Antes de empezar

---

Si tiene la intención de descargar los archivos, establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente:

1. Para consultar el valor de tamaño máximo de archivo, emita el mandato siguiente:


```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado siguiendo las instrucciones de la documentación de su sistema operativo.

## Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos Linux


- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
- c. Asegúrese de que el permiso ejecutable está establecido para el paquete. Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

- d. Extraiga el paquete emitiendo el siguiente mandato:

```
./package_name.bin
```

donde *nombre\_paquete* es el nombre del archivo descargado, por ejemplo:

 Sistemas operativos Linux

```
8.1.x.000-IBM-SPSRV-Linuxx86_64.bin  
8.1.x.000-IBM-SPSRV-Linuxs390x.bin  
8.1.x.000-IBM-SPSRV-Linuxppc64le.bin
```

3. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - Linux: Instalación de IBM Spectrum Protect en modalidad de consola
  - Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa
4. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación

---

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.

### Antes de empezar


---

Realice las acciones siguientes antes de iniciar la instalación:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:


Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación emitiendo el mandato siguiente:</p>  Sistemas operativos Linux

```
./install.sh
```

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.

Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.

- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## Linux: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.


### Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:


- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.

## Procedimiento



Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p>  Sistemas operativos Linux

```
./install.sh -c
```

Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique  para generar las respuestas.

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos Linux/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

## Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

## Antes de empezar

---

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento

---


1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.

Si está utilizando el archivo install\_response\_sample.xml, añada la contraseña en la línea siguiente del archivo, donde *mypassword* representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación



Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo update\_response\_sample.xml.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor *archivo\_respuestas* representa la vía de acceso del archivo de respuestas y el nombre del archivo:
  - o  Sistemas operativos Linux

```
./install.sh -s -input archivo_respuestas  
-acceptLicense
```

## Qué hacer a continuación

---

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  - o  Sistemas operativos Linux/var/ibm/InstallationManager/logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Linux Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.

 Sistemas operativos Linux

## Linux: Instalación de paquetes de idioma del servidor

---

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## Antes de empezar

---


Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.


- Linux: Idiomas locales del servidor  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- Linux: Configuración de un paquete de idiomas  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los

- paquetes de instalación se proporcionan con IBM Spectrum Protect.
- Linux: Actualización de un paquete de idiomas  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## Linux: Idiomas locales del servidor

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 Sistemas operativos Linux Este paquete de idioma se instala automáticamente para la siguiente opción de idioma predeterminado para los mensajes y la ayuda del servidor de IBM Spectrum Protect:

-  Sistemas operativos Linux LANGUAGE en\_US

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera.

Puede utilizar los idiomas que se muestran:



 Sistemas operativos Linux

Tabla 1. Idiomas del servidor para Linux

IDIOMA	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chino, tradicional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Inglés de Estados Unidos	en_US
	en_US.utf8
Francés	fr_FR
	fr_FR.utf8
Alemán	de_DE
	de_DE.utf8
Italiano	it_IT
	it_IT.utf8
Japonés	ja_JP
	ja_JP.utf8
Coreano	ko_KR
	ko_KR.utf8
Portugués, de Brasil	pt_BR
	pt_BR.utf8
Ruso	ru_RU
	ru_RU.utf8
Español	es_ES
	es_ES.utf8


 Sistemas operativos Linux Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.



## Linux: Configuración de un paquete de idiomas

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

## Acerca de esta tarea

---

 Sistemas operativos Linux Para definir el soporte para un determinado entorno nacional, realice una de las siguientes tareas:

- Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo:
  -  Sistemas operativos Linux Para utilizar el entorno `it_IT`, establezca la opción LANGUAGE en `it_IT`. Consulte Linux: Idiomas locales del servidor.
-  Sistemas operativos Linux Si está iniciando el servidor en segundo plano, establezca el entorno variable `LC_ALL` para que coincida con el valor que se establece en el archivo de opciones del servidor. Por ejemplo, para establecer la variable de entorno en italiano, especifique el siguiente valor:

```
exportar LC_ALL=it_IT
```

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## Linux: Actualización de un paquete de idiomas

---

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

---

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.

Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.





## Linux: Primeros pasos tras instalar IBM Spectrum Protect



---


Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

### Acerca de esta tarea

---

1.  Sistemas operativos Linux Actualice los valores de los parámetros del kernel.
  -  Sistemas operativos Linux Consulte el apartado Linux: Ajuste de parámetros del kernel en sistemas Linux.
2. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado Linux: Creación del ID de usuario y de directorios para la instancia del servidor.
3. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
  - Utilice el asistente de configuración, el método preferido. Consulte el apartado Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
  - Configure manualmente la nueva instancia. Consulte el apartado Linux: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
    - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte Linux: Creación de una instancia del servidor.
    - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  Sistemas operativos Linux Linux: Configuración de comunicaciones de servidor y de cliente.
    - c. Emita el mandato `DSMSERV FORMAT` para formatear la base de datos. Consulte el apartado Linux: Formateo de la base de datos y las anotaciones.
    - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
4. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
5. Inicie la instancia del servidor, si todavía no se ha iniciado.
  -  Sistemas operativos Linux Consulte el apartado Linux: Inicio de la instancia de servidor.
6. Registre su licencia. Consulte el apartado Linux: Registro de licencias.

7. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
  8. Supervise el servidor. Consulte el apartado Linux: Supervisión del servidor.
-  **Sistemas operativos LinuxLinux: Ajuste de parámetros del kernel en sistemas Linux**  
Para que IBM Spectrum Protect y DB2 se instalen y funcionen correctamente en Linux, debe actualizar los parámetros de configuración del kernel.
  - **Linux: Creación del ID de usuario y de directorios para la instancia del servidor**  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
  - **Linux: Configuración del servidor de IBM Spectrum Protect**  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
  - **Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor**  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
  -  **Sistemas operativos LinuxLinux: Inicio de la instancia de servidor**  
Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario root.
  - **Linux: Detención del servidor**  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
  - **Linux: Registro de licencias**  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
  - **Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos**  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
  - **Linux: Ejecución de varias instancias de servidor en un solo sistema**  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
  - **Linux: Supervisión del servidor**  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

 Sistemas operativos Linux

## Linux: Ajuste de parámetros del kernel en sistemas Linux



---

Para que IBM Spectrum Protect y DB2 se instalen y funcionen correctamente en Linux, debe actualizar los parámetros de configuración del kernel.

### Acerca de esta tarea

---

Si no actualiza estos parámetros, la instalación de DB2 y IBM Spectrum Protect puede fallar. Aunque la instalación se realice correctamente, pueden producirse problemas operativos si no establecer valores para los parámetros.

-  **Sistemas operativos LinuxLinux: Actualización de parámetros del kernel en Linux**  
DB2 aumenta automáticamente los valores de parámetros del kernel de comunicación entre procesos (IPC) a los valores recomendados.
-  **Sistemas operativos LinuxLinux: Valores recomendados para parámetros del kernel en Linux**  
Asegúrese de que los valores para los parámetros del kernel sean suficientes para evitar problemas operativos al ejecutar el servidor de IBM Spectrum Protect.

 Sistemas operativos Linux

## Linux: Actualización de parámetros del kernel en Linux

---

DB2 aumenta automáticamente los valores de parámetros del kernel de comunicación entre procesos (IPC) a los valores recomendados.

### Acerca de esta tarea

---

Para actualizar parámetros del kernel en servidores Linux, siga estos pasos


## Procedimiento

1. Emita el mandato `ipcs -l` para ver una lista de valores de parámetros.
2. Analice los resultados para determinar si su sistema requiere algún cambio: Si se necesitan cambios, puede definir el parámetro en el archivo `/etc/sysctl.conf`. El valor del parámetro se aplica cuando se inicia el sistema.

## Qué hacer a continuación

Para Red Hat Enterprise Linux 6 (RHEL6), debe definir el parámetro `kernel.shmmax` en el archivo `/etc/sysctl.conf` antes de iniciar automáticamente el servidor de IBM Spectrum Protect al arrancar el sistema.

Si desea detalles sobre la base de datos DB2 para Linux, consulte Información sobre el producto DB2.

 Sistemas operativos Linux

## Linux: Valores recomendados para parámetros del kernel en Linux

Asegúrese de que los valores para los parámetros del kernel sean suficientes para evitar problemas operativos al ejecutar el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

La tabla siguiente contiene los valores de parámetro de kernel recomendados para ejecutar IBM Spectrum Protect y DB2.

Parámetro	Descripción	Valor recomendado
<code>kernel.randomize_va_space</code>	El parámetro <code>kernel.randomize_va_space</code> configura el uso del kernel de ASLR de memoria. Si establece el valor en 0, <code>kernel.randomize_va_space=0</code> , se inhabilita ASLR. Los servidores de datos de DB2 se basan en direcciones finas para ciertos objetos de memoria compartida y ASLR puede ocasionar errores para ciertas actividades. Para obtener más información sobre Linux ASLR y DB2, consulte la nota técnica en: <a href="http://www.ibm.com/support/docview.wss?uid=swg21365583">http://www.ibm.com/support/docview.wss?uid=swg21365583</a> .	0
<code>vm.swappiness</code>	El parámetro <code>vm.swappiness</code> define si el kernel puede intercambiar memoria de aplicación de la memoria física de acceso aleatorio (RAM). Para obtener más información sobre los parámetros del kernel, consulte Información sobre el producto DB2.	0
<code>vm.overcommit_memory</code>	El parámetro <code>vm.overcommit_memory</code> afecta a la cantidad de memoria virtual que el kernel permite asignar. Para obtener más información sobre los parámetros del kernel, consulte Información sobre el producto DB2.	0

## Linux: Creación del ID de usuario y de directorios para la instancia del servidor

Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.


### Antes de empezar


Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado Linux: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento



1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.

 Sistemas operativos Linux

-  Sistemas operativos Linux Cree un ID de usuario y un grupo que actuarán como propietarios de la instancia del servidor.
- a. Los siguientes mandatos se pueden ejecutar desde un ID de usuario administrador que vaya a definir el usuario y el grupo. Cree el ID de usuario y el grupo en el directorio de inicio del usuario.

Restricción: El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos ( \_ ). El nombre del ID de usuario y del grupo deben cumplir las siguientes reglas:

- La longitud debe ser de 8 caracteres o menos.
- El ID de usuario y el nombre del grupo no pueden empezar por *ibm*, *sql*, *sys* o un número.
- El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

Cree, por ejemplo, el ID de usuario `tsminst1` en el grupo `tsmsrvrs`. Los siguientes ejemplos muestran cómo crear este ID de usuario y grupo utilizando mandatos del sistema operativo.


 Sistemas operativos Linux

```
groupadd tsmsrvrs -g 1111
useradd -d /home/tsminst1 -u 2222 -g 1111 -s /bin/bash tsminst1
passwd tsminst1
```

Restricción: DB2 no admite la autenticación directa de usuarios del sistema operativo a través de LDAP.

- b. Cierre sesión y, a continuación, inicie sesión en su sistema. Cambie a la cuenta de usuario que acaba de crear. Utilice un programa de conexión interactivo, como Telnet, para que se le pida la contraseña y pueda cambiarla en caso de ser necesario.

2. Cree los directorios necesarios para el servidor.

 Sistemas operativos Linux Cree directorios vacíos para cada elemento de la tabla y asegúrese de que los directorios son propiedad del nuevo ID de usuario que acaba de crear. Monte el almacenamiento asociado en cada directorio para el registro activo, el registro de archivado y los directorios de bases de datos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El <i>directorio de instancias</i> del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir /tsminst1</code>	
Los directorios de bases de datos	<code>mkdir /tsmdb001</code> <code>mkdir /tsmdb002</code> <code>mkdir /tsmdb003</code> <code>mkdir /tsmdb004</code>	
Directorio de registro de activo	<code>mkdir /tsmlog</code>	
Directorio de registro de archivado	<code>mkdir /tsmarchlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir /tsmlogmirror</code>	
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir /tsmarchlogfailover</code>	

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSEV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.

## Linux: Configuración del servidor de IBM Spectrum Protect

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

## Acerca de esta tarea

---

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:

- **Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **Linux: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

## Linux: Configuración de IBM Spectrum Protect utilizando el asistente de configuración

---

El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.



### Antes de empezar

---

Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.

### Procedimiento

---


1. Asegúrese de que se cumplen los siguientes requisitos:  **Sistemas operativos Linux**
  - El sistema en el que instaló IBM Spectrum Protect debe tener el cliente sistema X Window. Además, debe estar ejecutando un servidor de sistema X Window en su escritorio.
  - El sistema debe tener el protocolo Secure Shell (SSH) habilitado. Asegúrese de que el puerto está establecido en el valor predeterminado, 22, y que el puerto no está bloqueado por un cortafuegos. Debe habilitar la autenticación de contraseña en el archivo `sshd_config` en el directorio de `/etc/ssh/`. Asegúrese también de que el servicio del daemon de SSH tiene derechos de acceso para conectarse al sistema utilizando el valor `localhost`.
  - Debe poder iniciar sesión en IBM Spectrum Protect con el ID de usuario que ha creado para la instancia del servidor, mediante el protocolo SSH. Cuando utilice el asistente, debe proporcionar el ID de usuario y la contraseña para acceder a ese sistema.
  - Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
  -  **Sistemas operativos Linux** Abra el programa `dsmicfgx` en el directorio `/opt/tivoli/tsm/server/bin`. Este asistente sólo puede ejecutarse como usuario `root`.

Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.

## Linux: Configuración de la instancia del servidor manualmente

---

Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

- **Linux: Creación de una instancia del servidor**  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.
-  **Sistemas operativos Linux** **Linux: Configuración de comunicaciones de servidor y de cliente**  
Se crea un archivo de opciones de servidor de ejemplo predeterminado, `dmserv.opt.smp`, durante la instalación de IBM Spectrum Protect en el directorio `/opt/tivoli/tsm/server/bin`. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.
- **Linux: Formateo de la base de datos y las anotaciones**  
Utilice el programa de utilidad `DSMSERV FORMAT` para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- **Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos**  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de


datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## Linux: Creación de una instancia del servidor


Cree una instancia de IBM Spectrum Protect emitiendo el mandato db2icrt.


### Acerca de esta tarea

Puede tener una o más instancias del servidor en una estación de trabajo.


 Sistemas operativos Linux: Importante: Antes de ejecutar el mandato db2icrt, verifique los siguientes elementos:

- El directorio padre para el usuario (/home/tsminst1) existe. Si no existe ningún directorio de inicio, debe crearlo. El directorio de instancia almacena los siguientes archivos principales generados por el servidor de IBM Spectrum Protect:
  - El archivo de opciones de servidor dsmserv.opt
  - El archivo de la base de datos de la clave del servidor, cert.kdb, y los archivos .arm (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
  - El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
  - El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
  - Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
  - El usuario existe
  - Salida de rastreo (si no está cualificada al completo)
- Existe un archivo de configuración de shell (por ejemplo, .profile) en el directorio de inicio. El usuario root y el ID de usuario de instancia deben tener permiso de escritura para este archivo. Si desea más información, consulte Información sobre el producto DB2. Busque los ajustes de variable de entorno de Linux y UNIX.

 Sistemas operativos Linux

1. Inicie sesión utilizando el ID de usuario y cree una instancia de IBM Spectrum Protect. El nombre de la instancia debe coincidir con el del usuario que sea su propietario. Utilice el mandato db2icrt y entre el mandato en una línea: 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u  
nombre_instancia nombre_instancia
```

Por ejemplo, si el ID de usuario de esta instancia es tsminst1, utilice el siguiente mandato para crear la instancia. Escriba el mandato en una línea. 

```
/opt/tivoli/tsm/db2/instance/db2icrt -a server -u  
tsminst1 tsminst1
```

Recuerde: A partir de este momento, utilice este ID de nuevo usuario al configurar el servidor IBM Spectrum Protect. Cierre la sesión del ID de usuario root e inicie sesión con el nuevo ID de usuario de la instancia.

2. Cambie el directorio predeterminado de la base de datos para que sea la misma que el directorio de instancia del servidor. Si tiene varios servidores, inicie sesión en el ID de la instancia para cada servidor. Emita este mandato:

```
db2 update dbm cfg using dftdbpath directorio_instancia
```

Por ejemplo, si directorio\_instancia es el ID del usuario de la instancia:

```
db2 update dbm cfg using dftdbpath /tsminst1
```

3. Modifique la vía de acceso a biblioteca para utilizar la versión del IBM Global Security Kit (GSKit) que está instalada con el servidor. En los siguientes ejemplos, *server\_bin\_directory* es un subdirectorio del directorio de instalación del servidor. Por ejemplo, /opt/tivoli/tsm/server/bin.


- Debe actualizar los archivos siguientes para establecer la vía de acceso a biblioteca cuando se inicia DB2 o el servidor:

Ejemplo de shell Korn o bash:

```
directorio_inicio_usuarios_instancia/sqllib/userprofile
```

Ejemplo de C shell:

```
directorio_inicio_usuarios_instancia/sqllib/usercshrc
```


- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sqllib/userprofile* (shell Korn o bash). Cada entrada debe estar en una línea. 

```
LD_LIBRARY_PATH=server_bin_directory/dbbkapi:  
/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```

```
export LD_LIBRARY_PATH
```


Recuerde: Las siguientes entradas deben estar en la vía de acceso a biblioteca:

- /usr/local/ibm/gsk8\_64/lib64
  - /opt/ibm/lib
  - /opt/ibm/lib64
  - /usr/lib64
- Añada la siguiente entrada al archivo *directorio\_inicio\_usuarios\_instancia/sllib/usercshrc* (C shell), en una línea:

 Sistemas operativos Linux

```
setenv LD_LIBRARY_PATH server_bin_directory/dbbkapi:  
/opt/ibm/lib:/opt/ibm/lib64:/usr/lib64:$LD_LIBRARY_PATH
```


- Verifique los valores de la vía de acceso de la biblioteca y que el GSKit es la versión 8.0.14.43 o posterior. Emita los mandatos siguientes:

 Sistemas operativos Linux

```
echo $LD_LIBRARY_PATH  
gsk8capiCmd_64 -version  
gsk8ver_64
```

Si la versión de GSKit no es 8.0.14.43 o posterior, debe volver a instalar el servidor de IBM Spectrum Protect. La reinstalación garantiza que esté disponible la versión correcta de GSKit.

4. Cree un archivo de opciones de servidor. Consulte Linux: Configuración de comunicaciones de servidor y de cliente.

 Sistemas operativos Linux

## Linux: Configuración de comunicaciones de servidor y de cliente

---

Se crea un archivo de opciones de servidor de ejemplo predeterminado, *dsmerv.opt.smp*, durante la instalación de IBM Spectrum Protect en el directorio */opt/tivoli/tsm/server/bin*. Debe configurar comunicaciones entre el servidor y los clientes creando un archivo de opciones de servidor nuevo. Para ello, copie el archivo de muestra en el directorio para la instancia de servidor.

### Acerca de esta tarea

---




Asegúrese de que dispone de un directorio de instancias del servidor, como */tsminst1*, y copie el archivo de muestra a este directorio. Llame a este nuevo archivo *dsmerv.opt* y edite las opciones. Finalice esta configuración antes de inicializar la base de datos de servidor. Cada entrada de ejemplo o predeterminada del archivo de opciones de muestra es un comentario, una línea que empieza con un asterisco (\*). Las opciones no distinguen entre mayúsculas y minúsculas y se permiten uno o varios espacios en blanco entre las palabras clave y los valores.

Cuando modifique el archivo de opciones, siga estas indicaciones:

- Elimine el asterisco del principio de la línea para activar una opción.
- Puede empezar a especificar las opciones en cualquier columna.
- Escriba sólo una opción por línea. La opción debe ocupar sólo una línea.
- Si realiza varias entradas para una palabra clave, el servidor de IBM Spectrum Protect aplica la última.

Si modifica el archivo de opciones del servidor, deberá volver a arrancar el servidor para que los cambios surtan efecto.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- TCP/IP Versión 4 o Versión 6
- Memoria compartida
- capa de sockets seguros (SSL)  
Consejo: Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.
-  Sistemas operativos LinuxLinux: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos LinuxLinux: Establecimiento de opciones de memoria compartida  
Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.
-  Sistemas operativos LinuxLinux: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## Linux: Establecimiento de opciones de TCP/IP

---

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea

---

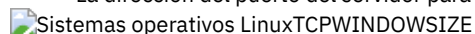
Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.

```
commethod          tcpip
tcpport            1500
tcpwindowsize     0
tcpnodelay        yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPOINT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.



Sistemas operativos LinuxTCPWINDOWSIZE

Especifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Puede especificar un entero de 0 a 2048. Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPOINT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## Linux: Establecimiento de opciones de memoria compartida

---

Puede utilizar comunicaciones de memoria compartida entre clientes y servidores del mismo sistema. Para utilizar la memoria compartida, es necesario que la máquina tenga instalado TCP/IP Versión 4.

### Acerca de esta tarea

---

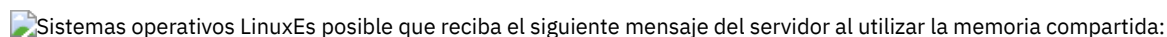
El siguiente ejemplo muestra un valor de memoria compartida:

```
commethod          sharedmem
shmport            1510
```

En este ejemplo, SHMPORT especifica la dirección de puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Utilice la opción SHMPORT para especificar un puerto TCP/IP diferente. La dirección de puerto predeterminada es 1510.

COMMETHOD se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:


```
commethod tcpip
commethod sharedmem
```



Sistemas operativos LinuxEs posible que reciba el siguiente mensaje del servidor al utilizar la memoria compartida:

```
ANR9999D shmcomm.c(1598): ThreadId<39>
Error de msgget (2), número de error = 28
```

El mensaje significa que se debe crear una cola de mensajes pero se superará el límite de sistema para el número máximo de colas de mensajes (MSGMNI).

 Sistemas operativos Linux Para averiguar el número máximo de colas de mensajes (MSGMNI) en el sistema, emita el mandato siguiente:

```
cat /proc/sys/kernel/msgmni
```

Para aumentar el valor de MSGMNI en el sistema, emita el mandato siguiente:

```
sysctl -w kernel.msgmni=n
```

siendo **n** el número máximo de colas de mensajes que desea que el sistema admita.

## Linux: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.

## Linux: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.


Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  Sistemas operativos Linux

```
db2set -i tsminst1 DB2NOEXITLIST=ON
```


### Inicialización de una instancia del servidor

---

Utilice el programa de utilidad DSMSERV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es */tsminst1*, emita los mandatos siguientes:  Sistemas operativos Linux


```
cd /tsminst1
dsmserve format dbdir=/tsmdb001 activelogsiz=32768
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

 Sistemas operativos Linux Consejo: Si DB2 no se inicia después de emitir el mandato DSMSERV FORMAT, puede que tenga que inhabilitar la opción de montaje NOSUID del sistema de archivos. Si esta opción está establecida en el sistema de archivos que contiene el directorio de propietario de instancia de DB2, o en cualquiera de los sistemas de archivos que contienen la base de datos de DB2 o registros activos, registros de archivos, registros de migración tras error o registros duplicados, la opción debe estar inhabilitada para iniciar el sistema.

Después de inhabilitar la opción NOSUID, vuelva a montar el sistema de archivos y después inicie DB2 emitiendo el siguiente mandato:


**Información relacionada:**

 [DSMSERV FORMAT](#) (Dar formato a la base de datos y a las anotaciones)

## Linux: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos


Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

### Acerca de esta tarea

 **Sistemas operativos Linux** Comenzando con IBM Spectrum Protect V7.1, ya no es necesario establecer la contraseña de API durante una configuración manual del servidor. Si establece la contraseña de API durante el proceso de configuración manual, los intentos para hacer una copia de seguridad de la base de datos pueden fallar.

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos BACKUP DB o RESTORE DB.

**Atención:** Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 **Sistemas operativos Linux** En los siguientes mandatos, sustituya los valores de ejemplo por los valores reales. Los ejemplos utilizan `tsminst1` para el ID de usuario de instancia del servidor, `/tsminst1` para el directorio de instancia del servidor, y `/home/tsminst1` como directorio de inicio de usuarios de instancia del servidor.

1. Establezca la configuración de la variable de entorno de IBM Spectrum Protect para la instancia de la base de datos:

- a. Inicie la sesión utilizando el ID de usuario `tsminst1`.
- b. Cuando el usuario `tsminst1` inicia sesión, asegúrese de que el entorno de DB2 esté debidamente inicializado. El entorno de DB2 se inicializa ejecutando el script `/home/tsminst1/sqllib/db2profile`, que normalmente se ejecuta de forma automática desde el perfil del ID de usuario. Asegúrese de que el archivo `.profile` existe en el directorio de inicio de los usuarios de instancia, por ejemplo `/home/tsminst1/.profile`. Si `.profile` no ejecuta el script `db2profile`, agregue las siguientes líneas:

```
Si [ -f /home/tsminst1/sqllib/db2profile ]; entonces
    . /home/tsminst1/sqllib/db2profile
fi
```

- c. En el archivo `directorio_instancia/sqllib/userprofile`, añada las líneas siguientes:

```
DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
DSMI_DIR=directorio_bin_servidor/dbbkapi
DSMI_LOG=directorio_instancia_servidor
export DSMI_CONFIG DSMI_DIR DSMI_LOG
```

donde:

- `directorio_instancia` es el directorio de inicio del usuario de instancia de servidor.
- `directorio_instancia_servidor` es el directorio de instancia de servidor.
- `directorio_bin_servidor` es el directorio bin de servidor. La ubicación predeterminada es `/opt/tivoli/tsm/server/bin`.

En el archivo `directorio_instancia/sqllib/usercshrc`, añada las líneas siguientes:

```
setenv DSMI_CONFIG=directorio_instancia_servidor/tsmdbmgr.opt
setenv DSMI_DIR=directorio_bin_servidor/dbbkapi
setenv DSMI_LOG=directorio_instancia_servidor
```

2. Cierre la sesión y vuelva a iniciar la sesión como `tsminst1` o emita este mandato:

```
. ~/.profile
```

Consejo: Asegúrese de que especifica un espacio en blanco después del primer carácter de punto (.)

3. Cree el archivo que se denomine `tsmdbmgr.opt` en el directorio `instancia_servidor`, que se encuentra en el directorio `/tsminst1` en este ejemplo, y añada la línea siguiente:

```
SERVERNAME TSMDBMGR_TSMINST1
```

Recuerde: El valor para `SERVERNAME` debe ser coherente en los archivos `tsmdbmgr.opt` y `dsm.sys`.


4. Como usuario root, agregue las siguientes líneas al archivo de configuración IBM Spectrum Protect API `dsm.sys`. De forma predeterminada, el archivo de configuración `dsm.sys` está en la ubicación predeterminada siguiente:

- `directorio_bin_servidor/dbbkapi/dsm.sys`

```
servername TSMDBMGR_TSMINST1
commmethod          tcpip
tcpserveraddr localhost
tcpport            1500
errorlogname /tsminst1/tsmdbmgr.log
nodename $$_TSMDBMGR_$$
```

donde

- `servername` coincide con el valor de `servername` en el archivo `tsmdbmgr.opt`.
- `commethod` especifica la API de cliente que se utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Este valor puede ser `tcpip` o `sharedmem`. Para obtener más información sobre la memoria compartida, consulte el paso 5.
- `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
- `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmserv.opt`.
- `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.
- `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Para asegurarse de que se puede hacer copia de seguridad de la base de datos, este valor debe ser `$_TSMDBMGR_`.

 **Sistemas operativos Linux** Atención: No agregue la opción `PASSWORDACCESS generate` al archivo de configuración de `dsm.sys`. Esta opción puede causar que la copia de seguridad de la base de datos falle.

5. Opcional: configura el servidor en el cual realizar la copia de seguridad mediante el uso de una memoria compartida. De esta manera, podría reducir la carga del procesador y mejorar la capacidad. Realice los siguientes pasos:
- a. Revise el archivo `dsmserv.opt`. Si las líneas siguientes no están en el archivo, añádalas:

```
commethod          sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

- b. En el archivo de configuración `dsm.sys`, localice las siguientes líneas:

```
commethod          tcpip
tcpserveraddr localhost
tcpport número_puerto
```

Reemplace las líneas especificadas con las siguientes líneas:

```
commethod          sharedmem
shmport número_puerto
```

donde `número_puerto` especifica el puerto a utilizar para la memoria compartida.

## Linux: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor

---


Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

### Acerca de esta tarea

---

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.




 Sistemas operativos Linux Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.

Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

## Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos Linux Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancia del servidor. Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `/opt/tivoli/tsm/server/bin`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.

- a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```

4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.

### Información relacionada:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 [Sistemas operativos Linux](#)

## Linux: Inicio de la instancia de servidor


---

Puede iniciar el servidor utilizando el ID de usuario de instancia, que es el método preferido, o el ID de usuario `root`.

### Antes de empezar

---


Asegúrese de establecer los permisos de acceso y los límites de usuario correctamente.

 Sistemas operativos Linux Para ver las instrucciones, consulte [Verificar los derechos de acceso y los límites del usuario](#).

### Acerca de esta tarea

---

Al iniciar el servidor utilizando el ID de usuario de la instancia, se simplifica el proceso de configuración y se evitan posibles problemas. Sin embargo, en algunos casos, es posible que sea necesario iniciar el servidor con el ID de usuario `root`. Por ejemplo, es posible que desee utilizar el ID de usuario `root` para garantizar que el servidor pueda acceder a determinados dispositivos. Puede configurar el servidor para que se inicie automáticamente utilizando el ID de usuario de instancia o el ID de usuario `root`.


 Sistemas operativos Linux Si necesita completar un mantenimiento o tareas de reconfiguración, inicie el servidor en la modalidad de mantenimiento.

## Procedimiento

---


Para iniciar el servidor, realice una de las siguientes acciones:


- Inicie el servidor haciendo uso del ID de usuario de la instancia.


 Sistemas operativos Linux Para obtener las instrucciones, consulte Inicio del servidor desde el ID del usuario de la instancia .

- Inicie el servidor utilizando el ID de usuario root.


Para obtener instrucciones sobre cómo autorizar a los ID de usuarios root a iniciar el servidor, consulte Autorización de los ID de usuario root para iniciar el servidor (V7.1.1). Para obtener instrucciones sobre cómo iniciar el servidor utilizando el ID de usuario root, consulte el apartado Inicio del servidor desde el ID de usuario root (V7.1.1).

-  Sistemas operativos Linux Inicie el servidor automáticamente.

 Sistemas operativos Linux Para obtener instrucciones, consulte Linux: Inicio automático de los servidores en sistemas Linux.

-  Sistemas operativos Linux Inicie el servidor en modalidad de mantenimiento.

Para obtener instrucciones, consulte Linux: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos Linux

## Linux: Comprobación de los derechos de acceso y límites de usuario

---

Antes de iniciar el servidor, compruebe los derechos de acceso y límites de usuario.

### Acerca de esta tarea

---

Si no verifica los límites de usuario, conocidos también como *límitesu*, podría experimentar inestabilidad del servidor o una falla del servidor al responder. También debe verificar el límite en todo el sistema para ver el número máximo de archivos abiertos. El límite de todo el sistema debe ser mayor que o equivalente al límite de usuario.

## Procedimiento

---

1. Compruebe que el ID del usuario de la instancia del servidor tenga autorizaciones para iniciar el servidor.
2. Para la instancia del servidor que piensa iniciar, asegúrese que tiene la autoridad para leer y escribir archivos en el directorio de la instancia del servidor. Compruebe que el archivo `dsmserv.opt` existe en el directorio de la instancia del servidor y de que el archivo incluye parámetros para la instancia del servidor.
3. Si el servidor está conectado a una unidad de cinta, cambiador de recursos o dispositivo de soporte extraíble y piensa iniciar el servidor mediante el uso del ID del usuario de la instancia, otorgue acceso de lectura/escritura al ID de usuario de instancias para esos dispositivos. Para establecer los permisos, realice una de las siguientes acciones:

- Si el sistema está dedicado a IBM Spectrum Protect y solo el administrador de IBM Spectrum Protect tiene acceso, haga que el archivo especial del dispositivo sea grabable para todos los usuarios. En la línea de mandatos del sistema operativo, emita el mandato siguiente:



```
chmod +w /dev/rmtX
```


- Si el sistema cuenta con varios usuarios, puede restringir el acceso si hace que el ID de usuario de la instancia de IBM Spectrum Protect sea el propietario de los archivos especiales de dispositivo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod u+w /dev/rmtX
```

- Si se están ejecutando varias instancias de usuario en el mismo sistema, cambie el nombre de grupo, por ejemplo TAPEUSERS, y añada cada ID de usuario de instancia IBM Spectrum Protect a dicho grupo. A continuación cambie la propiedad de los archivos especiales de dispositivo para que pertenezcan al grupo TAPEUSERS y haga que sean grabables para el grupo. En la línea de mandatos del sistema operativo, emita el mandato siguiente:

```
chmod g+w /dev/rmtX
```

4.  Sistemas operativos Linux Si está usando el controlador de dispositivos IBM Spectrum Protect y el programa de utilidad `autoconf`, use la opción `-a` para otorgar acceso de lectura/escritura al ID de usuario de la instancia.
5.  Sistemas operativos Linux Para evitar fallas del servidor, durante la interacción con DB2, ajuste los parámetros de kernel.

 Sistemas operativos Linux Para obtener instrucciones sobre cómo ajustar los parámetros de kernel, consulte Linux: Ajuste de parámetros del kernel en sistemas Linux.

6. Compruebe los siguientes límites de usuario con base en los lineamientos de la tabla.

Tabla 1. Valores del límite (no límite) de usuario

Tipo de límite de usuario	Valor recomendado	Mandato del valor de consulta
Tamaño máximo de archivos principales creados	Ilimitada	ilimitado -Hc
Tamaño máximo de un segmento de datos para un proceso	Ilimitada	ulimit -Hd
Tamaño de archivo máximo	Ilimitada	ulimit -Hf
Número máximo de archivos abiertos	65536	ulimit -Hn
La cantidad máxima de tiempo del procesador en segundos	Ilimitada	ilimitado -Ht

Para modificar los límites de usuario, siga las instrucciones en la documentación del sistema operativo.


Consejo: Si planea iniciar el servidor automáticamente haciendo uso de un script, puede establecer los límites de usuario en el script.

7. Asegúrese de que el límite de usuario de procesos de usuario máximos (el valor de `nproc`) se establece en el valor mínimo sugerido de 16384.

a. Para verificar el límite de usuario actual, emita el mandato `ulimit -Hu` utilizando el ID de usuario de instancia. Por ejemplo:


```
[user@Machine ~]$ ulimit -Hu
16384
```

b. Si el límite de procesos máximos del usuario no se establece en 16384, establezca el valor en 16384.


 Sistemas operativos Linux Añada la siguiente línea al archivo `/etc/security/limits.conf`:

```
id_usuario_instancia - nproc 16384
```

donde `id_usuario_instancia` especifica el ID de usuario de instancia de servidor.

 Sistemas operativos Linux Si el servidor está instalado en el sistema operativo Red Hat Enterprise Linux 6, establezca el límite de usuario al editar el archivo `/etc/security/limits.d/90-nproc.conf` en el directorio `/etc/security/limits.d`. Este archivo sustituye a los valores del archivo `/etc/security/limits.conf`.

Consejo: El valor predeterminado del límite de usuario de los procesos máximos de usuario cambió en algunas distribuciones y versiones del sistema operativo Linux. El valor predeterminado es 1024. Si no cambia el valor al valor mínimo sugerido de 16384, el servidor podría fallar o colgarse.

 Sistemas operativos Linux

## Linux: Inicio del servidor con el ID de usuario de la instancia

Para iniciar el servidor desde el ID de usuario de la instancia, inicie sesión con el ID de usuario de la instancia y emita el mandato correspondiente desde el directorio de la instancia del servidor.

### Antes de empezar

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para obtener instrucciones, consulte Linux: Comprobación de los derechos de acceso y límites de usuario.

### Procedimiento

1. Inicie sesión en el sistema donde instalado IBM Spectrum Protect utilizando el ID de usuario de instancia para el servidor.
2. Si no tiene un perfil de usuario que ejecuta el script de `db2profile`, emita el siguiente mandato:

```
. /home/tsminst1/sqllib/db2profile
```


Consejo: Para obtener instrucciones sobre cómo actualizar el script de inicio de sesión de ID de usuario para ejecutar el script `db2profile` automáticamente, consulte la documentación de DB2.

3. Inicie el servidor emitiendo el siguiente mandato en una línea desde el directorio de instancia del servidor:


 Sistemas operativos Linux

```
usr/bin/dmserv
```

Consejo: El mandato se ejecuta en primer plano para que pueda configurar un ID de administrador y conectarlo con la instancia del servidor.

 Sistemas operativos Linux Por ejemplo, si el nombre de la instancia del servidor es `tsminst1` y el directorio de la instancia de servidor es `/tsminst1`, puede iniciar la instancia emitiendo los mandatos siguientes:

```
cd /tsminst1
. ~/sqllib/db2profile
/usr/bin/dsmserve
```

 Sistemas operativos Linux

## Linux: Inicio automático de los servidores en sistemas Linux

---

Para iniciar automáticamente un servidor en un sistema operativo Linux, utilice el script `dsmserve.rc`.

### Antes de empezar

---

Asegúrese de que los parámetros de kernel están configuradas correctamente. Si desea instrucciones, consulte Ajuste de parámetro de kernel para sistemas Linux.

Asegúrese de que la instancia de servidor se ejecuta bajo el ID de usuario del propietario de instancia.

Asegúrese de que los derechos de acceso y límites de usuario se han establecido correctamente. Para ver las instrucciones, consulte Verificación de los derechos de acceso y límites de usuario.

### Acerca de esta tarea

---

El script `dsmserve.rc` está en el directorio de instalación del servidor, por ejemplo, `/opt/tivoli/tsm/server/bin`.

El script `dsmserve.rc` se puede usar para iniciar manualmente un servidor o para iniciar automáticamente el servidor al agregar entradas al directorio `/etc/rc.d/init.d`. El script funciona con los programas de utilidad Linux como por ejemplo `CHKCONFIG` y `SERVICE`.

### Procedimiento

---

Para cada instancia del servidor que desee iniciar automáticamente, realice los pasos siguientes:

1. Coloque una copia del script `dsmserve.rc` en el directorio `/init.d`, por ejemplo, `/etc/rc.d/init.d`.

Asegúrese de cambiar solo la copia del script. No modifique el script original.

2. Cambie el nombre de la copia del script de modo que coincida con el nombre del propietario de la instancia de servidor, por ejemplo, `tsminst1`.

El script se ha creado suponiendo que el directorio de instancia de servidor es *directorio\_raíz*/`tsminst1`, por ejemplo: `/home/tsminst1/tsminst1`.

3. Si el directorio de instancia de servidor no es *directorio\_raíz*/`tsminst1`, localice la línea siguiente en la copia del script:

```
instance_dir="${instance_home}/tsminst1"
```

Cambie la línea para que apunte al directorio de instancia de servidor, por ejemplo:

```
instance_dir="/tsminst1"
```

4. En la copia de script, localice la línea siguiente:

```
# pidfile: /var/run/dsmserve_instancename.pid
```

Cambie el valor de nombre de instancia por el nombre del propietario de instancia de servidor. Por ejemplo, si el propietario de instancia de servidor es `tsminst1`, actualice la línea como se muestra:

```
# pidfile: /var/run/dsmserve_tsminst1.pid
```

5. Configure el nivel de ejecución en el que el servidor se inicia automáticamente. Mediante el uso de herramientas como el programa de utilidad `CHKCONFIG`, especifique un valor que corresponda a una modalidad multiusuario, con la conexión de redes activada. Generalmente, el nivel de ejecución que se utilizará es 3 o 5, en función del sistema operativo y de su configuración. Para obtener más información acerca de la modalidad multiusuario y los niveles de ejecución, consulte la documentación del sistema operativo.
6. Para iniciar o detener el servidor, emita uno de los mandatos siguientes:
  - o Para iniciar el servidor:

```
service tsminst1 start
```

- Para detener el servidor:

```
service tsminst1 stop
```

## Ejemplo



---

Este ejemplo utiliza los siguientes valores:

- El propietario de instancia es tsminst1.
- El directorio de instancia de servidor es /home/tsminst1/tsminst1.
- La copia de script dsmserv.rc se denomina tsminst1.
- El programa de utilidad CHKCONFIG se utiliza para configurar que el script se inicie a los niveles de ejecución 3, 4 y 5.

```
cp /opt/tivoli/tsm/server/bin/dsmserv.rc /etc/rc.d/init.d/tsminst1
sed -i 's/dsmserv_instancename.pid/dsmserv_tsminst1.pid/' /etc/rc.d/init.d/tsminst1
chkconfig --list tsminst1
service tsminst1 supports chkconfig, but is not referenced in
any runlevel (run 'chkconfig --add tsminst1')
chkconfig --add tsminst1
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:off 4:off 5:off 6:off
chkconfig --level 345 tsminst1 on
chkconfig --list tsminst1
tsminst1 0:off 1:off 2:off 3:on 4:on 5:on 6:off
```

### Referencia relacionada:

-  Script de inicio del servidor: dsmserv.rc
-  Sistemas operativos Linux

## Linux: Inicio del servidor en modalidad de mantenimiento

---

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSEV con el parámetro MAINTENANCE.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, dsmserv.opt, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

### Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

### Qué hacer a continuación

---

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## Linux: Detención del servidor

---


Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

### Acerca de esta tarea

---


Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:

```
halt
```

 Sistemas operativos Linux Si no se puede conectar al servidor con un cliente administrativo y desea detener el servidor, debe cancelar el proceso utilizando el mandato kill con el número del ID de proceso (pid). El pid se muestra en la inicialización.

Importante: Antes de emitir el mandato kill, asegúrese de que conoce el ID de proceso correcto del servidor IBM Spectrum Protect. El archivo `dsmserv.v6lock`, en el directorio desde el cual se está ejecutando el servidor, se puede usar para identificar el ID de proceso del proceso que desea detener. Para mostrar el archivo, especifique:

```
cat /instance_dir/dsmserv.v6lock
```

 Sistemas operativos Linux Emita el siguiente mandato para detener el servidor:

```
kill -23 dsmserv_pid
```

donde `dsmserv_pid` es el número de ID del proceso.

## Linux: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

### Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

### Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## Linux: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

### Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

### Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

## Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

## Ejemplo

---

Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:


```
set dbrecovery dbback
```

## Linux: Ejecución de varias instancias de servidor en un solo sistema

---

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.

Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.


 Sistemas operativos LinuxEl conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos de Linux: Creación de una instancia del servidor para cada instancia nueva, incluida la creación del nuevo usuario de la instancia.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.

Puede actualizar directamente desde V6.3 a V7.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.2 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

### Tareas relacionadas:

-  Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## Linux: Supervisión del servidor

---

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## Procedimiento

---

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de

espacio de las anotaciones activas, pero durante poco tiempo.

- Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.
- Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tarden más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

## 2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible.

Recuerde: Si el registro de archivado y el registro de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.

Probablemente observará el siguiente patrón:

- a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
- b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.
- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## Linux: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.2 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.2, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de



configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado Linux: Revierta de la versión 8.1.2 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:



```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación. La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7.  Sistemas operativos Linux Conéctese como usuario root.
8. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
9.  Sistemas operativos Linux Cambie al directorio donde situó el archivo ejecutable y complete los pasos siguientes.  
Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.

- a. Cambie los permisos de archivo emitiendo el siguiente mandato:

```
chmod a+x 8.x.x.x-IBM-SPSRV-plataforma.bin
```

donde *plataforma* indica la arquitectura en la que se va a instalar IBM Spectrum Protect.

- b. Emita el siguiente mandato para extraer los archivos de instalación:

```
./8.x.x.x-IBM-SPSRV-plataforma.bin
```

10. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.

Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.

Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

#### Asistente de instalación

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

#### Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect en modalidad de consola

#### Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

Linux: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.

## Resultados

---

Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos Linux/var/ibm/InstallationManager/logs

## Linux: Reverta de la versión 8.1.2 a un servidor anterior

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

## Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:

- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

## Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.2 al 8.1.1 o del 8.1.2 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.


## Pasos para recuperar la versión anterior del servidor


---

### Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

### Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato:  Sistemas operativos Linux
 

```
dmserv removedb tsmdb1
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado Linux: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.2. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato:  Sistemas operativos Linux
 

```
./dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.
7. Restaure la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - Archivo de configuración de dispositivos
  - Archivo histórico de volúmenes
  - El archivo de opciones de servidor (generalmente dmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.2, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de seguridad de la base de datos. Utilice el mandato RESTORE VOLUME. Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:
 

```
audit volume nombre_volumen fix=yes
```
11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.2, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.2.

### Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.2:

- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.2. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

## Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:

- Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.2.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro REUSEDELAY para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.2. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.2, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.2.

## Linux: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect


Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.

### Finalidad

Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.

Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.

Tabla 1. Mandatos de DB2

Man dato	Descripción	Ejemplo
db2i crt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia.</p> <p>Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p> <p> Sistemas operativos Linux Este programa de utilidad está en el directorio DB2DIR/instance, donde DB2DIR representa la ubicación donde se instala la versión actual del sistema de base de datos de DB2.</p>	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre>/opt/tivoli/ts m/db2/instance / db2icrt -a server -u nombre_instanc ia nombre_instanc ia</pre>
db2s et	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> <pre>db2set</pre>

<b>Man dato</b>	<b>Descripción</b>	<b>Ejemplo</b>
CAT ALO G DAT ABASE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	Catalogue la base de datos:  db2 catalog database tsmdb1
CON NEC T TO DAT ABASE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:  db2 connect to tsmdb1
GET DAT ABASE CON FIG URATI ON	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Muestre la información de configuración para un alias de base de datos:  db2 get db cfg for tsmdb1  Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.  db2 get db config for tsmdb1 show detail
GET DAT ABASE MAN AGE R CON FIG URATI ON	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEA LTH SNA PSH OT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsmdb1

<b>Mandato</b>	<b>Descripción</b>	<b>Ejemplo</b>
GRANT (Autorizaciones de bases de datos)	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser
RUNSTATS	Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.  Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.  Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.  Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.	Actualice las estadísticas en una única tabla.  db2 runstats on table SCHEMA_NAME.TABLE_NAME with distribution and sampled detailed indexes all
SETSCHEMA	Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2.  Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.	Establezca el esquema para IBM Spectrum Protect:  db2 set schema tsmdb1
START DATABASE MANAGER	Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.  Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.	Inicie el gestor de base de datos:  db2start
STOP DATABASE MANAGER	Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.  Este mandato no es válido en un cliente.  El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.  Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.	Detenga el gestor de base de datos:  db2 stop dbm

## Linux: Desinstalar IBM Spectrum Protect

Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.
- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

## Acerca de esta tarea

---

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.
- Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- Linux: Desinstalación e instalación de IBM Spectrum Protect  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- Linux: Desinstalación de IBM Installation Manager  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

## Qué hacer a continuación

---

Consulte Linux: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## Linux: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico


---

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento

---

1. Inicie el Installation Manager.

 Sistemas operativos Linux En el directorio en donde se encuentra instalado Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:

```
./IBMIM
```

2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.

## Linux: Desinstalación de IBM Spectrum Protect en modalidad de consola


---

Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.

### Procedimiento

---


1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:

-  Sistemas operativos Linux/eclipse/tools

Por ejemplo:

-  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools

2. Desde el directorio herramientas, emita el siguiente mandato:

- o  Sistemas operativos Linux. `./imcl -c`
3. Para desinstalar, escriba 5.
  4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
  5. Especifique `N` para Siguiente.
  6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
  7. Especifique `N` para Siguiente.
  8. Escriba `U` para Desinstalar.
  9. Escriba `F` para Finalizar.

## Linux: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

---

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.

### Antes de empezar

---


Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.


Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  - o  Sistemas operativos Linux `eclipse/tools`

Por ejemplo:

- o  Sistemas operativos Linux `/opt/IBM/InstallationManager/eclipse/tools`
2. Desde el directorio herramientas, emita el siguiente mandato, donde `archivo_respuestas` representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

 Sistemas operativos Linux

```
./imcl -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos Linux

```
./imcl -input /tmp/input/uninstall_response.xml -silent
```

## Linux: Desinstalación e instalación de IBM Spectrum Protect


---

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.

### Acerca de esta tarea


---

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos Linux Realice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```


2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:

 Sistemas operativos Linux




```
db2 attach to instance_name
db2 get dbm cfg show detail
db2 detach
```

Mantenga un registro de la ruta de base de datos para casa instancia.


3. Desinstale IBM Spectrum Protect. Consulte el apartado Linux: Desinstalar IBM Spectrum Protect.
4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten los credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estos credenciales utilizando la variable `INSTANCE_CRED`.  
Puede encontrar el archivo de instancias en la siguiente ubicación:
  - o  Sistemas operativos Linux/etc/tivoli/tsm/instanceList.obj
5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado Linux: Instalación de los componentes de servidor.

Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- a. Vuelva a crear las instancias de servidor. Consulte el apartado Linux: Creación de una instancia del servidor.  
Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- b. Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos Linux

```
db2 catalog database tsmdb1
db2 attach to instance_name
db2 update dbm cfg using dftdbpath instance_directory
db2 detach
```

- c.  Sistemas operativos Linux Compruebe que la instancia de servidor se haya creado correctamente. Emita este mandato:

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

- d. Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```

Si figura TSMDB1 puede iniciar el servidor.

## Linux: Desinstalación de IBM Installation Manager

---

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

### Antes de empezar

---

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.

 Sistemas operativos Linux Para ver los paquetes instalados, emita el mandato siguiente desde una línea de mandatos:

```
cd /opt/IBM/InstallationManager/eclipse/tools
./imcl listInstalledPackages
```

### Procedimiento

---

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos Linux

1. Abra una línea de mandatos y cambie el directorio a `/var/ibm/InstallationManager/uninstall`.
2. Emita el mandato siguiente:

```
./uninstall
```

Restricción: Debe haber iniciado sesión en el sistema utilizando el ID de usuario `root`.

## Windows: Instalación del servidor

---


La instalación del servidor incluye la planificación, instalación y configuración inicial.

- Windows
- Windows: Planificación para instalar el servidor  
Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.
- Windows: Instalación de los componentes de servidor  
Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Windows: Primeros pasos tras instalar IBM Spectrum Protect  
Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.
- Windows: Instalación de un fixpack de servidor de IBM Spectrum Protect  
Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.
- Windows: Revertir de la versión 8.1.2 a un servidor anterior  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.
- Windows: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect  
Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.
- Windows: Desinstalar IBM Spectrum Protect  
Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

## Windows: Planificación para instalar el servidor

---

Instale el software de servidor en el sistema que gestiona dispositivos de almacenamiento e instale el software de cliente en cada estación de trabajo que transfiere datos al almacenamiento gestionado por el servidor IBM Spectrum Protect.


- Windows: Qué debe saber primero  
Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.
- Windows: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor  
Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.
- Windows: Planificación de rendimiento óptimo  
Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.
-  Sistemas operativos Windows: Requisitos mínimos del sistema para sistemas Windows  
El servidor puede requerir una gran cantidad de memoria, ancho de banda de red y recursos de procesador. En muchos casos, el servidor funciona mejor cuando las otras aplicaciones no están instaladas en el mismo sistema.
- Windows: IBM Installation Manager  
IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- Windows: Hojas de trabajo para planificar detalles para el servidor  
Puede utilizar las hojas de trabajo para ayudarlo a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.
- Windows: Planificación de la capacidad  
La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.
- Windows: Prácticas más adecuadas de denominación del servidor  
Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.
- Windows: Directorios de instalación  
Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.


## Windows: Qué debe saber primero

---

Antes de instalar IBM Spectrum Protect, familiarícese con los sistemas operativos, dispositivos de almacenamiento, protocolos de comunicación y configuraciones del sistema.

Los releases de mantenimiento de servidor, software de cliente y publicaciones están disponibles en IBM® Support Portal.

 **Sistemas operativos Windows** Restricción: No puede instalar y ejecutar el servidor de la Versión 8.1.2 en un sistema que ha tenga DB2 instalado en el mismo, tanto si DB2 se ha instalado por sí mismo o como parte de alguna otra aplicación. El servidor de la V8.1.2 necesita que se instale y utilice la versión de DB2 que está empaquetada con el servidor de la V8.1.2. No puede haber ninguna otra versión de DB2 en el sistema.

 **Sistemas operativos Windows** Puede instalar el servidor en IBM Spectrum Protect en un controlador de dominio. Sin embargo, el servidor puede tener un uso de procesador intensivo y esto podría afectar y detener otras aplicaciones.

Los administradores de DB2 con experiencia pueden optar por realizar consultas SQL avanzadas y utilizar herramientas de DB2 para supervisar la base de datos. Sin embargo, no utilice las herramientas de DB2 para cambiar la configuración de DB2 de los valores preestablecidos por IBM Spectrum Protect, ni para alterar el entorno DB2 para IBM Spectrum Protect de otra forma o con otros productos. El servidor V8.1.2 se ha creado y probado ampliamente utilizando el lenguaje de definición de datos (DDL) y la configuración de base de datos que despliega el servidor.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Windows: Qué debe saber sobre seguridad antes de instalar o actualizar el servidor

---

Antes de instalar IBM Spectrum Protect V8.1.2 o posterior, consulte la información sobre las características de seguridad ampliadas y los requisitos para actualizar el entorno.

### Acerca de esta tarea

---

Las mejoras de seguridad en V8.12 y posterior han aplicado parámetros de seguridad más estrictos. Para garantizar que no se interrumpa la comunicación entre servidores y clientes al instalar o actualizar el software IBM Spectrum Protect a V8.1.2, siga el procedimiento.

### Procedimiento

---

1. Instale o actualice los servidores IBM Spectrum Protect a 8.1.2 o posterior.
2. Instale o actualice los clientes de copia de seguridad y archivado. Si desea más información, consulte *Instalación y configuración de clientes*.  
Para obtener información sobre la planificación del despliegue de actualizaciones de clientes desde el servidor, consulte los siguientes documentos:
  - Para servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.
  - Para servidores IBM® Tivoli Storage Manager V7.1 y IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la nota técnica 1673299.
3. Configure las opciones para clientes de copia de seguridad y archivado. Para obtener más información, consulte *Actualización del servidor de IBM Spectrum Protect e IBM Spectrum Protect Client*.

## Windows: Planificación de rendimiento óptimo

---

Antes de instalar el servidor IBM Spectrum Protect, evalúe las características y la configuración del sistema para asegurarse de que el servidor esté configurado para su óptimo rendimiento.

### Procedimiento

---

1. Revise *Windows: Qué debe saber primero*.
2. Revise cada una de las siguientes subsecciones.
  - **Windows: Planificación del hardware del servidor y el sistema operativo**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
  - **Windows: Planificación de discos de base de datos del servidor**  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.



- Windows: Planificación de discos de registro de recuperación del servidor  
Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.
- Windows: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios  
Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.
- Windows: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE  
Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.
- Windows: Planificación del tipo correcto de tecnología de almacenamiento  
Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.
- Windows: Aplicación de prácticas recomendadas para la instalación del servidor  
Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

## Windows: Planificación del hardware del servidor y el sistema operativo

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿El sistema operativo y el hardware cumplen o superan los requisitos?</p> <ul style="list-style-type: none"> <li>• Número y velocidad de los procesadores</li> <li>• Memoria del sistema</li> <li>• Nivel de sistema operativo admitido</li> </ul>	<p>Si utiliza la cantidad mínima necesaria de memoria, puede soportar una carga de trabajo mínima.</p> <p>Puede experimentar añadiendo más memoria del sistema para determinar si el rendimiento ha mejorado. A continuación, decida si desea mantener la memoria del sistema dedicada al servidor. Compruebe las variaciones de memoria utilizando el ciclo diario completo de la carga de trabajo del servidor.</p> <p>Si ejecuta varios servidores en el sistema, añada los requisitos de cada servidor para obtener los requisitos del sistema.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309.</p> <p>Además, revise las instrucciones de Ajuste de tareas para sistemas operativos y otras aplicaciones.</p> <p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para obtener más información sobre requisitos de dimensionamiento para el servidor y el almacenamiento, consulte IBM Spectrum Protect Blueprint.</p>
<p>¿Están configurados los discos para un rendimiento óptimo?</p>	<p>Los ajustes que se pueden realizar para los distintos sistemas de disco varían. Asegúrese de que estén configuradas las profundidades de cola y demás opciones del sistema de discos correspondientes.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• "Planificación de discos de base de datos del servidor"</li> <li>• "Planificación de discos de registro de recuperación del servidor"</li> <li>• "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿El servidor tiene suficiente memoria?	<p>Las cargas de trabajo más pesadas y las funciones avanzadas como la eliminación de la duplicación de datos y la réplica de nodos requieren más del mínimo de memoria del sistema que se especifica en el documento de requisitos del sistema.</p> <p><b>**Para las bases de datos que no están habilitadas para la eliminación de duplicación de los datos, use los siguientes lineamientos para especificar los requisitos de memoria:</b></p> <ul style="list-style-type: none"> <li>• Para bases de datos inferiores a 500 GB, necesita 16 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 500 GB - 1 TB, necesita 24 GB de memoria.</li> <li>• Para bases de datos con un tamaño de 1 TB - 1.5 TB, necesita 32 GB de memoria.</li> <li>• Para bases de datos superiores a 1,5 TB, necesita 40 GB de memoria.</li> </ul> <p>Asegúrese de asignar espacio adicional para el registro activo y el registro de archivado para el proceso de réplica.</p>	<p>Para obtener más información acerca de los requisitos cuando estas características están en uso, vea los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> <li>• Requisitos de memoria</li> </ul>
¿Tiene el sistema suficientes adaptadores de bus de host (HBA) como para gestionar las operaciones de datos que el servidor de IBM Spectrum Protect tiene que ejecutar simultáneamente?	<p>Operaciones que requieren el uso de HBA al mismo tiempo.</p> <p>Por ejemplo, un servidor debe almacenar 1 GB/seg de datos de seguridad y, al mismo tiempo, realizar la migración de la agrupación de almacenamiento que requiere una capacidad de 0,5 GB/seg para completarse. Los HBA deben poder gestionar todos los datos a la velocidad necesaria.</p>	<p>Consulte Ajuste de la capacidad del adaptador de bus de host.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Es el ancho de banda mayor que el rendimiento máximo planificado para las copias de seguridad?	<p>El ancho de banda de red debe permitir que el sistema complete operaciones, como copias de seguridad, en el tiempo permitido o bien que se cumplan los compromisos de nivel de servicio.</p> <p>Para la réplica de nodo, el ancho de banda de red debe ser mayor que el rendimiento máximo planeado.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del rendimiento de red</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul>
¿Utiliza un sistema de archivos preferido para los archivos del servidor de IBM Spectrum Protect?	<p>Utilice un sistema de archivos que garantice un rendimiento y una disponibilidad de los datos óptimos. El servidor utiliza E/S directa con sistemas de archivos que den soporte a la característica. El uso de E/S directa puede mejorar el rendimiento y reducir el uso del procesador. La siguiente lista identifica el sistema de archivos preferido:</p> <p> Sistemas operativos</p> <ul style="list-style-type: none"> <li>• Windows Utilice New Technology File System (NTFS) sin compresión.</li> </ul>	<p>Para obtener más información, consulte Configuración del sistema operativo para el rendimiento del disco.</p>
¿Tiene pensado configurar suficiente espacio de paginación?	<p>El espacio de paginación, o espacio de intercambio, amplía la memoria disponible para el procesamiento. Si la cantidad de RAM libre en el sistema es baja, los programas o datos que no estén en uso se moverán de la memoria al espacio de paginación. Esta acción libera memoria para otras actividades, por ejemplo operaciones de la base de datos.</p> <p> Sistemas operativos Windows El espacio de paginación se configura automáticamente.</p>	

## Windows: Planificación de discos de base de datos del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Se encuentra la base de datos en discos rápidos de baja latencia?	<p>No utilice las unidades siguientes para la base de datos de IBM Spectrum Protect:</p> <ul style="list-style-type: none"> <li>• Nearline SAS (NL-SAS)</li> <li>• Conexión de tecnología avanzada en serie (SATA)</li> <li>• Conector de tecnología avanzada en paralelo (PATA).</li> </ul> <p>No utilice los discos internos que se han incluido de forma predeterminada en la mayoría del hardware del servidor.</p> <p>Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p> <p>Si quiere utilizar las funciones de deduplicación de datos de IBM Spectrum Protect, céntrese en el rendimiento de disco en términos de operaciones de E/S por segundo (IOPS).</p>	Para obtener más información, consulte Lista de comprobación para la optimización de almacenamiento de datos.
¿Está almacenada la base de datos en discos o LUN separados de los discos o LUN utilizados para el registro activo, el registro de archivado y los volúmenes de agrupación de almacenamiento?	<p>La separación de la base de datos del servidor de otros componentes de servidor ayuda a reducir los conflictos por los recursos por parte de distintas operaciones que se tienen que ejecutar al mismo tiempo.</p> <p>Consejo: La base de datos y el archivo de archivado pueden compartir una matriz si utiliza la tecnología de unidad de estado sólido (SSD).</p>	
Si utiliza RAID, ¿sabe cómo seleccionar el nivel de RAID óptimo para su sistema? ¿Está definiendo todos los LUN con el mismo tamaño y tipo de RAID?	<p>Cuando en un sistema se tienen que hacer muchas grabaciones, RAID 10 sobrepasa a RAID 5. De todas maneras, RAID 10 requiere más discos que RAID 5 para disponer de la misma cantidad de almacenamiento utilizable.</p> <p>Si su sistema de disco es RAID, defina todos los LUN con el mismo tipo y tamaño de RAID. Por ejemplo, no mezcle 4+1 RAID 5 con 4+2 RAID 6.</p>	
Si dispone de una opción para definir el tamaño de banda o segmento, ¿ha planificado optimizar el tamaño al configurar el sistema de discos?	Si puede definir el tamaño de la banda o del segmento, utilice los tamaños de 64 KB o 128 KB en los sistemas de disco para la base de datos.	El tamaño de bloque utilizado para la base de datos varía en función del espacio de tabla. La mayoría de los espacios de tabla utilizan bloques de 8 KB, pero algunos utilizan bloques de 32 KB.

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Tiene pensado crear al menos cuatro directorios, también denominadas vías de acceso de almacenamiento, en cuatro LUN independientes para la base de datos?</p> <p>Cree un directorio por cada matriz en el subsistema. Si tiene menos de tres matrices, cree un volumen de LUN independiente dentro de la matriz.</p>	<p>Las cargas de trabajo más pesadas y el uso de determinadas características requieren más vías de acceso de almacenamiento de base de datos que los requisitos mínimos.</p> <p>Las operaciones del servidor como la deduplicación de datos dirigen un gran número de operaciones de entrada/salida por segundo (IOPS) hacia la base de datos. Dichas operaciones se realizan de forma más adecuada cuando la base de datos tiene más directorios.</p> <p>Para las bases de datos del servidor de más de 2 TB o que se espera que alcancen ese tamaño, utilice ocho directorios.</p> <p>Tenga en cuenta el crecimiento previsto para el sistema cuando determine cuántas vías de acceso de almacenamiento ha de crear. El servidor utiliza el número más elevado de vías de acceso de almacenamiento con más eficacia si dichas vías de acceso de almacenamiento se encuentran presentes cuando se crea el servidor por primera vez.</p> <p>Utilice la variable <code>DB2_PARALLEL_IO</code> para forzar que se produzca la E/S paralela en espacios de tabla que tengan un contenedor, o en espacios de tabla que tengan contenedores en más de un disco físico. Si no establece la variable <code>DB2_PARALLEL_IO</code>, el paralelismo de E/S será igual al número de contenedores que utilice el espacio de tabla. Por ejemplo, si un espacio de tabla ocupa cuatro contenedores, el nivel de paralelismo de E/S utilizado será 4.</p>	<p>Para más información, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Lista de comprobación para la optimización de almacenamiento de datos</li> <li>• Lista de comprobación para la réplica de nodo</li> </ul> <p>Para ayudarle a predecir el crecimiento cuando el servidor deduplica datos, consulte la nota técnica 1596944.</p> <p>Para obtener la información más reciente sobre el tamaño de la base de datos, la reorganización de base de datos y consideraciones de rendimiento para servidores IBM Spectrum Protect, consulte la nota técnica 1683633.</p> <p>Para obtener información sobre cómo establecer la variable <code>DB2_PARALLEL_IO</code>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
<p>¿Son todos los directorios de la base de datos del mismo tamaño?</p>	<p>Los directorios que son del mismo tamaño garantizan un grado de paralelismo coherente para las operaciones de la base de datos. Si hay uno varios directorios en la base de datos que son más pequeños que el resto, reducirán el potencial para la captación previa paralela optimizada.</p> <p>Esta indicación se aplica también si es necesario añadir vías de acceso de almacenamiento tras la configuración inicial del servidor.</p>	
<p>¿Tiene pensado elevar la profundidad de cola de los LUN de base de datos en sistemas AIX?</p>	<p>La profundidad de cola predeterminada suele ser demasiado baja.</p>	<p>Consulte Configuración de sistemas AIX para rendimiento del disco.</p>

## Windows: Planificación de discos de registro de recuperación del servidor

Utilice la lista de comprobación para verificar que el sistema donde está instalado el servidor cumpla con los requisitos para la configuración de hardware y software.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------



Pregunta	Tareas, características, opciones o valores	Más información
¿Están el registro activo y el registro de archivado almacenados en discos o en LUN separados de los que se utilizan para los volúmenes de agrupación de almacenamiento y las bases de datos?	Asegúrese de que los discos donde se coloca el registro activo no se utilicen para otras funciones del servidor o el sistema. No coloque el registro activo en discos que contengan la base de datos del servidor, el registro de archivado ni los archivos del sistema, como un espacio de intercambio o página.	La separación de la base de datos del servidor, el registro activo y el registro de archivado ayuda a reducir los conflictos para los mismos recursos entre distintas operaciones que deben ejecutarse al mismo tiempo.
¿Se encuentran los registros en discos con memoria caché de escritura no volátil?	La memoria caché de escritura no volátil permite que se escriban datos en los registros lo más rápido posible. Operaciones de escritura más rápidas para los registros pueden mejorar el rendimiento de las operaciones de servidor.	
¿Está estableciendo los registros en un tamaño que dé el soporte adecuado para la carga de trabajo?	Si no está seguro sobre la carga de trabajo, utilice el tamaño más grande que pueda.  Registro activo El tamaño máximo es de 512 GB, definido con la opción de servidor ACTIVELOGSIZE.  Asegúrese de que existan al menos 8 GB de espacio libre en el sistema de archivos de registro activos después de crear los registros activos de tamaño fijo.  Registro de archivos El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que el registro de archivado tiene al menos el mismo tamaño que el registro activo.	<ul style="list-style-type: none"> <li>Para obtener detalles de dimensionamiento, consulte la información del registro de recuperación en la nota técnica 1421060.</li> <li>Para obtener información sobre dimensionamiento al utilizar la deduplicación de datos, consulte Lista de comprobación para la optimización de almacenamiento de datos.</li> </ul>
¿Ha definido un registro de migración tras error de archivado? ¿Está colocando este registro en un disco que sea independiente al registro de archivado?	El registro de migración tras error de archivado lo utilizará el servidor, en casos de emergencia, si el registro de archivado se llena. Se pueden utilizar discos más lentos para el registro de migración tras error de archivado.	Utilice la opción del servidor ARCHFAILOVERLOGDIRECTORY para especificar la ubicación del registro de migración tras error de archivado.  Supervise el uso del directorio del registro de migración tras error de archivado. Si el servidor tiene que utilizar el registro de migración tras error de archivado, es posible que el espacio del registro de archivado no sea lo suficientemente grande.
Si está duplicando el registro activo, ¿está utilizando un solo tipo de duplicación?	Puede duplicar el registro utilizando uno de los métodos siguientes. Utilice solo un tipo de duplicación para el registro. <ul style="list-style-type: none"> <li>Utilice la opción MIRRORLOGDIRECTORY disponible para el servidor de IBM Spectrum Protect para especificar una ubicación para la duplicación.</li> <li>Utilice la duplicación de software, como el gestor de volúmenes lógicos (LVM) en AIX.</li> <li>Utilice la duplicación en el hardware del sistema de disco.</li> </ul>	Si duplica el registro activo, asegúrese de que los discos del registro activo y la copia de duplicado tienen la misma velocidad y fiabilidad.  Para obtener más información, consulte Configuración y ajuste del registro de recuperación.

## Windows: Planificación de agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios

Revise cómo están configuradas las agrupaciones de almacenamiento de contenedores de nubes y contenedores de directorios para garantizar un rendimiento óptimo.

Pregunta	Tareas, características, opciones o valores	Más información
<p>Medido en términos de operaciones de entrada/salida por segundo (IOPS), ¿utiliza almacenamiento de disco rápido para la base de datos de IBM Spectrum Protect?</p>	<p>Utilice un disco de alto rendimiento para la base de datos. Utilice tecnología de unidad de estado sólido para el proceso de deduplicación de datos.</p> <p>Asegúrese de que la base de datos tiene una capacidad mínima de 3000 IOPS. Por cada TB de datos al que realice copia de seguridad diariamente (antes de la deduplicación de datos), añada 1000 IOPS a este mínimo.</p> <p>Por ejemplo, un servidor IBM Spectrum Protect que ingiera 3 TB de datos al día necesitaría 6000 IOPS para los discos de la base de datos:</p> $\text{mínimo de 3000 IOPS} + 3000 (3 \text{ TB} \times 1000 \text{ IOPS}) = 6000 \text{ IOPS}$	<p>Para recomendaciones sobre la selección de discos, consulte "Planificación de discos de base de datos del servidor".</p> <p>Para obtener más información sobre IOPS, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Tiene suficiente memoria para el tamaño de su base de datos?</p>	<p>Utilice un mínimo de 40 GB de memoria del sistema para los servidores IBM Spectrum Protect, con un tamaño de base de datos de 100 GB, que estén deduplicando datos. Si la capacidad retenida de los datos de copia de seguridad aumenta, el requisito de memoria podría tener que ser mayor.</p> <p>Supervise el uso de la memoria de forma regular para determinar si se necesita más memoria.</p> <p>Utilice más memoria del sistema para mejorar el almacenamiento en caché de páginas de bases de datos. Las siguientes directrices de tamaño de memoria se basan en la cantidad diaria de datos nuevos de los que se realiza una copia de seguridad:</p> <ul style="list-style-type: none"> <li>• 128 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 1 - 2 TB</li> <li>• 192 GB de memoria del sistema para copias de seguridad diarias de los datos, allí donde el tamaño de la base de datos sea 2 - 4 TB</li> </ul>	<p>Requisitos de memoria</p>

Pregunta	Tareas, características, opciones o valores	Más información
<p>¿Ha dimensionado correctamente la capacidad de almacenamiento para el registro activo y el registro de archivado de la base de datos?</p>	<p>Configure el servidor para que tenga un tamaño de registro activo mínimo de 128 GB estableciendo la opción de servidor ACTIVELOGSIZE en un valor de 131072.</p> <p>El tamaño de inicio sugerido para el registro de archivado es 1 TB. El tamaño del registro de archivado está limitado por el tamaño del sistema de archivos en el que está ubicado, no por una opción del servidor. Asegúrese de que haya al menos un 10% de espacio de disco adicional respecto al tamaño del registro de archivado para el sistema de archivos.</p> <p>Utilice un directorio para los registros de archivado de base de datos con una capacidad libre inicial de al menos 1 TB. Especifique el directorio utilizando la opción de servidor ARCHLOGDIRECTORY.</p> <p>Defina el espacio para el registro de migración tras error utilizando la opción de servidor ARCHFAILOVERLOGDIRECTORY.</p>	<p>Para obtener más información sobre el dimensionamiento del sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Está habilitada la compresión para el registro de archivado y las copias de seguridad de la base de datos?</p>	<p>Habilite la opción de servidor ARCHLOGCOMPRESS para ahorrar espacio de almacenamiento.</p> <p>Esta opción de compresión es diferente de la compresión en línea. La compresión en línea está habilitada de forma predeterminada con IBM Spectrum Protect V7.1.5 y posteriores.</p> <p>Restricción: No utilice esta opción si la cantidad de datos a los que se hace copia de seguridad supera los 6 TB al día.</p>	<p>Para obtener más información sobre compresión para el sistema, consulte IBM Spectrum Protect Blueprints.</p>
<p>¿Están los registros y la base de datos de IBM Spectrum Protect en volúmenes de disco separados (LUN)?</p> <p>¿Se ha configurado el disco que se utiliza para la base de datos de acuerdo con los métodos recomendados de una base de datos transaccional?</p>	<p>La base de datos no debe compartir los volúmenes de disco con agrupaciones de almacenamiento o registros de base de datos de IBM Spectrum Protect, o con cualquier otro sistema de archivos o aplicación.</p>	<p>Para obtener información sobre configuración del registro de recuperación y la base de datos del servidor, consulte Configuración y ajuste del registro de recuperación y la base de datos del servidor.</p>
<p>¿Está utilizando un mínimo de ocho núcleos (2,2 GHz o equivalente) para cada servidor de IBM Spectrum Protect que tenga pensado utilizar con deduplicación de datos?</p>	<p>Si tiene pensado utilizar la deduplicación de datos del lado del cliente, compruebe que los sistemas cliente tengan suficientes recursos disponibles durante una operación de copia de seguridad para completar el procesamiento de deduplicación de datos. Utilice un procesador que tenga al menos el mínimo equivalente a un núcleo de procesador de 2,2 GHz por proceso de copia de seguridad con la eliminación de datos duplicados del lado del cliente.</p>	<ul style="list-style-type: none"> <li>• Planificación y uso eficaces de la deduplicación</li> <li>• IBM Spectrum Protect Blueprints</li> </ul>

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha asignado suficiente espacio de almacenamiento para la base de datos?	<p>Para obtener una estimación aproximada, planifique 100 GB de almacenamiento de base de datos por cada 50 TB de datos que se protejan en las agrupaciones de almacenamiento deduplicadas. <i>Datos protegidos</i> es la cantidad de datos antes de la deduplicación, incluidas todas las versiones de objetos almacenados.</p> <p>Como práctica recomendada, defina una nueva agrupación de almacenamiento de contenedores exclusivamente para deduplicación de datos. La eliminación de duplicados de datos se lleva a cabo en el nivel de la agrupación de almacenamiento y se eliminan todos los datos duplicados de una agrupación de almacenamiento, excepto los datos cifrados.</p>	
¿Ha calculado la capacidad de almacenamiento para configurar el espacio suficiente para el tamaño de su entorno?	<p>Puede calcular los requisitos de capacidad de una agrupación de almacenamiento deduplicado utilizando la siguiente técnica:</p> <ol style="list-style-type: none"> <li>1. Calcule el tamaño de la base de los datos de origen.</li> <li>2. Calcule el tamaño de la copia de seguridad diaria utilizando un cambio estimado y la tasa de crecimiento.</li> <li>3. Determine los requisitos de retención.</li> <li>4. Calcule la cantidad total de datos de origen mediante la factorización en el tamaño de la base, el tamaño de la copia de seguridad diaria y los requisitos de retención.</li> <li>5. Aplique el factor de ratio de deduplicación.</li> <li>6. Aplique el factor de proporción de la optimización de almacenamiento.</li> <li>7. Redondee el cálculo para tener en cuenta la utilización de la agrupación de almacenamiento.</li> </ol>	Para ver un ejemplo sobre el uso de esta técnica, consulte el apartado Planificación y uso eficaces de la deduplicación.

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha distribuido muchas E/S de disco en muchos dispositivos y controladores de disco?	<p>Utilice matrices con tantos discos como sea posible, a lo que en ocasiones se denomina escritura en bandas amplia. Asegúrese de que utiliza un directorio de base de datos por cada matriz en el subsistema. .</p> <p>Establezca la variable de registro <i>DB2_PARALLEL_IO</i> para habilitar la E/S paralela para cada espacio de tabla utilizado si los contenedores del espacio de tabla abarcan varios discos físicos.</p> <p>Cuando el ancho de banda de E/S está disponible y los archivos son grandes, por ejemplo de 1 MB, el proceso de encontrar duplicados puede ocupar los recursos de todo un procesador. Cuando los archivos son más pequeños, pueden producirse otros cuellos de botella.</p> <p>Especifique ocho o más sistemas de archivos para la clase de dispositivo de agrupación de almacenamiento deduplicada para que la E/S se distribuya por tantos LUN y dispositivos físicos como sea posible.</p>	<p>Para obtener directrices sobre cómo configurar agrupaciones de almacenamiento, consulte "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE".</p> <p>Para obtener información sobre cómo establecer la variable <i>DB2_PARALLEL_IO</i>, consulte Configuración recomendada para variables de registro de IBM DB2.</p>
¿Ha planificado las operaciones diarias en función de su estrategia de copia de seguridad?	<p>La secuencia recomendada de operaciones está en el siguiente orden:</p> <ol style="list-style-type: none"> <li>1. Copia de seguridad del cliente</li> <li>2. Protección de agrupaciones de almacenamiento</li> <li>3. Réplica de nodo</li> <li>4. Copia de seguridad de base de datos</li> <li>5. Caducar inventario</li> </ol>	<ul style="list-style-type: none"> <li>• Planificación de los procesos de optimización de almacenamiento de datos y réplica de nodo</li> <li>• Operaciones diarias para agrupaciones de almacenamiento de contenedores de directorio</li> </ul>
¿Tiene suficiente almacenamiento para gestionar la lista de bloqueo de DB2?	<p>Si deduplica datos que incluyan grandes archivos o grandes números de archivos simultáneamente, el proceso podría producir espacio de almacenamiento insuficiente. Si el almacenamiento de la lista de bloqueos es insuficiente, pueden producirse errores de copia de seguridad, errores de proceso de gestión de datos o caídas de servidor.</p> <p>Los tamaños de archivo superiores a 500 GB que se procesen por deduplicación de datos tienen más probabilidad de agotar el espacio de almacenamiento. No obstante, si muchas operaciones de copia de seguridad utilizan deduplicación de datos del lado del cliente, este problema también puede producirse con archivos de tamaño más pequeño.</p>	<p>Para obtener más información sobre cómo ajustar el parámetro de DB2 LOCKLIST, consulte Ajuste de la eliminación de datos duplicados del lado del cliente.</p>

Pregunta	Tareas, características, opciones o valores	Más información
¿Hay suficiente ancho de banda disponible para transferir datos a un servidor IBM Spectrum Protect?	<p>Para transferir datos a un servidor IBM Spectrum Protect, utilice la compresión y deduplicación del lado del cliente o del lado del servidor para reducir el ancho de banda que sea necesario.</p> <p>Utilice un servidor versión 7.1.5 o superior para utilizar la compresión en línea o un cliente versión 7.1.6 o posterior para habilitar el procesamiento de compresión mejorada.</p>	Para obtener más información, consulte la opción de cliente enablededup.
¿Ha determinado cuántos directorios de agrupación de almacenamiento asignar a cada agrupación de almacenamiento?	<p>Asigne directorios a una agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY.</p> <p>Cree varios directorios de agrupación de almacenamiento y asegúrese de que se haya realizado una copia de seguridad de cada directorio en un volumen de disco (LUN) independiente.</p>	
¿Ha asignado suficiente espacio de disco en la agrupación de almacenamiento de contenedor de nube?	<p>Para impedir anomalías de copia de seguridad, asegúrese de que el directorio local tiene suficiente espacio. Utilice la siguiente lista como guía para el espacio de disco óptimo:</p> <ul style="list-style-type: none"> <li>• Para disco SCSI con conexión en serie (SAS) y giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad, en terabytes, para el espacio de disco.</li> <li>• Proporcione 3 TB para sistemas de almacenamiento basadas en flash con conexiones de red rápidas a sistemas en nube locales de alto rendimiento.</li> <li>• Proporcione 5 TB para sistemas de unidad de estado sólido (SSD) con conexiones de red rápidas a sistemas en nube de alto rendimiento.</li> </ul>	

Pregunta	Tareas, características, opciones o valores	Más información
¿Ha seleccionado el tipo apropiado de almacenamiento local?	<p>Asegúrese de que las transferencias de datos del almacenamiento local a nube finalizan antes de que se inicie el siguiente ciclo de copia de seguridad.</p> <p>Consejo: Los datos se eliminan del almacenamiento local poco después de que se hayan movido a la nube.</p> <p>Utilice las directrices siguientes:</p> <ul style="list-style-type: none"> <li>• Utilice flash o SSD para sistemas grandes que tienen sistemas en nube de alto rendimiento. Asegúrese de tener un enlace de red de área amplia (WAN) dedicada de 10 GB con una conexión de alta velocidad al almacenamiento de objeto. Por ejemplo, utilice flash o SSD si tiene un enlace WAN dedicado de 10 GB más una conexión de alta velocidad a una ubicación de IBM® Cloud Object Storage o a un centro de datos de Amazon Simple Storage Service (Amazon S3).</li> <li>• Utilice discos SAS de 15000 rpm de mayor capacidad para estos escenarios: <ul style="list-style-type: none"> <li>◦ Sistemas de tamaño medio</li> <li>◦ Conexiones de tipo nube más lentas, por ejemplo 1 GB</li> <li>◦ Cuando utilice IBM Cloud Object Storage como proveedor de servicios en varias regiones</li> </ul> </li> <li>• Para el disco SAS o giratorio, calcule la cantidad de datos nuevos que se esperan después de la reducción de datos diaria (compresión y deduplicación de datos). Como máximo asigne el 100 por cien de esa cantidad para el espacio de disco, en terabytes.</li> </ul>	

## Windows: Planificación para agrupaciones de almacenamiento en clases de dispositivo DISK o FILE

Utilice la lista de comprobación para revisar cómo están configuradas las agrupaciones de almacenamiento de disco. Esta lista de comprobación incluye consejos para agrupaciones de almacenamiento que utilicen clases de dispositivo DISK o FILE.

Pregunta	Tareas, características, opciones o valores	Más información
----------	---	-----------------

Pregunta	Tareas, características, opciones o valores	Más información
¿Pueden los LUN de agrupación de almacenamiento mantener las tasas de rendimiento durante 256 KB de lecturas y grabaciones secuenciales para gestionar adecuadamente la carga de trabajo sin las restricciones de tiempo?	<p>Si está planificando las cargas máximas, tenga en cuenta todos los datos que quiere que el servidor lea o escriba simultáneamente en las agrupaciones de almacenamiento de disco. Por ejemplo, tenga en cuenta el flujo de datos máximo de las operaciones de seguridad del cliente y las operaciones de movimiento de datos del servidor, como la migración que se ejecuta al mismo tiempo.</p> <p>El servidor de IBM Spectrum Protect lee y escribe en las agrupaciones de almacenamiento, normalmente en bloques de 256 KB.</p> <p>Si el sistema de disco incluye la capacidad, configure el sistema de disco para conseguir un rendimiento óptimo con operaciones de lectura/escritura secuenciales, en lugar de operaciones de lectura/escritura aleatorias.</p>	Para obtener más información, consulte Análisis del rendimiento básico de sistemas de disco.
¿Se ha configurado el disco para utilizar la memoria caché de escritura y lectura?	Utilice más memoria caché para un mejor rendimiento.	
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha determinado un tamaño adecuado que utilizar con los volúmenes de agrupación de almacenamiento?	Revise la información del apartado Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos. Si no tiene la información necesaria como para estimar un tamaño para los volúmenes de clase de dispositivo FILE, empiece por volúmenes que sean de 50 GB.	Normalmente, aparecen más problemas cuando los volúmenes son demasiado pequeños. Se notifican pocos problemas si los volúmenes son más grandes de lo necesario. Al determinar el tamaño de volumen que utilizar, como precaución, elija un tamaño que pueda ser más grande de lo necesario.
Para las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿está utilizando volúmenes asignados previamente?	<p>Los volúmenes reutilizables pueden provocar la fragmentación de archivos.</p> <p>Para asegurarse de que una agrupación de almacenamiento no se queden sin volúmenes, defina el parámetro MAXSCRATCH en un valor superior que cero.</p>	<p>Utilice el mandato de servidor DEFINE VOLUME para preasignar volúmenes en la agrupación de almacenamiento.</p> <p>Utilice el mandato de servidor DEFINE STGPOOL o UPDATE STGPOOL para definir el parámetro MAXSCRATCH.</p>
Para agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, ¿ha comparado el máximo de sesiones de cliente con el número de volúmenes definido?	Mantenga siempre suficientes volúmenes utilizables en las agrupaciones de almacenamiento como para permitir la ejecución simultánea del número máximo esperado de sesiones de cliente. Pueden ser volúmenes reutilizables, volúmenes vacíos o volúmenes llenados en parte.	Para aquellas agrupaciones de almacenamiento que utilicen las clases de dispositivo FILE, solo una sesión o un proceso pueden escribir en un volumen al mismo tiempo.



Pregunta	Tareas, características, opciones o valores	Más información
<p>En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, ¿ha definido el parámetro MOUNTLIMIT de la clase de dispositivo en un valor suficiente como para hacerse cargo del número de volúmenes que se pueden montar en paralelo?</p>	<p>En el caso de las agrupaciones de almacenamiento que utilizan la optimización de almacenamiento de datos, el parámetro MOUNTLIMIT suele estar en el rango 500 - 1000.</p> <p>Defina el valor de MOUNTLIMIT con el número máximo de puntos de montaje necesarios para todas las sesiones activas. Tenga en cuenta los parámetros que afectan a la cantidad máxima de puntos de montaje necesarios:</p> <ul style="list-style-type: none"> <li>• La opción de servidor MAXSESSIONS, que es el número máximo de sesiones de IBM Spectrum Protect que se pueden ejecutar de forma simultánea.</li> <li>• El parámetro MAXNUMMP, que define el número máximo de puntos de montaje que puede utilizar cada nodo de cliente.</li> </ul> <p>Por ejemplo, si el número máximo de sesiones de copia de seguridad del nodo de cliente es normalmente 100 y cada uno de los nodos tiene MAXNUMMP=2, multiplique 100 nodos por los 2 puntos de montaje para cada nodo para obtener un valor de 200 para el parámetro MOUNTLIMIT.</p>	<p>Utilice el mandato de servidor REGISTER NODE o UPDATE NODE para definir el parámetro MAXNUMMP para los nodos de cliente.</p>
<p>En el caso de agrupaciones de almacenamiento que utilizan clases de dispositivo DISK, ¿ha determinado cuántos volúmenes de agrupación de almacenamiento se colocarán en cada sistema de archivos?</p>	<p>La manera en la que configura el almacenamiento de una agrupación de almacenamiento que utiliza una clase de dispositivo DISK depende de si está utilizando RAID para el sistema de disco.</p> <p>Si no está utilizando RAID, configure un sistema de archivos por disco físico y defina un volumen de agrupación de almacenamiento para cada sistema de archivos.</p> <p>Si está utilizando RAID 5 con volúmenes <math>n+1</math>, configure el almacenamiento de una de las siguientes maneras:</p> <ul style="list-style-type: none"> <li>• Configure los sistemas de archivos <math>n</math> en el LUN y defina un volumen de agrupación de almacenamiento por sistema de archivos.</li> <li>• Configure un sistema de archivos y volúmenes de agrupación de almacenamiento <math>n</math> para el LUN.</li> </ul>	<p>Para ver un diseño de ejemplo que sigue esta directriz, consulte la Diseño de ejemplo de las agrupaciones de almacenamiento del servidor.</p>
<p>¿Ha creado las agrupaciones de almacenamiento con el fin de distribuir la entrada/salida en distintos sistemas de archivos?</p>	<p>Asegúrese de que cada sistema de archivos se encuentre en un LUN distinto en el sistema de disco.</p> <p>Normalmente, contar con 10 - 30 sistemas de archivos es un buen objetivo, pero asegúrese de que los sistemas de archivos no son inferiores a aproximadamente 250 GB.</p>	<p>Para obtener detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>• Ajuste del almacenamiento de disco para el servidor</li> <li>• Ajuste y configuración de los volúmenes y las agrupaciones de almacenamiento</li> </ul>

## Windows: Planificación del tipo correcto de tecnología de almacenamiento

Los dispositivos de almacenamiento tienen diferente capacidad y diferentes características de rendimiento. Estas características influyen en qué dispositivos son los más adecuados para utilizarlos con IBM Spectrum Protect.

### Procedimiento

Revise la siguiente tabla para elegir el tipo correcto de tecnología de almacenamiento para los recursos de almacenamiento que requiere el servidor.

Tabla 1. Tipos de tecnología de almacenamiento para requisitos de almacenamiento de IBM Spectrum Protect

<b>Tipo de tecnología de almacenamiento</b>	<b>Base de datos</b>	<b>Registro activo</b>	<b>Registro de archivado y registro de migración tras error de archivado</b>	<b>Agrupaciones de almacenamiento</b>
<b>Unidad de estado sólido (SSD)</b>	<p>Coloque la base de datos en SSD en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Utiliza deduplicación de datos de IBM Spectrum Protect.</li> <li>• Realiza copia de seguridad de más de 8 TB de datos nuevos al día.</li> </ul>	<p>Si coloca la base de datos de IBM Spectrum Protect en una SSD, como práctica recomendada, coloque el registro activo en una SSD. Si no hay espacio disponible, utilice el disco de alto rendimiento.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. El registro de archivado y los registros de migración tras error de archivado se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>	<p>Guarde las SSD para uso con el registro activo y la base de datos. Las agrupaciones de almacenamiento se pueden ubicar en tipos de tecnología de almacenamiento más lentos.</p>
<p><b>Disco de alto rendimiento con las siguientes características:</b></p> <ul style="list-style-type: none"> <li>• Disco de 15.000 rpm</li> <li>• Interfaz Fibre Channel o SCSI con conexión en serie (SAS)</li> </ul>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.</p>	<p>Utilice discos de alto rendimiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• El servidor no realiza deduplicación de datos.</li> <li>• El servidor no realiza replicación de nodo.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.</p>	<p>Puede utilizar discos de alto rendimiento para el registro de archivado y los registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.</p>	<p>Utilice discos de alto rendimiento para agrupaciones de almacenamiento en las siguientes circunstancias:</p> <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> <p>Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.</p>

Tipo de tecnología de almacenamiento	Base de datos	Registro activo	Registro de archivado y registro de migración tras error de archivado	Agrupaciones de almacenamiento
<b>Disco de rendimiento medio o de alto rendimiento en las siguientes circunstancias:</b> <ul style="list-style-type: none"> <li>• Disco de 10.000 rpm</li> <li>• Interfaz Fibre Channel o SAS</li> </ul>	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Separe la base de datos del servidor de sus registros y agrupaciones de almacenamiento, así como de los datos de otras aplicaciones.	Si el sistema de discos combina varias tecnologías, utilice los discos más rápidos para la base de datos y registro activo. Por cuestiones de rendimiento y disponibilidad, aisle el registro activo de la base de datos del servidor, registros de archivado y agrupaciones de almacenamiento.	Puede utilizar el disco de medio o alto rendimiento para el registro de archivado y registros de migración tras error de archivado. Por cuestiones de disponibilidad, aisle estos registros de la base de datos y registro activo.	Utilice disco de rendimiento medio o rendimiento alto para agrupaciones de almacenamiento en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se leen con frecuencia.</li> <li>• Los datos se escriben con frecuencia.</li> </ul> Por cuestiones de rendimiento y disponibilidad, aisle los datos de las agrupaciones de almacenamiento de la base de datos y registros del servidor, así como de los datos de otras aplicaciones.
<b>SATA, almac. adjunto de red</b>	No utilice este almacenamiento para la base de datos. No coloque la base de datos en sistemas de almacenamiento XIV.	No utilice este almacenamiento para el registro activo.	El uso de la tecnología de almacenamiento más lenta es aceptable porque estos registros se escriben una vez y no se leen con frecuencia.	Utilice esta tecnología de almacenamiento más lenta en las siguientes circunstancias: <ul style="list-style-type: none"> <li>• Los datos se escriben con poca frecuencia, por ejemplo, se escriben una vez.</li> <li>• Los datos se leen con poca frecuencia.</li> </ul>
<b>Cinta y cinta virtual</b>				Utilícela para la retención a largo plazo o si los datos se utilizan con poca frecuencia.

## Windows: Aplicación de prácticas recomendadas para la instalación del servidor

Normalmente, la configuración y selección del hardware tienen el efecto más importante en el rendimiento de una solución IBM Spectrum Protect. Otros factores que pueden afectar al rendimiento son la selección y configuración del sistema operativo, así como la configuración de IBM Spectrum Protect.

### Procedimiento

- Las siguientes prácticas recomendadas son lo más importante para que se dé un rendimiento óptimo y para evitar problemas.
- Revise la tabla que determina las mejores prácticas que se aplican a su entorno.

Práctica recomendada	Más información
----------------------	-----------------

<b>Práctica recomendada</b>	<b>Más información</b>
<p>Utilice discos rápidos para la base de datos de servidor. Los discos de estado sólido (SSD) de tipo empresarial, con interfaz SAS o de canal de fibra, ofrecen el mejor rendimiento.</p>	<p>Utilice discos rápidos de baja latencia para la base de datos. El uso de SSD es esencial si utiliza la deduplicación de datos y la réplica de nodo. No utilice discos de conector de tecnología avanzada en serie (SATA) o conector de tecnología avanzada en paralelo (PATA). Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación del tipo correcto de tecnología de almacenamiento"</li> </ul>
<p>Asegúrese de que el sistema del servidor tiene memoria suficiente.</p>	<p>Revise los requisitos del sistema operativo en la nota técnica 1243309. Las cargas de trabajo más pesadas requieren más requisitos que los mínimos. Las funciones avanzadas, como la optimización de almacenamiento de datos y la réplica de nodo, pueden requerir algo más que la memoria mínima especificada en el documento de requisitos de sistema.</p> <p>Si desea ejecutar varias instancias, cada instancia necesita la memoria que figura para un servidor. Multiplique la memoria para un servidor por el número de instancias planificadas para el sistema.</p>
<p>Separe la base de datos de servidor, el registro activo, el registro de archivado y las agrupaciones de almacenamiento de disco entre sí.</p>	<p>Guarde todos los recursos de almacenamiento de IBM Spectrum Protect en discos diferentes. Mantenga los discos de agrupación de almacenamiento separados de los discos de la base de datos y registros del servidor. Las operaciones de la agrupación de almacenamiento pueden interferir con las operaciones de bases de datos si ambas se encuentran en los mismos discos. Lo ideal sería que los registros y la base de datos del servidor estuviesen también separados entre ellos. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o "Planificación de discos de base de datos del servidor"</li> <li>o "Planificación de discos de registro de recuperación del servidor"</li> <li>o "Planificación de agrupaciones de almacenamiento en clases de dispositivo DISK o FILE"</li> </ul>
<p>Utilice al menos cuatro directorios para la base de datos de servidor. Para servidores más grandes o servidores que utilicen características avanzadas, utilice ocho directorios.</p>	<p>Coloque cada directorio en un LUN aislado del resto de las LUN y aplicaciones.</p> <p>Un servidor se considera grande si su base de datos es superior a 2 TB o se espera que alcance ese tamaño. Para dichos servidores, utilice ocho directorios.</p> <p>Consulte "Planificación para discos de base de datos de servidor".</p>
<p>Si utiliza la deduplicación de datos, la réplica de nodo, o ambas, siga las directrices indicadas a continuación para la configuración de la base de datos y otros elementos.</p>	<p>Configure la base de datos del servidor de acuerdo con las directrices, ya que la base de datos es extremadamente importante para saber cómo se ejecuta el servidor cuando se utilizan estas características. Para obtener información y otras sugerencias, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>o Lista de comprobación para la optimización de almacenamiento de datos</li> <li>o Lista de comprobación para la réplica de nodo</li> </ul>

Práctica recomendada	Más información
En el caso de las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE, siga las directrices sobre tamaño de los volúmenes de la agrupación de almacenamiento. Normalmente, los volúmenes de 50 GB son los mejores.	<p>Revise la información de Número y tamaño de volumen óptimo para las agrupaciones de almacenamiento que utilizan discos para que le ayude a determinar el tamaño de volumen.</p> <p>Configure los dispositivos de agrupación de almacenamiento y los sistemas de archivos basándose en los requisitos de rendimiento, no solo en los de capacidad.</p> <p>Aísle los dispositivos de almacenamiento utilizados por IBM Spectrum Protect de otras aplicaciones con E/S altas y asegúrese de que el rendimiento del almacenamiento es adecuado.</p> <p>Para conocer más detalles, consulte Lista de comprobación de agrupaciones de almacenamiento en DISK o FILE.</p>
Planifique las actividades de mantenimiento del servidor y las operaciones de clientes de IBM Spectrum Protect para evitar o minimizar el solapamiento de las operaciones.	<p>Para obtener más detalles, consulte los temas siguientes:</p> <ul style="list-style-type: none"> <li>○ Ajuste de la planificación para las operaciones diarias</li> <li>○ Lista de comprobación para la configuración de servidor</li> </ul>
Supervise las operaciones de forma constante.	<p>Supervisando las operaciones, puede detectar problemas e identificar las causas de manera más fácil y temprana. Realice registros de los informes de supervisión de todo un año como ayuda para identificar tendencias y planificar el crecimiento. Consulte el apartado Supervisión y mantenimiento del entorno para mejorar el rendimiento.</p>

## Windows: Requisitos mínimos del sistema para sistemas Windows

El servidor puede requerir una gran cantidad de memoria, ancho de banda de red y recursos de procesador. En muchos casos, el servidor funciona mejor cuando las otras aplicaciones no están instaladas en el mismo sistema.

## Requisitos de software y de hardware de la instalación del servidor de IBM Spectrum Protect

Estas tablas muestran los requisitos mínimos de hardware y software para la instalación de un servidor de IBM Spectrum Protect. Utilice estos requisitos como punto de partida para sistemas sin deduplicación de datos. El entorno óptimo de IBM Spectrum Protect se configura con deduplicación de datos, utilizando IBM Spectrum Protect Blueprints. Para obtener la información más actualizada sobre los requisitos del sistema, consulte la nota técnica 1243309.

## Requisitos de hardware

Tabla 1 describe los requisitos mínimos de hardware para el servidor. Si el servidor no cumple los requisitos mínimos, la instalación falla. Para obtener más información sobre la planificación del espacio de disco, consulte el apartado Windows: Planificación de la capacidad.

Tabla 1. Requisitos de hardware

Tipo de hardware	Requisitos de hardware
Hardware	Un procesador AMD64 o Intel EMT-64

Tipo de hardware	Requisitos de hardware
Espacio de disco	<p>Los siguientes valores de espacio mínimo de disco:</p> <ul style="list-style-type: none"> <li>• Al menos, 7,5 GB de almacenamiento de disco libre para una instalación típica</li> <li>• 60 MB en el espacio de directorio temporal</li> <li>• Una partición de 2 GB en la unidad C:\</li> <li>• 300 MB en el directorio de instancias</li> <li>• 2 GB para el área de recursos compartidos</li> </ul> <p>Si surge un problema y se necesita algún diagnóstico, es óptimo tener espacio temporal o de otro tipo disponible en el sistema para el registro FFDC (First Failure Data Capture) o para otros usos temporales como el de recopilación de registros de rastreo.</p> <p>Puede hacer falta más espacio para los archivos de registro y de la base de datos. El tamaño de la base de datos depende del número de archivos de cliente que deben almacenarse y de cómo los gestiona el servidor. El espacio de registro activo predeterminado es de 16 GB, el mínimo que se necesita para la mayoría de las cargas de trabajo y configuraciones. Cuando se crea el registro activo, se necesita como mínimo 64 GB para ejecutar la réplica. Si se están usando réplica y deduplicación, cree un registro activo de 128 GB. Asigne al menos el triple del espacio de registro activo predeterminado para el registro de archivado (48 GB). Asegúrese de disponer de recursos suficientes si está utilizando la eliminación de datos duplicados o tiene prevista una gran carga de trabajo de cliente.</p> <p>Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.</p> <p>Asegúrese de consultar la sección Windows: Planificación de la capacidad para obtener más detalles sobre el espacio de disco.</p>
Memoria	<p>Los siguientes valores mínimos para la memoria:</p> <ul style="list-style-type: none"> <li>• 16 GB para operaciones de servidor estándar sin deduplicación de datos y réplica de nodo</li> <li>• 24 GB para deduplicación de datos y réplica de nodo</li> <li>• 32 GB para réplica de nodo con deduplicación de datos</li> </ul> <p>Para conocer detalles de memoria específicos para bases de datos de mayor tamaño y una funcionalidad de ingestión superior, consulte la Tabla de ajuste de memoria del servidor IBM Spectrum Protect.</p> <p>Para obtener requisitos de memoria más específicos cuando está utilizando la deduplicación de datos, consulte el IBM Spectrum Protect Blueprint para su sistema operativo.</p>

## Requisitos de software

Tabla 2 describe los requisitos mínimos de software necesarios para un servidor en un sistema Windows.

Tabla 2. Requisitos de software

Tipo de software	Requisitos mínimos de software
Sistema operativo	<p>Uno de los siguientes sistemas operativos:</p> <ul style="list-style-type: none"> <li>• Microsoft Windows Server 2012: Standard, Enterprise o Datacenter Edition (64 bits)</li> <li>• Microsoft Windows Server 2012 R2 (64 bits)</li> <li>• Microsoft Windows Server 2016</li> </ul>
Protocolo de comunicaciones	<p>Al menos uno de los siguientes protocolos de comunicación (instalado de forma predeterminada con los sistemas operativos Windows actuales):</p> <ul style="list-style-type: none"> <li>• Named Pipes</li> <li>• TCP/IP Versión 4 o Versión 6</li> </ul>

Tipo de software	Requisitos mínimos de software
Controladores de dispositivo	<p>El controlador de dispositivo de paso directo IBM Spectrum Protect que se requiere para dispositivos y bibliotecas de cintas que no sean de IBM®. El controlador de dispositivos nativo de Windows se recomienda para las bibliotecas de cintas y controladores de cintas. De lo contrario, se puede usar el controlador de dispositivo kernel IBM Spectrum Protect.</p> <p>Para IBM 3590, 3592 o los controladores o biblioteca de cintas Ultrium, son necesarios los controladores de dispositivo IBM. Instale los controladores de dispositivos más actuales. Puede localizar paquetes de controladores IBM en Fix Central.</p> <p>Configure los controladores de dispositivo antes de utilizar el servidor con dispositivos de cinta.</p>
Otro software	<p>Windows 2012, Windows 2012 R2 y Windows 2016 requieren que .NET Framework 3.5 esté instalado y habilitado.</p> <p>Se deben desactivar las siguientes políticas de Control de la cuenta de usuario:</p> <ul style="list-style-type: none"> <li>• Control de la cuenta de usuario: modo de aprobación de administrador para la cuenta de administrador integrada</li> <li>• Control de la cuenta de usuario: ejecute todos los administradores en el modo de aprobación de administrador</li> </ul> <p>Para autenticar los usuarios de IBM Spectrum Protect con un servidor LDAP (Lightweight Directory Access Protocol), debe utilizar uno de los servidores de directorio siguientes:</p> <ul style="list-style-type: none"> <li>• Microsoft Active Directory (Windows Server 2012, Windows Server 2012 R2)</li> <li>• IBM Security Directory Server V6.3</li> <li>• IBM Security Directory Server V6.4</li> </ul>

## Windows: IBM Installation Manager

IBM Spectrum Protect utiliza IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager aún no está instalada, se instala o actualiza automáticamente cuando se instala IBM Spectrum Protect. Debe permanecer instalada en el sistema de manera que IBM Spectrum Protect se pueda actualizar o desinstalar posteriormente según sea necesario.

La lista siguiente contiene explicaciones de algunos términos que se utilizan en IBM Installation Manager:

### Oferta

Una unidad o producto de software instalable.

La oferta de IBM Spectrum Protect contiene todos los soportes que IBM Installation Manager necesita para instalar IBM Spectrum Protect.

### Paquete

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de IBM Spectrum Protect contiene los componentes siguientes:

- Programa de instalación de IBM Installation Manager
- Oferta de IBM Spectrum Protect

### Grupo de paquetes

Un conjunto de paquetes que comparten un directorio padre común.

El grupo de paquetes predeterminado para el paquete de IBM Spectrum Protect es IBM Installation Manager.

### Repositorio

Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de IBM Spectrum Protect se guarda en un repositorio de IBM Fix Central.


### Directorio de recursos compartidos

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluidos los archivos que se utilizan para retrotraer a una versión anterior de IBM Spectrum Protect.

## Windows: Hojas de trabajo para planificar detalles para el servidor

Puede utilizar las hojas de trabajo para ayudarle a planificar la cantidad y la ubicación del almacenamiento necesario para el servidor de IBM Spectrum Protect. También puede utilizarlas para realizar un seguimiento de nombres e ID de usuario.

 **Sistemas operativos Windows** Restricción: Si está utilizando una tabla de asignación de archivos (FAT o FAT32) o un formato NTFS (New Technology File System), no puede especificar el directorio raíz de dicho sistema como la ubicación de un directorio de base de datos o un directorio de registro. En su lugar, debe crear uno o varios subdirectorios dentro del directorio raíz. A continuación, cree los directorios de bases de datos y directorios de registros dentro de los subdirectorios.

Elemento	Espacio necesario	Número de directorios	Ubicación de los directorios
La base de datos			
Registro activo			
Registro de archivos			
Opcional: duplicado de registro para el registro activo			
Opcional: Registro de archivado secundario (ubicación de migración tras error para el registro de archivado)			

Elemento	Nombres e ID de usuario	Ubicación
El <i>ID de usuario de instancia</i> para el servidor, que es el ID que utiliza para iniciar y ejecutar el servidor de IBM Spectrum Protect		
El <i>directorio de inicio</i> del servidor, que es el directorio que contiene el ID de usuario de la instancia		
El nombre de instancia de la base de datos		
El <i>directorio de la instancia</i> del servidor, que es un directorio que contiene archivos específicos para esta instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor)		
El nombre del servidor; utilice un nombre exclusivo para cada servidor		

## Windows: Planificación de la capacidad

La planificación de la capacidad para IBM Spectrum Protect incluye la gestión de recursos, como la base de datos, el registro de recuperación y el área de recursos compartidos. Para maximizar los recursos como parte de la planificación de la capacidad, debe calcular las necesidades de espacio para la base de datos y el registro de recuperación. El área de recursos compartidos debe tener suficiente espacio disponible para cada instalación o actualización.

- **Windows: Estimación de los requisitos de espacio para la base de datos**  
Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.
- **Windows: Requisitos de espacio del registro de recuperación**  
En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.



- Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación  
Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.
- Windows: Supresión de archivos de retrotracción de instalación  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Windows: Estimación de los requisitos de espacio para la base de datos

---

Para estimar los requisitos de espacio para la base de datos, puede utilizar el número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado o puede utilizar la capacidad de la agrupación de almacenamiento.

### Acerca de esta tarea

---

Considere utilizar al menos 25 GB para espacio de base de datos inicial. Asigne el espacio del sistema de archivos adecuado. Un tamaño de base de datos de 25 GB resulta adecuado para un entorno de prueba o un entorno solo de gestor de bibliotecas. Para un servidor de producción que dé soporte a cargas de trabajo de cliente, el tamaño de la base de datos será superior. Si utiliza agrupaciones de almacenamiento de disco de acceso aleatorio (DISK), necesitará más espacio de almacenamiento de base de datos y registro que para las agrupaciones de almacenamiento de acceso secuencial.

El tamaño máximo de la base de datos de IBM Spectrum Protect es 6 TB.

Para obtener información sobre cómo planificar el tamaño de la base de datos en un entorno de producción que se base en el número de archivos y en el tamaño de la agrupación de almacenamiento, consulte los siguientes temas.

- Windows: Estimación de los requisitos de espacio de base de datos en función del número de archivos  
Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.
- Windows: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento  
Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.
- Windows: El gestor de bases de datos y el espacio temporal  
El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

## Windows: Estimación de los requisitos de espacio de base de datos en función del número de archivos

---

Si puede efectuar una estimación del número máximo de archivos que puede haber en el almacenamiento del servidor en un momento determinado, puede utilizar dicho número para estimar los requisitos de espacio de la base de datos.

### Acerca de esta tarea

---

Para estimar los requisitos de espacio que se basa en el número máximo de archivos en la agrupación del servidor, utilice las siguientes directrices:

- De 600 a 1000 bytes para cada versión guardada de un archivo, incluidas las copias de seguridad de imagen.  
Restricción: La directriz no incluye el espacio que se utiliza durante la deduplicación de datos.
- 100 - 200 bytes por cada archivo en memoria caché, archivo de agrupación de almacenamiento de copias, archivo de agrupación de datos activos y archivo con eliminación de duplicado.
- Se necesita espacio adicional para la optimización de la base de datos a fin de dar soporte a patrones variables de acceso a datos y al proceso de fondo del servidor de los datos. La cantidad de espacio adicional es igual al 50% de la estimación del número total de bytes para objetos de archivo.

En el siguiente ejemplo de un cliente individual, los cálculos se basan en los valores máximos de las directrices anteriores. Los ejemplos no tienen en cuenta que es posible que utilice la agregación de archivos. En general, cuando agrega archivos pequeños, se reduce la cantidad de espacio de base de datos necesario. La agregación de archivos no afecta a los archivos bajo gestión de espacio.

## Procedimiento

---

1. Calcule el número de versiones de archivos. Añada cada uno de los siguientes valores para obtener el número de las versiones de archivos:

- a. Calcule el número de archivos de los que se ha realizado copia de seguridad. Por ejemplo, se puede realizar una copia de seguridad de hasta 500.000 archivos de cliente a la vez. En este ejemplo, las políticas de almacenamiento se han establecido para mantener hasta tres copias de archivos de los que se ha realizado copia de seguridad:

$$500,000 \text{ files} * 3 \text{ copies} = 1,500,000 \text{ files}$$

- b. Calcule el número de archivos activos. Por ejemplo, es posible que hasta 100.000 archivos de cliente sean copias de archivado.
- c. Calcule el número de archivos gestionados por el espacio. Por ejemplo, es posible que hasta 200.000 archivos de cliente deben migrarse a las estaciones de trabajo de cliente.

Si se utilizan 1000 bytes por archivo, el número total de espacio de base de datos necesario para los archivos pertenecientes al cliente es 1,8 GB:

$$(1,500,000 + 100,000 + 200,000) * 1000 = 1.8 \text{ GB}$$

2. Calcule el número de archivos en memoria caché, archivos de agrupación de almacenamiento de copia, archivos de agrupación de datos activos y archivos con optimización de almacenamiento:

- a. Calcule el número de copias en memoria caché. Por ejemplo, el almacenamiento en memoria caché está habilitado en una agrupación de almacenamiento de disco de 5 GB. El umbral de migración alto de la agrupación es del 90% y el umbral de migración bajo de la agrupación es del 70%. Por lo tanto, el 20% de la agrupación del disco, o 1 GB, está ocupado por archivos almacenados en caché.

Si el tamaño medio de los archivos es de aproximadamente 10 KB, cerca de 100.000 archivos estarán en la memoria caché a la vez:

$$100,000 \text{ files} * 200 \text{ bytes} = 19 \text{ MB}$$

- b. Calcule el número de archivos de agrupación de almacenamiento de copia. La copia de seguridad de todas las agrupaciones de almacenamiento primarias se hace en la agrupación de almacenamiento de copia:

$$(1,500,000 + 100,000 + 200,000) * 200 \text{ bytes} = 343 \text{ MB}$$

- c. Calcule el número de archivos de agrupación de almacenamiento activos. Todos los datos de copia de seguridad activos del cliente de las agrupaciones de almacenamiento primarias se copian en la agrupación de almacenamiento de datos activos. Supongamos que 500.000 versiones de los 1.500.000 archivos de copia de seguridad de la agrupación de almacenamiento primaria están activos:

$$500,000 * 200 \text{ bytes} = 95 \text{ MB}$$

- d. Calcule el número de archivos con eliminación de duplicado. Supongamos que una agrupación de almacenamiento con eliminación de duplicado contiene 50.000 archivos:

$$50,000 * 200 \text{ bytes} = 10 \text{ MB}$$

Basándose en los cálculos anteriores, se requieren unos 0,5 GB de espacio de base de datos adicional para los archivos almacenados en la memoria caché del cliente, los archivos de la agrupación de datos activos y los archivos deduplicados.

3. Calcule la cantidad de espacio adicional necesario para la optimización de la base de datos. Para ofrecer un acceso de datos gestión por parte del servidor óptimos, se necesita espacio de base de datos adicional. La cantidad de espacio de base de datos adicional es igual al 50% de los requisitos de espacio total para objetos de archivo.

$$(1.8 + 0.5) * 50\% = 1.2 \text{ GB}$$

4. Calcule la cantidad total de espacio de base de datos necesaria para el cliente. El total es aproximadamente 3,5 GB:

$$1,8 + 0,5 + 1,2 = 3,5 \text{ GB}$$

5. Calcule la cantidad total de espacio de base de datos necesaria para todos los clientes. Si el cliente utilizado en los cálculos anteriores es un cliente típico y tiene 500 clientes, por ejemplo, puede utilizar el siguiente cálculo para estimar la cantidad total de espacio de base de datos necesario para todos los clientes:

$$500 * 3.5 = 1.7 \text{ TB}$$

## Resultados

---

Consejo: En los ejemplos anteriores, los resultados son estimaciones. El tamaño real de la base de datos puede diferir del estimado debido a factores como el número de directorios y la longitud de las vías de acceso y nombres de archivo. Supervise periódicamente la base de datos y ajuste el tamaño según sea necesario.

## Qué hacer a continuación

Durante operaciones normales, el servidor de IBM Spectrum Protect puede necesitar espacio de base de datos temporal. Este espacio se necesita por los siguientes motivos:

- Para albergar los resultados de clasificaciones que aún no se han conservado y optimizado en la base de datos directamente. Los resultados se colocan temporalmente en la base de datos para su proceso.
- Para ofrece acceso administrativo a la base de datos a través de uno de estos métodos:
  - Un cliente de DB2 ODBC (Open Database Connectivity)
  - Un cliente de Java™ Database Connectivity (JDBC)
  - Structured Query Language (SQL) con el servidor desde una línea de mandatos de cliente administrativo

Tenga en cuenta la posibilidad de utilizar 50 GB adicionales de espacio temporal por cada 500 GB de espacio para objetos de archivo y optimización. Consulte las directrices de la tabla siguiente. En el ejemplo que se utiliza en el paso anterior, se necesita un total de 1,7 TB de espacio en la base de datos necesario para los objetos de archivo y la optimización para 500 clientes. En función de este cálculo, se necesitan 200 GB para espacio temporal. La cantidad total de espacio de base de datos necesario es 1,9 TB.

Tamaño de la base de datos	Requisito mínimo de espacio temporal
< 500 GB	50 GB
≥ 500 GB y < 1 TB	100 GB
≥ 1 TB y < 1,5 TB	150 GB
≥ 1,5 y < 2 TB	200 GB
≥ 2 y < 3 TB	250 - 300 GB
≥ 3 y < 4 TB	350 - 400 GB

## Windows: Estimación de los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento

Para estimar los requisitos de espacio de base de datos en función de la capacidad de la agrupación de almacenamiento, utilice una proporción de 1 - 5 %. Por ejemplo, si necesita 200 TB de capacidad de agrupación de almacenamiento, el tamaño estimado de la base de datos es 2 - 10 TB. Como regla general, la base de datos debe ser lo mayor posible para evitar quedarse sin espacio. Si se queda sin espacio en la base de datos, las operaciones del servidor y del almacén del cliente pueden fallar.

## Windows: El gestor de bases de datos y el espacio temporal

El gestor de bases de datos del servidor de IBM Spectrum Protect administra y asigna la memoria del sistema y el espacio de disco para la base de datos. La cantidad de espacio de la base de datos que necesita depende de la cantidad de memoria disponible en el sistema y de la carga de trabajo del servidor.

El gestor de base de datos ordena datos en una secuencia específica, de acuerdo con la sentencia SQL que emite para solicitar los datos. Dependiendo de la carga de trabajo en el servidor y de si hay más datos de los que el gestor de bases de datos puede administrar, los datos (que se ordenan en secuencia) se asignan al espacio temporal en disco. Los datos se asignan al espacio temporal en disco cuando hay un conjunto de resultados grande. El gestor de base de datos gestiona dinámicamente la memoria utilizada cuando se asignan datos al espacio de disco temporal.

Por ejemplo, el procesamiento de la caducidad puede producir un conjunto de resultados grande. Si no hay suficiente memoria de sistema en la base de datos para almacenar el conjunto de resultados, algunos de los datos se asignan al espacio temporal en disco. Durante el proceso de caducidad, si se selecciona un nodo o espacio de archivos demasiado grande para procesar, el gestor de bases de datos no puede ordenar los datos en la memoria. El gestor de base de datos debe utilizar espacio temporal para ordenar los datos.

Para ejecutar operaciones de bases de datos, tenga en cuenta la posibilidad de añadir más espacio de base de datos en los siguientes escenarios:

- La base de datos tiene una cantidad pequeña de espacio y la operación del servidor que requiere espacio temporal utiliza el espacio libre restante.
- Los espacios de archivo son grandes o los espacios de archivo tienen asignada una política que crea muchas versiones de archivo.
- El servidor de IBM Spectrum Protect debe ejecutarse con memoria limitada. La base de datos utiliza la memoria del servidor principal de IBM Spectrum Protect para ejecutar operaciones de bases de datos. Sin embargo, si no hay suficiente memoria disponible, el servidor de IBM Spectrum Protect asigna el espacio temporal en disco a la base de datos. Por ejemplo, si hay 10G

de memoria disponible y las operaciones de base de datos requieren 12G de memoria, la base de datos utiliza el espacio temporal.

- Se mostrará un error de `sin espacio de base de datos` cuando despliegue un servidor de IBM Spectrum Protect. Supervise el registro de actividad de servidor para obtener mensajes que están relacionados con el espacio de base de datos.

Importante: No cambie el software de DB2 que está instalado con los paquetes de instalación y fixpacks de IBM Spectrum Protect. No instale o actualice a una versión, release o fixpack diferente de DB2 para evitar dañar la base de datos.

## Windows: Requisitos de espacio del registro de recuperación

---

En IBM Spectrum Protect, el término *registro de recuperación* comprende el registro activo, el registro de archivado, el duplicado del registro activo y el registro de migración tras error del archivo. La cantidad de espacio que necesita para el registro de recuperación depende de varios factores como, por ejemplo, el nivel de actividad del cliente con el servidor.

- Windows: Espacio del registro activo y archivado  
Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.
- Windows: Espacio del duplicado de registro activo  
El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.
- Windows: Espacio del registro de migración tras error del archivo  
El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

## Windows: Espacio del registro activo y archivado

---

Cuando estime los requisitos de espacio para registros activos y archivados, incluya espacio adicional para contingencias, como fuertes cargas de trabajo ocasionales y migración tras error.

En los servidores de IBM Spectrum Protect V7.1 y posteriores, el registro activo puede tener un tamaño máximo de 512 GB. El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado.

Utilice las siguientes directrices generales para calcular el tamaño del registro activo:

- El tamaño inicial recomendado para el registro activo es 16 GB.
- Asegúrese de que el registro activo sea lo suficientemente grande para la cantidad de actividad simultánea que suele manejar el servidor. Como precaución, intente calcular la mayor cantidad de trabajo que gestiona el servidor al mismo tiempo. Proporcione al registro activo espacio adicional que pueda utilizarse si hace falta. Piense en utilizar el 20% de espacio adicional.
- Supervise el espacio de registro activo utilizado y disponible. Ajuste el tamaño del registro activo según sea necesario, en función de factores como la actividad del cliente y el nivel de operaciones del servidor.
- Asegúrese de que el directorio que alberga el registro activo sea lo suficientemente grande, o mayor, que el tamaño del registro activo. Un directorio mayor que el registro activo puede acomodar migraciones tras error, si se producen.
- Asegúrese de que el sistema de archivos que contiene el directorio del registro activo tenga como mínimo 8 GB de espacio libre para requisitos de movimientos de registro temporal.

El tamaño inicial recomendado para el registro de archivado es de 48 GB.

El directorio del registro de archivado debe ser lo suficientemente grande para contener los archivos de registro generados desde la copia de seguridad completa anterior. Por ejemplo, si realiza una copia de seguridad completa de la base de datos todos los días, el directorio del registro de archivado tiene que ser lo suficientemente grande como para contener los archivos de registro de toda la actividad del cliente que tenga lugar durante 24 horas. Para recuperar espacio, el servidor suprime los archivos de registro de archivado obsoletos tras una copia de seguridad completa de la base de datos. Si el directorio de registro de archivado se llena y no existe un directorio para los registros de migración tras error de archivado, los archivos de registro permanecen en el directorio de registro activo. Esta condición puede causar que se llene el directorio de registro activo y se detenga el servidor. Cuando el servidor se reinicia, parte del espacio de registro activo existente se libera.

Después de que el servidor esté instalado, puede supervisar la utilización de los registros de archivado y el espacio en el directorio de anotaciones de archivado. Si el espacio en el directorio del registro de archivación se llena, puede causar los siguientes problemas:

- El servidor no puede realizar copias de seguridad de base de datos completas. Investigue y solucione este problema.
- Otras aplicaciones graban en el directorio de registro de archivado, agotando el espacio que necesita el registro de archivado. No comparta el espacio de registro de archivado con otras aplicaciones, incluidos otros servidores de IBM Spectrum Protect. Asegúrese de que cada servidor tenga una ubicación de almacenamiento separada que sea propiedad de dicho servidor específico y que este la gestione.

- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente  
Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones  
Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas  
Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor  
Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema  
Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.
- Windows: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas  
El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.
- Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados  
Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente

Las operaciones básicas de almacén del cliente incluyen copia de seguridad, archivado y gestión de espacio. El espacio de registro debe ser suficiente como para manejar todas las transacciones del almacén que se procesan simultáneamente.

Para determinar los tamaños de los registros activo y de archivado para operaciones básicas de almacén del cliente, utilice el siguiente cálculo:

número de clientes x archivos almacenados durante cada transacción  
x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones básicas de almacén del cliente

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.

Elemento	Valores de ejemplo	Descripción
Espacio de registro necesario para cada archivo	3053 bytes	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	19,5 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 3,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>3,5 + 16 = 19,5 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	58,5 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total.</p> <p><math>3,5 \times 3 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>10,5 + 48 = 58,5 \text{ GB}</math></p>
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para clientes que utilizan varias sesiones

Si la opción del cliente RESOURCEUTILIZATION tiene un valor mayor que el predeterminado, la carga de trabajo simultánea para el servidor aumenta.

Para determinar los tamaños de los registros activo y de archivado cuando los clientes utilizan varias sesiones, utilice el siguiente cálculo:

número de clientes x sesiones por cada cliente x archivos almacenados durante cada transacción x espacio de registro necesario para cada archivo

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Varias sesiones de cliente

Elemento	Valores de ejemplo	Descripción
----------	--------------------	-------------

Elemento	Valores de ejemplo		Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	1000	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Sesiones posibles para cada cliente	3	3	El valor de la opción del cliente RESOURCEUTILIZATION es mayor que el valor predeterminado. Cada sesión del cliente ejecuta un máximo de tres sesiones en paralelo.
Archivos almacenados durante cada transacción	4096	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3053	3053	<p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	26,5 GB <sup>1</sup>	51 GB <sup>1</sup>	<p>Se ha utilizado el siguiente cálculo para 300 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 10,5 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>10,5 + 16 = 26,5 \text{ GB}</math></p> <p>Se ha utilizado el siguiente cálculo para 1000 clientes. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(1000 \text{ clientes} \times 3 \text{ sesiones por cada cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3053 \text{ bytes por cada archivo}) \div 1.073.741.824 = 35 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>35 + 16 = 51 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado	79,5 GB <sup>1</sup>	153 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, la estimación del registro activo se multiplica por 3:</p> <p><math>10,5 \times 3 = 31,5 \text{ GB}</math></p> <p><math>35 \times 3 = 105 \text{ GB}</math></p> <p>Aumente estas cantidades en el tamaño inicial recomendado de 48 GB:</p> <p><math>31,5 + 48 = 79,5 \text{ GB}</math></p> <p><math>105 + 48 = 153 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise el registro activo y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de grabación simultáneas

Si las operaciones de copia de seguridad del cliente utilizan agrupaciones de almacenamiento configuradas para la grabación simultánea, la cantidad de espacio de registro necesaria para cada archivo aumenta.

El espacio de registro necesario para cada archivo aumenta en unos 200 bytes por cada agrupación de almacenamiento de copia utilizada para una operación de grabación simultánea. En el ejemplo de la tabla siguiente, los datos se almacenan en dos agrupaciones de almacenamiento de copia además de en una agrupación de almacenamiento primaria. El tamaño de registro estimado aumenta en 400 bytes por cada archivo. Si utiliza el valor recomendado de 3053 bytes de espacio de registro para cada archivo, el número total de bytes necesarios es 3453.

Este cálculo se utiliza en el ejemplo de la tabla siguiente.

Tabla 1. Operaciones de grabación simultáneas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes de copia de seguridad y archivado que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ cliente} \times 4096 \text{ archivos almacenados durante cada transacción} \times 3453 \text{ bytes para cada archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>



Elemento	Valores de ejemplo	Descripción
Registro de archivado: Tamaño recomendado	60 GB <sup>1</sup>	Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado:  $4 \text{ GB} \times 3 = 12 \text{ GB}$  Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:  $12 + 48 = 60 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones básicas de almacén del cliente y operaciones del servidor

Operaciones de migración de datos en almacenamiento del servidor, procesos de identificación para la eliminación de datos duplicados, reclamación y caducidad se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las tareas administrativas, como mandatos administrativos y consultas SQL desde clientes administrativos, también se pueden ejecutar simultáneamente con operaciones de almacén del cliente. Las operaciones del servidor y las tareas administrativas que se ejecutan simultáneamente pueden aumentar el espacio de registro activo necesario.

Por ejemplo, la migración de archivos de la agrupación de almacenamiento de acceso aleatorio (DISK) a la agrupación de almacenamiento de disco de acceso secuencial (FILE) utiliza aproximadamente 110 bytes de espacio de registro para cada archivo que se migra. Por ejemplo, suponga que tiene 300 clientes de copia de seguridad y archivado y cada uno de ellos hace copia de seguridad de 100.000 archivos cada noche. Los archivos se almacenan inicialmente en la agrupación de almacenamiento DISK y luego se migran a la agrupación FILE. Para estimar la cantidad de espacio de registro activo necesario para la migración de datos, utilice el siguiente cálculo. El número de clientes del cálculo representa el número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento

`300 clientes x 100.000 archivos por cada cliente x 110 bytes = 3,1 GB`

Sume a este valor la estimación del tamaño del registro activo calculado para operaciones básicas de almacén del cliente.

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado bajo condiciones de variación extrema

Pueden producirse problemas de falta de espacio de registro activo si tiene muchas transacciones que se ejecutan rápidamente y algunas transacciones tardan mucho en ejecutarse. Un caso típico se produce cuando hay varias sesiones de copia de seguridad de estación de trabajo o de servidor de archivos activas y muy pocas sesiones de copia de seguridad del servidor de bases de datos grandes activas. Si se produce esta situación en su entorno, es posible que tenga que aumentar el tamaño del registro activo para que el trabajo se realice correctamente.

## Windows: Ejemplo: Estimación de tamaños de registro de archivado con copias de seguridad de base de datos completas

El servidor de IBM Spectrum Protect suprime los archivos innecesarios del registro de archivado solo cuando se realiza una copia de seguridad de base de datos completa. Por lo tanto, cuando estime el espacio necesario para el registro de archivado, también debe tener en cuenta la frecuencia de las copias de seguridad de base de datos completas.

Por ejemplo, si se realiza una copia de seguridad de base de datos completa una vez por semana, el espacio del registro de archivado debe poder contener la información del registro de archivado correspondiente a una semana completa.

La diferencia en el tamaño del registro de archivado para copias de seguridad de seguridad de base de datos diarias y completas se muestra en el ejemplo de la tabla siguiente.

Tabla 1. Copias de seguridad de base de datos completas

Elemento	Valores de ejemplo	Descripción
Número máximo de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos simultáneamente en cualquier momento	300	El número de nodos de cliente que realizan operaciones de copia de seguridad, archivado o migración de archivos cada noche.
Archivos almacenados durante cada transacción	4096	El valor predeterminado de la opción del servidor TXNGROUPMAX es 4096.
Espacio de registro necesario para cada archivo	3453 bytes	<p>3053 bytes para cada archivo más 200 bytes para cada agrupación de almacenamiento de copia.</p> <p>El valor de 3053 bytes para cada archivo de una transacción representa los bytes de registro necesarios cuando se hace copia de seguridad de archivos de un cliente Windows en el que los nombres de archivo tienen entre 12 y 120 bytes.</p> <p>Este valor se basa en los resultados de pruebas realizadas bajo condiciones de laboratorio. Las pruebas consisten en clientes que realizan operaciones de copia de seguridad en una agrupación de almacenamiento de disco de acceso aleatorio (DISK). Las agrupaciones DISK utilizan más cantidad de registro que las agrupaciones de almacenamiento de acceso secuencial. Tenga en cuenta la posibilidad de asignar un valor mayor que 3053 si los datos que se almacenan tienen nombres de archivo de más de entre 12 y 120 bytes.</p>
Registro activo: Tamaño recomendado	20 GB <sup>1</sup>	<p>Utilice el siguiente cálculo para determinar el tamaño del registro activo. Un GB equivale a 1.073.741.824 bytes.</p> <p><math>(300 \text{ clientes} \times 4096 \text{ archivos por transacción} \times 3453 \text{ bytes por archivo}) \div 1.073.741.824 \text{ bytes} = 4,0 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> <p><math>4 + 16 = 20 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada día	60 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total:</p> <p><math>4 \text{ GB} \times 3 = 12 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>12 + 48 = 60 \text{ GB}</math></p>
Registro de archivado: Tamaño recomendado con una copia de seguridad de base de datos completa cada semana	132 GB <sup>1</sup>	<p>Debido al requisito de poder almacenar registros de archivado entre tres ciclos de copia de seguridad de base de datos del servidor, multiplique la estimación del registro activo por 3 para estimar el requisito de registro de archivado total. Multiplique el resultado por el número de días entre copias de seguridad de base de datos completas:</p> <p><math>(4 \text{ GB} \times 3) \times 7 = 84 \text{ GB}</math></p> <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> <p><math>84 + 48 = 132 \text{ GB}</math></p>

Elemento	Valores de ejemplo	Descripción
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que no utilice eliminación de duplicados, 16 GB es el tamaño mínimo recomendado para un registro activo. El tamaño inicial recomendado para un registro de archivado en un entorno de producción que no utilice eliminación de duplicados es 48 GB. Si sustituye los valores del entorno y los resultados son mayores que 16 GB y 48 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>		

## Windows: Ejemplo: Estimación de los tamaños de registro activo y de archivado para operaciones de eliminación de datos duplicados

Si elimina los datos duplicados, debe tener en cuenta sus efectos en los requisitos de espacio para registros activos y de archivado.

Los siguientes factores afectan a los requisitos de espacio de registro activo y de archivado.

### La cantidad de eliminación de datos duplicados

El efecto de la eliminación de datos duplicados en el espacio de registro activo y de registro de archivado depende del porcentaje de datos aptos para la eliminación de duplicados. Si el porcentaje de datos cuya duplicación se puede eliminar es relativamente alto, se necesita más espacio de registro.

### El tamaño y el número de extensiones

Se necesitan aproximadamente 1.500 de espacio de registro activo por cada extensión identificada por un proceso de identificación de duplicados. Por ejemplo, si el proceso de identificación de duplicados identifica 250.000 extensiones, el tamaño estimado del registro activo es 358 MB:

```
250.000 extensiones identificadas durante cada proceso x 1.500 bytes
por cada extensión = 358 MB
```

Tenga en cuenta el siguiente caso de ejemplo. Trescientos clientes de copia de seguridad y archivado hacen copia de seguridad de 100.000 archivos cada noche. Esta actividad crea una carga de trabajo de 30.000.000 archivos. El número medio de extensiones por archivo es dos. Por lo tanto, el número total de extensiones es 60.000.000, y el requisito de espacio para el registro de archivado es 84 GB:

```
60.000.000 extensiones x 1.500 bytes por extensión = 84 GB
```

Un proceso de identificación de duplicados opera sobre agregados de archivos. Un agregado consiste en archivos almacenados en una determinada transacción, según lo especificado en la opción del servidor TXNGROUPMAX. Supongamos que la opción del servidor TXNGROUPMAX tiene el valor predeterminado, 4096. Si el número medio de extensiones por archivo es dos, el número total de extensiones en cada agregado es 8192, y el espacio necesario para el registro activo es 12 MB:

```
8192 extensiones en cada agregado x 1500 bytes por cada extensión =
12 MB
```

### El tiempo y el número de proceso de identificación de duplicados

El tiempo y el número de procesos de identificación de duplicados también afectan al tamaño del registro activo. Si se utiliza el tamaño de registro activo de 12 MB calculado en el ejemplo anterior, la carga simultánea en el registro activo es 120 MB si se ejecutan 10 procesos de identificación de duplicados en paralelo:

```
12 MB para cada proceso x 10 procesos = 120 MB
```

### El tamaño de archivo

Los archivos grandes que se procesan para la identificación de duplicados también pueden afectar al tamaño del registro activo. Por ejemplo, supongamos que un cliente de archivado y copia de seguridad hace copia de seguridad de una imagen del sistema de archivos de 80 GB. Este objeto puede tener un gran número de extensiones duplicadas si, por ejemplo, se ha hecho copia de seguridad incremental del archivo incluido en la imagen del sistema de archivos. Por ejemplo, supongamos que una imagen del sistema de archivos tiene 1,2 millones de extensiones duplicadas. El 1,2 millones de extensiones de este gran archivo representa una sola transacción para un proceso de identificación de duplicados. El espacio total necesario en el registro activo para este objeto es 1,7 GB:

```
1.200.000 extensiones x 1.500 bytes por cada extensión = 1,7 GB
```

Si se producen otros procesos menores de identificación de duplicaciones a la vez que el proceso de identificación de duplicados para un solo objeto de gran tamaño, es posible que el registro activo no tenga suficiente espacio. Por ejemplo, supongamos que

una agrupación de almacenamiento está habilitada para la eliminación de duplicados. La agrupación de almacenamiento tiene una combinación de datos que incluye archivos relativamente pequeños comprendidos entre 10 KB y varios cientos de KB. La agrupación de almacenamiento también tiene unos pocos objetos grandes que tienen un alto porcentaje de extensiones duplicadas.

Para tener en cuenta no solo los requisitos de espacio sino también el tiempo y la duración de las transacciones simultáneas, aumente el tamaño estimado del registro activo por un factor de dos. Por ejemplo, suponga que los cálculos de requisitos de espacio son 25 GB (23,3 GB + 1,7 GB para la eliminación de duplicados de un objeto grande). Si los procesos de eliminación de duplicados se están ejecutando simultáneamente, el tamaño recomendado del registro activo es 50 GB. El tamaño recomendado del registro de archivado es 150 GB.

Los ejemplos de las tablas siguientes muestran cálculos de registros activos y de archivado. El ejemplo de la primera tabla utiliza un tamaño medio de 700 KB para extensiones. El ejemplo de la segunda tabla utiliza un tamaño medio de 256 KB. Tal como muestran los ejemplos, el tamaño medio de extensión de eliminación de duplicados de 256 KB indica un tamaño estimado mayor para el registro activo. Para minimizar o evitar problemas operativos para el servidor, utilice 256 KB para estimar el tamaño del registro activo en el entorno de producción.

Tabla 1. Tamaño medio de extensión duplicada de 700 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.
Tamaño medio de extensiones	700 KB	700 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio para extensiones.
Extensiones para un determinado archivo	1.198.372 bits	6.135.667 bits	Utilizando el tamaño medio de extensión (700 KB), estos cálculos representan el número total de extensiones para un determinado objeto.  Se ha utilizado el siguiente cálculo para un objeto de 800 GB: $(800 \text{ GB} \div 700 \text{ KB}) = 1.198.372 \text{ bits}$  Se ha utilizado el siguiente cálculo para un objeto de 4 TB: $(4 \text{ TB} \div 700 \text{ KB}) = 6.135.667 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	1,7 GB	8,6 GB	El espacio de registro activo estimado necesario para esta transacción.

Elemento	Valores de ejemplo		Descripción
Registro activo: Tamaño total recomendado	66 GB <sup>1</sup>	79,8 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por dos. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 1,7 \text{ GB}) \times 2 = 50 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $50 + 16 = 66 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 8,6 \text{ GB}) \times 2 = 63,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $63,8 + 16 = 79,8 \text{ GB}$
Registro de archivado: Tamaño recomendado	198 GB <sup>1</sup>	239,4 GB <sup>1</sup>	<p>Multiplique el tamaño estimado del registro activo por 3.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $50 \text{ GB} \times 3 = 150 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $150 + 48 = 198 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $63,8 \text{ GB} \times 3 = 191,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $191,4 + 48 = 239,4 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

Tabla 2. Tamaño medio de extensión duplicada de 256 KB

Elemento	Valores de ejemplo		Descripción
Tamaño de un solo objeto grande del que eliminar duplicados	800 GB	4 TB	La granularidad del proceso de eliminación de duplicados está al nivel de archivo. Por lo tanto, el archivo de mayor tamaño del que eliminar duplicados representa la transacción mayor y una carga grande correspondiente en los registros activo y de archivado.

Elemento	Valores de ejemplo		Descripción
Tamaño medio de extensiones	256 KB	256 KB	El algoritmo de eliminación de duplicados utiliza un método de bloque de variable. No todas las extensiones de las que se han eliminado duplicados para un determinado archivo tienen el mismo tamaño, de modo que en este cálculo se utiliza un tamaño medio de extensión.
Extensiones para un determinado archivo	3.276.800 bits	16.777.216 bits	<p>Utilizando el tamaño medio de extensión, estos cálculos representan el número total de extensiones para un determinado objeto.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(800 \text{ GB} \div 256 \text{ KB}) = 3.,276.800 \text{ bits}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(4 \text{ TB} \div 256 \text{ KB}) = 16.777.216 \text{ bits}$
Registro activo: Tamaño recomendado necesario para la eliminación de duplicados de un solo objeto grande durante un solo proceso de identificación de duplicados	4,5 GB	23,4 GB	El tamaño estimado del espacio de registro activo necesario para esta transacción.
Registro activo: Tamaño total recomendado	71,6 GB <sup>1</sup>	109,4 GB <sup>1</sup>	<p>Después de tener en cuenta otros aspectos de la carga de trabajo del servidor, además de la eliminación de duplicados, multiplique la estimación existente por 2. En estos ejemplos, se tiene en cuenta el espacio de registro activo necesario para eliminar los duplicados de un solo objeto grande junto con estimaciones anteriores del tamaño de registro activo necesario.</p> <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 800 GB:</p> $(23,3 \text{ GB} + 4,5 \text{ GB}) \times 2 = 55,6 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $55,6 + 16 = 71,6 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para varias transacciones y un objeto de 4 TB:</p> $(23,3 \text{ GB} + 23,4 \text{ GB}) \times 2 = 93,4 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 16 GB:</p> $93,4 + 16 = 109,4 \text{ GB}$

Elemento	Valores de ejemplo		Descripción
Registro de archivado: Tamaño recomendado	214,8 GB <sup>1</sup>	328,2 GB <sup>1</sup>	<p>El tamaño estimado del registro activo multiplicado por 3.</p> <p>Se ha utilizado el siguiente cálculo para un objeto de 800 GB:</p> $55,6 \text{ GB} \times 3 = 166,8 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $166,8 + 48 = 214,8 \text{ GB}$ <p>Se ha utilizado el siguiente cálculo para un objeto de 4 TB:</p> $93,4 \text{ GB} \times 3 = 280,2 \text{ GB}$ <p>Aumente esta cantidad en el tamaño inicial recomendado de 48 GB:</p> $280,2 + 48 = 328,2 \text{ GB}$
<p><sup>1</sup> Los valores de ejemplo de esta tabla solo se utilizan para ilustrar el modo en que se calculan los tamaños de los registros activos y de los registros de archivado. En un entorno de producción que utilice eliminación de duplicados, 32 GB es el tamaño mínimo recomendado para un registro activo. El tamaño mínimo recomendado para un registro de archivado en un entorno de producción que utilice eliminación de duplicados es 96 GB. Si sustituye los valores del entorno y los resultados son mayores que 32 GB y 96 GB, utilice sus resultados para calcular el tamaño del registro activo y del registro de archivado.</p> <p>Supervise los registros y ajuste su tamaño si es necesario.</p>			

## Windows: Espacio del duplicado de registro activo

El registro activo se puede duplicar para que se pueda utilizar la copia duplicada si no se pueden leer los archivos del registro activo. Solo puede haber un duplicado de registro activo.

La creación de un duplicado de registro es opcional y recomendable. Si aumenta el tamaño del registro activo, el tamaño del duplicado de registro aumenta automáticamente. El duplicado del registro puede afectar al rendimiento debido a la doble actividad de entrada/salida necesaria para mantener el duplicado. El espacio adicional que necesita un duplicado de registro es otro factor a tener en cuenta a la hora de decidir si se crea un duplicado de registro.

Si el directorio del registro duplicado se llena, el servidor emite mensajes de error en el registro de actividades y en el archivo db2diag.log. La actividad del servidor continúa.

## Windows: Espacio del registro de migración tras error del archivo

El servidor utiliza el registro de migración tras error del archivo si el directorio de registro del archivo se queda sin espacio.

Especificar un directorio de registro de migración tras error del archivo puede evitar problemas que se producen si el registro del archivo se queda sin espacio. Si el directorio del registro de archivado y la unidad o el sistema de archivos en el que se encuentra el directorio del registro de migración tras error del archivo se llena, los datos se conservan en el directorio de registro activo. Esta condición puede hacer que el registro activo se llene, lo que hace que el servidor se pare.

## Windows: Supervisión de la utilización de espacio para los registros de base de datos y recuperación

Para determinar la cantidad de espacio de registro activo utilizado y disponible, emita el mandato QUERY LOG. Para supervisar la utilización de espacio en los registros de base de datos y de recuperación, también puede comprobar el registro de actividad en busca de mensajes.

### Registro activo

Si la cantidad de espacio de registro activo disponible es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR4531I: IC\_AUTOBACKUP\_LOG\_USED\_SINCE\_LAST\_BACKUP\_TRIGGER

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. El servidor de IBM Spectrum Protect comienza una copia de seguridad de base de datos completa.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR0297I: IC\_BACKUP\_NEEDED\_LOG\_USED\_SINCE\_LAST\_BACKUP

Este mensaje se muestra cuando el espacio de registro activo supera el tamaño máximo especificado. Debe hacer copia de seguridad de la base de datos de forma manual.

Para cambiar el tamaño máximo de registro, detenga el servidor. Abra el archivo dsmserv.opt y especifique un nuevo valor para la opción ACTIVELOGSIZE. Cuando termine, reinicie el servidor.

#### ANR4529I: IC\_AUTOBACKUP\_LOG\_UTILIZATION\_TRIGGER

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Si se ha realizado al menos una copia de seguridad de base de datos completa, el servidor de IBM Spectrum Protect inicia una copia de seguridad de base de datos incremental. De lo contrario, el servidor inicia una copia de seguridad de base de datos completa.

#### ANR0295I: IC\_BACKUP\_NEEDED\_LOG\_UTILIZATION

La proporción de espacio de registro activo utilizado y espacio de registro activo disponible supera el umbral de utilización de registro. Debe hacer copia de seguridad de la base de datos de forma manual.

## Registro de archivos

---

Si la cantidad de espacio de registro de archivado disponible es demasiado baja, se muestra el siguiente mensaje en el registro de actividad:

#### ANR0299I: IC\_BACKUP\_NEEDED\_ARCHLOG\_USED

La proporción de espacio de registro de archivado utilizado y espacio de registro de archivado disponible supera el umbral de utilización de registro. El servidor de IBM Spectrum Protect comienza una copia de seguridad automática de base de datos completa.

## Base de datos

---

Si la cantidad de espacio disponible para actividades de base de datos es demasiado baja, se muestran los siguientes mensajes en el registro de actividad:

#### ANR2992W: IC\_LOG\_FILE\_SYSTEM\_UTILIZATION\_WARNING\_2

El espacio de base de datos utilizado supera el umbral correspondiente a utilización de espacio de base de datos. Para aumentar el espacio para la base de datos, utilice el mandato EXTEND DBSPACE, el mandato EXTEND DBSPACE o el programa de utilidad DSMSERV FORMAT con el parámetro DBDIR.

#### ANR1546W: FILESYSTEM\_DBPATH\_LESS\_1GB

El espacio disponible en el directorio en el que se encuentran los archivos de base de datos del servidor es menor que 1 GB.

Cuando se crea un servidor de IBM Spectrum Protect con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, también se crea un registro de base de datos y recuperación del servidor. Además, los archivos se crean para mantener la información de base de datos que utiliza el gestor de base de datos. La vía de acceso especificada en este mensaje indica la ubicación de la información de base de datos que utiliza el gestor de bases de datos. Si no hay espacio en la vía de acceso, el servidor no puede seguir funcionando.

Debe añadir espacio al sistema de archivos o dejar espacio disponible en el sistema de archivos o disco.

## Windows: Supresión de archivos de retrotracción de instalación

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación para liberar espacio en el directorio de recursos compartidos. Por ejemplo, los archivos que pueden haber sido necesarios para una operación de retrotracción son tipos de archivos que puede suprimir.

## Acerca de esta tarea

---

Para suprimir los archivos que ya no son necesarios, utilice el asistente gráfico de instalación o la línea de mandatos en modalidad de consola.

- Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la



interfaz de usuario de IBM® Installation Manager.

- Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos  
Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

## Windows: Supresión de archivos de retrotracción de instalación utilizando un asistente gráfico

---

Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación utilizando la interfaz de usuario de IBM® Installation Manager.

### Procedimiento

---

1. Abra IBM Installation Manager.
2. Pulse Archivo > Preferencias.
3. Seleccione Archivos a restaurar.
4. Pulse Suprimir archivos guardados y pulse Aceptar.

## Windows: Supresión de archivos de retrotracción de instalación utilizando la línea de mandatos

---



Puede suprimir determinados archivos de instalación que se hayan guardado durante el proceso de instalación si utiliza la línea de mandatos.

### Procedimiento

---

1. En el directorio en el que está instalado IBM® Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Windowseclipse\tools

Por ejemplo:

-  Sistemas operativos WindowsC:\Archivos de programa\IBM\Installation Manager\eclipse\tools
2. Desde el directorio tools, emita el mandato siguiente para iniciar una línea de mandatos de IBM Installation Manager:
    -  Sistemas operativos Windowsimcl.exe -c
  3. Especifique P para seleccionar Preferencias.
  4. Especifique 3 para seleccionar Archivos a restaurar.
  5. Especifique D para Suprimir los Archivos a restaurar.
  6. Especifique A para Aplicar cambios y volver al menú Preferencias.
  7. Especifique C para salir del Menú Preferencias.
  8. Especifique X para Salir de Installation Manager.

## Windows: Prácticas más adecuadas de denominación del servidor

---

Utilice estas descripciones como referencia cuando instale o actualice un servidor de IBM Spectrum Protect.

### Identificador de usuario de la instancia

---

El identificador de usuario de la instancia se utiliza como base para otros nombres relacionados con la instancia del servidor. El identificador de usuario de la instancia también se conoce como propietario de la instancia.

Por ejemplo: tsminst1

El ID de usuario de la instancia es el ID de usuario que debe tener la propiedad o autoridad de acceso de lectura/escritura a todos los directorios que cree para la base de datos y el registro de recuperación. La forma estándar de ejecutar el servidor es bajo el ID de usuario de la instancia. Este ID de usuario también debe tener acceso de lectura y grabación en los directorios que se utilizan para cualquier clase de dispositivo FILE.


 Sistemas operativos Windows

### Nombre de la instancia de la base de datos

---

El nombre de la instancia de la base de datos es el nombre de la instancia del servidor tal y como aparece en el registro.

Por ejemplo: Server1

 Sistemas operativos Windows

## Directorio de la instancia

---

El directorio de la instancia es un directorio que contiene archivos específicos para una instancia del servidor (el archivo de opciones de servidor y otros archivos específicos del servidor). Puede tener el nombre que desee. Para que la identificación sea más sencilla, utilice un nombre que relacione el directorio al nombre de la instancia.

Puede utilizar un nombre que incluya el nombre de la instancia del servidor tal y como aparece (o aparecerá) en el registro. Los nombres de las instancias del servidor predeterminadas tienen la forma Serverx.

Por ejemplo: C:\tsm\server1

El directorio de instancia almacena los siguientes archivos en la instancia del servidor:

- El archivo de opciones de servidor dsmserv.opt
- El archivo de la base de datos de la clave del servidor, cert.kdb, y los archivos .arm (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor DEVCONFIG no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor VOLUMEHISTORY no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento DEVTYPE=FILE si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Nombre de la base de datos


---

El nombre de la base de datos es siempre TSMDB1, para todas las instancias del servidor. Este nombre no puede modificarse.


## Nombre de servidor

---

El nombre del servidor es un nombre interno para IBM Spectrum Protect, y se utiliza para operaciones que implican una comunicación entre múltiples servidores IBM Spectrum Protect servers. Los ejemplos incluyen comunicaciones de servidor a servidor y bibliotecas compartidas.

 Sistemas operativos Windows El nombre del servidor se utiliza asimismo al añadir el servidor al Centro de operaciones para poder gestionarlo a través de la interfaz. Utilice un nombre único para cada servidor. Para facilitar su identificación en el Centro de operaciones (o desde un mandato QUERY SERVER), utilice un nombre que refleje la ubicación o el propósito del servidor. No cambie el nombre de un servidor de IBM Spectrum Protect después de que se haya configurado como servidor concentrador o servidor spoke.

Si utiliza un asistente, el nombre predeterminado que se sugiere es el nombre de host del sistema que está utilizando. Puede utilizar un nombre diferente que tenga significado en su entorno. Si tiene más de un servidor en el sistema y utiliza un asistente, puede utilizar el nombre predeterminado sólo para uno de los servidores. Debe introducir un nombre único para cada servidor.

 Sistemas operativos Windows Por ejemplo,

- TUCSON\_SERVER1
- TUCSON\_SERVER2

## Directorios del espacio de base de datos y el registro de recuperación

---

A los directorios se les puede asignar un nombre de acuerdo a prácticas locales. Para facilitar la identificación utilice nombres que asocien los directorios a la instancia del servidor.

Por ejemplo, para el registro de archivado:

-  Sistemas operativos Windows f:\server1\archlog

## Windows: Directorios de instalación

---

Los directorios de instalación para el servidor de IBM Spectrum Protect incluyen los directorios de servidor, DB2, dispositivo, idioma y otros directorios. Cada uno contiene diversos directorios adicionales.

/opt/tivoli/tsm/server/bin es el directorio predeterminado que contiene el código de servidor y la licencia.

El producto DB2 instalado como parte de la instalación del servidor de IBM Spectrum Protect tiene la estructura del directorio tal como se documenta en las fuentes de información de DB2. Proteja los directorios y los archivos mientras prepara los directorios del servidor. El directorio predeterminado es /opt/tivoli/tsm/db2.

Puede utilizar inglés de Estados Unidos, alemán, francés, italiano, español, portugués de Brasil, coreano, japonés, chino tradicional, chino simplificado, chino GBK, chino Big5 y ruso.

## Windows: Instalación de los componentes de servidor

---


Para instalar los componentes del servidor de la versión 8.1.2, puede utilizar el asistente de instalación, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Acerca de esta tarea

---

Al urukuzar ek software de instalación IBM Spectrum Protect, puede instalar los siguientes componentes:

- servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM® Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- idiomas de servidor
- licencia
- dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones

 Sistemas operativos Windows Deje aproximadamente entre 15 y 30 minutos para instalar un servidor V 8.1.2, utilizando esta guía.

- Windows: Obtener el paquete de instalación  
Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM como Passport Advantage o IBM Fix Central.
- Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación  
Puede instalar el servidor utilizando el asistente gráfico de IBM Installation Manager.
- Windows: Instalación de IBM Spectrum Protect en modalidad de consola  
Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.
- Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa  
Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.
- Windows: Instalación de paquetes de idioma del servidor  
Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.

## Windows: Obtener el paquete de instalación


---

Puede obtener el paquete de instalación de IBM Spectrum Protect desde un sitio de descarga de IBM® como Passport Advantage o IBM Fix Central.

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de estos sitios web.
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información, las actualizaciones y los arreglos de mantenimiento más recientes, vaya a IBM Support Portal.
2. Si ha descargado el paquete de un sitio de descarga de IBM, complete los pasos siguientes:

 Sistemas operativos Windows

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio consulte el documento de descarga:
  - IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Cambie al directorio en el que colocó el archivo ejecutable.

Importante: En el siguiente paso, los archivos se extraen al directorio actual. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.

- c. Pulse dos veces en el siguiente archivo ejecutable o introduzca el siguiente mandato en la línea de mandatos para extraer los archivos de instalación. Los archivos se extraen al directorio actual.

`nombre_paquete.exe`

donde `nombre_paquete` es como el siguiente ejemplo: `8.1.x.000-IBM-SPSRV-WindowsX64.exe`


3. Seleccione uno de los siguientes métodos para instalar IBM Spectrum Protect:
  - o Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación
  - o Windows: Instalación de IBM Spectrum Protect en modalidad de consola
  - o Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa
4. Tras instalar IBM Spectrum Protect, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Soporte y descargas y aplique todo arreglo aplicable.

## Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación

Puede instalar el servidor utilizando el asistente gráfico de IBM® Installation Manager.



### Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:

- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
-  Sistemas operativos Windows Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.



### Procedimiento

Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación emitiendo el mandato siguiente:</p> <p> Sistemas operativos Windows</p> <pre>install.bat</pre> <p> Sistemas operativos Windows O, en el directorio en donde se extrajeron los archivos de instalación, haga doble clic en el archivo <code>install.bat</code>.</p>

### Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro se almacenan en el directorio de registros de IBM Installation Manager.


Puede ver los archivos de registro de la instalación pulsando Archivo > Ver registro desde la herramienta Installation Manager. Para recopilar estos archivos de registro, pulse Ayuda > Exportar datos para el análisis de problemas desde la herramienta Installation Manager.
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Windows Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos Windows Si hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es `C:\Program Files\Tivoli\TSM\device\drivers`.

## Windows: Instalación de IBM Spectrum Protect en modalidad de consola

Puede instalar IBM Spectrum Protect utilizando la línea de mandatos en modalidad de consola.


## Antes de empezar

Realice las acciones siguientes antes de iniciar la instalación:




- Compruebe que el sistema operativo esté establecido en el idioma que necesita. De forma predeterminada, el idioma del sistema operativo es el idioma del asistente de instalación.
-  Sistemas operativos Windows Asegúrese de que el ID de usuario que piensa utilizar durante la instalación es un usuario con autoridad de administrador local.

## Procedimiento

Instale IBM Spectrum Protect utilizando este método:

Opción	Descripción
<b>Instalación del software de un paquete descargado:</b>	<p>a. Cambie al directorio donde ha descargado el paquete.</p> <p>b. Inicie el asistente de instalación en modalidad de consola emitiendo el siguiente mandato:</p> <p> Sistemas operativos Windows</p> <pre>install.bat -c</pre> <p>Opcional: Genere un archivo de respuestas como parte de una instalación en modalidad de consola. Complete las opciones de instalación en el modo de consola, y en el panel Resumen, especifique G para generar las respuestas.</p>

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  -  Sistemas operativos Windows C:\ProgramData\IBM\Installation Manager\logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos Windows Después de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos Windows Si hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es C:\Program Files\Tivoli\TSM\device\drivers.

## Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa

Puede instalar o actualizar el servidor en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

## Antes de empezar

Para proporcionar entrada de datos cuando se utiliza el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

install\_response\_sample.xml

Utilice este archivo para instalar los componentes de IBM Spectrum Protect.

update\_response\_sample.xml

Utilice este archivo para actualizar los componentes de IBM Spectrum Protect.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento

1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.
2. Si instala el servidor y Centro de operaciones en el modo silencioso, cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.

Si está utilizando el archivo `install_response_sample.xml`, añada la contraseña en la línea siguiente del archivo, donde `mypassword` representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de instalación




Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo `update_response_sample.xml`.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor `archivo_respuestas` representa la vía de acceso del archivo de respuestas y el nombre del archivo:

- o  Sistemas operativos Windows

```
install.bat -s -input archivo_respuestas  
-acceptLicense
```

## Qué hacer a continuación

- Si se producen errores durante el proceso de instalación, los errores se registran en los archivos de registro que se almacenan en el directorio de registros de IBM® Installation Manager, por ejemplo:
  - o  Sistemas operativos WindowsC:\ProgramData\IBM\Installation Manager\logs
- Tras instalar el servidor y los componentes, y antes de personalizarlo para su uso, vaya a IBM Support Portal. Pulse Downloads (fixes and PTFs) y aplique los arreglos pertinentes.
-  Sistemas operativos WindowsDespués de instalar un nuevo servidor, revise Realizar los primeros pasos tras instalar IBM Spectrum Protect para aprender a configurar el servidor.
-  Sistemas operativos WindowsSi hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos nativo disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect emitiendo el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es `C:\Program Files\Tivoli\TSM\device\drivers`.

 Sistemas operativos Windows

## Windows: Instalación de paquetes de idioma del servidor

Las traducciones del servidor permiten que el servidor muestre los mensajes y la ayuda en idiomas distintos al inglés de Estados Unidos. Las traducciones también permiten utilizar convenios de entorno local para el formato de fechas, horas y números.


### Antes de empezar

Para obtener instrucciones sobre la instalación de paquetes de idioma del agente de almacenamiento, consulte Configuración de paquetes de idioma para agentes de almacenamiento.

- Windows: Idiomas locales del servidor  
Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.
- Windows: Configuración de un paquete de idiomas  
Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.
- Windows: Actualización de un paquete de idiomas  
Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

## Windows: Idiomas locales del servidor

Utilice la opción de paquete de idioma predeterminado o seleccione otro paquete de idioma para mostrar los mensajes del servidor y la ayuda.

 Sistemas operativos WindowsEste paquete de idioma se instala automáticamente para la opción de idioma predeterminada siguiente para los mensajes de servidor y de ayuda: LANGUAGE AMENG.

Para los idiomas o entornos locales distintos del valor predeterminado, instale el paquete de idioma que su instalación requiera. Puede utilizar los idiomas que se muestran:



 Sistemas operativos Windows

Tabla 1. Idiomas del servidor para Windows

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	chs
Chino, tradicional	cht
Inglés	ameng
Francés	fra
Alemán	deu
Italiano	ita
Japonés (Shift-JIS)	jpn
Coreano	kor
Portugués, de Brasil	ptb
Ruso	rus
Español	esp

 Sistemas operativos Windows Restricción: Para los usuarios de Centro de operaciones, es posible que algunos caracteres no se muestren correctamente si el navegador web no usa el mismo lenguaje que el servidor. Si ocurre este problema, configure el navegador para usar el mismo lenguaje que el servidor.


## Windows: Configuración de un paquete de idiomas

---

Tras configurar un paquete de idioma, se muestran mensajes y ayuda en el servidor en idiomas distintos al inglés de EE. UU. Los paquetes de instalación se proporcionan con IBM Spectrum Protect.

### Acerca de esta tarea

---

 Sistemas operativos Windows Establezca la opción LANGUAGE del archivo de opciones del servidor en el nombre del entorno que desea utilizar. Por ejemplo: para utilizar el entorno local `ita`, establezca la opción LANGUAGE en `ita`. Consulte Windows: Idiomas locales del servidor.

Si el entorno nacional se inicia correctamente, cambia el formato de la fecha, la hora y los números para el servidor. Si el entorno local no se ha inicializado correctamente, el servidor utiliza los archivos de mensajes de inglés de EE. UU. y el formato de fecha, hora y número.

## Windows: Actualización de un paquete de idiomas

---

Puede modificar o actualizar un paquete de idioma utilizando IBM® Installation Manager.

### Acerca de esta tarea

---

Puede instalar otro paquete de idiomas dentro de la misma instancia de IBM Spectrum Protect.

- Utilice la función Modificar de IBM Installation Manager para instalar otro paquete de idioma.
- Utilice la función Actualizar de IBM Installation Manager para actualizar a versiones más nuevas de los paquetes de idioma.

Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.



## Windows: Primeros pasos tras instalar IBM Spectrum Protect


---

Tras instalar la versión de 8.1.2, prepárese para la configuración. La utilización del asistente de configuración es el método preferido para configurar la instancia de IBM Spectrum Protect.

### Acerca de esta tarea

---

1. Cree los directorios y el ID de usuario para la instancia del servidor. Consulte el apartado Windows: Creación del ID de usuario y de directorios para la instancia del servidor.
2. Configure una instancia de servidor. Seleccione una de las siguientes opciones:
  - Utilice el asistente de configuración, el método preferido. Consulte el apartado Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración.
  - Configure manualmente la nueva instancia. Consulte el apartado Windows: Configuración de la instancia del servidor manualmente. Complete los pasos siguientes durante la configuración manual.
    - a. Configure los directorios y cree la instancia IBM Spectrum Protect. Consulte Windows: Creación de una instancia del servidor.
    - b. Cree un nuevo archivo de opciones de servidor copiando el archivo de muestra para configurar las comunicaciones entre el servidor y los clientes. Consulte  Sistemas operativos Windows Windows: Configuración de comunicaciones de servidor y de cliente.
    - c. Emita el mandato DSMSERV FORMAT para formatear la base de datos. Consulte el apartado Windows: Formateo de la base de datos y las anotaciones.
    - d. Configure su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos.
3. Configure opciones para controlar cuando debe ejecutarse la reorganización de base de datos. Consulte Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor.
4. Inicie la instancia del servidor, si todavía no se ha iniciado.
  -  Sistemas operativos Windows Consulte el apartado Windows: Inicio de la instancia del servidor en sistemas Windows.
5. Registre su licencia. Consulte el apartado Windows: Registro de licencias.
6. Prepare su sistema para realizar copias de seguridad de la base de datos. Consulte el apartado Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos.
7. Supervise el servidor. Consulte el apartado Windows: Supervisión del servidor.

- Windows: Creación del ID de usuario y de directorios para la instancia del servidor  
Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.
- Windows: Configuración del servidor de IBM Spectrum Protect  
Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.
- Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor  
Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.
-  Sistemas operativos Windows Windows: Inicio de la instancia del servidor en sistemas Windows  
En un entorno de producción, el método preferido para iniciar el servidor es como un servicio Windows. En un entorno en el que va a reconfigurar, probar o completar tareas de mantenimiento, inicie el servidor en primer plano o utilice la modalidad de mantenimiento.
- Windows: Detención del servidor  
Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.
- Windows: Registro de licencias  
Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.
- Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos  
Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.
- Windows: Ejecución de varias instancias de servidor en un solo sistema  
Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.
- Windows: Supervisión del servidor  
Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

## Windows: Creación del ID de usuario y de directorios para la instancia del servidor

---

Cree el ID de usuario para la instancia del servidor IBM Spectrum Protect y cree los directorios que necesita la instancia del servidor para los registros de base de datos y de recuperación.

### Antes de empezar

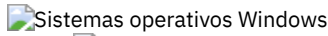
---



Revise la información acerca del espacio de planificación para el servidor antes de completar esta tarea. Consulte el apartado Windows: Hojas de trabajo para planificar detalles para el servidor.

## Procedimiento

1. Cree el ID de usuario que será propietario de la instancia del servidor. Este ID de usuario se utiliza al crear la instancia del servidor en un paso posterior.



Cree un ID de usuario que será el propietario de la instancia del servidor IBM Spectrum Protect. Un ID de usuario puede poseer varias instancias del servidor de IBM Spectrum Protect. Identifique la cuenta de usuario que poseerá la instancia del servidor.

Cuando el servidor se inicia como un servicio de Windows, esta cuenta es la única en la que iniciará sesión dicho servicio. La cuenta de usuario debe tener autoridad administrativa en el sistema. Una cuenta de usuario puede poseer más de una instancia de servidor.

Si tiene varios servidores en un sistema y desea ejecutar cada uno de ellos con una cuenta de usuario distinta, cree una nueva cuenta de usuario en este paso.

Cree el ID de usuario.

Restricción: El ID de usuario debe cumplir la siguiente regla:

El ID de usuario sólo puede contener minúsculas (a-z), numerales (0-9) y guiones bajos (\_). El ID de usuario debe tener 30 caracteres o menos y no puede empezar por *ibm*, *sql*, *sys* o un número. El ID de usuario y el nombre del grupo no pueden ser *user*, *admin*, *guest*, *public*, *local* o cualquier palabra reservada por SQL.

- a. Utilice el siguiente mandato de sistema operativo para crear el ID de usuario:

```
net user user_ID */add
```

Se le pedirá que cree y verifique una contraseña para el nuevo ID de usuario.

- b. Emita los siguientes mandatos del sistema operativo para añadir un nuevo ID de usuario a los grupos Administradores:

```
net localgroup Administrators user_ID /add
net localgroup DB2ADMNS ID_usuario /add
```

2. Cree los directorios necesarios para el servidor.

Cree directorios vacíos para cada elemento de la tabla y asegúrese de que el nuevo ID de usuario que acaba de crear tiene permiso de lectura y escritura en los directorios. La base de datos, el registro de archivado y el registro activo deben residir en volúmenes físicos distintos.

Elemento	Mandatos de ejemplo para crear los directorios	Sus directorios
El directorio de instancias del servidor, que contendrá archivos específicos para esta instancia de servidor (el archivo de opciones del servidor y otros archivos específicos del servidor)	<code>mkdir d:\tsm\server1</code>	
Los directorios de bases de datos	<code>mkdir d:\tsm\db001</code> <code>mkdir e:\tsm\db002</code> <code>mkdir f:\tsm\db003</code> <code>mkdir g:\tsm\db004</code>	
Directorio de registro de activo	<code>mkdir h:\tsm\log</code>	
Directorio de registro de archivado	<code>mkdir i:\tsm\archlog</code>	
Opcional: Directorio para la duplicación de registros de los registros activos	<code>mkdir j:\tsm\logmirror</code>	
Opcional: Directorio de registro de archivado secundario (ubicación de recuperación tras error para los registros activos)	<code>mkdir k:\tsm\archlogfailover</code>	

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

3. Cierre la sesión con el nuevo ID de usuario.


## Windows: Configuración del servidor de IBM Spectrum Protect

---

Después de haber instalado el servidor y preparado para la configuración, configure la instancia de servidor.

### Acerca de esta tarea

---

 **Sistemas operativos Windows Consejo:** La consola de gestión de IBM Spectrum Protect, que es un complemento de Microsoft Management Console (MMC), ya no se entrega con IBM Spectrum Protect. El método preferido para configurar el servidor consiste en utilizar el asistente de configuración. Puede utilizar el asistente para completar varias tareas de configuración de servidor. Sin embargo, no puede utilizar el asistente para ampliar el esquema de Active Directory para que los clientes puedan descubrir servidores automáticamente.

Configure una instancia de servidor de IBM Spectrum Protect seleccionando una de las opciones siguientes:

- **Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración**  
El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.
- **Windows: Configuración de la instancia del servidor manualmente**  
Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

## Windows: Configuración de IBM Spectrum Protect utilizando el asistente de configuración


---

El asistente ofrece un acercamiento guiado para configurar un servidor. Mediante la interfaz gráfica de usuario (GUI), puede evitar algunos pasos de configuración que son complicados cuando se realizan manualmente. Inicie el asistente en el sistema en que ha instalado el programa del servidor IBM Spectrum Protect.

### Antes de empezar


---

Antes de empezar a utilizar el asistente de configuración, debe completar todos los pasos precedentes para prepararse para la configuración. Estos pasos incluyen la instalación de IBM Spectrum Protect, la creación de la base de datos y los directorios de registro y la creación de los directorios y el ID de usuario para la instancia de servidor.

 **Sistemas operativos Windows**


### Acerca de esta tarea

---



 **Sistemas operativos Windows Consejo:** La consola de IBM Spectrum Protect, que es un complemento MMC, ya no se suministra con IBM Spectrum Protect. El método preferido para configurar la instancia de servidor es utilizar el asistente de configuración. Puede utilizar el asistente para completar varias tareas de configuración.

### Procedimiento

---

1. Asegúrese de que se cumplen los siguientes requisitos:  **Sistemas operativos Windows**
  - Asegúrese de que se cumplen los siguientes requisitos:
    - a. Pulse Inicio > Herramientas administrativas > Servicios.
    - b. En la ventana Servicios, seleccione el servicio Registro remoto si no está iniciado y, a continuación, pulse Iniciar.
  - Asegúrese de que los puertos 137, 139 y 445 no están bloqueados por un cortafuegos:
    - a. Pulse Inicio > Panel de control > Firewall de Windows.
    - b. Seleccione Configuración avanzada.
    - c. Seleccione Reglas de entrada en el panel izquierdo.
    - d. Seleccione Nueva regla en el panel derecho.
    - e. Cree una regla de puerto para los puertos TCP 137, 139 y 445 para permitir conexiones de dominio y redes privadas.
  - Configure Control de cuenta de usuario:


Acceda a los tres valores de configuración de control de cuentas de usuario accediendo en primer lugar a las opciones de Seguridad de política de seguridad local, utilizando los pasos siguientes:

- a. Habilite la cuenta de Administrador incorporada:
    - Seleccione Cuentas: estado de la cuenta de administrador.
    - Seleccione Habilitar y pulse Aceptar.
  - b. Inhabilite el Control de cuentas de usuario para todos los administradores de Windows:
    - Seleccione el Control de cuentas de usuario: ejecutar todos los administradores en modalidad de aprobación de administrador.
    - Seleccione Inhabilitar y pulse Aceptar.
  - c. Inhabilite el Control de cuentas de usuario para la cuenta de Administrador incorporada:
    - Seleccione el Control de cuentas de usuario: modalidad de aprobación de administrador para la cuenta de Administrador incorporada.
    - Seleccione Inhabilitar y pulse Aceptar.
- Reinicie el servidor antes de continuar con el asistente de configuración.
2. Inicie la versión local del asistente:
-  Sistemas operativos Windows Pulse Inicio > Todos los programas > IBM Spectrum Protect > Asistente de configuración. O, pulse dos veces en el programa `dsmicfgx.exe` en `installation_directory\server`. El directorio predeterminado es `C:\Archivos de programa\Tivoli\TSM`.
- Siga las instrucciones para completar la configuración. El asistente se puede detener y reiniciar, pero el servidor no funcionará hasta que no haya finalizado completamente el proceso de configuración.
-  Sistemas operativos Windows Windows: Configuración de Remote Execution Protocol en Windows Configurar valores de acceso remoto utilizando estos procedimientos.

## Windows: Configuración de la instancia del servidor manualmente

---

Después de instalar IBM Spectrum Protect Versión 8.1.2, puede configurar IBM Spectrum Protect manualmente en lugar de utilizar el asistente de configuración.

- Windows: Creación de una instancia del servidor  
Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.
-  Sistemas operativos Windows Windows: Configuración de comunicaciones de servidor y de cliente  
Tras instalar el servidor, puede configurar comunicaciones de cliente y servidor especificando opciones en los archivos de opciones de servidor y cliente.
- Windows: Formateo de la base de datos y las anotaciones  
Utilice el programa de utilidad `DSMSERV FORMAT` para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos  
Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.

## Windows: Creación de una instancia del servidor


---

Cree una instancia de IBM Spectrum Protect emitiendo el mandato `db2icrt`.

### Acerca de esta tarea

---

Puede tener una o más instancias del servidor en una estación de trabajo.

 Sistemas operativos Windows Importante: Antes de ejecutar el mandato `db2icrt`, asegúrese de que el usuario y el directorio de la instancia del usuario existen. Si no existe ningún directorio de instancia, debe crearlo.

El directorio de instancia almacena los siguientes archivos para la instancia del servidor:

- El archivo de opciones de servidor `dsmserv.opt`
- El archivo de la base de datos de la clave del servidor, `cert.kdb`, y los archivos `.arm` (utilizados por los clientes y otros servidores para importar los certificados Secure Sockets Layer del servidor)
- El archivo de configuración de dispositivo si la opción de servidor `DEVCONFIG` no especifica un nombre completo
- El archivo de historial de volumen si la opción de servidor `VOLUMEHISTORY` no especifica un nombre completo
- Volúmenes para agrupaciones de almacenamiento `DEVTYPE=FILE` si el directorio de la clase de dispositivo no se ha especificado completamente no tiene un nombre completo
- El usuario existe
- Salida de rastreo (si no está cualificada al completo)

## Sistemas operativos Windows

1. Inicie sesión como administrador y cree una instancia de IBM Spectrum Protect utilizando el mandato `db2icrt`. Especifique el siguiente mandato en una línea. La cuenta de usuario que especifique pasará a ser el ID de usuario que posea la Versión 8.1.2 o un servidor posterior (el ID de usuario de la instancia).

```
db2icrt -u cuenta_usuario nombre_instancia
```

Por ejemplo, si la cuenta de usuario es `tsminst1` y la instancia de servidor es `Server1`, debe especificar el siguiente mandato:

```
db2icrt -u tsminst1 server1
```

Se le pedirá la contraseña del ID de usuario `tsminst1`. Posteriormente, cuando crea y formatea la base de datos, utiliza el nombre de la instancia que especificó con este mandato con la opción `-k`.

2. Cambie la vía de acceso predeterminada para la base de datos para que sea la unidad en la que se encuentra el directorio de instancia del servidor. Realice los siguientes pasos:
  - a. Haga clic en Inicio > Programas > IBM DB2 > DB2TSM1 > Command Line Tools > Command Line Processor.
  - b. Escriba `abandonar` para salir del procesador de línea de mandatos.

Ahora debería abrirse una ventana con un indicador de mandatos, con el entorno correctamente configurado para emitir mandatos en los siguientes pasos.

- c. Desde el indicador de mandatos de esa ventana, emita el siguiente mandato para configurar la variable de entorno para la instancia de servidor con la que trabaja:

```
set db2instance=instance_name
```

Aquí `nombre_instancia` es el mismo nombre de instancia especificado al emitir el mandato `db2icrt`. Por ejemplo, para establecer la variable de entorno para la instancia del servidor `Server1`, emita el siguiente mandato:

```
set db2instance=server1
```

- d. Emita el mandato para configurar la unidad predeterminada:

```
db2 update dbm cfg using dftdbpath instance_location
```

Por ejemplo, el directorio de instancia es `d:\tsm\server1` y la ubicación de la instancia es la unidad `d:`. Escriba el mandato:

```
db2 update dbm cfg using dftdbpath d:
```

3. Cree un archivo de opciones de servidor. Consulte Windows: Configuración de comunicaciones de servidor y de cliente.

## Sistemas operativos Windows

# Windows: Configuración de comunicaciones de servidor y de cliente

---

Tras instalar el servidor, puede configurar comunicaciones de cliente y servidor especificando opciones en los archivos de opciones de servidor y cliente.

## Acerca de esta tarea

---

Establezca estas opciones del servidor antes de iniciar el servidor. Cuando inicie el servidor, entrarán en vigor las nuevas opciones. Si modifica cualquiera de las opciones del servidor después de iniciarlo, debe detener el servidor y reiniciarlo para activar las opciones actualizadas.




Revise el archivo de opciones del servidor (`dsmserv.opt.smp`) que se encuentra en el directorio de instancias del servidor para ver y especificar las opciones de comunicaciones del servidor. De forma predeterminada, el servidor utiliza los métodos de comunicación TCP/IP y Named Pipes.

Consejo: Si al iniciar la consola del servidor ve mensajes de aviso que advierten de que el servidor no puede utilizar un protocolo, puede deberse a que el protocolo no esté instalado o a que la configuración no coincida con la del protocolo de Windows.

Para que un cliente utilice un protocolo activado en el servidor, el archivo de opciones del cliente debe contener los valores correspondientes para las opciones de comunicación. En el archivo de opciones del servidor, puede ver los valores de cada protocolo.

Puede especificar uno o varios de los métodos de comunicación siguientes:

- Protocolo de control de transmisiones/protocolo Internet, versión 4 o versión 6
- Named Pipes
- Memoria compartida

- capa de sockets seguros (SSL)  
Consejo: Puede autenticar contraseña con el servidor de directorio LDAP o autenticar contraseñas con el servidor. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.
-  Sistemas operativos Windows: Establecimiento de opciones de TCP/IP  
Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.
-  Sistemas operativos Windows: Establecimiento de opciones de Named Pipes  
El método de comunicación Named Pipes es idóneo cuando se ejecuta el servidor y el cliente en la misma máquina Windows. Named Pipes no necesita una configuración especial.
-  Sistemas operativos Windows: Configuración de las opciones de la capa de sockets seguros  
Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

## Windows: Establecimiento de opciones de TCP/IP

Seleccione a partir de un rango de opciones de TCP/IP para el servidor de IBM Spectrum Protect o conserve la opción predeterminada.

### Acerca de esta tarea

Lo siguiente es un ejemplo de una lista de opciones de TCP/IP que puede utilizar para configurar el sistema.


```
commethod          tcpip
tcpport            1500
tcpwindowsize     0
tcpnodelay        yes
```

Consejo: Puede utilizar la versión 4, 6 o ambas de TCP/IP.

#### TCPPOINT

La dirección del puerto del servidor para la comunicación SSL y TCP/IP. El valor predeterminado es 1500.

#### Sistemas operativos Windows: TCPWINDOWSIZE

 Sistemas operativos Windows: Especifica el tamaño del búfer de TCP/IP que se utiliza para enviar o recibir datos. El tamaño de la ventana utilizada en una sesión es el menor entre los de la ventana del cliente y del servidor. Tamaños de ventana mayores utilizan más memoria, pero pueden mejorar el rendimiento.

Para usar el tamaño de ventana predeterminado para el sistema operativo, especifique 0.

#### TCPNODELAY

Determina si el servidor envía mensajes pequeños o deja que TCP/IP los coloque en el búfer. El envío de mensajes pequeños puede mejorar el rendimiento, pero aumenta el número de paquetes enviados por la red. Especifique YES para enviar mensajes pequeños, o NO para que TCP/IP los coloque en el búfer. El valor predeterminado es YES.

#### TCPADMINPORT

Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor va a esperar las solicitudes habilitadas para SSL o TCP/IP que no sean sesiones de cliente. El valor predeterminado es el valor de TCPPOINT.

#### SSLTCPPOINT

(Sólo SSL) Especifica el número de puerto de SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL de cliente de copia de seguridad/archivado de línea de mandatos y del cliente de administración de línea de mandatos.

#### SSLTCPADMINPORT

(Solo SSL) Especifica la dirección de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL del cliente de administración de línea de mandatos.

## Windows: Establecimiento de opciones de Named Pipes

El método de comunicación Named Pipes es idóneo cuando se ejecuta el servidor y el cliente en la misma máquina Windows. Named Pipes no necesita una configuración especial.

### Acerca de esta tarea

Éste es un ejemplo de configuración de Named Pipes:

```
commethod          namedpipe
namedpipename      \\.\pipe\adsmpipe
```

COMMETHOD se puede utilizar varias veces en el archivo de opciones de servidor de IBM Spectrum Protect, con un valor diferente cada vez. Por ejemplo, el siguiente ejemplo es posible:

```
commmethod tcpip
commmethod namedpipe
```

## Windows: Configuración de las opciones de la capa de sockets seguros

---

Puede añadir más protección a sus datos y contraseñas utilizando la capa de sockets seguros (SSL).

### Antes de empezar

---

SSL es la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL proporciona un canal seguro para que los servidores y los clientes se puedan comunicar mediante vías de acceso de comunicación abiertas. Con SSL, la identidad del servidor se verifica utilizando certificados digitales.

Para conseguir un mejor rendimiento del sistema, sólo utilice SSL para sesiones cuando realmente sea necesario. Considere la posibilidad de añadir recursos del procesador adicionales en el servidor de IBM Spectrum Protect para gestionar los requisitos aumentados.


## Windows: Formateo de la base de datos y las anotaciones

---

Utilice el programa de utilidad DSMSEV FORMAT para inicializar una instancia de servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Una vez configuradas las comunicaciones del servidor, puede inicializar la base de datos. Asegúrese de iniciar la sesión utilizando el ID de usuario de la instancia. No coloque los directorios en sistemas de archivos que puedan quedarse sin espacio. Si algunos directorios (por ejemplo, el registro de archivado) se llenan o no están disponibles, el servidor se detiene.

Para el rendimiento óptimo y para facilitar la E/S, especifique al menos dos contenedores de igual tamaño o dos números de unidad lógica (LUN) para la base de datos. Además, cada recurso activo y registro de archivo debe tener su propio contenedor o LUN.


 **Sistemas operativos Windows** Importante: El programa de instalación crea un conjunto de claves de registro. Una de estas claves señala al directorio en el que se crea el servidor predeterminado, denominado SERVER1. Para instalar un servidor adicional, cree un directorio y utilice el programa de utilidad DSMSEV FORMAT con el parámetro -k, desde dicho directorio. Ese directorio se convierte en la ubicación del servidor. El registro realiza un seguimiento de los servidores instalados.

### Configuración del manejador de listas de salida

---

Establezca la variable de registro DB2NOEXITLIST en ON para cada instancia de servidor. Inicie sesión en el sistema como propietario de la instancia de servidor y emita este mandato:


```
db2set -i nombre_instancia_servidor DB2NOEXITLIST=ON
```

Por ejemplo:  **Sistemas operativos Windows**

```
db2set -i server1 DB2NOEXITLIST=ON
```

### Inicialización de una instancia del servidor


---

Utilice el programa de utilidad DSMSEV FORMAT para inicializar una instancia de servidor. Por ejemplo, si el directorio de instancia de servidor es */tsminst1*, emita los mandatos siguientes:  **Sistemas operativos Windows**

```
cd \tsminst1
dsmsevr -k server2 format dbdir=d:\tsm\db001 activelogsiz=32768
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

#### Información relacionada:

 DSMSEV FORMAT (Dar formato a la base de datos y a las anotaciones)

## Windows: Preparación del gestor de bases de datos para la copia de seguridad de la base de datos

---


Para hacer una copia de seguridad de los datos de la base de datos en IBM Spectrum Protect, debe habilitar el gestor de base de datos y configurar la interfaz de programación de aplicación (API) de IBM Spectrum Protect.


## Acerca de esta tarea

---

Si utiliza el asistente de configuración para crear una instancia de servidor de IBM Spectrum Protect, no debe completar estos pasos. Si va a configurar una instancia manualmente, complete los pasos siguientes antes de emitir los mandatos BACKUP DB o RESTORE DB.

Atención: Si la base de datos se encuentran en un estado que no permite su utilización, el servidor IBM Spectrum Protect completo no está disponible. Si se pierde una base de datos y no se puede recuperar, sería muy difícil o imposible recuperar los datos gestionados por ese servidor. Por lo tanto, es muy importante realizar copia de seguridad de la base de datos.

 **Sistemas operativos Windows** Restricción: La copia de seguridad y restauración de base de datos sobre memoria compartida no está disponible en sistemas Windows.

 **Sistemas operativos Windows** En los siguientes mandatos, los ejemplos empleados son `server1` como instancia de la base de datos y `d:\tsmsvr1` para el directorio del servidor de IBM Spectrum Protect. Sustituya estos valores por sus valores reales en los mandatos.

1. Cree un archivo que se llame `tsmdbmgr.env` en el directorio `d:\tsmsvr1` con el siguiente contenido:

```
DSMI_CONFIG=directorio_instancia_servidor\tsmdbmgr.opt
DSMI_LOG=directorio_instancia_servidor
```

2. Establezca la configuración de la variable de entorno `DSMI_api` para la instancia de la base de datos:

- a. Abra una ventana de mandatos de DB2. Uno de los métodos consiste en ir al directorio `C:\Archivo de programas\Tivoli\TSM\db2\bin`, o si ha instalado IBM Spectrum Protect en una ubicación diferente, ir al subdirectorio `db2\bin` de su directorio de instalación principal. Después, emita este mandato:

```
db2cmd
```

- b. Emita este mandato:

```
db2set -i server1 DB2_VENDOR_INI=d:\tsmsvr1\tsmdbmgr.env
```

3. Cree un archivo que se denomine `tsmdbmgr.opt` en el directorio `d:\tsmsvr1` con el siguiente contenido:

```
*****
nodename $$_TSMDBMGR_$$
commethod          tcpip
tcpserveraddr localhost
tcpport            1500
passwordaccess generate
errorlogname d:\tsmsvr1\tsmdbmgr.log
```

donde

- o `nodename` especifica el nombre de nodo que la API de cliente utiliza para conectarse al servidor durante una copia de seguridad de base de datos. Este valor debe ser `$$_TSMDBMGR_$$` para que una copia de seguridad de base de datos funcione.
- o `commethod` especifica la API de cliente utilizada para ponerse en contacto con el servidor para la copia de seguridad de base de datos.
- o `tcpserveraddr` especifica la dirección de servidor que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Para asegurarse que se puede hacer copia de seguridad de la base de datos, este valor debe ser `localhost`.
- o `tcpport` especifica el número de puerto que la API de cliente utiliza para ponerse en contacto con el servidor para la copia de seguridad de base de datos. Asegúrese de entrar el mismo valor de `tcpport` que se ha especificado en el archivo de opciones del servidor `dsmserv.opt`.
- o se requiere `passwordaccess` para que el nodo de copia de seguridad se conecte al servidor en el sistema Windows.
- o `errorlogname` especifica el registro de errores donde la API de cliente registra los errores que se encuentran durante una copia de seguridad de base de datos. Este registro por lo general está en el directorio de la instancia del servidor. Sin embargo, este registro se puede poner en cualquier ubicación en la que el ID de usuario de instancia tenga permiso de escritura.

## Windows: Configuración de las opciones de servidor para el mantenimiento de la base de datos del servidor


---

Para evitar problemas debido al crecimiento de la base de datos y el rendimiento del servidor, el servidor supervisa automáticamente sus tablas de base de datos y las reorganiza cuando es necesario. Antes de iniciar el servidor para su uso en producción, establezca las opciones del servidor para controlar cuándo se ejecuta la reorganización. Si tiene planificado utilizar la deduplicación de datos, asegúrese de que la opción de ejecutar la reorganización de índice esté habilitada.

## Acerca de esta tarea

---

La reorganización de índice y tabla requiere recursos de procesador, espacio de anotaciones activas y espacio de anotaciones de archivado considerables. Debido a que la copia de seguridad de la base de datos tiene preferencia sobre la reorganización, seleccione la hora y la duración para la reorganización para garantizar que los procesos no se solapen y que se pueda completar la reorganización.


 Sistemas operativos Windows Puede optimizar la reorganización de tablas e índices en la base de datos del servidor. De este modo, puede ayudar a evitar problemas de rendimiento y el crecimiento inesperado de la base de datos. Si desea instrucciones, consulte la nota técnica 1683633.

Si actualiza estas opciones del servidor mientras el servidor está en ejecución, debe detener y reiniciar el servidor para que se apliquen los valores actualizados.

## Procedimiento

---

1. Modifique las opciones del servidor.

 Sistemas operativos Windows Edite el archivo de opciones del servidor, `dsmserv.opt`, en el directorio de instancias del servidor mediante el editor de texto. Siga estas instrucciones al editar el archivo de opciones del servidor:

- Para habilitar una opción, elimine el asterisco al principio de la línea.
- Entre una opción en cualquier línea.
- Escriba sólo una opción por línea. Toda la opción, con su valor, debe estar en una sola línea.
- Si tiene varias entradas para una opción en el archivo, el servidor utiliza la última.

Para ver las opciones disponibles del servidor, consulte el archivo de ejemplo, `dsmserv.opt.smp`, en el directorio `c:\Program Files\Tivoli\TSM`.

2. Si tiene pensado utilizar la deduplicación de datos, habilite la opción del servidor `ALLOWREORGINDEX`. Agregue la siguiente opción y valor al archivo de opciones del servidor:

```
allowreorgindex yes
```

3. Establezca las opciones de servidor `REORGBEGINTIME` y `REORGDURATION` para controlar cuándo se inicia la reorganización y durante cuánto tiempo se ejecuta. Seleccione una hora y una duración para que la reorganización se ejecute cuando se espera que el servidor esté menos ocupado. Estas opciones del servidor controlan los procesos de reorganización de índice y de tabla.
  - a. Establezca la hora de inicio de la reorganización mediante la opción del servidor `REORGBEGINTIME`. Especifique la hora utilizando el sistema de 24 horas. Por ejemplo, para establecer la hora de inicio de la reorganización en las 20:30, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgbegintime 20:30
```

- b. Establezca el intervalo durante el cual el servidor puede iniciar la reorganización. Por ejemplo, para especificar que el servidor pueda iniciar la reorganización durante cuatro horas después de la hora fijada por la opción de servidor `REORGBEGINTIME`, especifique la siguiente opción y valor en el archivo de opciones del servidor:

```
reorgduration 4
```

4. Si el servidor estaba en ejecución al actualizar el archivo de opciones del servidor, detenga y reinicie el servidor.


### Información relacionada:

 [ALLOWREORGINDEX](#)

 [ALLOWREORGTABLE](#)

 [REORGBEGINTIME](#)

 [REORGDURATION](#)

 Sistemas operativos Windows

## Windows: Inicio de la instancia del servidor en sistemas Windows

---

En un entorno de producción, el método preferido para iniciar el servidor es como un servicio Windows. En un entorno en el que va a reconfigurar, probar o completar tareas de mantenimiento, inicie el servidor en primer plano o utilice la modalidad de mantenimiento.

### Antes de empezar

---

Seleccione uno de los siguientes métodos para iniciar el servidor:

Como un servicio de Windows

Este método resulta útil en un entorno de producción. Cuando configure el servidor para que se ejecute como un servicio, puede especificar que el servidor se inicie automáticamente siempre que se inicie el sistema.

En el primer plano



Este método es útil cuando está configurando o probando el servidor. Cuando inicia el servidor en segundo plano, IBM Spectrum Protect proporciona un ID de usuario de administrador especial que se denomina SERVER\_CONSOLE. Todos los mensajes de servidor se muestran en primer plano. Los mensajes pueden ser útiles si debe depurar problemas de inicio.


En modalidad de mantenimiento

Este método resulta útil cuando va a completar tareas de mantenimiento o reconfiguración. Cuando inicie el servidor en modalidad de mantenimiento, debe inhabilitar las operaciones que puedan interrumpir las tareas de mantenimiento o reconfiguración.

## Procedimiento

Siga las instrucciones para la opción seleccionada:

Opción	Descripción
<b>Inicio del servidor como un servicio de Windows.</b>	Para iniciar el servidor como un servicio de Windows, lleve a cabo una de las siguientes acciones: <ul style="list-style-type: none"><li>• Si ha configurado el servidor utilizando el asistente de configuración, realice los siguientes pasos:<ol style="list-style-type: none"><li>a. Configure el servidor para que se inicie como un servicio de Windows siguiendo las instrucciones de Windows: Configuración del servidor para que se inicie como un servicio de Windows.</li><li>b. Inicie el servidor siguiendo las instrucciones de Windows: Inicio del servidor como un servicio de Windows..</li></ol></li><li>• Si no ha utilizado el asistente de configuración cree y configure el servicio Windows siguiendo las instrucciones de Windows: Creación manual y configuración de un servicio de Windows.</li></ul>
<b>Inicio del servidor en segundo plano</b>	Para iniciar el servidor en segundo plano, siga las instrucciones en Windows: Inicio del servidor en segundo plano.
<b>Inicio del servidor en modalidad de mantenimiento</b>	Para iniciar el servidor en modalidad de mantenimiento, siga las instrucciones de Windows: Inicio del servidor en modalidad de mantenimiento.

 Sistemas operativos Windows

## Windows: Configuración del servidor para que se inicie como un servicio de Windows

Antes de poder iniciar el servidor como un servicio de Windows, debe asegurarse de que las opciones y los derechos de acceso se han establecido correctamente.

### Antes de empezar

Se debe crear un servicio de Windows. Si ha configurado el servidor utilizando el asistente de configuración,, se ha creado automáticamente un servicio Windows. En ese caso, utilice este procedimiento para configurar el servidor para que se inicie como un servicio de Windows.

Si no ha utilizado un asistente, debe crear y configurar el servicio de Windows de forma manual siguiendo los pasos de Windows: Creación manual y configuración de un servicio de Windows.

## Procedimiento

1. Desde el menú de Windows Inicio, pulse Ejecutar, escriba `services.msc`, y pulse Aceptar.
2. En la ventana Servicios, seleccione la instancia del servidor que desea iniciar como servicio, y pulse Propiedades. Por ejemplo, seleccione TSM INST1, y pulse Propiedades.
3. Para asegurarse de que el servicio del servidor inicia automáticamente, pulse la pestaña General. Desde la lista Tipo de inicio, seleccione Automático.
4. Para establecer el usuario para que inicie el servicio de servidor, pulse el separador Iniciar sesión y realice una de las acciones siguientes:
  - Si tiene previsto ejecutar el servicio de servidor bajo la cuenta de sistema local, seleccione Cuenta de sistema local y pulse Aceptar.
  - Si piensa ejecutar el servicio de servidor bajo el ID de usuario de instancia, realice las acciones siguientes:
    - a. Seleccione Esta cuenta, y navegue hasta el ID de usuario propietario de la instancia DB2 del servidor y que tiene permisos para iniciar el servidor.
    - b. En la ventana Seleccionar usuario, en el campo Escriba el nombre de objeto a seleccionar, escriba el ID de usuario.
    - c. Pulse Comprobar nombres.

- d. Pulse Aceptar dos veces.
5. Si ha configurado el servicio de servidor para que se ejecute bajo la cuenta de sistema local, otorgue acceso de base de datos a la cuenta de sistema local:
- Inicie sesión con el ID de usuario que se utilizó para crear la base de datos de servidor. Este ID de usuario es el ID de usuario que se utiliza para ejecutar el programa de utilidad DSMSEV FORMAT para inicializar la base de datos de servidor. De forma alternativa, si ha configurado el servidor con el asistente de configuración dsmicfgx, este ID de usuario es el ID de usuario que se ha utilizado para crear la instancia.
  - Abra una ventana de mandatos de DB2. Si el servidor está instalado en Windows Server 2012, abra la ventana Inicio y pulse Ventana de mandatos DB2 - Administrador.
  - En la ventana de mandatos de DB2, especifique los siguientes mandatos:

```
set DB2INSTANCE=server1
db2 connect to TSMDB1
db2 grant dbadm with dataaccess with accessctrl on database to user system
db2 grant secadm on database to user system
```

Consejo: Si se configura el servicio del servidor para que se ejecute bajo la cuenta del Sistema local, cualquier administrador del sistema puede acceder a la base de datos. Además, cualquier administrador que pueda iniciar sesión en el sistema puede ejecutar el servidor.

## Qué hacer a continuación

---

Para iniciar el servicio, siga las instrucciones en Windows: Inicio del servidor como un servicio de Windows..

 Sistemas operativos Windows

## Windows: Inicio del servidor como un servicio de Windows.

---

Si está ejecutando el sistema operativo IBM Spectrum Protect on a Windows, puede iniciar el servidor como un servicio.

### Antes de empezar

---

Se debe crear un servicio de Windows. El servicio se ha creado automáticamente si ha configurado el servidor utilizando el asistente de configuración.. Si el servicio se ha creado automáticamente, debe configurar el servidor para que se inicie como un servicio siguiendo los pasos en Windows: Configuración del servidor para que se inicie como un servicio de Windows. A continuación, utilice este procedimiento para iniciar el servidor como un servicio.

Si no ha utilizado el asistente de configuración para crear el servicio, debe crear y configurar el servicio manualmente. Siga los pasos descritos en Windows: Creación manual y configuración de un servicio de Windows.

### Procedimiento

---

Para iniciar el servidor como un servicio de Windows, siga estos pasos:

- Inicie sesión en el servidor con un ID de usuario que está en el grupo de administradores.
- Desde el menú de Windows Inicio, pulse Ejecutar, escriba `services.msc`, y pulse Aceptar.
- En la ventana Servicios, seleccione la instancia del servidor que desea iniciar, y pulse Iniciar.

## Qué hacer a continuación

---

Debido que el servicio del servidor puede emitir solicitudes que requieren tomar una acción, es importante supervisar la actividad del servidor con el Centro de operaciones o el cliente administrativo.

Para ver los mensajes de inicio y detención registrados en el registro de aplicaciones de Windows, use la herramienta Visor de sucesos en la carpeta Herramientas administrativas.

 Sistemas operativos Windows

## Windows: Creación manual y configuración de un servicio de Windows

---

Si ha configurado el servidor utilizando el asistente de configuración, se ha creado automáticamente un servicio Windows. Si no se ha creado un servicio automáticamente, debe crearlo.

### Antes de empezar

---

Para completar este procedimiento, debe iniciar la sesión con un ID de usuario que esté en el grupo de administradores.

## Procedimiento

Para crear un servicio de Windows y configurar las opciones de inicio del servicio, complete el paso siguiente:

Abra una ventana de mandatos y entre el mandato `sc.exe create`:

```
sc.exe create nombre_servidor binPath= "vía_acceso_a_servidor -k nombre_instancia"  
start= tipo_inicio obj= nombre_cuenta password= contraseña
```

donde:

*nombre\_servidor*

Especifica el nombre del servicio de servidor.

*vía\_acceso\_a\_servidor*

Especifica la vía de acceso al archivo ejecutable `dedsmsvc.exe`, incluyendo el nombre de archivo. Esta vía de acceso es la vía de acceso predeterminada:

C:\Archivos de programa\Tivoli\TSM\server

*nombre\_instancia*

Especifica el nombre de la instancia de DB2, que también es el nombre de la instancia de servidor, por ejemplo `Server1`.

*tipo\_inicio*

Especifica el método para iniciar el servicio. Para iniciar automáticamente el servicio, entre `auto`. Si especifica la opción `auto`, el servicio se inicia automáticamente al arrancar el sistema y se reinicia automáticamente siempre que se reinicia el sistema. Para iniciar manualmente el servicio, entre `demand`.

*nombre\_cuenta*

Especifica el ID de usuario de la cuenta bajo la que se ejecuta el servicio. Por ejemplo, el nombre de cuenta puede ser `Administrator`. Este parámetro es opcional. Si no se especifica, se utiliza la cuenta del sistema local.

*contraseña*

Especifica la contraseña para la cuenta de usuario de *nombre\_cuenta*.

Consejo: Cuando entre el mandato, asegúrese de entrar un espacio después de cada signo de igual (=).

## Resultados

El servidor se inicia como un servicio Windows.

 Sistemas operativos Windows

## Windows: Inicio del servidor en segundo plano

Para interactuar de forma directa con un servidor de IBM Spectrum Protect, inicie el servidor en segundo plano. Por ejemplo, si desea escribir mandatos, inicie el servidor en segundo plano.

## Procedimiento

1. Cambie al directorio donde está instalado el servidor. Por ejemplo, cambie el directorio `c:\Archivos de programa\tivoli\tsm\server`.
2. Entre el mandato siguiente:

```
dsmserv -k nombre_instancia
```

donde *nombre\_instancia* especifica la instancia de servidor.

 Sistemas operativos Windows


## Windows: Servicios asociados al servidor en sistemas Windows

Cuando se inicia el servidor IBM Spectrum Protect como un servicio, otros servicios se inician automáticamente. Estos servicios están asociados con el gestor de la base de datos, DB2.

Los servicios siguientes están asociados al servidor.

Nombre del servicio	Finalidad	Comentarios.
---------------------	-----------	--------------

Nombre del servicio	Finalidad	Comentarios.
TSM <i>Server_instance</i>	El servicio para la instancia de servidor que se llama <i>instancia_servidor</i> .  Por ejemplo: TSM Server1	Defina las opciones de inicio y parada de este servicio para que inicien y detengan la instancia del servidor automáticamente.  Cada instancia del servidor se ejecuta como un servicio diferente.
DB2 - DB2TSM1 - <i>SERVER_INSTANCE</i>	El servicio de DB2 para la instancia del servidor se llama <i>Server_instance</i> .  Por ejemplo: DB2 - DB2TSM1 - SERVER1	Este servicio se inicia automáticamente cuando se inicia el servicio para la instancia de servidor. El servicio DB2 no se detiene de forma automática cuando detiene el servicio del servidor.  El sistema tiene uno de estos servicios para cada servicio de la instancia del servidor que se inicia en el sistema.
DB2 Governor (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 License Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 Management Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.
DB2 Remote Command Server (DB2TSM1)	Un servicio DB2 que se crea durante la instalación, y se requiere para todas las instancias del servidor.	No modifique las opciones de este servicio.

 Sistemas operativos Windows

## Windows: Inicio del servidor en modalidad de mantenimiento

Puede iniciar el servidor en modalidad de mantenimiento para evitar interrupciones durante las tareas de mantenimiento y reconfiguración.

### Acerca de esta tarea

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las operaciones siguientes están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación de espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, no se permite que los clientes inicien sesiones con el servidor.

Consejos:

- No es necesario que edite el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Mientras el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente los procesos de reclamación de espacio de almacenamiento, caducidad de inventario y migración de agrupaciones de almacenamiento.

### Procedimiento

Para iniciar el servidor en modalidad de mantenimiento, emita el mandato siguiente:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca del inicio del servidor en modalidad de mantenimiento, consulte Inicio de un servidor en modalidad de mantenimiento.

### Qué hacer a continuación

Para reanudar las operaciones del servidor en modalidad de producción, realice los pasos siguientes:

1. Concluya el servidor emitiendo el mandato HALT:

```
halt
```

2. Inicie el servidor utilizando el método que utilice en la modalidad de producción.

Se vuelven a habilitar las operaciones que se inhabilitaron durante la modalidad de mantenimiento.

## Windows: Detención del servidor

---

Puede detener el servidor cuando sea necesario para regresar el control al sistema operativo. Para impedir la pérdida de conexiones de administración y de nodo de cliente, detenga el servidor únicamente después de que las sesiones actuales hayan finalizado o se hayan cancelado.

### Acerca de esta tarea

---

Para detener el servidor, emita el siguiente mandato desde la línea de mandatos IBM Spectrum Protect:

```
halt
```

## Windows: Registro de licencias

---

Registre inmediatamente todas las características bajo licencia de IBM Spectrum Protect que adquiera para evitar perder datos una vez que empiece a realizar operaciones de servidor, como por ejemplo copias de seguridad de datos.

### Acerca de esta tarea

---

Para esta tarea, utilice el mandato REGISTER LICENSE. Consulte REGISTER LICENSE para ver más detalles.

### Ejemplo: registrar una licencia

---

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## Windows: Especificación de una clase de dispositivo en la preparación de copias de seguridad de bases de datos

---

Para preparar el sistema con el fin de realizar copias de seguridad automáticas y manuales de la base de datos, debe especificar la clase de dispositivo que se va a utilizar.

### Antes de empezar

---

Asegúrese de haber definido una clase de dispositivo de archivo o cinta. Para obtener detalles, consulte DEFINE DEVCLASS o busque cómo definir una clase de dispositivo.

### Acerca de esta tarea

---

Complete los pasos siguientes para configurar el sistema para copias de seguridad de base de datos.

### Procedimiento

---

1. Si no ha utilizado el asistente de configuración (dsmicfgx) para configurar el servidor, asegúrese de haber completado los pasos necesarios para configurar el sistema de forma manual para la realización de copias de seguridad de la base de datos.
2. Seleccione la clase de dispositivo que se utilizará para realizar las copias de seguridad de la base de datos. Emita el mandato siguiente desde una línea de mandatos de administración de IBM Spectrum Protect.

```
set dbrecovery device_class_name
```

La clase de dispositivo especificada será utilizada por el gestor de la base de datos para realizar las copias de seguridad de la misma. Si no especifica una clase de dispositivo con el mandato SET DBRECOVERY, la copia de seguridad falla.

## Ejemplo


Por ejemplo, para especificar el uso de la clase de dispositivo DBBACK, emita el siguiente mandato:

```
set dbrecovery dbback
```

## Windows: Ejecución de varias instancias de servidor en un solo sistema

Puede crear más de una instancia del servidor en el sistema. Cada instancia del servidor tiene su propio directorio de instancias y directorios de registro y base de datos.


Multiplique la memoria y otros requisitos del sistema para un servidor por el número de instancias planeadas para el sistema.


 Sistemas operativos Windows El conjunto de archivos para una instancia del servidor se almacena separado de los archivos que utiliza otra instancia de servidor en el mismo sistema. Siga los pasos detallados en Windows: Creación de una instancia del servidor para cada instancia nueva, de forma opcional creando el usuario de instancia nuevo.

Para gestionar la memoria del sistema utilizada por cada servidor, utilice la opción de servidor DBMEMPERCENT para limitar el porcentaje de memoria del sistema. Si todos los servidores tienen la misma importancia, utilice el mismo valor para cada uno. Si un servidor es de producción y los demás son de prueba, establezca el valor del servidor de producción por encima del valor de los servidores de prueba.


Puede actualizar directamente desde V6.3 a V7.1. Consulte la sección de actualización (Actualización a V8.1) para ver más detalles. Cuando actualiza y tiene varios servidores en el sistema, debe ejecutar el asistente de instalación solamente una vez. El asistente de instalación recopila la base de datos y la información de variables de las instancias originales del servidor.

Si actualiza desde IBM Spectrum Protect V6.3 a V8.1.2 y tiene muchos servidores en el sistema, todas las instancias que existan en DB2 V9.7 se descartarán y se volverán a crear en DB2 V11.1. El asistente emite el mandato `db2 upgrade db dbname` para cada base de datos. Las variables de entorno de la base de datos para cada una de las instancias del sistema también se reconfiguran durante el proceso de actualización.

 Sistemas operativos Windows Una instalación típica de IBM Spectrum Protect incluye una instancia del servidor en el sistema servidor de IBM Spectrum Protect. Es posible que desee instalar una segunda instancia si está configurando un entorno en clúster. También puede que desee ejecutar más de un servidor en un sistema grande si tiene varias bibliotecas de cintas o una configuración sólo de disco. Después de instalar y configurar el primer servidor de IBM Spectrum Protect, utilice el asistente de inicialización del servidor para crear instancias adicionales del servidor de IBM Spectrum Protect en el mismo sistema.

 Sistemas operativos Windows mediante el asistente de inicialización del servidor puede instalar hasta cuatro instancias del servidor de IBM Spectrum Protect en un solo sistema o clúster.

### Tareas relacionadas:

 Ejecución de varias instancias de servidor en un sistema único (V7.1.1)

## Windows: Supervisión del servidor

Cuando empiece a utilizar el servidor en producción, supervise el espacio utilizado por el servidor para asegurarse de que la cantidad de espacio es adecuada. Ajuste el espacio si fuera necesario.

### Procedimiento

1. Supervise las anotaciones activas para garantizar que el tamaño de la carga de trabajo gestionada por la instancia del servidor es correcto.

Cuando la carga de trabajo del servidor alcanza su nivel típico aceptado, el espacio que utiliza el registro activo es del 80% - 90% del espacio que está disponible en el directorio de registro activo. En este punto, es posible que necesite aumentar la cantidad de espacio. Aumentar o no el espacio depende de los tipos de transacciones de la carga del servidor. Las características de la transacción afectan a cómo se utiliza el espacio de registro de archivos.

Las siguientes características de una transacción pueden afectar la utilización del espacio en el registro activo:

- El número y el tamaño de los archivos de las operaciones de copia de seguridad
  - Los clientes como los servidores de archivo que respaldan grandes cantidades de archivos pequeños pueden causar un gran número de transacciones realizan rápido. Estas transacciones pueden utilizar una gran cantidad de espacio de las anotaciones activas, pero durante poco tiempo.
  - Los clientes, como el servidor de correo o el servidor de base de datos, que realizan copias de seguridad de grandes cantidades de datos en pocas transacciones pueden hacer que un número reducido de transacciones tarde mucho

tiempo en completarse. Es posible que las transacciones utilicen poco espacio en el registro de archivado, pero durante mucho tiempo.

- o Tipos de conexiones de red
  - Las operaciones de copia de seguridad que se producen a través de conexiones de red rápidas hacen que las transacciones se completen más rápidamente. Las transacciones utilizan espacio en el registro activo durante poco tiempo.
  - Las operaciones de copia de seguridad que se producen a través de conexiones relativamente más lentas hacen que las transacciones tardan más tiempo en completarse. Las transacciones utilizan espacio en el registro activo durante un tiempo más largo.

Si el servidor está manejando transacciones con una amplia variedad de características, es posible que el espacio que se utiliza para el registro activo aumente o disminuya con el paso del tiempo. En este caso, quizá necesite garantizar que, por regla general, se utilice un porcentaje menor del espacio de registro activo. El espacio adicional permite que el registro activo pueda aumentar para transacciones que tardan un tiempo considerable en completarse.

2. Supervise el registro de archivado para garantizar que haya siempre espacio disponible. Recuerde: Si el registro de archivado y el registro de archivado de migración tras error llegan al máximo de su capacidad, el registro activo puede llenarse y hacer que el servidor se detenga. El objetivo es crear suficiente espacio libre para el registro de archivado, de forma que nunca utilicen todo el espacio del que dispone.

Probablemente observará el siguiente patrón:

- a. En un principio, el registro de archivado aumenta rápidamente, como suele ocurrir en las operaciones de copia de seguridad de cliente.
- b. Se realizan copias de seguridad de base de datos regularmente, tanto planificadas como manuales.
- c. Después de al menos dos copias de seguridad de base de datos completas, se produce una poda de registros de forma automática. El espacio que utiliza el registro de archivado decrece tras la poda.
- d. Siguen las operaciones de cliente normales y el registro de archivado vuelve a aumentar.
- e. Se realizan copias de seguridad de base de datos regularmente y se producen podas de registros con la misma frecuencia que las copias de seguridad completas.

Con este patrón, el registro de archivado crece inicialmente, decrece y después es posible que vuelva a crecer. A lo largo del tiempo, mientras las operaciones normales continúan, la cantidad de espacio que utiliza el registro de archivado debería alcanzar un nivel constante relativo.

Si el registro de archivado continúa creciendo, puede tomar una de las siguientes medidas:

- o Añadir espacio al registro de archivado. Es posible que necesite trasladar el registro de archivado a un sistema de archivos diferente.
  - o Aumentar la frecuencia de las copias de seguridad de base de datos completas para que la poda de archivos tenga lugar más a menudo.
3. Si definió un directorio para el registro de archivado de migración tras error, compruebe si durante las operaciones normales se almacenan registros en este directorio. Si se está utilizando el espacio de registro de migración tras error, es recomendable que aumente el tamaño del registro de archivado. El fin de esto es que el registro de archivado de migración tras error se utilice exclusivamente en situaciones excepcionales, no durante el funcionamiento normal.

## Windows: Instalación de un fixpack de servidor de IBM Spectrum Protect

---

Las actualizaciones de mantenimiento de IBM Spectrum Protect, también denominadas fixpacks, actualizan el servidor al nivel de mantenimiento actual.

### Antes de empezar

---

Para instalar un fixpack o arreglo temporal en el servidor, instale el servidor al nivel al que desea ejecutarlo. No es necesario que inicie la instalación del servidor al nivel del release base. Por ejemplo, si actualmente tiene instalada la V8.1.1, puede ir directamente al último fixpack de la V8.1. No tiene que empezar con la instalación de V8.1.0 si hay disponible una actualización de mantenimiento.

Debe tener instalado el paquete de licencias de IBM Spectrum Protect. El paquete de licencias se proporciona con la adquisición de un release básico. Al descargar un fixpack o un arreglo temporal de Fix Central, instale la licencia del servidor que está disponible en el sitio web de Passport Advantage. Para visualizar los mensajes y la ayuda en un idioma distinto al inglés de Estados Unidos, instale el paquete de idioma que elija.

Si actualiza el servidor a V8.1.2 o posterior, y luego revierte el servidor a un nivel anterior a V8.1.2, tiene que restaurar la base de datos a un momento anterior a la actualización. Durante el proceso de actualización, complete los pasos necesarios para asegurarse de que se pueda restaurar la base de datos: realice copias de seguridad de la misma, del archivo de historial de volumen, del archivo de configuración de dispositivo y del archivo de opciones de servidor. Para obtener más información, consulte el apartado Windows: Revertida de la versión 8.1.2 a un servidor anterior.

Si utiliza el servicio de gestión de clientes, asegúrese de actualizarlo a la misma versión que el servidor de IBM Spectrum Protect.

Asegúrese de conservar los recursos de instalación desde el release base del servidor instalado. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Visite IBM® Support Portal para ver la información siguiente:

- Una lista de los últimos arreglos de mantenimiento y descarga. Pulse **Downloads** y aplique los arreglos pertinentes.
- Detalles sobre cómo obtener un paquete de licencias base. Busque **Downloads > Passport Advantage**.
- Plataformas soportadas y requisitos del sistema. Busque sistemas operativos soportados de **IBM Spectrum Protect**.

Asegúrese de actualizar el servidor antes de actualizar los clientes de archivado y copia de seguridad. Si no actualiza el servidor primero, la comunicación entre el servidor y los clientes puede verse interrumpida.

Atención: No altere el software de DB2 que se ha instalado con los paquetes de instalación de IBM Spectrum Protect y los fixpacks. No instale ni actualice a una versión, release o fixpack diferente del software de DB2 porque puede dañar la base de datos.

## Procedimiento

---

Para instalar un fixpack o arreglo temporal, complete los siguientes pasos:

1. Realice una copia de seguridad de la base de datos. El método preferido es el uso de una copia de seguridad instantánea. Una copia de seguridad instantánea es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de bases de datos planificadas. Por ejemplo, emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración del dispositivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:


```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Guarde el archivo histórico de volúmenes en otro directorio o cambie el nombre del archivo. Emita el siguiente mandato administrativo de IBM Spectrum Protect:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga el servidor antes de instalar un fixpack o arreglo temporal. Utilice el mandato HALT.
6. Asegúrese de disponer de espacio adicional en el directorio de instalación La instalación de este fixpack puede requerir espacio de disco temporal adicional en el directorio de instalación del servidor. La cantidad de espacio de disco adicional puede ser tanta como la necesaria para instalar una nueva base de datos como parte de una instalación de IBM Spectrum Protect. El asistente de instalación de IBM Spectrum Protect muestra la cantidad de espacio necesaria para instalar el fixpack y la cantidad disponible. Si la cantidad de espacio necesaria es mayor que la cantidad disponible, la instalación se detiene. Si la instalación se detiene, añada el espacio de disco necesario al sistema de archivos y reinicie la instalación.
7. Obtenga el archivo de paquete para el fixpack o el arreglo temporal que desea instalar en IBM Support Portal, Passport Advantage o Fix Central.
8.  Sistemas operativos Windows Cambie al directorio en el que colocó el archivo ejecutable. A continuación, pulse dos veces en el siguiente archivo ejecutable o introduzca el siguiente mandato en la línea de mandatos para extraer los archivos de instalación. Consejo: Los archivos se extraen al directorio actual. Asegúrese de que el archivo ejecutable está en el directorio en el que desea que se ubiquen los archivos extraídos.

```
8.x.x.x-IBM-SPSRV-plataforma.exe
```

donde: *plataforma* indica el sistema operativo en el que se va a instalar IBM Spectrum Protect.

9. Seleccione una de los siguientes métodos de instalación de IBM Spectrum Protect.  
Importante: Después de instalar un fixpack, no es necesario ir a través de la configuración de nuevo. Puede parar después de completar la instalación, arreglar cualquier error y, después, iniciar sus servidores.  
Instale el software de IBM Spectrum Protect utilizando uno de los siguientes métodos:

Asistente de instalación

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect mediante el asistente de instalación



Consejo: Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Update; no pulse el icono Install o Modify.

Línea de mandatos en modalidad de consola

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect en modalidad de consola

Modalidad silenciosa

Siga las instrucciones para el sistema operativo:

Windows: Instalación de IBM Spectrum Protect en modalidad silenciosa

Consejo: Si tiene varias instancias del servidor en el sistema, ejecute el asistente de instalación una sola vez. El asistente de instalación actualiza todas las instancias de servidor.

## Resultados

---

Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.

Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:

-  Sistemas operativos WindowsC:\ProgramData\IBM\Installation Manager\logs
-  Sistemas operativos WindowsWindows: Aplicación de un fixpack a IBM Spectrum Protect 8.1.2 en un entorno en clúster para Windows  
Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.2.

## Windows: Revierta de la versión 8.1.2 a un servidor anterior

---

Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.

### Antes de empezar

---

Debe tener los siguientes elementos de la versión anterior del servidor:


- Una copia de seguridad de base de datos completa
- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor

### Acerca de esta tarea

---

Utilice las mismas instrucciones si está realizando una reversión entre releases o a un release anterior, por ejemplo, del 8.1.2 al 8.1.1 o del 8.1.2 al 7.1.2. La versión más antigua debe coincidir con la versión que se utilizaba antes de la actualización a la versión 8.1.

Atención: Especifique el parámetro REUSEDELAY para ayudar a evitar la pérdida de datos del cliente de copia de seguridad/archivado al revertir el servidor a una versión anterior.

-  Sistemas operativos WindowsWindows: Reversión a la versión de servidor anterior en una configuración de clúster  
Si debe volver a la versión anterior del servidor después de una actualización, debe tener una copia completa de la base de datos de su versión original. Asimismo, debe tener el soporte de instalación del servidor para la versión original y los archivos de configuración de clave. Siga atentamente los pasos de preparación antes de actualizar el servidor. Al hacerlo, se puede volver a la versión anterior del servidor de IBM Spectrum Protect con una mínima pérdida de datos.


### Pasos para recuperar la versión anterior del servidor


---

#### Acerca de esta tarea

Complete los pasos siguientes en el sistema que tiene la versión V8.1 del servidor.

## Procedimiento

1. Pare el servidor para cerrar todas las operaciones del servidor utilizando el mandato HALT.
2. Elimine la base de datos del gestor de bases de datos y luego suprima los directorios de registro de base de datos y de recuperación.
  - a. Elimine manualmente la base de datos. Una forma de eliminarla es emitiendo este mandato:  
 Sistemas operativos Windows  

```
dsmserv -k nombre_instancia removedb tsmdb1
```
  - b. Si debe reutilizar el espacio ocupado por los directorios de registro de recuperación y base de datos, puede eliminar estos directorios.
3. Utilice el programa de desinstalación para desinstalar el servidor de la versión 8.1. La desinstalación elimina el servidor y el gestor de bases de datos, con sus directorios. Para obtener detalles, consulte el apartado Windows: Desinstalar IBM Spectrum Protect.
4. Detenga el servicio de clúster. Reinstale la versión del programa del servidor que estaba utilizando antes de la actualización a V8.1.2. Esta versión debe coincidir con la versión que estaba ejecutando el servidor cuando creó la copia de seguridad de la base de datos que restaurará en un paso posterior. Por ejemplo, el servidor estaba en la versión 7.1.7 antes de la actualización y quiere utilizar la copia de seguridad de base de datos que se estaba utilizando en este servidor. Debe instalar el fixpack V7.1.7 para poder restaurar la copia de seguridad de la base de datos.
5. Configure la nueva base de datos del servidor usando el asistente de configuración. Para iniciar el asistente, emita el siguiente mandato:  Sistemas operativos Windows  

```
/dsmicfgx
```
6. Asegúrese de que no se esté ejecutando ningún servidor en segundo plano.
7. Restaure la base de datos a un momento determinado anterior a la actualización.
8. Copie los siguientes archivos en el directorio de instancias.
  - o Archivo de configuración de dispositivos
  - o Archivo histórico de volúmenes
  - o El archivo de opciones de servidor (generalmente dsmserv.opt)
9. Si ha habilitado la eliminación de la duplicación de datos para toda agrupación de almacenamiento de tipo FILE que pudiera existir antes de la actualización, o si ha movido datos que existían antes de la actualización a nuevas agrupaciones de almacenamiento utilizando el servidor de la V8.1.2, deberá completar pasos de recuperación adicionales. Para conocer más detalles, consulte Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados.
10. Si el parámetro REUSEDELAY de las agrupaciones de almacenamiento es menor que la antigüedad de la base de datos que ha restaurado, restaure volúmenes en cualquier agrupación de almacenamiento de acceso secuencial reclamada tras la copia de seguridad de la base de datos. Utilice el mandato RESTORE VOLUME.  
Si no tiene una copia de seguridad de una agrupación de almacenamiento, realice una auditoría de los volúmenes reclamados con el mandato AUDIT VOLUME, con el parámetro FIX=YES para resolver incoherencias. Por ejemplo:  

```
audit volume nombre_volumen fix=yes
```
11. Si se completaron operaciones de archivado o de copia de seguridad usando el servidor V8.1, audite los volúmenes de la agrupación de almacenamiento en los cuales se almacenaron los datos.

## Pasos de recuperación adicionales si ha creado nuevas agrupaciones de almacenamiento o ha habilitado la eliminación de datos duplicados

---

Si creó nuevas agrupaciones de almacenamiento, habilitó la optimización de almacenamiento de cualquier agrupación de almacenamiento tipo FILE o hizo ambas cosas mientras el servidor se ejecutaba como servidor V8.1.2, deberá completar más pasos para volver a la versión anterior del servidor.

### Antes de empezar

Para completar esta tarea, debe tener una copia de seguridad completa de la agrupación de almacenamiento que se creó antes de la actualización a V8.1.2.

### Acerca de esta tarea

Utilice esta información si ha realizado una de las siguientes acciones, o las dos, cuando el servidor se estaba ejecutando como un servidor V8.1.2:

- Ha activado la función de optimización de almacenamiento de datos de cualquier agrupación de almacenamiento que existiera antes de la actualización del programa V8.1.2. La eliminación de datos duplicados sólo se aplica a agrupaciones de almacenamiento que utilizan un tipo de dispositivo FILE.
- Ha creado nuevas agrupaciones de almacenamiento primario después de la actualización y ha transferido datos que estaban almacenados en otras agrupaciones de almacenamiento a las nuevas.

Complete estos pasos después de que el servidor se restaure nuevamente a V7.

## Procedimiento

- Para cada agrupación de almacenamiento para la que haya habilitado la función de eliminación de datos duplicados, restaure la agrupación de almacenamiento completa mediante el mandato RESTORE STGPOOL.
- Para agrupaciones de almacenamiento que haya creado tras la actualización, determine qué acción emprender. Es posible que se hayan perdido datos que se han trasladado de agrupaciones de almacenamiento V8 existentes a las nuevas agrupaciones de almacenamiento debido a que las nuevas agrupaciones de almacenamiento ya no existen en el servidor V8 restaurado. La posible recuperación depende del tipo de agrupación de almacenamiento:
  - Si los datos se movieron de agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, el espacio que ocupaban los datos que se movieron probablemente se haya reutilizado. Por lo tanto, debe restaurar las agrupaciones de almacenamiento V8 originales mediante las copias de seguridad de dichas agrupaciones de almacenamiento que se crearon antes de la actualización a V8.1.2.

Si *no* se movió ningún dato de las agrupaciones de almacenamiento tipo DISK V8 a una nueva agrupación de almacenamiento, entonces audite los volúmenes de la agrupación de almacenamiento en estas agrupaciones de almacenamiento tipo DISK.

- Si no se transfirieron datos de las agrupaciones de almacenamiento de acceso en secuencia de V8 hacia una nueva agrupación de almacenamiento, es posible que esos datos aún existan y se puedan usar en los volúmenes de la agrupación de almacenamiento en el servidor V8 restaurado. Los datos pueden ser utilizables si el parámetro REUSEDELAY para la agrupación de almacenamiento se definió con un valor que evitaba la reclamación mientras el servidor se ejecutaba como servidor V8.1.2. Si se ha reclamado algún volumen mientras el servidor se estaba ejecutando como un servidor V8.1.2, restaure esos volúmenes a partir de las copias de seguridad de la agrupación de almacenamiento que se crearon antes de la actualización a V8.1.2.

## Windows: Referencia: Mandatos de DB2 para bases de datos del servidor de IBM Spectrum Protect




Utilice esta lista como referencia cuando el soporte de IBM® le ordene emitir mandatos de DB2.


### Finalidad




Después de utilizar los asistentes para instalar y configurar IBM Spectrum Protect, rara vez necesitará emitir mandatos de DB2. En la Tabla 1 se enumera un conjunto limitado de mandatos de DB2 que puede utilizar o que puede que le soliciten que emita. Esta lista es sólo material complementario y no es una lista exhaustiva. No implica en absoluto que un administrador de IBM Spectrum Protect la vaya a utilizar de forma diaria o continua. Se proporcionan ejemplos de algunos mandatos. No se muestran detalles de la salida.

Si desea una explicación completa de los mandatos descritos aquí y de su sintaxis, consulte el Información sobre el producto DB2.

Tabla 1. Mandatos de DB2

Man dato	Descripción	Ejemplo
 Sistemas operativos Windows	 Sistemas operativos Windows Abra la ventana del procesador de línea de mandatos de DB2 e inicializa el entorno de línea de mandatos de DB2.	 Sistemas operativos Windows Abra la ventana de mandatos de DB2:  db2cmd

Man dato	Descripción	Ejemplo
db2icrt	<p>Crea instancias de DB2 en el directorio de inicio del propietario de la instancia.</p> <p>Consejo: El asistente de configuración de IBM Spectrum Protect crea la instancia utilizada por el servidor y la base de datos. Una vez que un servidor está instalado y configurado a través del asistente de configuración, no se suele utilizar el mandato db2icrt.</p> <p> Sistemas operativos Windows Este programa de utilidad se encuentra en el directorio DB2PATH\bin, donde DB2PATH es la ubicación en la que se instala la copia de DB2.</p>	<p>Cree manualmente una instancia de IBM Spectrum Protect. Especifique el mandato en una línea:</p> <pre>/opt/tivoli/tsm/db2/instance / db2icrt -a server -u nombre_instancia nombre_instancia</pre>
db2set	Muestra las variables de DB2.	<p>Enumere las variables de DB2:</p> <pre>db2set</pre>
CATALOG DATABASE	Almacena información de ubicación de bases de datos en el directorio de bases de datos del sistema. La base de datos puede estar ubicada en la estación de trabajo local o en un servidor de partición de base de datos remoto. El asistente de configuración del servidor se ocupa de cualquier catálogo necesario para utilizar la base de datos del servidor. Ejecute este mandato manualmente, después de que un servidor esté configurado y ejecutándose, únicamente si en el entorno ha cambiado o se ha dañado algo.	<p>Catalogue la base de datos:</p> <pre>db2 catalog database tsmdb1</pre>
CONNECT TO DATABASE	Se conecta a una base de datos especificada para utilizar la interfaz de línea de mandatos (CLI).	<p>Conéctese con la base de datos de IBM Spectrum Protect desde una CLI de DB2:</p> <pre>db2 connect to tsmdb1</pre>
GET DATABASE CONFIGURATION	<p>Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico.</p> <p>Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante el uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .</p>	<p>Muestre la información de configuración para un alias de base de datos:</p> <pre>db2 get db cfg for tsmdb1</pre> <p>Recupere información con el fin de comprobar valores como la configuración de la base de datos, la modalidad de registro y el mantenimiento.</p> <pre>db2 get db config for tsmdb1 show detail</pre>

Mandato	Descripción	Ejemplo
GET DATA BASE MAN AGER CON FIGU RATI ON	Devuelve los valores de entradas individuales en un archivo de configuración de bases de datos específico. Importante: Este mandato y los parámetros son establecidos y gestionados directamente por DB2. Se enumeran aquí con fines informativos y como una manera de ver los valores existentes. Puede que el cambio de estos valores le sea recomendado por el servicio de soporte de IBM o a través de boletines de servicio, como los APAR o los documentos de Orientación Técnica (notas técnicas). No cambie estos valores manualmente. Cámbielos únicamente por indicación de IBM y únicamente mediante del uso de los procedimientos o mandatos del servidor de IBM Spectrum Protect .	Recupere información de configuración para el gestor de base de datos:  db2 get dbm cfg
GET HEAL TH SNAP SHOT	Recupera la información de estado del gestor de base de datos y de sus bases de datos. La información devuelta representa una instantánea del estado en el momento de emisión de la orden. IBM Spectrum Protect supervisa el estado de la base de datos utilizando la instantánea de estado y otros mecanismos que se proporcionan con DB2. Puede haber casos en los que la instantánea de estado u otro tipo de documentación de DB2 indiquen que un elemento o recurso de base de datos puede estar en estado de alerta. Tal caso indica que deben plantearse medidas para remediar la situación. IBM Spectrum Protect supervisa la condición y responde apropiadamente. No se actúa sobre todas las alertas declaradas por la base de datos de DB2.	Reciba un informe sobre los indicadores de supervisión de estado de DB2:  db2 get health snapshot for database on tsmdb1
GRA NT (Auto rizaci ones de base de datos )	Otorga autorizaciones que se aplican a toda la base de datos en lugar de los privilegios que se aplican a objetos específicos dentro de la base de datos.	Otorgue acceso al ID de usuario itmuser:  db2 GRANT CONNECT ON DATABASE TO USER itmuser db2 GRANT CREATETAB ON DATABASE TO USER itmuser
RUN STAT S	Actualiza las estadísticas acerca de las características de una tabla y los índices asociados o vistas estadísticas. Estas características incluyen el número de registros, el número de páginas y la duración media del registro.  Para ver una tabla, emita esta utilidad después de actualizar o reorganizar la tabla.  Debe haber una vista habilitada para la optimización antes de que sus estadísticas se puedan utilizar para optimizar una consulta. Una vista que está habilitada para la optimización se conoce como una vista estadística. Utilice la sentencia DB2 ALTER VIEW para habilitar una vista para la optimización. Emita la utilidad RUNSTATS cuando los cambios en las tablas subyacentes afecten sustancialmente a las filas devueltas por la vista.  Consejo: El servidor configura DB2 para ejecutar el mandato RUNSTATS según sea necesario.	Actualice las estadísticas en una única tabla.  db2 runstats on table SCHEMA_NAME.TA BLE_NAME with distribution and sampled detailed indexes all
 Sis tema s oper ativo s Wind ows set db2i nstan ce	 Sistemas operativos WindowsDetermina qué instancia se aplica a la sesión actual.	 Sistemas operativos Windows Determine qué instancia es aplicable:  set db2instance=ts minst1

Man dato	Descripción	Ejemplo
SET SCHEMA	Cambia el valor del registro especial CURRENT SCHEMA, como preparación para emitir mandatos SQL directamente a través de la CLI de DB2. Consejo: Un registro especial es un área de almacenamiento que se define para un proceso de aplicación del administrador de base de datos. Se utiliza para almacenar información a la que se puede hacer referencia en sentencias SQL.	Establezca el esquema para IBM Spectrum Protect:  db2 set schema tsmdb1
START DATABASE MANAGER	Inicia los procesos en segundo plano de la instancia del gestor de base de datos actual. El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor. Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.	Inicie el gestor de base de datos:  db2start
STOP DATABASE MANAGER	Detiene la instancia del gestor de base de datos actual. A menos que se detenga de forma explícita, el gestor de base de datos seguirá estando activo. Este mandato no detiene la instancia del gestor de base de datos si hay alguna aplicación conectada a bases de datos. Si no hay conexiones de base de datos pero hay conexiones con instancias, el mandato fuerza a las conexiones de la instancia a que se detengan primero. A continuación, detiene al gestor de base de datos. Este mandato también desactiva cualquier activación de base de datos pendiente antes de detener el gestor de base de datos.  Este mandato no es válido en un cliente.  El servidor inicia y detiene la instancia y la base de datos, cada que se de inicia y detiene el servidor.  Importante: Deje que el servidor gestione el inicio y la parada de la instancia y la base de datos, a menos que se lo indique de otro modo el equipo de soporte de IBM.	Detenga el gestor de base de datos:  db2 stop dbm


## Windows: Desinstalar IBM Spectrum Protect

Puede realizar el siguiente procedimiento para desinstalar IBM Spectrum Protect. Antes de eliminar IBM Spectrum Protect, asegúrese de que no pierde los datos de copia de seguridad y archivado.

### Antes de empezar

Realice los siguientes pasos antes de desinstalar IBM Spectrum Protect:

- Realice una copia de seguridad completa de la base de datos.
- Guarde una copia del historial del volumen y los archivos de configuración de dispositivo.
- Guarde los volúmenes de salida en un lugar seguro.

 Sistemas operativos Windows Atención: No utilice la herramienta Agregar/Eliminar programas en el panel de control de Windows para desinstalar IBM Spectrum Protect. Use solamente el procedimiento de desinstalación que se describe en esta sección.

### Acerca de esta tarea

Puede desinstalar IBM Spectrum Protect haciendo uso de cualquiera de los métodos siguientes: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

- Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico  
Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.
- Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola  
Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.
- Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa  
Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.
- Windows: Desinstalación e instalación de IBM Spectrum Protect  
Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.
- Windows: Desinstalación de IBM Installation Manager  
Puede desinstalar IBM Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.

## Qué hacer a continuación

---

Consulte Windows: Instalación de los componentes de servidor para conocer los pasos de instalación para volver a instalar los componentes de IBM Spectrum Protect.

## Windows: Desinstalación de IBM Spectrum Protect mediante el uso de un asistente gráfico


---

Puede desinstalar IBM Spectrum Protect utilizando el asistente de instalación de IBM® Installation Manager.

### Procedimiento

---

1. Inicie el Installation Manager.

 Sistemas operativos Windows Abra el Installation Manager desde el menú de Inicio.

2. Pulse en Desinstalar.
3. Seleccione el servidor de IBM Spectrum Protect y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.


## Windows: Desinstalación de IBM Spectrum Protect en modalidad de consola

---



Para desinstalar IBM Spectrum Protect utilizando la línea de mandatos, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con el parámetro para la modalidad de consola.

### Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  -  Sistemas operativos Windows eclipse\tools

Por ejemplo:

-  Sistemas operativos Windows C:\Archivos de programa\IBM\Installation Manager\eclipse\tools
2. Desde el directorio herramientas, emita el siguiente mandato:
  -  Sistemas operativos Windows imcl.exe -c
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique N para Siguiente.
6. Elija desinstalar el paquete del servidor IBM Spectrum Protect.
7. Especifique N para Siguiente.
8. Escriba U para Desinstalar.
9. Escriba F para Finalizar.

## Windows: Desinstalación de IBM Spectrum Protect en modalidad silenciosa

---

Para desinstalar IBM Spectrum Protect en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros para la modalidad silenciosa.

### Antes de empezar

---


Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa los componentes de servidor de IBM Spectrum Protect. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Si desea desinstalar todos los componentes de IBM Spectrum Protect, deje establecido `modify="false"` para cada componente en el archivo de respuestas. Si no desea desinstalar un componente, establezca el valor en `modify="true"`.


Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.


## Procedimiento

---

1. En el directorio donde está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  - o  Sistemas operativos Windowseclipse\tools


Por ejemplo:

- o  Sistemas operativos WindowsC:\Archivos de programa\IBM\Installation Manager\eclipse\tools
2. Desde el directorio herramientas, emita el siguiente mandato, donde *archivo\_respuestas* representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

 Sistemas operativos Windows

```
imcl.exe -input archivo_respuestas -silent
```

El siguiente mandato es un ejemplo:

 Sistemas operativos Windows

```
imcl.exe -input C:\tmp\input\uninstall_response.xml -silent
```

## Windows: Desinstalación e instalación de IBM Spectrum Protect


---

Si desea volver a instalar IBM Spectrum Protect manualmente, en lugar de utilizar el asistente, debe realizar varias tareas para conservar los nombres de instancia de servidor y los directorios de base de datos. Durante una desinstalación, cualquier instancia de servidor configurada anteriormente se elimina, pero los catálogos de la base de datos de esas instancias, aún existe.

### Acerca de esta tarea

---

Para desinstalar manualmente y volver a instalar IBM Spectrum Protect, complete los siguientes pasos:

1.  Sistemas operativos WindowsRealice una lista de las instancias de servidor actuales antes de continuar con la desinstalación. Ejecute este mandato:

```
db2ilist
```


2. Ejecute los siguientes mandatos para cada una de las instancias del servidor:

 Sistemas operativos Windows

```
db2 attach to server1
db2 get dbm cfg show detail
db2 detach
```


Mantenga un registro de la ruta de base de datos para casa instancia.

3. Desinstale IBM Spectrum Protect. Consulte el apartado Windows: Desinstalar IBM Spectrum Protect.

 Sistemas operativos WindowsTras desinstalar IBM Spectrum Protect, compruebe en el Panel de control > Añadir o quitar programas con el fin de verificar que la base de datos IBM Spectrum Protect DB2 está desinstalada.


4. Cuando desinstala cualquier versión soportada de IBM Spectrum Protect, incluido un fixpack, se crea un archivo de instancias. El archivo de instancias se crea para ayudar a reinstalar IBM Spectrum Protect. Compruebe este archivo y utilice la información cuando se le soliciten los credenciales de la instancia al reinstalar. En la modalidad de instalación silenciosa, proporciona estos credenciales utilizando la variable `INSTANCE_CRED`.

Puede encontrar el archivo de instancias en la siguiente ubicación:

- o  Sistemas operativos WindowsC:\ProgramData\IBM\Tivoli\TSM\instanceList.obj en el directorio de instalación del servidor de IBM Spectrum Protect
5. Vuelva a instalar IBM Spectrum Protect. Consulte el apartado Windows: Instalación de los componentes de servidor.

Si el archivo `instanceList.obj` no existe, deberá volver a crear las instancias del servidor realizando los pasos siguientes:

- a. Vuelva a crear las instancias de servidor. Consulte el apartado Windows: Creación de una instancia del servidor. Consejo: El asistente de instalación configura las instancias del servidor pero debe verificar que existen. Si no existen, debe configurarlas manualmente.
- b. Catalogue la base de datos. Inicie sesión en cada instancia de servidor como el usuario de la instancia, de una en una, y emita los siguientes mandatos:

 Sistemas operativos Windows

```
set db2instance=server1
db2 catalog database tsmdb1
db2 attach to server1
```



```
db2 update dbm cfg using dftdbpath instance_drive
db2 detach
```

- c. Verifique que IBM Spectrum Protect reconoce la instancia de servidor haciendo una lista de los directorios. El directorio padre aparece si no lo cambia. Si utilizó el asistente de configuración aparecerá el directorio de instancia. Emita este mandato:

```
db2 list database directory
```


Si figura TSMDB1 puede iniciar el servidor.

## Windows: Desinstalación de IBM Installation Manager

Puede desinstalar IBM® Installation Manager si ya no tiene ningún producto instalado por IBM Installation Manager.


### Antes de empezar

Antes de desinstalar IBM Installation Manager, debe asegurarse de que todos los paquetes que instaló IBM Installation Manager están desinstalados. Cierre IBM Installation Manager antes de iniciar el proceso de desinstalación.

 Sistemas operativos Windows Para ver los paquetes instalados, pulse Inicio > Todos los programas > IBM Installation Manager > Ver paquetes instalados.

### Procedimiento

Para desinstalar IBM Installation Manager, complete los siguientes pasos:

 Sistemas operativos Windows


1. En el menú Inicio, pulse Panel de control > Programas y características.
2. Seleccione IBM Installation Manager y pulse Desinstalar.


## Actualización a V8.1


Para sacar partido de las nuevas características del producto y de las actualizaciones, actualice el servidor IBM Spectrum Protect a la versión 8.1.2.

### Antes de empezar

Actualice al servidor IBM Spectrum Protect antes de actualizar los clientes. Para obtener más información, consulte:

 Sistemas operativos AIX Qué debe saber sobre seguridad antes de instalar o actualizar el servidor




 Sistemas operativos Linux Qué debe saber sobre seguridad antes de instalar o actualizar el servidor




 Sistemas operativos Windows Qué debe saber sobre seguridad antes de instalar o actualizar el servidor

### Acerca de esta tarea

Para actualizar el servidor en el mismo sistema operativo, consulte las instrucciones de actualización. Para ver las instrucciones sobre la migración del servidor a un sistema operativo distinto, consulte IBM Spectrum Protect Proceso de migración y actualización: preguntas más frecuentes.

Tabla 1. Instrucciones de actualización


Para actualizar desde esta versión	A esta versión	Consulte esta información
V8.1	Fixpack o arreglo temporal V8.1	 Sistemas operativos AIX Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Linux Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Windows Instalación de un fixpack de servidor de IBM Spectrum Protect
V7.1	V8.1	Instalación del servidor y comprobación de la actualización

Para actualizar desde esta versión	A esta versión	Consulte esta información
V7.1	Fixpack o arreglo temporal V8.1	 Sistemas operativos AIX Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Linux Instalación de un fixpack de servidor de IBM Spectrum Protect  Sistemas operativos Windows Instalación de un fixpack de servidor de IBM Spectrum Protect
V5.5, V6.2 o V6.3	V8.1	IBM Spectrum Protect Proceso de actualización y migración: preguntas más frecuentes


Una actualización de la versión 7 a la 8.1 ocupa entre 20 y 50 minutos. El entorno puede generar resultados distintos que los obtenidos en los laboratorios.

Para obtener información acerca de las actualizaciones en un entorno en clúster, consulte Actualización del servidor en un entorno en clúster.

Para volver a una versión anterior del servidor después de una actualización o migración, debe tener una copia de seguridad de la base de datos completa y el software de instalación para el servidor original. También debe tener archivos de configuración claves siguientes:

- Archivo histórico de volúmenes
- Archivo de configuración de dispositivos
- Archivo de opciones del servidor
- Actualización a V8.1  
Puede actualizar el servidor directamente de la versión 7.1 a la 8.1. No tiene que desinstalar la versión 7.1.
- Actualización del servidor en un entorno en clúster  
Para actualizar un servidor a V8.1.2 en un entorno en clúster, debe completar las tareas de preparación e instalación. Los procedimientos varían, dependiendo del sistema operativo y el release.
-  Sistemas operativos Windows Eliminación de GSKit Versión 7 después de actualizar a IBM Spectrum Protect Versión 8.1.2  
El asistente de instalación de IBM Spectrum Protect actualiza GSKit Versión 8 y posterior. GSKit Versión 7 no se elimina ni se actualiza cuando actualiza a IBM Spectrum Protect Versión 8.1.2, aunque se haya instalado con una versión anterior de IBM Spectrum Protect.

#### Información relacionada:

 [IBM Spectrum Protect Proceso de migración y actualización: preguntas más frecuentes](#)

## Actualización a V8.1

Puede actualizar el servidor directamente de la versión 7.1 a la 8.1. No tiene que desinstalar la versión 7.1.

### Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor que se va a actualizar. Si ha instalado los componentes de servidor desde un DVD, asegúrese de que el DVD está disponible. Si ha instalado los componentes del servidor desde un paquete descargado, asegúrese de que los archivos descargados están disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

Consejo: A partir de la versión 8.1, dejará de haber DVD disponibles.

### Procedimiento

Para actualizar el servidor a V8.1, realice estas tareas:

- Planificación de la actualización  
Antes de actualizar el servidor de V7.1 a V8.1, debe revisar la información de planificación más importante, como los requisitos del sistema y las notas del release. A continuación, seleccione el día y la hora correspondiente para actualizar el sistema de manera que pueda minimizar el impacto sobre las operaciones de producción.
- Preparación del sistema  
Para preparar el sistema para la actualización de V7.1 a V8.1, tiene que recopilar información sobre cada instancia de DB2. Luego, realice una copia de seguridad de la base de datos del servidor, guarde los archivos de configuración, cancele las sesiones y detenga el servidor.

- Instalación del servidor y comprobación de la actualización  
Para completar el proceso de actualización del servidor a V8.1, tiene que instalar el servidor V8.1. A continuación, compruebe que la actualización haya sido satisfactoria al iniciar la instancia del servidor.

## Planificación de la actualización

---

Antes de actualizar el servidor de V7.1 a V8.1, debe revisar la información de planificación más importante, como los requisitos del sistema y las notas del release. A continuación, seleccione el día y la hora correspondiente para actualizar el sistema de manera que pueda minimizar el impacto sobre las operaciones de producción.

### Acerca de esta tarea


---

En las pruebas de laboratorio, el proceso de actualización del servidor de V7.1 a V8.1 ocupó entre 14 y 45 minutos. Los resultados que obtiene pueden variar, dependiendo del entorno de hardware y de software y el tamaño de la base de datos del servidor.


### Procedimiento

---

1. Revise los requisitos de hardware y software:

 Sistemas operativos AIX Requisitos del sistema para los sistemas AIX

 Sistemas operativos Linux Requisitos del sistema para los sistemas Linux

 Sistemas operativos Windows Requisitos del sistema para los sistemas Windows

Para ver las últimas actualizaciones relacionadas con los requisitos del sistema, consulte el sitio web de soporte de IBM Spectrum Protect, nota técnica 1243309.

2. Para obtener instrucciones especiales o información específica para su sistema operativo, revise las Notas del release de los componentes del servidor de la Versión 8.1 y IBM Spectrum Protect los archivos readme del fixpack Versión 8.1.
3. Seleccione la fecha y la hora adecuadas para actualizar el sistema para minimizar el impacto en las operaciones de producción. La cantidad de tiempo necesaria para actualizar el sistema depende del tamaño de la base de datos y varios otros factores. Al iniciar el proceso de actualización, los clientes no pueden conectarse al servidor hasta que el nuevo software esté instalado y todas las licencias necesarias se registren de nuevo.
4. Si está actualizando el servidor de V6 o V7 a V8.1, verifique que dispone del ID de sistema y de la contraseña para la instancia de DB2 del servidor IBM Spectrum Protect. Estas credenciales son necesarias para actualizar el sistema.

## Preparación del sistema

---


Para preparar el sistema para la actualización de V7.1 a V8.1, tiene que recopilar información sobre cada instancia de DB2. Luego, realice una copia de seguridad de la base de datos del servidor, guarde los archivos de configuración, cancele las sesiones y detenga el servidor.

### Procedimiento

---

1. Inicie la sesión en el sistema donde se haya instalado el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux Asegúrese de haber iniciado sesión con el ID del usuario de la instancia.

 Sistemas operativos Windows Asegúrese de haber iniciado sesión con el ID del usuario administrativo que se usó para instalar el servidor V7.1.

2. Obtenga una lista de instancias DB2. Emita el siguiente mandato del sistema:

 Sistemas operativos AIX  Sistemas operativos Linux

```
/opt/tivoli/tsm/db2/instance/db2ilist
```

 Sistemas operativos Windows

```
db2ilist
```




La información podría ser similar al siguiente ejemplo:

 Sistemas operativos AIX  Sistemas operativos Linux

```
tsminst1
```

SERVER1

Asegúrese de que cada instancia corresponde a un servidor que se está ejecutando en el sistema.

3.  Sistemas operativos AIX  Sistemas operativos Linux Para cada instancia de DB2, tenga en cuenta la vía de acceso predeterminada de la base de datos, la vía de acceso real de la base de datos, el nombre de la base de datos, el alias de la base de datos y cualquier variable de DB2 que esté configurada para la instancia. Conserve el registro para referencias futuras. Esta información es obligatoria para restaurar la base de datos V7.1.
4.  Sistemas operativos Windows Reúna la información acerca de cada instancia de DB2. Tenga en cuenta la vía de acceso a la base de datos predeterminada, la vía de acceso a la base de datos real, el nombre de la base de datos, el alias de la base de datos y cualquier variable de DB2 que esté configurada para la instancia. Conserve el registro para referencias futuras. Esta información es obligatoria para restaurar la base de datos V7.1.
  - a. Abra la ventana de mandatos de DB2 emitiendo el siguiente mandato del sistema:

```
db2cmd
```

- b. Para cambiar la instancia, emita el siguiente mandato del sistema:

```
set DB2INSTANCE=instance
```

en donde *instancia* especifica la instancia de DB2.

- c. Obtenga la vía de acceso predeterminada de la base de datos para la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2 get dbm cfg | findstr DFTDBPATH
```

La información podría ser similar al siguiente ejemplo:

```
Vía acceso base datos predeterminada (DFTDBPATH) = D:
```

- d. Obtenga información acerca de las bases de datos de la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2 list database directory
```

La información podría ser similar al siguiente ejemplo:

Directorio de bases de datos del sistema

```
Número de entradas del directorio = 2
```

Entrada 1 de base de datos:

```
Alias de la base de datos = TSMAL001
Nombre de la base de datos = TSMDB1
Nombre del nodo = TSMNODE1
Nivel de release de la base de datos = d.00
Comentario = TSM SERVER DATABASE VIA TCPIP
Tipo de entrada de directorio = Remote
Número de partición de base de datos de catálogo = -1
Nombre host del servidor alternativo =
Número de puerto del servidor alternativo =
```

Entrada 2 de base de datos:

```
Alias de la base de datos = TSMDB1
Nombre de la base de datos = TSMDB1
Directorio local de la base de datos = D:
Nivel de release de la base de datos = d.00
Comentario =
Tipo de entrada de directorio = Indirect
Número partición base datos catálogo = 0
Nombre host del servidor alternativo =
Número de puerto del servidor alternativo =
```

- e. Obtenga las variables de la instancia de DB2 emitiendo el siguiente mandato del sistema:

```
db2set -all
```

La información podría ser similar al siguiente ejemplo:

```
[e] DB2CODEPAGE=1208
[e] DB2PATH=D:\TSM\db2
[i] DB2_PMODEL_SETTINGS=MAX_BACKGROUND_SYSAPPS:500
[i] DB2_SKIPINSERTED=ON
```

```

[i] DB2_KEEPTABLELOCK=OFF
[i] DB2_EVALUNCOMMITTED=ON
[i] DB2_VENDOR_INI=D:\Server1\tsmdbmgr.env
[i] DB2_SKIPDELETED=ON
[i] DB2INSTPROF=C:\ProgramData\IBM\DB2\DB2TSM1
[i] DB2COMM=TCPIP
[i] DB2CODEPAGE=819
[i] DB2_PARALLEL_IO=*
[g] DB2_EXTSECURITY=YES
[g] DB2_COMMON_APP_DATA_PATH=C:\ProgramData

[g] DB2PATH=D:\TSM\db2
[g] DB2INSTDEF=SERVER1

```

5. Conéctese al servidor utilizando un ID de usuario de administración.
6. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es crear una copia de seguridad de instantánea, que es una copia de seguridad de base de datos completa que no interrumpe las copias de seguridad de base de datos planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea emitiendo el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

7. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio emitiendo el siguiente mandato de administración:

```
backup devconfig filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo. Consejo: Si decide restaurar la base de datos V7.1, se requiere este archivo.

8. Realice una copia de seguridad del archivo del historial del volumen a otro directorio. Emita el siguiente mandato de administración:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes. Consejo: Si decide restaurar la base de datos V7.1, se requiere este archivo.

9. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
10. Evite que haya actividad en el servidor inhabilitando nuevas sesiones. Emita los siguientes mandatos de administración:

```
disable sessions client
disable sessions server
```

11. Verifique si existen sesiones en curso y notifique a los usuarios que el servidor va a detenerse. Para comprobar las sesiones existentes, emita el siguiente mandato de administración:

```
query session
```

12. Cancele las sesiones emitiendo el siguiente mandato de administración:



```
cancel session all
```

Este mandato cancela todas las sesiones excepto la sesión actual.


13. Detenga el servidor emitiendo el siguiente mandato de administración:

```
halt
```

14. Verifique que el servidor está apagado y no hay ningún proceso en ejecución.

 Sistemas operativos AIX  Sistemas operativos Linux Emita el mandato siguiente:

```
ps -ef | grep dsmserv
```

 Sistemas operativos Windows Abra la aplicación del gestor de tareas de Windows y revise la lista de los procesos activos.

15. En el directorio de la instancia del servidor de la instalación, localice el archivo NODELOCK y trasládalo a otro directorio, donde va a guardar los archivos de configuración. El archivo NODELOCK contiene la información de las licencias anteriores de la instalación. Esta información de licencia se sustituye cuando finaliza la actualización.

#### Referencia relacionada:

BACKUP DB (copia de seguridad de la base de datos)  
 BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)  
 BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)  
 DISABLE SESSIONS (Impedir que nuevas sesiones accedan a Tivoli Storage Manager)  
 QUERY SESSION (Consultar sesiones de cliente)

CANCEL SESSION (Cancelar una o más sesiones cliente)  
HALT (Concluir el servidor)



## Instalación del servidor y comprobación de la actualización


---

Para completar el proceso de actualización del servidor a V8.1, tiene que instalar el servidor V8.1. A continuación, compruebe que la actualización haya sido satisfactoria al iniciar la instancia del servidor.



### Antes de empezar

---

 Sistemas operativos AIX  Sistemas operativos Linux Debe haber iniciado sesión en el sistema haciendo uso del ID del usuario root.

 Sistemas operativos Windows Debe haber iniciado sesión en el sistema con el ID de usuario de administración que se utilizó para instalar el servidor anterior.

Puede obtener el paquete de instalación desde un sitio de descarga de IBM®.

 Sistemas operativos AIX  Sistemas operativos Linux Establezca el límite de usuario del sistema para el tamaño máximo de archivo en ilimitado para garantizar que los archivos se pueden descargar correctamente.

1. Para consultar el valor de tamaño máximo de archivo, ejecute el mandato siguiente:

```
ulimit -Hf
```

2. Si el límite de usuario del sistema para el tamaño máximo de archivo no está establecido en ilimitado, cámbielo a ilimitado completando las instrucciones de la documentación de su sistema operativo.

### Acerca de esta tarea

---

Haciendo uso del software de instalación de IBM Spectrum Protect, puede instalar los siguientes componentes:

- Servidor  
Consejo: La base de datos (DB2), el Kit de seguridad global (GSKit) e IBM Java™ Runtime Environment (JRE) se instalan automáticamente cuando selecciona el componente del servidor.
- Idiomas de servidor
- Licencia
- Dispositivos
- IBM Spectrum Protect for SAN
- Centro de operaciones

### Procedimiento

---

1. Descargue el archivo de paquete correspondiente de uno de los siguientes sitios web:
  - Descargue el paquete de servidor de Passport Advantage o Fix Central.
  - Para ver la información más reciente, actualizaciones y arreglos de mantenimiento, vaya al sitio de soporte de Tivoli Storage Manager: IBM Support Portal.

2. Realice los siguientes pasos:

 Sistemas operativos AIX  Sistemas operativos Linux

 Sistemas operativos AIX  Sistemas operativos Linux

- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio, consulte el documento descargado de su producto.

- IBM Spectrum Protect nota técnica 4042944
- IBM Spectrum Protect Extended Edition nota técnica 4042945
- IBM Spectrum Protect for Data Retention nota técnica 4042946

- b. Descargue el archivo del paquete al directorio de su elección. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.

También, asegúrese de tener la autorización ejecutable del archivo del paquete.

- c. En caso necesario, ejecute el siguiente mandato para cambiar los permisos de archivo:

```
chmod a+x package_name.bin
```

en donde *package\_name* es como el siguiente ejemplo:

### Sistemas operativos AIX

`8.1.x.000-IBM-SPSRV-AIX.bin`

### Sistemas operativos Linux

`8.1.x.000-IBM-SPSRV-Linuxs390x.bin`  
`8.1.x.000-IBM-SPSRV-Linuxx86_64.bin`  
`8.1.x.000-IBM-SPSRV-Linuxppc64le.bin`

En los ejemplos, `8.1.x.000` representa el nivel de release del producto.

- d. Extraiga los archivos de instalación ejecutando el siguiente mandato:

```
./package_name.bin
```

El paquete es grande. Por lo tanto, la extracción tarda un tiempo.

### Sistemas operativos Windows

#### Sistemas operativos Windows



- a. Compruebe que tiene espacio suficiente para almacenar los archivos de instalación cuando estos sean extraídos del paquete del producto. Para conocer los requisitos de espacio, consulte el documento descargado de su producto.
- IBM Spectrum Protect nota técnica 4042944
  - IBM Spectrum Protect Extended Edition nota técnica 4042945
  - IBM Spectrum Protect for Data Retention nota técnica 4042946
- b. Cambie al directorio en el que colocó el archivo ejecutable.  
Consejo: En el siguiente paso, los archivos se extraen al directorio actual. La vía de acceso no debe contener más de 128 caracteres. Asegúrese de extraer los archivos de instalación en un directorio vacío. No extraiga en un directorio que contenga archivos extraídos anteriormente ni ningún otro archivo.
- c. Para extraer los archivos de instalación, haga doble clic en el archivo ejecutable:

```
package_name.exe
```


Donde `package_name` es similar al siguiente ejemplo:


```
8.1.x.000-SPSRV-WindowsX64.exe
```


El paquete es grande. Por lo tanto, la extracción tarda un tiempo.

3.  Sistemas operativos AIX Para asegurarse que los asistentes de IBM Spectrum Protect funcionen correctamente, compruebe que esté habilitado el siguiente mandato:
-  Sistemas operativos AIX `lsuser`  
De manera predeterminada, el mandato está habilitado.
4. Instale el software de IBM Spectrum Protect haciendo uso de uno de los siguientes métodos. Instale la licencia de IBM Spectrum Protect durante el proceso de instalación.  
Consejo: Si tiene varias instancias de servidor en el sistema, instale el software de IBM Spectrum Protect solo una vez para actualizar todas las instancias de servidor.

#### Asistente de instalación


 Sistemas operativos AIX Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.


 Sistemas operativos Linux Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.


 Sistemas operativos Windows Para instalar el servidor utilizando el asistente gráfico de IBM Installation Manager, siga las instrucciones de Instalación de IBM Spectrum Protect utilizando el asistente de instalación.

Asegúrese que su sistema cumpla con los prerrequisitos para usar el asistente de instalación. A continuación, complete el procedimiento de instalación. En la ventana IBM Installation Manager, pulse el icono Update o Modify.

#### Instalación del servidor utilizando la modalidad de consola


 Sistemas operativos AIX Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.


 Sistemas operativos Linux Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.


 Sistemas operativos Windows Para instalar el servidor utilizando la modalidad de consola, siga las instrucciones de Instalación de Tivoli Storage Manager en modalidad de consola.

Revise la información sobre la instalación del servidor en modalidad de consola y, a continuación, complete el procedimiento de instalación.

#### Modalidad silenciosa

 Sistemas operativos AIX Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.

 Sistemas operativos Linux Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.

 Sistemas operativos Windows Para instalar el servidor utilizando la modalidad silenciosa, siga las instrucciones de Instalación Tivoli Storage Manager en modalidad silenciosa.




Revise la información sobre la instalación del servidor en modalidad silenciosa y, a continuación, complete el procedimiento de instalación.

Tras instalar el software, no es necesario volver a configurar el sistema.

#### 5. Corrija cualquier error que se detecte durante el proceso de instalación.

Si ha instalado el servidor utilizando el asistente de instalación, podrá ver registros de instalación mediante la herramienta IBM Installation Manager. Pulse Archivo > Ver anotaciones. Para recopilar los archivos de registro, desde la herramienta IBM Installation Manager, pulse Ayuda > Exportar datos para el análisis de problemas.


Si ha instalado el servidor utilizando la modalidad de consola o la modalidad silenciosa, podrá ver los registros de error en el directorio de registros de IBM Installation Manager, por ejemplo:


- o  Sistemas operativos AIX  Sistemas operativos Linux/var/ibm/InstallationManager/logs
- o  Sistemas operativos Windows C:\ProgramData\IBM\Installation Manager\logs

#### 6. Vaya a IBM Support Portal para obtener arreglos. Pulse Arreglos, actualizaciones y controladores y aplique todo arreglo aplicable.

#### 7. Sistemas operativos AIX Sistemas operativos Linux Verifique que la actualización haya finalizado correctamente:

- a. Inicie la instancia de servidor.

 Sistemas operativos AIX Para obtener instrucciones, consulte Inicio de la instancia de servidor.

 Sistemas operativos Linux Para obtener instrucciones, consulte Inicio de la instancia de servidor.

- b. Supervise los mensajes que el servidor emita al comenzar. Esté atento a los mensajes de error y advertencia, y resuelva cualquier problema.
- c. Compruebe que puede conectarse al servidor mediante el cliente de administración. Para iniciar una sesión de cliente de administración, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
dsmadm
```

- d. Para obtener la información sobre el sistema actualizado, ejecute los mandatos QUERY. Por ejemplo, para obtener información consolidada acerca del sistema, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query system
```

Para obtener información acerca de la base de datos, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query db format=detailed
```

#### 8. Sistemas operativos Windows Verifique que la actualización haya finalizado correctamente:

- a. Inicie la instancia del servidor. Para iniciar el servidor desde el directorio predeterminado, C:\Program Files\Tivoli\TSM, ejecute el siguiente mandato administrativo IBM Spectrum Protect:

```
dsmserv -k server_instance
```

*instancia\_servidor* es el nombre de la instancia del servidor. Server1 es el nombre predeterminado de la primera instancia del servidor IBM Spectrum Protect.

Si tiene previsto ejecutar el servidor como un servicio bajo la cuenta Sistema local, se debe haber otorgado de forma explícita a la cuenta del sistema local acceso a la base de datos del servidor. Para ver las instrucciones, consulte Inicio del servidor haciendo uso de los servicios de Windows.

- b. Supervise los mensajes que el servidor emita al comenzar. Esté atento a los mensajes de error y advertencia, y resuelva cualquier problema.
- c. Compruebe que puede conectarse al servidor mediante el cliente de administración. Para iniciar una sesión de cliente de administración, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:





```
dsmadm
```

d. Para obtener la información sobre el sistema actualizado, ejecute los mandatos QUERY. Por ejemplo, para obtener información consolidada acerca del sistema, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query system
```

Para obtener información acerca de la base de datos, ejecute el siguiente mandato administrativo de IBM Spectrum Protect:

```
query db format=detailed
```

9.  Sistemas operativos AIX  Sistemas operativos Linux Registre las licencias para los componentes del servidor de IBM Spectrum Protect que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifica la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, /opt/tivoli/tsm, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio /opt/tivoli/tsm, ejecute el siguiente mandato:


```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

10.  Sistemas operativos Windows Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory\server\component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifica la abreviatura del componente.

Por ejemplo, si instaló el servidor en el directorio predeterminado, c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato para registrar la licencia:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmbasic.lic
```

Por ejemplo, si instaló IBM Spectrum Protect Extended Edition en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmee.lic
```

Por ejemplo, si ha instaló IBM Spectrum Protect for Data Retention en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:


- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

11. Opcional: Para instalar un paquete de idiomas adicional, utilice la función de modificar de IBM Installation Manager.
12. Opcional: Para actualizar a una versión más reciente del paquete de idiomas, utilice la función de actualizar de IBM Installation Manager.

## Qué hacer a continuación

Puede autenticar contraseñas con el servidor del directorio LDAP o autenticar contraseñas con el servidor de IBM Spectrum Protect. Las contraseñas que se autentican con el servidor de directorio LDAP pueden proporcionar mejoras en la seguridad del sistema.




 Sistemas operativos Windows Si hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, instale el controlador de dispositivos de IBM Spectrum Protect ejecutando el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos. El directorio predeterminado es `C:\Program Files\Tivoli\TSM\device\drivers`.

### Referencia relacionada:

QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)

QUERY DB (Visualizar información de base de datos)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Actualización del servidor en un entorno en clúster

Para actualizar un servidor a V8.1.2 en un entorno en clúster, debe completar las tareas de preparación e instalación. Los procedimientos varían, dependiendo del sistema operativo y el release.

### Procedimiento

Siga el procedimiento para su sistema operativo, release de origen y release de destino:


 Sistemas operativos AIX

Tabla 1. Procedimientos para la actualización del servidor en un entorno en clúster en un sistema operativo AIX

Release de origen	Release de destino	Procedimiento
V8.1.2	Fixpack V8.1.2	Aplicación de un fixpack a V8 en un entorno en clúster para AIX
V6.3 o V7.1	V8.1.2	Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.2 en un entorno en clúster para AIX con una instancia de base de datos compartida  Actualización de V6.3 a V8.1.2 en un entorno en clúster para AIX con instancias de base de datos independientes
V6.1	V8.1.2	Actualización de IBM Spectrum Protect desde V6.1 a V8.1.2 en un entorno en clúster for AIX
V5	V7.1.1 o posterior	Actualización del servidor a V7.1.1 en un entorno de clúster de AIX


 Sistemas operativos Linux

Tabla 2. Procedimientos para actualizar el servidor en un entorno en clúster en un sistema operativo Linux

Release de origen	Release de destino	Procedimiento
V6 o V7	V8.1.2	Actualización de un servidor configurado con Tivoli System Automation



 Sistemas operativos Windows

Tabla 3. Procedimientos para la actualización del servidor en un entorno en clúster en un sistema operativo Windows

Release de origen	Release de destino	Procedimiento
V8.1.2	Fixpack V8.1.2	Aplicación de un fixpack a V8 en un entorno en clúster para Windows
V6.3 o V7.1	V8.1.2	Actualización de V6.3 o V7.1 a V8.1 en un entorno de clúster en Windows
V6.1	V8.1.2	Actualización de V6.1 a V8.1 en un entorno de clúster en Windows

Release de origen	Release de destino	Procedimiento
V5	V7.1 o posterior	Actualización del servidor a V7.1 o posterior en un entorno en clúster de Windows

- Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.2 en un entorno en clúster para AIX con una instancia de base de datos compartida  
Puede actualizar un servidor de IBM Spectrum Protect de V6.3 o V7.1 a V8.1.2 en un entorno en clúster en AIX con una instancia de base de datos compartida. De esta forma, puede beneficiarse de las nuevas características de IBM Spectrum Protect V8.1.2.
- Actualización de V6.3 a V8.1.2 en un entorno en clúster para AIX con instancias de base de datos independientes  
Puede actualizar un servidor de V6.3 a V8.1.2 en un entorno en clúster en AIX con instancias de base de datos independientes. De esta forma, puede aprovechar las nuevas características de V8.1.2.
- Actualización de IBM Spectrum Protect desde V6.1 a V8.1.2 en un entorno en clúster for AIX  
Puede actualizar un servidor de IBM Spectrum Protect on AIX de V6.1 a V8.1.2 en un entorno en clúster. Complete la actualización para aprovechar las nuevas características de la V8.1.2.
- Actualización de IBM Spectrum Protect a V8.1.2 en un entorno en clúster for Linux  
Para aprovechar las nuevas características de IBM Spectrum Protect, puede actualizar el servidor IBM Spectrum Protect que está instalado en un sistema operativo Linux en un entorno en clúster.
- Actualización de un servidor V6.3 o V7.1 a V8.1.2 en un entorno en clúster para Windows  
Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.2.
- Actualización de IBM Tivoli Storage Manager V6.1 a IBM Spectrum Protect V8.1.2 en un entorno en clúster para Windows  
Para aprovechar las características nuevas, puede actualizar un servidor instalado en un sistema operativo Windows en un entorno en clúster de la V6.1 a la V8.1.2.

 Sistemas operativos AIX

## Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.2 en un entorno en clúster para AIX con una instancia de base de datos compartida

Puede actualizar un servidor de IBM Spectrum Protect de V6.3 o V7.1 a V8.1.2 en un entorno en clúster en AIX con una instancia de base de datos compartida. De esta forma, puede beneficiarse de las nuevas características de IBM Spectrum Protect V8.1.2.

### Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado IBM Spectrum Protect desde un DVD, asegúrese de que el DVD esté disponible. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

### Acerca de esta tarea

Utilice el siguiente procedimiento cuando el directorio de instancias DB2 se comparte entre los nodos del clúster. El directorio de instancias DB2 se encuentra en la siguiente ubicación:

```
/home/tsminst1/sqlllib
```

Si el directorio de instancias DB2 no se comparte entre nodos, siga las instrucciones en Actualización de V6.3 a V8.1.2 en un entorno en clúster para AIX con instancias de base de datos independientes.

### Procedimiento

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad de instantánea, lo que crea una copia de seguridad completa de base de datos sin interrumpir ninguna de las copias de seguridad planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea ejecutando el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio, ejecutando el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio, ejecutando el siguiente mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado `dsmserv.opt`, que está en el directorio de instancia de servidor.
5. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución. Si está usando supervisión a nivel de la aplicación del servidor IBM Spectrum Protect, use su herramienta para formar clústeres para el recurso de la aplicación `dsmserv`.
6. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso `db2sysc` en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

7. En el nodo primario, instale el servidor IBM Spectrum Protect V8.1.2 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. Después de iniciar el asistente, en la ventana de IBM Installation Manager, pulse el icono Install; no pulse el icono Update o Modify.
8. Inicie cada servidor V8.1.2 en el primer plano:
  - a. Compruebe que haya iniciado sesión con el ID del propietario de la instancia
  - b. Navegue al directorio de la instancia y ejecute el siguiente mandato:

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Espere hasta que vea el indicador de servidor, lo que indica que se ha iniciado el servidor.

9. Detenga el servidor para cada instancia de IBM Spectrum Protect que se esté actualizando. Emita el mandato siguiente:

```
halt
```

Consejo: Debido a que el directorio de instancias de DB2 se comparte entre los nodos del clúster, no es necesario que mueva los recursos compartidos al nodo secundario del clúster.

10. En cada nodo secundario del clúster, siga estos pasos:
  - a. Instale el servidor IBM Spectrum Protect V8.1.2 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor.
    - i. Si va a ejecutar el asistente de instalación, en la ventana IBM Installation Manager, pulse sobre el icono Instalar; no pulse sobre el icono Actualizar ni sobre el icono Modificar.
    - ii. Si ejecuta el asistente de instalación, en el panel Credenciales de instancia, deseleccione el recuadro de selección Actualizar esta instancia para cada instancia.
    - iii. Si va a instalar el servidor en modalidad de consola, en la solicitud `¿Desea actualizar esta instancia?`, especifique `NO` para cada una de las instancias.
    - iv. Si va a instalar el servidor en modalidad silenciosa, especifique `FALSE` para el valor de la variable `user.nombre_instancia_update` para cada una de las instancias.
  - b. Asegúrese de que se inicie cada servidor de IBM Spectrum Protect V8.1.2. Si está utilizando supervisión a nivel de la aplicación, utilice la herramienta de agrupación en clústeres para iniciar el servidor.

Para obtener instrucciones sobre cómo iniciar el servidor, consulte Inicio de la instancia de servidor.

11. Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifique la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, `/opt/tivoli/tsm`, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

**Referencia relacionada:**


BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

HALT (Concluir el servidor)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX

## Actualización de V6.3 a V8.1.2 en un entorno en clúster para AIX con instancias de base de datos independientes

Puede actualizar un servidor de V6.3 a V8.1.2 en un entorno en clúster en AIX con instancias de base de datos independientes. De esta forma, puede aprovechar las nuevas características de V8.1.2.

### Antes de empezar

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado IBM Spectrum Protect desde un DVD, asegúrese de que el DVD esté disponible. Si ha instalado IBM Spectrum Protect desde un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

### Acerca de esta tarea

Utilice el siguiente procedimiento cuando la instancia del directorio de DB2 no se comparta entre los nodos en el clúster. El directorio de la instancia de DB2 se encuentra en la siguiente ubicación:

```
/home/tsminst1/sqlllib
```

Si la instancia del directorio de DB2 se comparten entre los nodos del clúster, siga las instrucciones en Actualización de IBM Spectrum Protect desde V6.3 o V7.1 a V8.1.2 en un entorno en clúster para AIX con una instancia de base de datos compartida.

### Procedimiento

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad de instantánea, lo que crea una copia de seguridad completa de base de datos sin interrumpir ninguna de las copias de seguridad planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea ejecutando el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio, ejecutando el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio, ejecutando el siguiente mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt, que está en el directorio de instancia de servidor.
5. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución. Si está usando supervisión a nivel de la aplicación del servidor IBM Spectrum Protect, use su herramienta para formar clústeres para el recurso de la aplicación dsmserv.
6. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso db2sysc en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

db2stop

7. Asegúrese de que todos los recursos compartidos para todas las instancias de IBM Spectrum Protect se encuentren en el nodo primario. Verifique que ningún otro nodo tenga acceso de grabación sobre estos recursos durante la actualización. Si el entorno incluya varias instancias del servidor, el nodo primario debe poder acceder a los recursos compartidos para todas las instancias.
8. En el nodo primario, instale el servidor V8.1.2 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. Después de iniciar el asistente, en la ventana de IBM Installation Manager, pulse el icono Install; no pulse el icono Update o Modify. Para completar la actualización de V6.3 a V8.1.2, tiene que instalar el servidor V8.1.2.
9. Inicie cada servidor V8.1.2 en el primer plano:
  - a. Compruebe que haya iniciado sesión con el ID del propietario de la instancia
  - b. Navegue al directorio de la instancia y ejecute el siguiente mandato:

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Espere hasta que vea el indicador de servidor, lo que indica que se ha iniciado el servidor.

10. Detenga el servidor para cada instancia de IBM Spectrum Protect que se esté actualizando. Ejecute este mandato:

```
halt
```

11. En cada nodo secundario del clúster, siga estos pasos:
  - a. Mueva todos los recursos compartidos al nodo secundario. Si el entorno incluye varias instancias del servidor, el nodo secundario debe poder acceder a los recursos compartidos para todas las instancias durante la actualización.
  - b. Detenga todas las instancias del servidor. Verifique que no haya ningún proceso de servidor en ejecución.
  - c. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso `db2sysc` en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

- d. Instale el servidor V8.1.2 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor.
  - i. Si va a utilizar el asistente de instalación, en la ventana IBM Installation Manager, pulse sobre el icono Instalar; no pulse sobre el icono Actualizar ni sobre el icono Modificar.
  - ii. Si está utilizando el asistente de instalación, en la página Credenciales de instancia, seleccione el recuadro de selección Configurar esta instancia en un nodo secundario del clúster para cada instancia que está configurando.
  - iii. Si va a instalar el servidor en modalidad de consola, en la solicitud `¿Desea configurar esta instancia en un nodo secundario del clúster?`, especifique `YES (Sí)` para cada una de las instancias.
  - iv. Si va a instalar el servidor en modalidad silenciosa, especifique `TRUE` para el valor de la variable `user.nombre_instancia_secondaryNode` para cada una de las instancias.
- e. Asegúrese de que se inicia cada servidor V8.1.2. Si está utilizando supervisión a nivel de la aplicación, utilice la herramienta de agrupación en clústeres para iniciar el servidor.

Para obtener instrucciones sobre cómo iniciar el servidor, consulte Inicio de la instancia de servidor.

12. Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde `installation_directory` especifique el directorio en el cual instaló el componente, y `component_name` especifica la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, `/opt/tivoli/tsm`, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- o IBM Spectrum Protect for Mail

- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

**Referencia relacionada:**


BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

HALT (Concluir el servidor)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos AIX

## Actualización de IBM Spectrum Protect desde V6.1 a V8.1.2 en un entorno en clúster for AIX

---

Puede actualizar un servidor de IBM Spectrum Protect on AIX de V6.1 a V8.1.2 en un entorno en clúster. Complete la actualización para aprovechar las nuevas características de la V8.1.2.

### Antes de empezar

---

Asegúrese de conservar los recursos de instalación del release base de los servidores V6.1 y V6.3. Si obtuvo el software del servidor de un DVD, asegúrese de tenerlo disponible. Si obtuvo el software del servidor de un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

### Acerca de esta tarea

---

Si el entorno en clúster contiene varias instancias de servidor, mueva todos los recursos que son necesarios para las instancias en un solo nodo de clúster, que es el nodo primario, durante el proceso de actualización.

### Procedimiento

---

1. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad de instantánea, lo que crea una copia de seguridad completa de base de datos sin interrumpir ninguna de las copias de seguridad planificadas. Por ejemplo, puede crear una copia de seguridad de instantánea ejecutando el siguiente mandato:

```
backup db type=dbsnapshot devclass=tapeclass
```

2. Realice una copia de seguridad de la información de configuración de dispositivos en otro directorio, ejecutando el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

3. Realice una copia de seguridad del archivo del historial del volumen a otro directorio, ejecutando el siguiente mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

4. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt. El archivo está en el directorio de instancia del servidor.
5. Detenga todas las instancias del servidor de IBM Spectrum Protect. Compruebe que no haya ningún proceso del servidor de IBM Spectrum Protect en ejecución. Si está usando supervisión a nivel de la aplicación del servidor IBM Spectrum Protect, use su herramienta para formar clústeres para el recurso de la aplicación dsmserv.
6. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso db2sysc en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

7. Asegúrese de que todos los recursos compartidos para todas las instancias de IBM Spectrum Protect se encuentren en el nodo primario. Verifique que ningún otro nodo tenga acceso de grabación sobre estos recursos durante la actualización.

8. En el nodo primario, instale el servidor V6.3 mediante el uso del mandato `./install.bin`. Para obtener instrucciones detalladas sobre la instalación del servidor V6.3, consulte *Instalación de los componentes de servidor*.
9. En el nodo primario, instale el servidor IBM Spectrum Protect V8.1.2 ejecutando el mandato `./install.sh`. Para obtener instrucciones, consulte el apartado *Instalación de los componentes de servidor*. Después de iniciar el asistente, en la ventana de IBM Installation Manager, pulse el icono *Install*; no pulse el icono *Update* o *Modify*.
10. Inicie cada servidor de IBM Spectrum Protect V8.1.2 en primer plano. Utilizando el ID de propietario de la instancia, navegue hasta el directorio de la instancia y emita el siguiente mandato:

```
/opt/tivoli/tsm/server/bin/dsmserve
```

Espere hasta que vea el indicador de servidor, lo que indica que se ha iniciado el servidor.

11. Detenga el servidor para cada instancia de IBM Spectrum Protect que se esté actualizando.
12. En cada nodo secundario del clúster, siga estos pasos:
  - a. Mueva todos los recursos compartidos al nodo secundario. Si el entorno incluye varias instancias de IBM Spectrum Protect, los nodos secundarios deberán poder acceder a los recursos compartidos de todas las instancias durante la actualización.
  - b. Detenga todas las instancias del servidor de IBM Spectrum Protect. Compruebe que no haya ningún proceso del servidor de IBM Spectrum Protect en ejecución.
  - c. Verifique que el gestor de bases de datos no se está ejecutando para ninguna instancia. Determine si hay algún proceso `db2sysc` en ejecución. El propietario de los procesos en ejecución indica qué instancias están activas. Para cada propietario de instancias del servidor, ejecute el siguiente mandato para detener DB2:

```
db2stop
```

- d. Desinstale el servidor V6.1:

- i. En el directorio `/opt/tivoli/tsm/_uninst`, emita el siguiente mandato:

```
cd _uninst
```

- ii. Emita el mandato siguiente:

```
./Uninstall_Tivoli_Storage_Manager
```

Para obtener instrucciones detalladas sobre la desinstalación del servidor, consulte *Documentación de Tivoli Storage Manager V6.1*.

- e. Instale el servidor IBM Spectrum Protect V8.1.2 ejecutando el mandato `./install.sh`. En la ventana IBM Installation Manager, pulse el icono *Install*; no pulse el icono *Update* o *Modify*. Para obtener instrucciones sobre cómo instalar el servidor, consulte el apartado *Instalación de los componentes del servidor*.
  - f. Asegúrese de que se inicie cada servidor de IBM Spectrum Protect V8.1.2.
13. Registre las licencias para los componentes del servidor que están instalados en el sistema ejecutando el mandato `REGISTER LICENSE`:

```
register license file=installation_directory/server/bin/component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifica la abreviatura del componente.

Por ejemplo, si ha instalado el servidor en el directorio predeterminado, `/opt/tivoli/tsm`, ejecute el siguiente mandato para registrar la licencia:

```
register license file=/opt/tivoli/tsm/server/bin/tsmbasic.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect Extended Edition en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/tsmee.lic
```

Por ejemplo, si ha instalado IBM Spectrum Protect for Data Retention en el directorio `/opt/tivoli/tsm`, ejecute el siguiente mandato:

```
register license file=/opt/tivoli/tsm/server/bin/dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato `REGISTER LICENSE` no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.



**Referencia relacionada:**

BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

HALT (Concluir el servidor)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos Linux

## Actualización de IBM Spectrum Protect a V8.1.2 en un entorno en clúster for Linux

---

Para aprovechar las nuevas características de IBM Spectrum Protect, puede actualizar el servidor IBM Spectrum Protect que está instalado en un sistema operativo Linux en un entorno en clúster.

### Procedimiento

---

Siga las instrucciones de Configuración de un entorno de Linux para la agrupación en clúster.

 Sistemas operativos Windows

## Actualización de un servidor V6.3 o V7.1 a V8.1.2 en un entorno en clúster para Windows

---

Para aprovechar las características nuevas del producto, puede actualizar un servidor que esté instalado en un sistema operativo Windows en un entorno en clúster desde V6.3 o V7.1 a IBM Spectrum Protect V8.1.2.

### Antes de empezar

---

Asegúrese de conservar el soporte de instalación del release base del servidor V6.3 o V7.1 que se va a actualizar. Si ha instalado el servidor desde un paquete descargado, asegúrese de que los archivos descargados están disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, debe reinstalarse la licencia desde el soporte de instalación del release base del servidor.

### Procedimiento

---

1. Si planea instalar el servidor IBM Spectrum Protect V8.1.2 en el sistema operativo Windows Server 2012, instale el servidor de automatización del clúster de migración y la interfaz del mandato del clúster de migración primero. Para instalar estos componentes, emita los siguientes mandatos desde Windows 2.0 PowerShell:

```
Install-WindowsFeature -Name RSAT-Clustering-AutomationServer  
Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
```

2. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad instantánea, que proporciona una copia de seguridad completa de la base de datos sin interrumpir las copias de seguridad programadas. Por ejemplo, puede ejecutar el siguiente mandato para crear una copia de seguridad de instantánea:

```
backup db type=dbsnapshot devclass=tapeclass
```

3. Realice una copia de seguridad de la información de configuración del dispositivo a otro directorio. Ejecute el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

4. Realice una copia de seguridad del archivo del historial del volumen a otro directorio. Ejecute este mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

5. Guarde una copia del archivo de opciones del servidor, normalmente denominado dsmserv.opt, que está en el directorio de instancia de servidor.
6. Asegúrese de que el grupo de recursos esté en el nodo primario y de que todos los nodos del clúster se estén ejecutando. Realice las acciones siguientes en el nodo primario:
  - a. En la ventana Gestor de clúster de migración, desactive el recurso del servidor y elimínelo:
    - i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor se mostrará en la sección Otros recursos.
    - ii. Seleccione el recurso del servidor y pulse Desactivar este recurso.

- iii. Para suprimir el recurso del servidor, selecciónelo y pulse Suprimir.
  - b. En la ventana Gestor de clúster de migración tras error, suprima el nombre de red y la dirección IP:
    - i. En la sección Nombre del servidor, expanda el nombre de la red para ver la dirección IP. Anote el nombre de la red y la dirección IP.
    - ii. Seleccione el nombre de la red y la dirección IP, y pulse Eliminar.
  - c. En la ventana Gestor de clúster de migración, desactive el recurso del servidor DB2:
    - i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor de IBM Spectrum Protect se mostrará en la sección Otros recursos.
    - ii. Seleccione un recurso del servidor DB2, por ejemplo, SERVER1, y pulse Desactivar este recurso.
7. En el nodo primario, ejecute el siguiente mandato para eliminar la agrupación en clúster de DB2 de cada instancia de IBM Spectrum Protect en el clúster:

```
db2mscs -u:instancename
```

Por ejemplo, ejecute el siguiente mandato para eliminar la agrupación en clúster de DB2 desde la instancia de SERVER1:

```
db2mscs -u:server1
```

Consejo: Es posible que aparezca un mensaje de error acerca de un recurso de clúster perdido. Ignore este mensaje.

8. En el nodo primario, en la ventana Gestor de clúster de migración tras error, revise la sección Resumen de grupo de recursos. Compruebe que únicamente los discos compartidos y los recursos de cintas se mantienen en el grupo de recursos.
9. Detenga el servicio de clúster en cada nodo del clúster y suprima los archivos DLL del clúster del servidor. Después, reinicie el servicio de clúster.
10. Instale el servidor IBM Spectrum Protect V8.1.2 en cada nodo del clúster. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor de IBM Spectrum Protect. Si utiliza el asistente de instalación para instalar el servidor, en la ventana IBM Installation Manager, pulse el icono Actualizar. No pulse en el icono Instalar ni el icono Modificar.
11. En el nodo primario, inicie el servidor en primer plano para permitir que la configuración y reconciliación del esquema de base de datos pueda completarse. Cuando se inicie el servidor, párelo ejecutando el mandato HALT. Si el entorno tiene varias instancias de servidor, realice este paso para cada una de ellas.
12. En el nodo primario, inicie el asistente de configuración pulsando Inicio > Todos los programas > Servidor de IBM Spectrum Protect > Asistente de configuración. Realice los pasos siguientes en el asistente de configuración:
  - a. Cuando se le indique que escriba el ID de usuario, escriba el nombre de la cuenta de dominio asociada con el clúster.
  - b. Cuando se le solicite que escriba el nombre de la instancia, especifique el nombre de la instancia que está volviendo a organizar en clúster.
  - c. Pulse Sí cuando se le solicite que indique si desea volver a agrupar en clúster.
  - d. Continúe avanzando a través del asistente hasta que aparezca un mensaje indicando que la configuración ha finalizado correctamente.
13. Registre las licencias para los componentes del servidor de IBM Spectrum Protect que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory\server\component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifica la abreviatura del componente.

Por ejemplo, si instaló el servidor en el directorio predeterminado, c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato para registrar la licencia:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmbasic.lic
```

Por ejemplo, si instaló IBM Spectrum Protect Extended Edition en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmee.lic
```

Por ejemplo, si ha instaló IBM Spectrum Protect for Data Retention en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- o IBM Spectrum Protect for Mail
- o IBM Spectrum Protect for Databases
- o IBM Spectrum Protect for ERP
- o IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

## Qué hacer a continuación

---

Si hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos disponible, instale el controlador de dispositivos de IBM Spectrum Protect ejecutando el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos y la ubicación predeterminada es `C:\Program Files\Tivoli\TSM\device\drivers`.

### Referencia relacionada:

BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos Windows

## Actualización de IBM® Tivoli Storage Manager V6.1 a IBM Spectrum Protect V8.1.2 en un entorno en clúster para Windows

---

Para aprovechar las características nuevas, puede actualizar un servidor instalado en un sistema operativo Windows en un entorno en clúster de la V6.1 a la V8.1.2.

### Antes de empezar

---

Asegúrese de conservar el soporte de instalación de los releases base del servidor V6.1 y V6.3. Si obtuvo el software del servidor de un paquete descargado, asegúrese de que los archivos descargados estén disponibles. Si la actualización falla y se desinstala el módulo de licencia del servidor, el soporte de instalación del release base del servidor es necesario para poder reinstalar la licencia.

### Procedimiento

---

1. Si planea instalar el servidor IBM Spectrum Protect V8.1.2 en el sistema operativo Windows Server 2012, instale el servidor de automatización del clúster de migración y la interfaz del mandato del clúster de migración primero. Para instalar estos componentes, emita los siguientes mandatos desde Windows 2.0 PowerShell:

```
Install-WindowsFeature -Name RSAT-Clustering-AutomationServer  
Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
```

2. Realice una copia de seguridad de la base de datos utilizando el mandato BACKUP DB. El método preferido es utilizar una copia de seguridad instantánea, que proporciona una copia de seguridad completa de la base de datos sin interrumpir las copias de seguridad programadas. Por ejemplo, puede ejecutar el siguiente mandato para crear una copia de seguridad de instantánea:

```
backup db type=dbsnapshot devclass=tapeclass
```

3. Realice una copia de seguridad de la información de configuración del dispositivo a otro directorio. Ejecute el siguiente mandato:

```
backup devconfig filenames=nombre_archivo
```

Donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información de configuración del dispositivo.

4. Realice una copia de seguridad del archivo del historial del volumen a otro directorio. Ejecute este mandato:

```
backup volhistory filenames=nombre_archivo
```

donde *nombre\_archivo* especifica el nombre del archivo en el que se almacena la información histórica de volúmenes.

5. Guarde una copia del archivo de opciones del servidor, normalmente denominado `dsmserv.opt`, que está en el directorio de instancia de servidor.
6. Asegúrese de que el grupo de recursos esté en el nodo primario y de que todos los nodos del clúster se estén ejecutando. Realice las acciones siguientes en el nodo primario:
  - a. En la ventana Gestor de clúster de migración, desactive el recurso del servidor y elimínelo:
    - i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor se mostrará en la sección Otros recursos.
    - ii. Seleccione el recurso del servidor y pulse Desactivar este recurso.
    - iii. Para suprimir el recurso del servidor, selecciónelo y pulse Suprimir.
  - b. En la ventana Gestor de clúster de migración tras error, suprima el nombre de red y la dirección IP:
    - i. En la sección Nombre del servidor, expanda el nombre de la red para ver la dirección IP. Anote el nombre de la red y la dirección IP.
    - ii. Seleccione el nombre de la red y la dirección IP, y pulse Eliminar.
  - c. En la ventana Gestor de clúster de migración, desactive el recurso del servidor DB2:

- i. Seleccione Servicios y aplicaciones y, a continuación, seleccione el grupo de clúster. El recurso del servidor de IBM Spectrum Protect se mostrará en la sección Otros recursos.
  - ii. Seleccione un recurso del servidor DB2, por ejemplo, SERVER1, y pulse Desactivar este recurso.
7. En el nodo primario, para eliminar la agrupación en clúster de DB2 de la instancia, para cada instancia de IBM Spectrum Protect del clúster, emita el mandato siguiente:

```
db2mscs -u:instancename
```

Por ejemplo:

```
db2mscs -u:server1
```

Consejo: Es posible que aparezca un mensaje de error acerca de un recurso de clúster perdido. Ignore este mensaje.

8. En el nodo primario, en la ventana Gestor de clúster de migración tras error, en la sección Resumen de grupo de recursos, verifique que solo los discos compartidos y los recursos de cinta se mantienen en el grupo de recursos.
9. En el nodo primario, instale el servidor V6.3 haciendo uso del mandato install.exe. Para obtener instrucciones detalladas sobre la instalación del servidor V6.3, consulte Instalación de los componentes de servidor.
10. En el nodo primario, instale el servidor IBM Spectrum Protect V8.1.2. Para obtener instrucciones, consulte el apartado Instalación de los componentes de servidor. Si utiliza el asistente de instalación para instalar el servidor, en la ventana IBM Installation Manager, pulse el icono Instalar. No pulse en el icono Actualizar o Modificar.
11. En cada nodo secundario, desinstale V6.1:
  - a. Cámbiese al directorio siguiente:

```
C:\Program Files\Tivoli\TSM\_uninst
```

- b. Emita el mandato siguiente:

```
Desinstale Tivoli Storage Manager.exe
```

12. En el nodo primario, inicie el asistente de configuración pulsando Inicio > Todos los programas > Servidor de IBM Spectrum Protect > Asistente de configuración. Avance a través del asistente de configuración:
  - a. Cuando se le solicite que escriba el nombre de la instancia, especifique el nombre de la instancia que está volviendo a organizar en clúster.
  - b. Cuando se le indique que escriba el ID de usuario, escriba el nombre de la cuenta de dominio asociada con el clúster.
  - c. Cuando se le pide que indique si desea volver a organizar en clúster, pulse Sí.
  - d. Continúe avanzando a través del asistente hasta que aparezca un mensaje indicando que la configuración ha finalizado correctamente.
13. Registre las licencias para los componentes del servidor de IBM Spectrum Protect que están instalados en el sistema ejecutando el mandato REGISTER LICENSE:

```
register license file=installation_directory\server\component_name.lic
```

en donde *installation\_directory* especifique el directorio en el cual instaló el componente, y *component\_name* especifica la abreviatura del componente.

Por ejemplo, si instaló el servidor en el directorio predeterminado, c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato para registrar la licencia:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmbasic.lic
```

Por ejemplo, si instaló IBM Spectrum Protect Extended Edition en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\tsmee.lic
```

Por ejemplo, si ha instaló IBM Spectrum Protect for Data Retention en el directorio c:\Program Files\Tivoli\TSM, ejecute el siguiente mandato:

```
register license file=c:\Program Files\Tivoli\TSM\server\dataret.lic
```

Restricción:

No puede utilizar el servidor IBM Spectrum Protect para registrar licencias de los siguientes productos:

- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Databases
- IBM Spectrum Protect for ERP
- IBM Spectrum Protect for Space Management

El mandato REGISTER LICENSE no se aplica a estas licencias. La licencia para estos productos se obtiene mediante los clientes de IBM Spectrum Protect.

## Qué hacer a continuación

Si hay un controlador de dispositivos disponible en Windows para las unidades de cintas o conmutadores de soportes que tiene pensado utilizar, utilice el controlador de dispositivos nativo. Si no hay un controlador de dispositivos disponible, instale el controlador de dispositivos de IBM Spectrum Protect ejecutando el mandato `dpinst.exe /a`. El archivo `dpinst.exe` se encuentra en el directorio del controlador de dispositivos y la ubicación predeterminada es `C:\Program Files\Tivoli\TSM\device\drivers`.


**Referencia relacionada:**

BACKUP DB (copia de seguridad de la base de datos)

BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)

BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

REGISTER LICENSE (Registrar una nueva licencia)

 Sistemas operativos Windows

## Eliminación de GSKit Versión 7 después de actualizar a IBM Spectrum Protect Versión 8.1.2

---

El asistente de instalación de IBM Spectrum Protect actualiza GSKit Versión 8 y posterior. GSKit Versión 7 no se elimina ni se actualiza cuando actualiza a IBM Spectrum Protect Versión 8.1.2, aunque se haya instalado con una versión anterior de IBM Spectrum Protect.

### Acerca de esta tarea

---

Si ya no necesita GSKit V7 y desea liberar espacio en el sistema, puede eliminarlo después de actualizar a IBM Spectrum Protect Versión 8.1.2.

Importante: La eliminación de SKit V7 puede afectar a otros programas en el sistema basados en él.

### Procedimiento

---

Para eliminar GSKit V7, realice los pasos siguientes:

1. Haga una copia de seguridad del registro.
  - a. Pulse Inicio y, a continuación, Ejecutar.
  - b. Escriba `Regedit`. Pulse Aceptar.
  - c. Para guardar una copia del registro, seleccione Archivo > Exportar.
  - d. Si luego tiene que restaurar el registro, seleccione Archivo > Importar.

Para obtener más información, consulte la documentación de Windows.

2. Localice el directorio en el que está instalado GSKit. El directorio predeterminado es `C:\Archivos de programa\IBM\gsk7\`.
3. Elimine el directorio de instalación de GSKit, `gsk7`, y todos los archivos y subdirectorios. Pulse con el botón derecho sobre la carpeta y pulse Suprimir.
4. Elimine la clave de registro de GSKit 7 y todas las subclaves y valores.

Importante: La eliminación de la clave errónea puede ocasionar problemas en el sistema, como por ejemplo que no se pueda reiniciar la estación de trabajo.

  - a. Pulse Inicio y, a continuación, Ejecutar.
  - b. Escriba `Regedit`. Pulse Aceptar.
  - c. La clave de registro de GSKit se encuentra en este directorio: `HKEY_LOCAL_MACHINE\SOFTWARE\IBM`. Pulse con el botón derecho sobre la clave de registro, `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\GSK7`, y pulse Suprimir.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalación y actualización del Centro de operaciones

---

IBM Spectrum Protect Operations Center es la interfaz basada en web para gestionar el entorno de almacenamiento.

### Antes de empezar

---

Antes de instalar y configurar el Centro de operaciones, revise la siguiente información:

- Requisitos del sistema del Centro de operaciones
  - Requisitos de sistema del Centro de operaciones
  - Requisitos del servidor concentrador y spoke
  - Requisitos de sistema operativo
  - Requisitos del navegador web
  - Requisitos de idioma
  - Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect
- Los ID de administrador que requiere el centro de operaciones

- IBM Installation Manager
- Lista de comprobación de la instalación
- Obtención del paquete de instalación de Centro de operaciones



## Acerca de esta tarea


Tabla 1 enumera los métodos para instalar o desinstalar Centro de operaciones e indica en dónde encontrar las instrucciones relacionadas.

Para obtener información sobre la actualización de Centro de operaciones, consulte Actualización del Centro de operaciones.

Tabla 1. Métodos para instalar o desinstalar Centro de operaciones

comunicaciones	Instrucciones
Asistente gráfico	<ul style="list-style-type: none"> <li>• Instalación de Centro de operaciones utilizando el asistente gráfico</li> <li>• Desinstalación de Centro de operaciones utilizando el asistente gráfico</li> </ul>
Modalidad de consola	<ul style="list-style-type: none"> <li>• Instalar el Centro de operaciones en modalidad de consola</li> <li>• Desinstalación del Centro de operaciones en modalidad de consola</li> </ul>
Modalidad silenciosa	<ul style="list-style-type: none"> <li>• Instalación de Centro de operaciones en el modo silencioso</li> <li>• Desinstalar Centro de operaciones en modalidad silenciosa</li> </ul>

- Planificación para instalar el Centro de operaciones  
Antes de instalar Centro de operaciones, debe entender los requisitos del sistema, los ID de administrador que requiere Centro de operaciones y la información que debe proporcionarle al programa de instalación.
- Instalar el Centro de operaciones  
Puede instalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Actualización del Centro de operaciones  
Puede actualizar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.
- Guía de inicio de la Centro de operaciones  
Antes de poder utilizar Centro de operaciones para gestionar el entorno de almacenamiento, debe configurarlo.
-  Sistemas operativos AIX  Sistemas operativos Linux Resolución de problemas de la instalación de Centro de operaciones  
Si ocurre un problema con la instalación del Centro de operaciones y no puede resolverlo, puede consultar las descripciones de problemas conocidos para una posible solución.
- Desinstalación de Centro de operaciones  
Puede desinstalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.
- Volver a una versión anterior de Centro de operaciones  
De forma predeterminada, IBM Installation Manager guarda versiones anteriores de un paquete para poder regresar a una versión anterior si experimenta un problema con versiones posteriores de actualizaciones, arreglos o paquetes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Planificación para instalar el Centro de operaciones

Antes de instalar Centro de operaciones, debe entender los requisitos del sistema, los ID de administrador que requiere Centro de operaciones y la información que debe proporcionarle al programa de instalación.

## Acerca de esta tarea

Desde Centro de operaciones, puede gestionar los siguientes aspectos principales del entorno de almacenamiento:

- servidores y clientes de IBM Spectrum Protect
- Servicios como copia de seguridad y restauración, archivar y restablecer y migrar y recuperar
- Agrupaciones de almacenamiento y dispositivos de almacenamiento

Centro de operaciones incluye las funciones siguientes:

Interfaz de usuario para varios servidores

Puede usar Centro de operaciones para gestionar uno o más servidores IBM Spectrum Protect.

En un entorno con varios servidores, puede designar un servidor como un *servidor concentrador* y los otros como *servidores de radio*. El servidor central puede recibir alertas e información del estado desde los servidores de radio y presentar la información de manera consolidada en Centro de operaciones.

#### Supervisor de alertas




Una *alerta* es una notificación de un problema importante en el servidor y se desencadena mediante un mensaje de servidor. Puede definir qué mensajes del servidor se envían como alertas, y sólo esos mensajes se clasifican como alertas en Centro de operaciones o en un correo electrónico.

Esta supervisión de la alerta puede ayudarle a identificar y rastrear problemas importantes en el servidor.

#### Interfaz conveniente de la línea de mandatos

Centro de operaciones incluye una interfaz de línea de mandatos para configuración y características avanzadas.

- **Requisitos del sistema del Centro de operaciones**  
Antes de instalar el Centro de operaciones, asegúrese de que su sistema cumple con los requisitos mínimos.
- **Los ID de administrador que requiere el centro de operaciones**  
Un administrador debe tener un ID y contraseña válidos en el servidor hub para iniciar sesión en el Centro de operaciones. Un ID de administrador también se asigna al Centro de operaciones para que el Centro de operaciones pueda gestionar los servidores.
- **IBM Installation Manager**  
El Centro de operaciones utiliza el IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.
- **Lista de comprobación de la instalación**  
Antes de instalar Centro de operaciones, debe verificar cierta información, como las credenciales de instalación y debe determinar la información de entrada que debe proporcionarle a IBM Installation Manager para la instalación.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos del sistema del Centro de operaciones

Antes de instalar el Centro de operaciones, asegúrese de que su sistema cumple con los requisitos mínimos.

Utilice la Calculadora de requisitos del sistema del Centro de operaciones para realizar una estimación de los requisitos del sistema para ejecutar el Centro de operaciones y los servidores concentrador y de radio que supervisa el Centro de operaciones.

### Requisitos que se verifican durante la instalación




Tabla 1 enumera los requerimientos que son un prerrequisito y que se verifican durante la instalación e indica en dónde encontrar más información sobre estos requerimientos.

Tabla 1. Requisitos que se verifican durante la instalación

Requisito	Detalles
Requisito mínimo de memoria	Requisitos de sistema del Centro de operaciones
Requisito del sistema operativo	Requisitos de sistema operativo
Nombre de host del sistema en el que se instalará Centro de operaciones	Lista de comprobación de la instalación
Requisitos para el directorio de instalación de Centro de operaciones	Lista de comprobación de la instalación

- **Requisitos de sistema del Centro de operaciones**  
Puede instalar Centro de operaciones en un sistema que también está ejecutando el servidor IBM Spectrum Protect o en un sistema diferente. Si instala Centro de operaciones en el mismo sistema que un servidor, dicho sistema debe cumplir los requisitos del sistema para ambos, Centro de operaciones y el servidor.
- **Requisitos del servidor concentrador y spoke**  
Cuando se abre el centro de operaciones por primera vez, es necesario asociarlo a un servidor de IBM Spectrum Protect designado como *servidor concentrador*. En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- **Requisitos de sistema operativo**  
El Centro de operaciones está disponible para los sistemas de AIX, Linux y Windows.
- **Requisitos del navegador web**  
Centro de operaciones puede ejecutarse en los navegadores web Apple, Google, Microsoft, y Mozilla.
- **Requisitos de idioma**  
De forma predeterminada, el Centro de operaciones utiliza el idioma que utiliza el navegador web. Sin embargo, el proceso de instalación utiliza el idioma que utiliza el sistema operativo. Compruebe que el navegador web y el sistema operativo estén establecidos en el idioma que necesita.

- Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect  
servicios de gestión de cliente de IBM Spectrum Protect es un componente que se instala en clientes de archivado y copia de seguridad para recopilar información de diagnóstico como, por ejemplo, archivos de registro de cliente. Antes de instalar el servicio de gestión de clientes en el sistema, debe conocer los requisitos y las limitaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos de sistema del Centro de operaciones




Puede instalar Centro de operaciones en un sistema que también está ejecutando el servidor IBM Spectrum Protect o en un sistema diferente. Si instala Centro de operaciones en el mismo sistema que un servidor, dicho sistema debe cumplir los requisitos del sistema para ambos, Centro de operaciones y el servidor.

### Requisitos de recursos

Se requieren los siguientes recursos para ejecutar el Centro de operaciones:

- Un núcleo de procesador
- 4 GB de memoria
- 1 GB de espacio en disco

El servidor de radio y el servidor central que supervisa el Centro de operaciones requiere recursos adicionales, según se describe en Requisitos del servidor concentrador y spoke.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos del servidor concentrador y spoke

Cuando se abre el centro de operaciones por primera vez, es necesario asociarlo a un servidor de IBM Spectrum Protect designado como *servidor concentrador*. En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

Si Centro de operaciones solo supervisa un servidor, dicho servidor se sigue denominando servidor concentrador, aunque no tenga conectado ningún servidor de radio.

Tabla 1 indica la versión del servidor IBM Spectrum Protect que debe instalarse en el servidor concentrador y en cada servidor spoke que es gestionado por Centro de operaciones.



Tabla 1. IBM Spectrum Protect requisitos de la versión del servidor para el servidor hub y el servidor de radio

Centro de operaciones	Versión en el servidor concentrador	Versión en cada servidor de radio
V8.1.2	V8.1.2	V6.3.4 o posteriores Restricción: Algunas funciones de Centro de operaciones no están disponibles para servidores que utilizan una versión anterior a la V8.1.2.

### Número de servidores spoke que un servidor concentrador puede admitir

El número de servidores spoke que un servidor concentrador puede soportar depende de la configuración y de la versión de IBM Spectrum Protect en cada servidor spoke. Sin embargo, una guía general es que el servidor concentrador puede admitir de 10 a 20 servidores spoke V6.3.4, pero puede admitir más servidores spoke V7.1 o posteriores.

- Consejos para designar la configuración del servidor concentrador y el servidor de radio  
Al diseñar la configuración central y de radio, considere especialmente los requisitos de recursos para la supervisión del estado. También, considere cómo quiere agrupar los servidores centrales y de radio y si quiere usar varios servidores centrales.
- Consejos para elegir un servidor concentrador  
Para el servidor concentrador, debe elegir un servidor que tenga los recursos adecuados y que se encuentre para una latencia de red de viaje de ida y vuelta mínima.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows



## Consejos para designar la configuración del servidor concentrador y el servidor de radio

---

Al diseñar la configuración central y de radio, considere especialmente los requisitos de recursos para la supervisión del estado. También, considere cómo quiere agrupar los servidores centrales y de radio y si quiere usar varios servidores centrales.

Utilice la Calculadora de requisitos del sistema del Centro de operaciones para realizar una estimación de los requisitos del sistema para ejecutar el Centro de operaciones y los servidores concentrador y de radio que supervisa el Centro de operaciones.

### Factores principales que afectan al rendimiento

---

Los factores siguientes tienen mayor impacto en el rendimiento del Centro de operaciones:

- El procesador y la memoria del sistema en el que está instalado el Centro de operaciones
- Los recursos del sistema del servidor concentrador y los servidores de radio, incluyendo el sistema de disco que está en uso para la base de datos del servidor concentrador
- El número de nodos de cliente y espacios de archivos de máquina virtual gestionados por los servidores concentrador y de radio.
- La frecuencia a la cual se renuevan los datos en Centro de operaciones

### Cómo agrupar los servidores concentradores y de radio

---

Tenga en cuenta agrupar los servidores concentradores y de radio por ubicación geográfica. Por ejemplo, la gestión de los servidores dentro del mismo centro de datos puede ayudar a impedir problemas provocados por los cortafuegos o por un ancho de banda de red inadecuado entre las distintas ubicaciones. Si fuera necesario, puede dividir los servidores según una o más de las siguientes características:

- El administrador que gestiona los servidores
- La entidad de organización que funda los servidores
- Sistema operativo del servidor
- El idioma en que se ejecutan los servidores

Consejo: Si los servidores concentradores y de radio no se están ejecutando en el mismo idioma, podría ver texto corrupto en el Centro de operaciones.

### Cómo agrupar servidores concentradores y de radio en una configuración empresarial

---

En una configuración empresarial, una red de servidores de IBM Spectrum Protect se gestiona como un grupo. Los cambios que se realizan en el *gestor de configuración* se pueden distribuir automáticamente en uno o más *servidores gestionados* de la red.

Normalmente el Centro de operaciones registra y mantiene un ID de administrador dedicado en los servidores concentradores y de radio. Este *administrador de supervisión* debe tener siempre la misma contraseña en todos los servidores.

Si utiliza una configuración empresarial, puede mejorar el proceso mediante el cual las credenciales de administrador se sincronizan en los servidores de radio. Para mejorar el rendimiento y la eficiencia de mantener el ID de administrador de supervisión, realice los pasos siguientes:

1. Designe el servidor de gestor de configuración como servidor concentrador del Centro de operaciones. Durante la configuración del servidor concentrador, se registra un ID de administrador de supervisión denominado *IBM-OC-nombre\_servidor\_concentrador*.
2. En el servidor concentrador, añada el ID de administrador de supervisión a un perfil de configuración empresarial nuevo o existente. Emita el mandato NOTIFY SUBSCRIBERS para distribuir el perfil a los servidores gestionados.
3. Añada uno o más de los servidores gestionados como servidores de radio del Centro de operaciones.

El Centro de operaciones detecta esta configuración y permite al gestor de configuración distribuir y actualizar el ID de administrador de supervisión en los servidores de radio.

### Cuándo usar varios servidores concentradores

---

Si tiene más de 10 - 20 servidores de radio V6.3.4, o si las limitaciones de recursos requieren que se particione el entorno, puede configurar varios servidores concentradores y conectar un subconjunto de servidores de radio a cada servidor concentrador.

Restricciones:

- Un único servidor no puede utilizarse como servidor hub y servidor spoke.
- Cada servidor spoke puede asignarse a un único servidor hub.
- Cada servidor hub necesita una instancia independiente de Centro de operaciones, con una dirección web separada.

## Consejos para elegir un servidor concentrador

---

Para el servidor concentrador, debe elegir un servidor que tenga los recursos adecuados y que se encuentre para una latencia de red de viaje de ida y vuelta mínima.

Atención: No utilice el mismo servidor como servidor concentrador para varios centros de operaciones. Utilice las directrices siguientes para decidir qué servidor designar como servidor concentrador:

Elija un servidor con carga ligera

Considere un servidor que tenga una carga ligera para operaciones como, por ejemplo, copia de seguridad y archivado de cliente. Un servidor con carga ligera es también una buena opción como sistema host para el Centro de operaciones.

Asegúrese de que el servidor tiene los recursos para manejar tanto su carga de trabajo de servidor típica y la carga de trabajo estimada para actuar como servidor concentrador.

Ubique el servidor para obtener una latencia de red de ida y vuelta mínima

Ubique el servidor concentrador de manera que la conexión de red entre el servidor concentrador y los servidores de radio tenga una latencia de viaje de ida y vuelta que no sea superior a 5 ms. Esta latencia puede conseguirse habitualmente cuando los servidores están en la misma red de área local (LAN).

Las redes mal ajustadas, que sean muy utilizadas por otras aplicaciones, o que tengan una latencia de ida y vuelta mucho mayor que 5 ms, pueden degradar las comunicaciones entre los servidores de radio y concentrador. Por ejemplo, una latencia de ida y vuelta de 50 ms o superior puede resultar en tiempos de comunicación que hagan que los servidores de radio se desconecten o vuelvan a conectar al Centro de operaciones. Estas altas latencias pueden experimentarse en comunicaciones de red área amplia (WAN) de larga distancia.

Si los servidores de radio están a gran distancia del servidor concentrador y experimentan desconexiones frecuentes en el Centro de operaciones, puede aumentar el valor de la opción ADMINCOMMTIMEOUT en cada servidor para atenuar el problema.

Verifique que el servidor concentrador cumple los requisitos de recurso de supervisión de estado

La supervisión de estado requiere recursos adicionales en cada servidor en los que está habilitada. Los recursos necesarios dependen principalmente del número de clientes gestionados por los servidores concentrador y de radio. Se utilizan menos recursos en un servidor concentrador con un servidor spoke V7.1 o posterior que en un servidor concentrador con un servidor spoke V6.3.4.

Compruebe que el servidor concentrador cumple los requisitos de recurso de uso de procesador, espacio de base de datos, espacio de registro de archivado y capacidad de operaciones de E/S por segundo (IOPS).

Un servidor concentrador con una capacidad de IOPS alta puede manejar una mayor cantidad de datos de estado entrantes de los servidores de radio. El uso de los dispositivos de almacenamiento siguientes para la base de datos del servidor concentrador puede ayudarle a alcanzar esta capacidad:

- Una unidad de estado sólido (SSD) de nivel de empresa
- Un dispositivo de almacenamiento de disco SAN externo con varios volúmenes o varios pernos en cada volumen

En un entorno con menos de 1000 clientes, considere establecer una capacidad de línea de base de 1000 IOPS para la base de datos del servidor concentrador si el servidor concentrador gestiona cualquier servidor de radio.

Determine si el entorno requiere varios servidores concentradores


Si hay más de 10.000 - 20.000 nodos de cliente y espacios de archivos de máquina virtual gestionados por un conjunto de servidores concentrador y de radio, los requisitos de recurso podrían exceder lo que tiene disponible el servidor concentrador, especialmente, si los servidores de radio son servidores V6.3.4. Plántese designar un segundo servidor como servidor concentrador y trasladar los servidores de radio al servidor concentrador nuevo para equilibrar la carga.





## Requisitos de sistema operativo

---




El Centro de operaciones está disponible para los sistemas de AIX, Linux y Windows.

Puede ejecutar Centro de operaciones en los siguientes sistemas:

-  Sistemas operativos AIX:
  - IBM® AIX V7.1 (64 bits) TL 4 y SP 2
  - IBM AIX V7.2 (64 bits) TL 0 y SP 2

-  Sistemas operativos LinuxLinux en sistemas x86\_64:
  - Red Hat Enterprise Linux 6.7
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 11, Service Pack 4 o posterior
  - SUSE Linux Enterprise Server 12
-  Sistemas operativos LinuxSistemas Linux on System z (arquitectura s390x de 64 bits):
  - Red Hat Enterprise Linux 7.1
  - SUSE Linux Enterprise Server 12
-  Sistemas operativos LinuxSistemas Linux on Power Systems (little endian):
  - Red Hat Enterprise Linux 7 con la arquitectura PPC64LE
-  Sistemas operativos WindowsSistemas Windows:
  - Microsoft Windows Server 2012: Standard, Enterprise o Datacenter Edition (64 bits)
  - Microsoft Windows Server 2012 R2 (64 bits)
  - Microsoft Windows Server 2016

Para obtener la información más actualizada sobre requisitos, consulte Requisitos de software y hardware.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos del navegador web

Centro de operaciones puede ejecutarse en los navegadores web Apple, Google, Microsoft, y Mozilla.

Para obtener una vista óptima de Centro de operaciones en el navegador web, asegúrese de que la resolución en pantalla del sistema esté configurada en un mínimo de 1024 X 768 píxeles.




Para obtener un rendimiento óptimo, utilice un navegador web que tenga un buen rendimiento de JavaScript y habilite el almacenamiento en memoria caché del navegador.

Centro de operaciones puede ejecutarse en los siguientes navegadores web:

- Apple Safari en el iPad  
Restricción: Si Apple Safari se está ejecutando en iOS 8.x o iOS 9.x, no puede utilizar un certificado firmado automáticamente para la comunicación segura con el Centro de operaciones sin una configuración adicional del certificado. Utilice un certificado de entidad emisora de certificados (CA) o configure el certificado autofirmado como sea necesario. Para obtener instrucciones, consulte la nota técnica <http://www.ibm.com/support/docview.wss?uid=swg21963153>.
- Google Chrome 40 o posterior
- Microsoft Internet Explorer 11 o posterior
- Mozilla Firefox ESR 31 o posterior

Para ejecutar el Centro de operaciones en conformidad con la recomendación 800-131A para Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST), la comunicación entre el Centro de operaciones y el navegador web debe protegerse utilizando el protocolo TLS (Seguridad de la capa de transporte) 1.2. Durante la instalación, especifique si la conformidad 800-131A de SP es necesaria y el nivel de conformidad. Si durante la instalación se especifica conformidad 800-131A de SP estricta, el navegador web debe soportar TLS 1.2 y se debe habilitar TLS 1.2.

El navegador web visualiza un error de SSL si se especifica el cumplimiento estricto de SP 800-131A durante la instalación y el navegador web no cumple los requisitos anteriores.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos de idioma

De forma predeterminada, el Centro de operaciones utiliza el idioma que utiliza el navegador web. Sin embargo, el proceso de instalación utiliza el idioma que utiliza el sistema operativo. Compruebe que el navegador web y el sistema operativo estén establecidos en el idioma que necesita.


 Sistemas operativos AIX

Tabla 1. Centro de operaciones valores de idioma que puede usar en los sistemas AIX

Idioma	Valor opción LANGUAGE
Chino simplificado	zh_CN
Chino, simplificado (UTF-8)	ZH_CN

<b>Idioma</b>	<b>Valor opción LANGUAGE</b>
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (UTF-8)	ZH_TW
Chino tradicional (euc_tw)	zh_TW
Inglés	en_US
Inglés (UTF-8)	EN_US
Francés	fr_FR
Francés (UTF-8)	FR_FR
Alemán	de_DE
Alemán (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonés (EUC)	ja_JP
Japonés (PC)	Ja_JP
Japonés (UTF-8)	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Portugués, Brasileño	pt_BR
Portugués de Brasil (UTF-8)	PT_BR
Ruso	ru_RU
Ruso (UTF-8)	RU_RU
Español	es_ES
Español (UTF-8)	ES_ES


 Sistemas operativos Linux

Tabla 2. Centro de operaciones valores de idioma que puede usar en los sistemas Linux

<b>Idioma</b>	<b>Valor opción LANGUAGE</b>
Chino simplificado	zh_CN
Chino simplificado (GBK)	zh_CN.gb18030
Chino, simplificado (UTF-8)	zh_CN.utf8
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (euc_tw)	zh_TW
Chino, tradicional (UTF-8)	zh_TW.utf8
Inglés de Estados Unidos	en_US
Inglés (UTF-8)	en_US.utf8
Francés	fr_FR
Francés (UTF-8)	fr_FR.utf8
Alemán	de_DE
Alemán (UTF-8)	de_DE.utf8
Italiano	it_IT
Italiano (UTF-8)	it_IT.utf8
Japonés (EUC)	ja_JP
Japonés (UTF-8)	ja_JP.utf8

Idioma	Valor opción LANGUAGE
Coreano	ko_KR
Coreano (UTF-8)	ko_KR.utf8
Portugués, Brasileño	pt_BR
Portugués, de Brasil (UTF-8)	pt_BR.utf8
Ruso	ru_RU
Ruso (UTF-8)	ru_RU.utf8
Español	es_ES
Español (UTF-8)	es_ES.utf8





 Sistemas operativos Windows

Tabla 3. Centro de operaciones valores de idioma que puede usar en los sistemas Windows

Idioma	Valor opción LANGUAGE
Chino simplificado	chs
Chino, Tradicional	cht
Inglés	ameng
Francés	fra
Alemán	deu
Italiano	ita
Japonés (Shift-JIS)	jpn
Coreano	kor
Portugués, Brasileño	ptb
Ruso	rus
Español	esp

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect

servicios de gestión de cliente de IBM Spectrum Protect es un componente que se instala en clientes de archivado y copia de seguridad para recopilar información de diagnóstico como, por ejemplo, archivos de registro de cliente. Antes de instalar el servicio de gestión de clientes en el sistema, debe conocer los requisitos y las limitaciones.

En la documentación de servicio de gestión de clientes, *sistema cliente* es el sistema donde está instalado el cliente de archivado y copia de seguridad.

La información de diagnóstico se puede recopilar solo desde clientes Linux y Windows. pero los administradores pueden ver la información de diagnóstico en Centro de operaciones en sistemas operativos AIX, Linux o Windows.

### Requisitos para el servicio de gestión de clientes

Compruebe los siguientes requisitos antes de instalar servicio de gestión de clientes:

- Para acceder de forma remota al cliente, el administrador del Centro de operaciones debe tener autoridad de sistema y uno de los siguientes niveles de autoridad de cliente:
  - Autoridad de política
  - Autoridad de propietario de cliente
  - Autoridad de acceso de nodo de cliente
- Asegúrese de que el sistema cliente cumple estos requisitos:
  - El servicio de gestión de clientes solo se puede instalar en sistemas cliente que se ejecutan en sistemas operativos Linux o Windows:

- Sistemas operativos Linux x86 de 64 bits soportados para el cliente de archivado y copia de seguridad.
    - Sistemas operativos Windows de 32 bits y de 64 bits soportados para el cliente de archivado y copia de seguridad.
  - Debe instalarse TLS (seguridad de la capa de transporte) 1.2 para la transmisión de datos entre servicio de gestión de clientes y Centro de operaciones. Se proporciona autenticación básica y los datos y la información de autenticación se cifran a través del canal SSL. TLS 1.2 se instala de forma automática junto con los certificados SSL necesarios al instalar el servicio de gestión de clientes.
  - En los sistemas cliente Linux, debe tener autorización de usuario root para instalar servicio de gestión de clientes.
  - Para los sistemas cliente que puede tener varios nodos de cliente, como los sistemas clientes de Linux, asegúrese de que cada nombre de nodo sea exclusivo en el sistema cliente.
- Consejo: Después de instalar el servicio de gestión de clientes, no tiene que instalarlo otra vez porque el servicio puede descubrir varios archivos de opciones de cliente.

## Limitaciones de servicio de gestión de clientes




servicio de gestión de clientes proporciona los servicios básicos para recopilar información de diagnóstico de los clientes de archivado y copia de seguridad. Existen las siguientes limitaciones para servicio de gestión de clientes:

- Puede instalar servicio de gestión de clientes solo en sistemas con clientes de archivado y copia de seguridad, incluidos los clientes de archivado y copia de seguridad que están instalados en nodos de transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.
- No puede instalar servicio de gestión de clientes en otros productos o componentes de cliente IBM Spectrum Protect que no tengan clientes de copia de seguridad/archivado.
- Si los clientes de archivado y copia de seguridad están protegidos mediante un cortafuegos, asegúrese de que el Centro de operaciones se puede conectar a los clientes de archivado y copia de seguridad a través del cortafuegos utilizando el puerto configurado para servicio de gestión de clientes. El puerto predeterminado es el 9028, pero no se puede cambiar.
- El cliente de servicio de gestión de clientes lee todos los archivos de registro para localizar entradas para el periodo anterior de 72 horas.
- La página Diagnóstico de Centro de operaciones proporciona información de resolución de problemas básica de los clientes de archivado y copia de seguridad. Sin embargo, para algunos problemas de copia de seguridad, es posible que tenga que acceder al sistema cliente y obtener información de diagnóstico adicional.
- Si el tamaño combinado de los archivos de registro de errores de cliente y de los archivos de registro de planificación es superior a 500 MB, se pueden producir retardos al enviar registros de anotaciones al Centro de operaciones. Puede controlar el tamaño de los archivos de registro habilitando la depuración o el ajuste de los archivos de registro especificando la opción de cliente errorlogretention o errorlogmax.
- Si utiliza el mismo nombre de nodo de cliente para conectarse a varios servidores de IBM Spectrum Protect que están instalados en el mismo servidor, solo puede ver los archivos de registro para uno de los nodos de cliente.

Para obtener las actualizaciones con respecto a servicio de gestión de clientes, incluyendo requisitos, limitaciones y actualizaciones de documentación, consulte la nota técnica 1963610.

### Tareas relacionadas:

Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Los ID de administrador que requiere el centro de operaciones

Un administrador debe tener un ID y contraseña válidos en el servidor hub para iniciar sesión en el Centro de operaciones. Un ID de administrador también se asigna al Centro de operaciones para que el Centro de operaciones pueda gestionar los servidores.

Centro de operaciones requiere los siguientes ID de administrador IBM Spectrum Protect:

Los ID de administrador que están registrados en el servidor central

Cualquier ID de administrador de que está registrado en el servidor hub puede utilizarse para iniciar sesión en el Centro de operaciones. El nivel de autorización del ID determina las tareas que pueden completarse. Para crear IDs de administrador, utilice el mandato REGISTER ADMIN.

Restricción: Para utilizar un ID de administrador en una configuración de varios servidores, el ID debe estar registrado en los servidores centrales y de radio con la misma contraseña y nivel de autorización.

Para gestionar la autenticación de estos servicios, considere utilizar uno de los siguientes métodos:

- Un servidor LDAP(Lightweight Directory Access Protocol)
- Las funciones de configuración empresarial para distribuir automáticamente los cambios en las definiciones de administrador.

Supervisión del ID de administrador




Cuando configura el servidor hub de forma inicial, un ID de administrador llamado IBM-OC-server\_name se registra con autoridad de sistema en el servidor hub y se asocia a la contraseña inicial que especificó. Este ID, que a veces se denomina *administrador de supervisión*, está diseñado para que lo utilice solo el Centro de operaciones.

No elimine, bloquee o modifique este ID. El mismo ID de administrador con la misma contraseña se registra en los servidores de radio que añade. La contraseña se cambia de forma automática en los servidores concentrador y spoke cada 90 días. No es necesario utilizar ni gestionar dicha contraseña.

Restricción: El Centro de operaciones mantiene el ID de administrador de supervisión y la contraseña en servidores spoke a menos que se utilice una configuración empresarial para gestionar estas credenciales. Para obtener más información acerca de la utilización de una configuración empresarial para gestionar las credenciales, consulte el apartado Consejos para designar la configuración del servidor concentrador y el servidor de radio.

**Referencia relacionada:**

REGISTER ADMIN (Registrar un ID de administrador)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## IBM Installation Manager

---

El Centro de operaciones utiliza el IBM® Installation Manager, que es un programa de instalación que puede utilizar repositorios de software remotos o locales para instalar o actualizar muchos productos de IBM.

Si la versión necesaria de IBM Installation Manager todavía no está instalada, se instala de forma automática o se actualiza al instalar Centro de operaciones. Debe permanecer instalada en el sistema para que Centro de operaciones pueda actualizarse o desinstalarse posteriormente según sea necesario.

La siguiente lista contiene explicaciones de algunos de los términos que se utilizan en el gestor de instalación de IBM:

**Oferta**

Una unidad o producto de software instalable.

La oferta de Centro de operaciones contiene todos los medios que IBM Installation Manager requiere para instalar el Centro de operaciones.

**Paquete**

El grupo de componentes de software que se requiere para instalar una oferta.

El paquete de Centro de operaciones contiene los componentes siguientes:

- programa de instalación de IBM Installation Manager
- Oferta de Centro de operaciones

**Grupo de paquetes**

Un conjunto de paquetes que comparten un directorio padre común.

**Repositorio**




Un área de almacenamiento local para los datos y otros recursos de aplicación.

El paquete de Centro de operaciones se guarda en un repositorio de IBM Fix Central.

**Directorio de recursos compartidos**

Un directorio que contiene archivos de software o complementos compartidos por los paquetes.

IBM Installation Manager almacena archivos relacionados con la instalación en el directorio de recursos compartidos, incluyendo archivos que se usan para volver a una versión anterior de Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Lista de comprobación de la instalación

---










Antes de instalar Centro de operaciones, debe verificar cierta información, como las credenciales de instalación y debe determinar la información de entrada que debe proporcionarle a IBM® Installation Manager para la instalación.

La siguiente lista de verificación destaca la información que debe verificar o determinar antes de instalar Centro de operaciones, y Tabla 1 describe los detalles de esta información:




- Verifique el nombre de host del sistema en donde se instalará Centro de operaciones.
- Verifique las credenciales de instalación.
- Determine el directorio de instalación del Centro de operaciones, si no desea aceptar la vía de acceso predeterminada.

- Determine el directorio de instalación de IBM Installation Manager, si no desea aceptar la vía de acceso predeterminada.
- Determine el número de puerto a utilizar por el servidor web Centro de operaciones, si no desea aceptar el número de puerto predeterminado.
- Determine la contraseña para comunicaciones seguras.
- Determinar si las comunicaciones seguras deben cumplir con la recomendación 800-131A para Publicaciones especiales (SP) del Instituto Nacional de Estándares y Tecnología (NIST).

Tabla 1. Información para verificar o determinar antes de instalar Centro de operaciones

Información	Detalles
Nombre de host del sistema en el que se instalará Centro de operaciones.	<p>El nombre de host debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> <li>• No debe contener juegos de caracteres de doble bytes (DBCS) o guiones bajos (_).</li> <li>• A pesar de que el nombre de host puede contener el carácter de guión (-), no puede tener un guión como el último carácter del nombre.</li> </ul>
Credenciales de instalación	<p>Para instalar Centro de operaciones, debe usar la siguiente cuenta de usuario:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux El usuario root</li> <li>•  Sistemas operativos Windows Administrador</li> </ul>
Directorio de instalación de Centro de operaciones	<p>El Centro de operaciones está instalado en el subdirectorio de instalación de ui.</p> <p>La siguiente vía de acceso es la vía de acceso predeterminada para el directorio de instalación de Centro de operaciones:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux/opt/tivoli/tsm Por ejemplo, si usa esta vía de acceso predeterminada, Centro de operaciones se instala en el siguiente directorio:  <code>/opt/tivoli/tsm/ui</code></li> <li>•  Sistemas operativos Windows c:\Program Files\Tivoli\TSM Por ejemplo, si usa esta vía de acceso predeterminada, Centro de operaciones se instala en el siguiente directorio:  <code>c:\Program Files\Tivoli\TSM\ui</code></li> </ul> <p>La vía de acceso del directorio de instalación debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> <li>• La vía de acceso no debe contener más de 128 caracteres.</li> <li>• La vía de acceso debe incluir solo caracteres ASCII.</li> <li>• La vía de acceso no debe incluir caracteres de control que no se puedan mostrar.</li> <li>• La vía de acceso no debe ninguno de los siguientes caracteres:  <code>%   &lt; &gt; ' " \$ &amp; ; *</code></li> </ul>
Directorio de instalación de IBM Installation Manager	<p>La siguiente vía de acceso es la vía de acceso predeterminada del directorio de instalación de IBM Installation Manager:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/InstallationManager</li> <li>•  Sistemas operativos Windows C:\Program Files\IBM\Installation Manager</li> </ul>






Información	Detalles
<p>Número de puerto que utiliza el servidor web Centro de operaciones</p>	<p>El valor para el número de puerto seguro (https) debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> <li>• El número debe ser un valor entero entre el rango de 1024 - 65535.</li> <li>• El número no puede estar en uso ni estar asignado a otros programas.</li> </ul> <p>Si no especifica un número de puerto, el valor predeterminado es 11090.</p> <p>Consejo: Si posteriormente no recuerda el número de puerto que especificó, consulte el siguiente archivo, donde <i>dir_instalación</i> representa el directorio en donde está instalado Centro de operaciones:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux <i>dir_instalación/ui/Liberty/usr/servers/guiServer/bootstrap.properties</i></li> <li>•  Sistemas operativos Windows <i>dir_instalación\ui\Liberty\usr\servers\guiServer\bootstrap.properties</i></li> </ul> <p>El archivo bootstrap.properties contiene información de conexión del servidor IBM Spectrum Protect.</p>
<p>Contraseña para comunicaciones seguras</p>	<p>Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web.</p> <p>El Centro de operaciones requiere una comunicación segura entre el servidor y el Centro de operaciones. Para proteger la comunicación, tiene que añadir el certificado de TLS (seguridad de la capa de transporte) del servidor concentrador al archivo de almacén de confianza del Centro de operaciones.</p> <p>El archivo del almacén de confianza del Centro de operaciones contiene el certificado que el Centro de operaciones utiliza para la comunicación HTTPS con los navegadores web. Durante la instalación de Centro de operaciones, usted crea una contraseña para el archivo del almacén de confianza. Al configurar la comunicación segura entre el Centro de operaciones y el servidor concentrador, debe usar la misma contraseña para agregar el certificado SSL del servidor central al archivo del almacén de confianza.</p> <p>La contraseña del archivo del almacén de confianza debe cumplir con los siguientes criterios:</p> <ul style="list-style-type: none"> <li>• La contraseña debe incluir un mínimo de 6 caracteres y un máximo de 64 caracteres.</li> <li>• La contraseña debe contener como mínimo los siguientes caracteres: <ul style="list-style-type: none"> <li>◦ Una letra mayúscula (A - Z)</li> <li>◦ Una letra minúscula (a - z)</li> <li>◦ Un dígito (de 0 a 9).</li> <li>◦ Dos de los caracteres no alfanuméricos que se listan en las siguientes series:</li> </ul> </li> </ul> <pre> ~ ! @ # \$ % ^ &amp; * _ - + = `   ( ) { } [ ] : ; &lt; &gt; , . ? / </pre>

**Tareas relacionadas:**

Configuración para la comunicación segura

Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalar el Centro de operaciones



Puede instalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

### Antes de empezar

No puede configurar el Centro de operaciones hasta que instale, configure e inicie el servidor de IBM Spectrum Protect. Por lo tanto, antes de instalar Centro de operaciones, instale el paquete de servidor adecuado, de acuerdo con los requisitos de versión del servidor en Requisitos del servidor concentrador y spoke.

Puede instalar el Centro de operaciones en un equipo con el servidor IBM Spectrum Protect o en un sistema independiente.

- Obtención del paquete de instalación de Centro de operaciones  
Puede obtener el paquete de instalación de un sitio de descarga de IBM®, como IBM Passport Advantage o IBM Fix Central.
- Instalación de Centro de operaciones utilizando el asistente gráfico  
Puede instalar o actualizar Centro de operaciones mediante el asistente gráfico de IBM Installation Manager.
- Instalar el Centro de operaciones en modalidad de consola  
Puede instalar o actualizar el Centro de operaciones utilizando la línea de mandatos en la modalidad de consola.
- Instalación de Centro de operaciones en el modo silencioso  
Puede instalar o actualizar Centro de operaciones en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Obtención del paquete de instalación de Centro de operaciones

---

Puede obtener el paquete de instalación de un sitio de descarga de IBM®, como IBM Passport Advantage o IBM Fix Central.

### Acerca de esta tarea

---

Tras obtener el paquete de un sitio de descarga de IBM, debe extraer los archivos de instalación.

### Procedimiento

---

Complete los pasos siguientes para extraer los archivos de instalación de Centro de operaciones. En los pasos siguientes, sustituya *número\_versión* con la versión de Centro de operaciones que está instalando.

 Sistemas operativos AIX En los sistemas AIX:

- Descargue el siguiente archivo del paquete al directorio de su elección:

```
número_versión.000
-IBM-SPOC-AIX.bin
```

- Asegúrese de que tiene permisos ejecutables para el archivo del paquete.  
Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x número_versión.000-IBM-SPOC-AIX.bin
```

- Emita el siguiente mandato para extraer los archivos de instalación:

```
./número_versión.000-IBM-SPOC-AIX.bin
```

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos Linux En los sistemas Linux:

- Descargue uno de los siguientes archivos del paquete al directorio de su elección:
  - *número\_versión.000-IBM-SPOC-LinuxS390.bin*
  - *número\_versión.000-IBM-SPOC-Linuxx86\_64.bin*
- Asegúrese de que tiene permisos ejecutables para el archivo del paquete.  
Si es necesario, cambie las autorizaciones del archivo al emitir el mandato siguiente:

```
chmod a+x package_name.bin
```

- Emita el siguiente mandato para extraer los archivos de instalación:




```
./package_name.bin
```

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos Windows En sistemas Windows:


- Descargue el siguiente archivo del paquete al directorio de su elección:  
*número\_versión.000-IBM-SPOC-WindowsX64.exe*
- En Windows Explorer, pulse dos veces sobre el nombre del archivo para extraer los archivos de instalación.

El archivo del paquete de extracción automática se extrae al directorio.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

# Instalación de Centro de operaciones utilizando el asistente gráfico

Puede instalar o actualizar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.





 Sistemas operativos AIX

## Antes de empezar

Si los siguientes archivos RPM no están instalados en el sistema, instálelos. Para obtener instrucciones, consulte Instalación de archivos RPM para el asistente gráfico.

- atk-1.12.3-2.aix5.2.ppc.rpm
- cairo-1.8.8-1.aix5.2.ppc.rpm
- expat-2.0.1-1.aix5.2.ppc.rpm
- fontconfig-2.4.2-1.aix5.2.ppc.rpm
- freetype2-2.3.9-1.aix5.2.ppc.rpm
- gettext-0.10.40-6.aix5.1.ppc.rpm
- glib2-2.12.4-2.aix5.2.ppc.rpm
- gtk2-2.10.6-4.aix5.2.ppc.rpm
- libjpeg-6b-6.aix5.1.ppc.rpm
- libpng-1.2.32-2.aix5.2.ppc.rpm
- libtiff-3.8.2-1.aix5.2.ppc.rpm
- pango-1.14.5-4.aix5.2.ppc.rpm
- pixman-0.12.0-3.aix5.2.ppc.rpm
- xcursor-1.1.7-3.aix5.2.ppc.rpm
- xft-2.1.6-5.aix5.1.ppc.rpm
- xrender-0.9.1-3.aix5.2.ppc.rpm
- zlib-1.2.3-3.aix5.1.ppc.rpm

## Procedimiento

1. Desde el directorio en el que se extrae el paquete de instalación de Centro de operaciones, emita el siguiente mandato:
  -  Sistemas operativos AIX  Sistemas operativos Linux `./install.sh`
  -  Sistemas operativos Windows `install.bat`
2. Siga las instrucciones del asistente para instalar el IBM Installation Manager y los paquetes de Centro de operaciones.  
 Sistemas operativos AIX Es posible que se muestre el siguiente mensaje, y que el asistente de instalación funcione de forma lenta si el entorno local utiliza codificación UTF-8:


```
No se puede crear el conjunto de la fuente
```

Si se muestra el mensaje, lleve a cabo una de las siguientes acciones:

- Cambie a un entorno local que no utilice codificación UTF 8. Para los valores de la opción de idiomas que no utilizan codificación UTF 8, consulte Requisitos de idioma.
- Instale el Centro de operaciones mediante la línea de mandatos en la modalidad de consola.
- Instale el Centro de operaciones en modalidad silenciosa.

## Qué hacer a continuación

Consulte el apartado Configurar el Centro de Operaciones.



-  Sistemas operativos AIX Instalación de archivos RPM para el asistente gráfico  
Antes de poder utilizar el asistente gráfico de IBM Installation Manager para instalar Centro de operaciones, se deben instalar ciertos archivos RPM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalar el Centro de operaciones en modalidad de consola

Puede instalar o actualizar el Centro de operaciones utilizando la línea de mandatos en la modalidad de consola.

## Procedimiento

1. En el directorio en el que se extrae el archivo del paquete de instalación, ejecute el siguiente mandato:  
 Sistemas operativos AIX  Sistemas operativos Linux

```
./install.sh -c
```

 Sistemas operativos Windows




```
install.bat -c
```

2. Siga las instrucciones de la consola para instalar Installation Manager y los paquetes de Centro de operaciones.

## Qué hacer a continuación

---

Consulte el apartado Configurar el Centro de Operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalación de Centro de operaciones en el modo silencioso

---

Puede instalar o actualizar Centro de operaciones en la modalidad silenciosa. En el modo silencioso, la instalación no envía mensajes a una consola sino en cambio almacena mensajes y errores en archivos de registro.

## Antes de empezar

---

Para proporcionar entrada de datos cuando utilice el método de instalación silenciosa, puede utilizar un archivo de respuestas. Los archivos de respuestas de ejemplo siguientes se proporcionan en el directorio input, donde se ha extraído el paquete de instalación:

```
install_response_sample.xml
```

Utilice este archivo para instalar Centro de operaciones.

```
update_response_sample.xml
```

Utilice este archivo para actualizar Centro de operaciones.

Estos archivos contienen valores predeterminados que pueden ayudarle a evitar cualquier aviso innecesario. Para utilizar estos archivos, siga las instrucciones que se proporcionan en los archivos.

Si desea personalizar un archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento



---


1. Cree un archivo de respuestas. Puede modificar el archivo de respuestas de ejemplo o crear el suyo propio.  
Consejo: Para generar un archivo de respuesta como parte de la instalación, efectúe la selección de las opciones de instalación de la modalidad de consola. A continuación en el panel Resumen, escriba G para generar el archivo de respuesta según las opciones seleccionadas anteriormente.
2. Cree una contraseña para el almacén de confianza de Centro de operaciones en el archivo de respuestas.  
Si está utilizando el archivo `install_response_sample.xml`, añada la contraseña en la línea siguiente del archivo, donde `mypassword` representa la contraseña:

```
<variable name='ssl.password' value='micontraseña' />
```

Si desea más información sobre esta contraseña, consulte Lista de comprobación de la instalación.

Consejo: Para actualizar Centro de operaciones, no es necesaria la contraseña del almacén de confianza si está utilizando el archivo `update_response_sample.xml`.

3. Inicie la instalación silenciosa emitiendo el mandato siguiente desde el directorio donde se ha extraído el paquete de instalación. El valor `archivo_respuestas` representa la vía de acceso del archivo de respuestas y el nombre del archivo:
  - o  Sistemas operativos AIX  Sistemas operativos Linux



```
./install.sh -s -input archivo_respuestas -acceptLicense
```
  - o  Sistemas operativos Windows

```
install.bat -s -input archivo_respuestas -acceptLicense
```

## Qué hacer a continuación

---

Consulte el apartado Configurar el Centro de Operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Actualización del Centro de operaciones

---

Puede actualizar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en el modo de consola o el modo silencioso.

## Antes de empezar

---




Antes de actualizar el Centro de operaciones, revise los requisitos de sistema y la lista de comprobación de instalación. La nueva versión del Centro de operaciones puede tener requisitos y consideraciones adicionales o diferentes de los de la versión que se está utilizando actualmente.

## Acerca de esta tarea

---

Las instrucciones para actualizar Centro de operaciones son las mismas que las instrucciones para instalar Centro de operaciones, con las siguientes excepciones:

- Puede usar la función Actualizar de IBM® Installation Manager en vez de la función Instalar.  
Consejo: En IBM Installation Manager, el término *actualizar* significa descubrir e instalar actualizaciones y arreglos en paquetes de software instalados. En este contexto, *actualizar* y *actualización* son sinónimos.
- Si está actualizando Centro de operaciones en el modo silencioso, puede omitir el paso de crear una contraseña para el archivo del almacén de confianza.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Guía de inicio de la Centro de operaciones

---

Antes de poder utilizar Centro de operaciones para gestionar el entorno de almacenamiento, debe configurarlo.

## Acerca de esta tarea

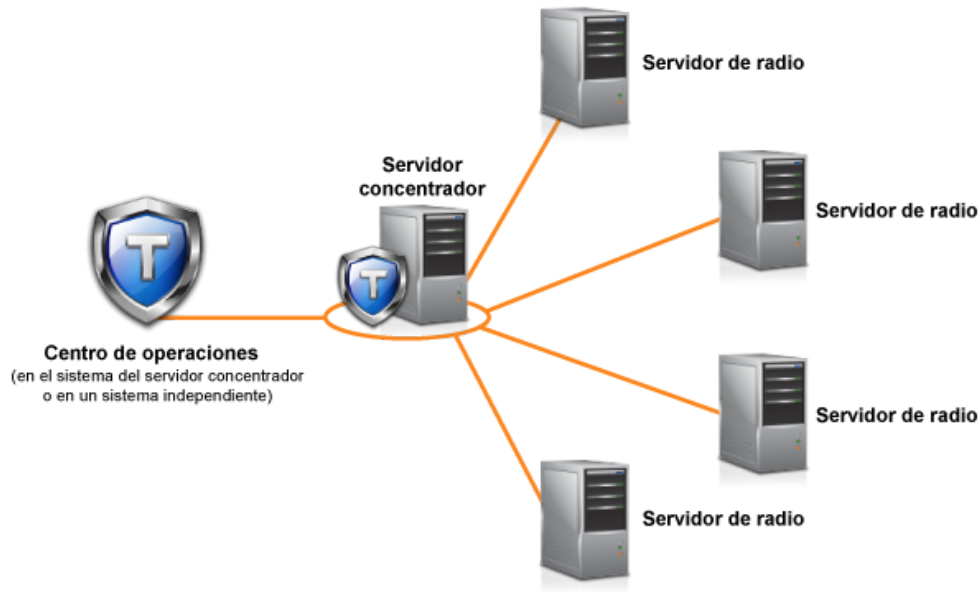
---

Después de instalar el Centro de operaciones, realice los pasos de configuración básicos siguientes:

1. Designe el servidor concentrador.
2. Añada los servidores de radio.
3. Si lo desea, configure alertas de correo electrónico en los servidores concentrador y de radio.

Figura 1 ilustra una configuración del Centro de operaciones.

Figura 1. Ejemplo de una configuración de Centro de operaciones con los servidores concentrador y de radio



- **Configurar el Centro de Operaciones**  
Al abrir Centro de operaciones por primera vez, debe configurarlo para gestionar el entorno de almacenamiento. Debe asociar Centro de operaciones con el servidor IBM Spectrum Protect que se ha designado como el servidor concentrador. A continuación puede conectar servidores IBM Spectrum Protect adicionales como servidores de radio.
- **Configuración para la comunicación segura**  
Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web. El protocolo TLS (seguridad de la capa de transporte) protege las comunicaciones entre el centro de operaciones y el servidor concentrador, y entre el servidor concentrador y los servidores spoke asociados.
- **Iniciar y detener el servidor web**  
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- **Apertura del Centro de operaciones**  
La página Visión general es la vista inicial predeterminada del Centro de operaciones. Sin embargo, en el navegador web, puede marcar la página que desea que se abra cuando inicie la sesión en el Centro de operaciones.
- **Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect**  
El servicio de gestión de clientes recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y hace que la información esté disponible para el Centro de operaciones para la prestación de supervisión básica.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows

## Configurar el Centro de Operaciones

---

Al abrir Centro de operaciones por primera vez, debe configurarlo para gestionar el entorno de almacenamiento. Debe asociar Centro de operaciones con el servidor IBM Spectrum Protect que se ha designado como el servidor concentrador. A continuación puede conectar servidores IBM Spectrum Protect adicionales como servidores de radio.

- Designar el servidor central  
Cuando se conecta a Centro de operaciones por primera vez, debe designar qué servidor IBM Spectrum Protect es el servidor central.
- Adición de un servidor de radio  
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Envío de alertas por correo electrónico a los administradores  
Una alerta es una notificación de un problema importante en el servidor IBM Spectrum Protect y se desencadena mediante un mensaje de servidor. Las alertas se muestran en Centro de operaciones y se pueden enviar desde el servidor a los administradores por correo electrónico.
- Adición de texto personalizado a la pantalla de inicio de sesión  
Puede añadir texto personalizado, por ejemplo los términos de uso del software de la organización, a la pantalla de inicio de sesión del Centro de operaciones de modo que los usuarios del Centro de operaciones vean el texto antes de que entren el nombre de usuario y la contraseña.
- Habilitación de servicios REST  
Las aplicaciones que utilizan servicios REST (Representational State Transfer) pueden consultar y gestionar el entorno de almacenamiento conectándose al Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Designar el servidor central

---

Quando se conecta a Centro de operaciones por primera vez, debe designar qué servidor IBM Spectrum Protect es el servidor central.

### Antes de empezar

---

El Centro de operaciones requiere la comunicación segura entre el servidor concentrador y el Centro de operaciones. Para proteger la comunicación, tiene que añadir el certificado de TLS (seguridad de la capa de transporte) del servidor concentrador al archivo de almacén de confianza del Centro de operaciones. Para obtener más información, consulte el apartado Protección de la comunicación entre el centro de operaciones y el servidor concentrador.

### Procedimiento

---

En un navegador web, escriba la siguiente dirección, en donde *hostname* representa el nombre del sistema en donde está instalado Centro de operaciones *secure\_port*, y representa el número de puerto que utiliza Centro de operaciones para la comunicación HTTPS en ese sistema:

```
https://nombrehost:puerto_seguro/oc
```

Consejos:

- El URL es sensible a las mayúsculas y minúsculas. Por ejemplo, asegúrese de que escribe "oc" en minúsculas como se indica.
- Para obtener más información sobre el número de puerto, consulte la Lista de comprobación de instalación.
- Si se está conectando al Centro de operaciones por primera vez, debe proporcionar la siguiente información:
  - La información de conexión para el servidor que desea designar como servidor concentrador.
  - Credenciales de inicio de sesión para un ID de administrador que está definido para dicho servidor
- Si el periodo de retención del registro de sucesos es inferior al de 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor concentrador.

### Qué hacer a continuación

---

Si tiene varios servidores IBM Spectrum Protect en el entorno, añada los otros servidores como servidores de radio al servidor concentrador.

Atención: No cambie el nombre de un servidor, después de que se haya configurado como servidor de radio o servidor concentrador.

#### Conceptos relacionados:

Requisitos del servidor concentrador y spoke

Los ID de administrador que requiere el centro de operaciones

## Adición de un servidor de radio

---

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

### Antes de empezar

---

La comunicación entre el servidor spoke y el servidor concentrador debe protegerse utilizando el protocolo TLS (Seguridad de la capa de transporte). Para proteger la comunicación, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

### Procedimiento

---




1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
  - o Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
  - o Si el servidor que quiere añadir no aparece en la tabla y no es necesaria la comunicación SSL/TLS segura, pulse + Spoke en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.  
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor de radio.

#### Referencia relacionada:

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Envío de alertas por correo electrónico a los administradores

---

Una alerta es una notificación de un problema importante en el servidor IBM Spectrum Protect y se desencadena mediante un mensaje de servidor. Las alertas se muestran en Centro de operaciones y se pueden enviar desde el servidor a los administradores por correo electrónico.

### Antes de empezar

---

Para poder configurar la notificación por correo electrónico para los administradores sobre las alertas, asegúrese de que se cumplan los requisitos siguientes:

- Es necesario un servidor SMTP para enviar y recibir alertas por correo electrónico, y el servidor que envía las alertas por correo electrónico debe tener acceso al servidor SMTP.  
Consejo: Si Centro de operaciones está instalado en un sistema independiente, dicho sistema no necesita acceder al servidor SMTP.
- Un administrador debe tener privilegio de sistema para poder configurar la notificación por correo electrónico.

### Acerca de esta tarea

---

Solo se envía una notificación de correo electrónico para la primera aparición de una alerta. Además, si se genera una alerta antes de configurar la notificación de correo electrónico, no se enviará ninguna notificación de correo electrónico para dicha alerta.

Puede configurar la notificación por correo electrónico de las maneras siguientes:

- Enviar notificación para alertas individuales
- Enviar resúmenes de alertas

Un resumen de alerta contiene información sobre las alertas actuales. El resumen incluye el número total de alertas, el número total de alertas activas e inactivas, la alerta más antigua, la alerta más reciente y la alerta que se produce con más frecuencia.



Puede especificar hasta tres administradores para recibir resúmenes de alertas por correo electrónico. Los resúmenes de alertas se envían, aproximadamente, cada hora.

## Procedimiento

---

Para configurar las notificaciones de correo electrónico para los administradores sobre las alertas, realice los pasos siguientes en cada servidor rápido y concentrador del que desee recibir alertas de correo electrónico:

1. Para verificar que la supervisión de alertas está activada, emita el mandato siguiente:

```
QUERY MONITORSETTINGS
```

2. Si la salida del mandato indica que la supervisión de alertas está desactivada, emita el mandato siguiente. De lo contrario, continúe con el paso siguiente.

```
SET ALERTMONITOR ON
```

3. Para habilitar el envío de notificaciones por correo electrónico, emita el mandato siguiente:

```
SET ALERTEMAIL ON
```

4. Para definir el servidor SMTP que se utilizará para enviar las notificaciones por correo electrónico, emita el mandato siguiente:

```
SET ALERTEMAILSMTPHOST nombre_host
```

5. Para especificar el número de puerto para el servidor SMTP, emita el mandato siguiente:

```
SET ALERTEMAILSMTPPORT número_puerto
```

El número de puerto predeterminado es 25.

6. Para especificar la dirección de correo electrónico del remitente de las alertas, emita el mandato siguiente:

```
SET ALERTEMAILFROMADDR dirección_correo_electrónico
```

7. Para cada ID de administrador que debe recibir una notificación por correo electrónico, emita uno de los mandatos siguientes para activar la notificación de correo electrónico y especificar la dirección de correo electrónico:

```
REGISTER ADMIN nombre_admin ALERT=YES EMAILADDRESS=dirección_correo_electrónico
```

```
UPDATE ADMIN nombre_admin ALERT=YES EMAILADDRESS=dirección_correo_electrónico
```

8. Elija una de las dos opciones siguientes, o ambas, y especifique el ID de administrador para recibir una notificación por correo electrónico:

- o Enviar notificación para alertas individuales

Para especificar o actualizar los ID de administrador para recibir una notificación por correo electrónico para una alerta individual, emita uno de los mandatos siguientes:

```
DEFINE ALERTTRIGGER número_mensaje Admin=nombre_admin1,nombre_admin2
```

```
UPDATE ALERTTRIGGER número_mensaje ADDadmin=nombre_admin3 DELadmin=nombre_admin1
```

Consejo: En la página Configurar alertas del Centro de operaciones, puede seleccionar los administradores que recibirán la notificación de correo electrónico.

- o Enviar resúmenes de alertas

Para especificar o actualizar los ID de administrador para recibir resúmenes de alertas por correo electrónico, emita el mandato siguiente:

```
SET ALERTSUMMARYTOADMINS nombre_admin1,nombre_admin2,nombre_admin3
```

Si desea recibir resúmenes de alertas, pero no desea recibir notificaciones sobre alertas individuales, realice los pasos siguientes:

- a. Suspenda la notificación sobre alertas individuales, tal como se describe en Suspensión temporal de alertas por correo electrónico.
- b. Asegúrese de que el ID de administrador correspondiente figure en el mandato siguiente:

```
SET ALERTSUMMARYTOADMINS nombre_admin1,nombre_admin2,nombre_admin3
```

## Envío de alertas por correo electrónico a varios administradores

---

El ejemplo siguiente muestra los mandatos que hacen que las alertas para el mensaje ANR1075E se envíen en un correo electrónico a los administradores `myadmin`, `djadmin` y `csadmin`:

```

SET ALERTMONITOR ON
SET ALERTEMAIL ON
SET ALERTEMAILSMTPHOST mymailserver.domain.com
SET ALERTEMAILSMTPPORT 450
SET ALERTEMAILFROMADDR srvadmin@mydomain.com
UPDATE ADMIN myadmin ALERT=YES EMAILADDRESS=myaddr@anycompany.com
UPDATE ADMIN djadmin ALERT=YES EMAILADDRESS=djaddr@anycompany.com
UPDATE ADMIN csadmin ALERT=YES EMAILADDRESS=csaddr@anycompany.com
DEFINE ALERTTRIGGER anr0175e ADMIN=myadmin,djadmin,csadmin

```

- Suspensión temporal de alertas por correo electrónico  
En determinadas situaciones, es posible que desee suspender las alertas de correo electrónico de forma temporal. Por ejemplo, es posible que desee recibir resúmenes de alertas pero no suspender las notificaciones sobre alertas individuales, o es posible que desee suspender las alertas por correo electrónico cuando un administrador esté de vacaciones.

#### Referencia relacionada:

DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)  
 QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)  
 REGISTER ADMIN (Registrar un ID de administrador)  
 SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)  
 SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)  
 SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)  
 SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)  
 SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)  
 SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)  
 UPDATE ADMIN (Actualizar un administrador)  
 UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Windows


## Adición de texto personalizado a la pantalla de inicio de sesión

Puede añadir texto personalizado, por ejemplo los términos de uso del software de la organización, a la pantalla de inicio de sesión del Centro de operaciones de modo que los usuarios del Centro de operaciones vean el texto antes de que entren el nombre de usuario y la contraseña.

### Procedimiento

Para añadir texto personalizado a la pantalla de inicio de sesión, realice los pasos siguientes:

1. En el sistema donde está instalado Centro de operaciones, vaya al directorio siguiente, donde *dir\_instalación* representa el directorio en el cual está instalado Centro de operaciones.

 Sistemas operativos AIX
  Sistemas operativos Linux
 *dir\_instalación/ui/Liberty/usr/servers/guiServer*

 Sistemas operativos Windows
 *dir\_instalación\ui\Liberty\usr\servers\guiServer*

2. En el directorio, cree un archivo denominado loginText.html que contiene el texto que desea añadir a la pantalla de inicio de sesión. Cualquier texto especial que no sea ASCII debe estar codificado en UTF-8.  
Consejo: Puede formatear el texto añadiendo las etiquetas HTML.
3. Revise el texto añadido en la pantalla de inicio de sesión del Centro de operaciones.  
Para abrir el Centro de operaciones, entre la siguiente dirección en un navegador web, donde *nombrehost* representa el nombre del sistema donde está instalado el Centro de operaciones y *puerto\_seguro* representa el número de puerto que el Centro de operaciones utiliza para la comunicación HTTPS en ese sistema:

*https://nombrehost:puerto\_seguro/oc*

## Habilitación de servicios REST

Las aplicaciones que utilizan servicios REST (Representational State Transfer) pueden consultar y gestionar el entorno de almacenamiento conectándose al Centro de operaciones.

### Acerca de esta tarea

Habilite esta característica para permitir que los servicios REST interactúen con los servidores concentrador y de radio enviando llamadas a la siguiente dirección:

*https://nombre\_host\_co:puerto/oc/api*


donde *nombre\_host\_co* es el nombre de red o la dirección IP del sistema host del Centro de operaciones y *puerto* es el número de puerto del Centro de operaciones. El número de puerto predeterminado es 11090.




Para obtener información sobre los servicios REST que están disponibles para el Centro de operaciones, consulte la nota técnica <http://www.ibm.com/support/docview.wss?uid=swg21973011> o emita la siguiente llamada REST:

`https://nombre_host_co:puerto/oc/api/help`

## Procedimiento

---

1. En la barra de menús del Centro de operaciones, pase el cursor por encima del icono de configuración  y pulse Configuración.
2. En la página General, marque el recuadro de selección Habilitar API de REST administrativa.
3. Pulse Guardar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Configuración para la comunicación segura

---

Centro de operaciones utiliza Hypertext Transfer Protocol Secure (HTTPS) para comunicarse con los navegadores web. El protocolo TLS (seguridad de la capa de transporte) protege las comunicaciones entre el centro de operaciones y el servidor concentrador, y entre el servidor concentrador y los servidores spoke asociados.

### Acerca de esta tarea

---

Se requiere TLS 1.2 para la comunicación segura entre el servidor IBM Spectrum Protect y el Centro de operaciones, y entre el servidor concentrador y los servidores spoke.

- Protección de la comunicación entre el centro de operaciones y el servidor concentrador  
Para proteger las comunicaciones entre el Centro de operaciones y el servidor concentrador, debe añadir el certificado TLS (seguridad de la capa de transporte) a un archivo de almacén de confianza del Centro de operaciones.
- Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke  
Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke mediante el protocolo de capa de sockets seguros (TLS), es necesario definir el certificado del servidor spoke en el servidor concentrador. También debe configurar Centro de operaciones para supervisar el servidor de radio.
- Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones  
Para configurar la comunicación segura entre Centro de operaciones y el servidor central, debe conocer la contraseña del archivo del almacén de confianza de Centro de operaciones. Se crea esta contraseña durante la instalación de Centro de operaciones. Si no conoce la contraseña, puede restaurarla.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Protección de la comunicación entre el centro de operaciones y el servidor concentrador

---

Para proteger las comunicaciones entre el Centro de operaciones y el servidor concentrador, debe añadir el certificado TLS (seguridad de la capa de transporte) a un archivo de almacén de confianza del Centro de operaciones.

### Antes de empezar

---

El archivo de almacén de confianza del Centro de operaciones es un contenedor para certificados al que puede acceder Centro de operaciones. El archivo del almacén de confianza contiene el certificado que Centro de operaciones usa para la comunicación HTTPS con los navegadores web.

Durante la instalación de Centro de operaciones, cree una contraseña para el archivo del almacén de confianza. Para proteger la comunicación entre el Centro de operaciones y el servidor concentrador, debe usar la misma contraseña para agregar el certificado SSL del servidor central al archivo del almacén de confianza. Si no recuerda la contraseña, puede restaurarla. Consulte el apartado Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones.

## Procedimiento

---

1. Especifique el certificado cert256.arm como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador.

Para especificar cert256.arm como el certificado predeterminado, siga los pasos a continuación:

a. Emita el siguiente mandato desde el directorio de la instancia del servidor central:

```
gsk8capicmd_64 -cert -setdefault -db cert.kdb -stashed  
-label "TSM Server SelfSigned SHA Key"
```

b. Reinicie el servidor central de manera que pueda recibir los cambios en el archivo de la base de datos clave.

2. Para verificar que el certificado cert256.arm está establecido como el certificado predeterminado en el archivo de base de datos de claves del servidor concentrador, emita el siguiente mandato:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

3. Detenga el servidor web de Centro de operaciones.

4. Vaya a la línea de mandatos del sistema operativo en el cual está instalado Centro de operaciones.

5. Añada el certificado al archivo de almacén de confianza de Centro de operaciones utilizando el mandato iKeycmd o el mandato iKeyman. El mandato iKeyman abre la interfaz gráfica de usuario de IBM® Key Management, mientras que iKeycmd es una interfaz de línea de mandatos.

Para añadir el certificado SSL utilizando la interfaz de línea de mandatos, emita el mandato iKeycmd para añadir el certificado cert256.arm como certificado predeterminado en el archivo de base de datos de claves del servidor concentrador:

```
ikeycmd -cert -add  
-db /dir_instalación/Liberty/usr/servers/guiServer/gui-truststore.jks  
-file /fvt/comfrey/srv/cert256.arm  
-label 'descripción etiqueta'  
-pw 'contraseña' -type jks -format ascii -trust enable
```

donde:

**dir\_instalación**

El directorio en el cual está instalado Centro de operaciones.

**descripción etiqueta**




Descripción que asigna a la etiqueta.

**contraseña**

La contraseña que ha creado al instalar Centro de operaciones. Para restablecer la contraseña, desinstale Centro de operaciones, suprima el archivo .jks y vuelva a instalar Centro de operaciones.

Para añadir el certificado utilizando la ventana IBM Key Management, realice los pasos siguientes:

a. Vaya al directorio siguiente, donde *dir\_instalación* representa el directorio en el cual está instalado Centro de operaciones:




-  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/jre/bin*
-  Sistemas operativos Windows *dir\_instalación/ui/jre/bin*

b. Abra la ventana IBM Key Management emitiendo el siguiente mandato:

```
ikeyman
```

c. Pulse Archivo de base de datos de claves > Abrir.

d. En la ventana Open, pulse Browse, y vaya al siguiente directorio, en donde *dir\_instalación* representa el directorio en el cual está instalado el Centro de operaciones:

-  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/Liberty/usr/servers/guiServer*
-  Sistemas operativos Windows *dir\_instalación/ui/Liberty/usr/servers/guiServer*

e. En el directorio guiServer, seleccione el archivo gui-truststore.jks.




f. Pulse Abrir, y pulse Aceptar.

g. Especifique la contraseña del archivo de almacén de confianza y pulse Aceptar.

h. En el área Contenido de la base de datos clave de la ventana Gestión de claves de IBM, pulse la flecha y seleccione Certificados del signatario de la lista.

i. Pulse Añadir.




j. En la ventana Abrir, pulse Examinar, y vaya al directorio de la instancia del servidor central que se muestra en el siguiente ejemplo:

-  Sistemas operativos AIX  Sistemas operativos Linux *opt/tivoli/tsm/server/bin*
-  Sistemas operativos Windows *c:\Program Files\Tivoli\TSM\server1*




El directorio contiene el certificado cert256.arm.

Si no puede acceder al directorio de la instancia del servidor central desde la ventana Open, complete los siguientes pasos:

i. Utilice FTP u otro método de transferencia de archivos para copiar los archivos de cert256.arm en el servidor concentrador en el siguiente directorio del sistema donde se ha instalado el Centro de operaciones:

-  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/Liberty/usr/servers/guiServer*
-  Sistemas operativos Windows *dir\_instalación/ui/Liberty/usr/servers/guiServer*

ii. En la ventana Open, vaya al directorio guiServer.




- k. Seleccione el certificado cert256.arm como certificado.  
Consejo: El certificado que elija debe establecerse como certificado predeterminado en el archivo de base de datos de claves del servidor concentrador. Para obtener más información, consulte el paso 1 y 2.
  - l. Pulse Abrir, y pulse Aceptar.
  - m. Escriba una etiqueta para el certificado. Por ejemplo, escriba el nombre del servidor central.
  - n. Pulse Aceptar. El certificado SSL del servidor central se añade al archivo del almacén de confianza, y se muestra la etiqueta en el área Contenido de la base de datos clave de la ventana Gestión de claves de IBM.
  - o. Cierre la ventana IBM Key Management.
6. Inicie el servidor web del Centro de operaciones.
7. Al conectarse al Centro de operaciones por primera vez, se le solicita que identifique la dirección IP o el nombre de red del servidor concentrador, y el número de puerto para comunicarse con el servidor concentrador. Si la opción de servidor ADMINONCLIENTPORT está habilitada para el servidor IBM Spectrum Protect, especifique el número de puerto especificado por la opción de servidor TCPADMINPORT. Si la opción de servidor ADMINONCLIENTPORT no está habilitada, especifique el número de puerto especificado por la opción de servidor TCPPORT.
- Si Centro de operaciones se ha configurado previamente, puede revisar el contenido del archivo serverConnection.properties para verificar la información de conexión. El archivo serverConnection.properties se encuentra en el directorio siguiente en el sistema donde está instalado Centro de operaciones:
- o  Sistemas operativos AIX  Sistemas operativos Linux `dir_instalación/ui/Liberty/usr/servers/guiServer`
  - o  Sistemas operativos Windows `dir_instalación\ui\Liberty\usr\servers\guiServer`

## Qué hacer a continuación

Para establecer la comunicación SSL entre el servidor central y un servidor de radio, consulte Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke.

### Referencia relacionada:

QUERY OPTION (Consultar opciones del servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Protección de la comunicación SSL entre el servidor concentrador y un servidor spoke

Para asegurar las comunicaciones entre el servidor concentrador y un servidor spoke mediante el protocolo de capa de sockets seguros (TLS), es necesario definir el certificado del servidor spoke en el servidor concentrador. También debe configurar Centro de operaciones para supervisar el servidor de radio.

## Procedimiento

1. En el servidor de radio, cambie al directorio de la instancia del servidor de radio.
2. Especifique el certificado cert256.arm necesario como el certificado predeterminado en el archivo de base de datos de claves del servidor spoke. Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -setdefault -db cert.kdb -stashed
-label "TSM Server SelfSigned SHA Key"
```

3. Verifique los certificados que hay en el archivo de base de datos de claves del servidor spoke: Emita el mandato siguiente:

```
gsk8capiCmd_64 -cert -list -db cert.kdb -stashed
```

4. Transfiera de forma el archivo cert256.arm del servidor de radio al servidor central.
5. En el servidor central, cambie el directorio de la instancia del servidor central.
6. Defina el certificado del servidor spoke en el servidor concentrador. Emita el siguiente mandato desde el directorio de la instancia del servidor concentrador, donde `nombre_servidor_spoke` es el nombre del servidor spoke y `spoke_cert256.arm` es el nombre de archivo del certificado del servidor spoke:

```
gsk8capiCmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label spoke_servername -file spoke_cert256.arm
```

El servidor de radio no requiere el certificado del servidor central para la comunicación del servidor central al de radio. Sin embargo, otras configuraciones de servidor que requieren servidores de definición cruzada no requieren que el servidor spoke tenga el certificado del servidor concentrador.

7. Reinicie el servidor central y el servidor de radio.
8. Para el servidor concentrador, emita el mandato DEFINE SERVER, de acuerdo con el ejemplo siguiente:

```
DEFINE SERVER spoke_servername HLA=spoke_address
LLA=spoke_SSLTCPADMINPort SERVERPA=spoke_serverpassword
```

Consejo: De forma predeterminada, la comunicación del servidor está cifrada excepto cuando el servidor envía o recibe datos de objeto. Los datos de objeto se envían y reciben mediante el protocolo TCP/IP. Si elige no cifrar los datos de objeto, el rendimiento del servidor será similar a la comunicación sobre una sesión TCP/IP y la sesión es segura. Para cifrar toda la comunicación con el servidor especificado, incluso cuando el servidor envía y recibe datos de objeto, especifique el parámetro SSL=YES en el mandato DEFINE SERVER.

9. En la barra de menús de Centro de operaciones, pulse Servidores.




En la tabla de la página Servidores, el servidor spoke que ha definido en el paso 8, normalmente, tiene un estado de "No supervisado." En función del valor del intervalo de renovación del estado, es posible que no vea el servidor spoke inmediatamente.

10. Pulse el servidor de radio (spoke) para resaltar el elemento y, en la barra de menús de tabla, pulse Supervisar radio.

#### Referencia relacionada:

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

QUERY OPTION (Consultar opciones del servidor)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




## Reiniciar la contraseña para el archivo del almacén de confianza del Centro de operaciones

Para configurar la comunicación segura entre Centro de operaciones y el servidor central, debe conocer la contraseña del archivo del almacén de confianza de Centro de operaciones. Se crea esta contraseña durante la instalación de Centro de operaciones. Si no conoce la contraseña, puede restaurarla.

### Acerca de esta tarea

Para restablecer la contraseña, debe crear una nueva contraseña, eliminar el archivo del almacén de confianza de Centro de operaciones, y reiniciar el servidor web Centro de operaciones.

### Procedimiento

1. Detenga el servidor web de Centro de operaciones.
2. Vaya al directorio siguiente, donde *dir\_instalación* representa el directorio en el cual está instalado Centro de operaciones:
  - o  Sistemas operativos AIX  Sistemas operativos Linux *dir\_instalación/ui/Liberty/usr/servers/guiServer*
  - o  Sistemas operativos Windows *dir\_instalación\ui\Liberty\usr\servers\guiServer*
3. Abra el archivo *bootstrap.properties*, que contiene la contraseña del archivo del almacén de confianza. Si la contraseña no está cifrada, puede usarla para abrir el archivo del almacén de confianza sin tener que restablecerla. El siguiente ejemplo indica la diferencia entre una contraseña cifrada y una no cifrada:

#### Ejemplo de una contraseña cifrada

Las contraseñas cifradas comienzan con la cadena de texto {xor}.

El siguiente ejemplo muestra la contraseña cifrada como el valor del parámetro *tsm.truststore.pswd*:

```
tsm.truststore.pswd={xor}MiYPPiwsKDAtoW==
```

#### Ejemplo de contraseña no cifrada

El siguiente ejemplo muestra la contraseña no cifrada como el valor del parámetro *tsm.truststore.pswd*:

```
tsm.truststore.pswd=J8b%^B
```








4. Reinicie la contraseña sustituyéndola en el archivo *bootstrap.properties* por la contraseña nueva. Puede sustituir la contraseña con una contraseña cifrada o no cifrada. Recuerde la contraseña no cifrada para uso en el futuro. Para crear una contraseña encriptada, siga estos pasos:
  - a. Cree una contraseña sin cifrar.

La contraseña del archivo del almacén de confianza debe cumplir con los siguientes criterios:

- La contraseña debe incluir un mínimo de 6 caracteres y un máximo de 64 caracteres.
- La contraseña debe contener como mínimo los siguientes caracteres:
  - Una letra mayúscula (A - Z)
  - Una letra minúscula (a - z)
  - Un dígito (de 0 a 9).
  - Dos de los caracteres no alfanuméricos que se listan en las siguientes series:

```
~ ! @ # $ % ^ & * _ - + = ` |
```

```
( ) { } [ ] : ; < > , . ? /
```

- b. Desde la línea de mandatos del sistema operativo, vaya al siguiente directorio:
-  Sistemas operativos AIX  Sistemas operativos Linux `dir_instalación/ui/Liberty/bin`
  -  Sistemas operativos Windows `dir_instalación\ui\Liberty\bin`
- c. Para cifrar la contraseña, emita el siguiente mandato, en donde *myPassword* representa la contraseña cifrada:
-  Sistemas operativos AIX  Sistemas operativos Linux `securityUtility encode myPassword`
  -  Sistemas operativos Windows `securityUtility.bat encode myPassword`
-  Sistemas operativos Windows Podría aparecer el mensaje siguiente:

```
! "java" is not recognized as an internal or external command,
programa operativo o archivo por lotes.
```




Si se muestra este mensaje, siga estos pasos:

- i. Emita el siguiente mandato, en donde *dir\_instalación* representa el directorio en donde está instalado Centro de operaciones:

```
set JAVA_HOME="dir_instalación\ui\jre"
```

- ii. Vuelva a emitir el siguiente mandato para cifrar la contraseña:




```
securityUtility.bat encode myPassword
```

5. Cierre el archivo `bootstrap.properties`.
6. Vaya al directorio siguiente:
  -  Sistemas operativos AIX  Sistemas operativos Linux `dir_instalación/ui/Liberty/usr/servers/guiServer`
  -  Sistemas operativos Windows `dir_instalación\ui\Liberty\usr\servers\guiServer`
7. Elimine el archivo `gui-truststore.jks`, que es el archivo del almacén de confianza de Centro de operaciones.
8. Inicie el servidor web Centro de operaciones.

## Resultados

---

Se crea automáticamente un nuevo archivo del almacén de confianza para Centro de operaciones, y el certificado TLS de Centro de operaciones se incluye de manera automática en el archivo del almacén de confianza.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Iniciar y detener el servidor web


---

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.


## Procedimiento

---

Detenga e inicie el servidor web.

-  Sistemas operativos AIX Desde el directorio `/dir_instalación/ui/utils`, donde *dir\_instalación* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:
  - Para detener el servidor:

```
./stopserver.sh
```
  - Para iniciar el servidor:

```
./startserver.sh
```
-  Sistemas operativos Linux Emita los mandatos siguientes:
  - Para detener el servidor:


```
service opscenter.rc stop
```
  - Para iniciar el servidor:

```
service opscenter.rc start
```
  - Para reiniciar el servidor:

```
service opscenter.rc restart
```

Para determinar si el servidor está ejecutándose, emita el siguiente mandato:

```
service opscenter.rc status
```

-  Sistemas operativos Windows Desde la ventana Servicios, detenga o inicie el servicio Centro de operaciones.

## Apertura del Centro de operaciones

---

La página Visión general es la vista inicial predeterminada del Centro de operaciones. Sin embargo, en el navegador web, puede marcar la página que desea que se abra cuando inicie la sesión en el Centro de operaciones.

### Procedimiento

---

1. En un navegador web, escriba la siguiente dirección, en donde *hostname* representa el nombre del sistema en donde está instalado Centro de operaciones *secure\_port*, y representa el número de puerto que utiliza Centro de operaciones para la comunicación HTTPS en ese sistema:




```
https://nombrehost:puerto_seguro/oc
```

Consejos:

- El URL es sensible a las mayúsculas y minúsculas. Por ejemplo, asegúrese de que escribe "oc" en minúsculas como se indica.
  - El número de puerto predeterminado para la comunicación HTTPS es 11090, pero se puede especificar un número de puerto diferente durante la instalación de Centro de operaciones.
2. Inicie la sesión, utilizando un ID de administrador registrado en el servidor concentrador.

En la página Visión general, puede ver información de resumen para clientes, servicios, servidores, agrupaciones de almacenamiento y dispositivos de almacenamiento. Puede ver más detalles pulsando elementos o utilizando la barra de menú del Centro de operaciones.

Supervisión desde un dispositivo móvil: Para supervisar de forma remota el entorno de almacenamiento, puede ver la página Visión general del Centro de operaciones en el navegador web de un dispositivo móvil. El Centro de operaciones soporta el navegador web Safari de Apple en el iPad. También se pueden utilizar otros dispositivos móviles.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Recopilación de información de diagnóstico con el servicios de gestión de cliente de IBM Spectrum Protect

---

El servicio de gestión de clientes recopila información de diagnóstico sobre clientes de archivado y copia de seguridad y hace que la información esté disponible para el Centro de operaciones para la prestación de supervisión básica.

### Acerca de esta tarea

---

Después de instalar el servicio de gestión de clientes, puede ver la página Diagnóstico en el Centro de operaciones para obtener información de resolución de problemas para los clientes de archivado y copia de seguridad.

La información de diagnóstico se puede recopilar solo desde clientes Linux y Windows. pero los administradores pueden ver la información de diagnóstico en Centro de operaciones en sistemas operativos AIX, Linux o Windows.




También puede instalar el servicio de gestión de clientes en nodos de transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware para recopilar información de diagnóstico sobre los transportadores de datos.

Consejo: En la documentación de servicio de gestión de clientes, *sistema cliente* es el sistema donde está instalado el cliente de archivado y copia de seguridad.

- Instalación de servicio de gestión de clientes utilizando el asistente gráfico  
Para recopilar información de diagnóstico sobre los clientes de archivado y copia de seguridad, por ejemplo archivos de registro de cliente, debe instalar el servicio de gestión de clientes en los sistemas cliente que gestiona.
- Instalación de servicio de gestión de clientes en modalidad silenciosa  
Puede instalar el servicio de gestión de clientes en modalidad silenciosa. Cuando se utiliza la modalidad silenciosa, se proporcionan los valores de instalación en un archivo de respuestas y, a continuación, se ejecuta un mandato de instalación.
- Verificación de que el servicio de gestión de clientes está instalado correctamente  
Antes de utilizar el servicio de gestión de clientes para recopilar información de diagnóstico acerca de un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de clientes esté instalado y configurado correctamente.
- Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes  
Si no ha utilizado la configuración predeterminada para el servicio de gestión de clientes, debe configurar el Centro de operaciones para acceder al servicio de gestión de clientes.



- Inicio y detención del servicio de gestión de clientes  
El servicio de gestión de clientes se inicia automáticamente después de instalarse en el sistema cliente. Es posible que necesite detener e iniciar el servicio en determinadas situaciones.
- Desinstalación de servicio de gestión de clientes  
Si ya no tiene que recopilar información de diagnóstico de cliente, puede desinstalar el servicio de gestión de clientes del sistema cliente.
- Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas  
El servicio de gestión de clientes utiliza información del archivo de configuración de cliente (client-configuration.xml) para descubrir información de diagnóstico. Si el servicio de gestión de clientes no puede descubrir la ubicación de los archivos de registro, debe ejecutar el programa de utilidad CmsConfig para añadir la ubicación de los archivos de registro al archivo client-configuration.xml.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalación de servicio de gestión de clientes utilizando el asistente gráfico

Para recopilar información de diagnóstico sobre los clientes de archivado y copia de seguridad, por ejemplo archivos de registro de cliente, debe instalar el servicio de gestión de clientes en los sistemas cliente que gestiona.

### Antes de empezar

Revise Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect.

### Acerca de esta tarea

Debe instalar el servicio de gestión de clientes en el mismo sistema que el cliente de archivado y copia de seguridad.

### Procedimiento

1. Descargue el paquete de instalación para el servicio de gestión de clientes de un sitio de descarga de IBM®, por ejemplo IBM Passport Advantage o IBM Fix Central. Busque un nombre de archivo que sea similar a `<version>-IBM-SPCMS-<sistema operativo>.bin`.

La tabla siguiente muestra los nombres de los paquetes de instalación.

Sistema operativo del cliente	Nombre de paquete de instalación
Linux x86 de 64 bits	8.1.x.000-IBM-SPCMS-Linuxx64.bin
Windows de 32 bits	8.1.x.000-IBM-SPCMS-Windows32.exe
Windows de 64 bits	8.1.x.000-IBM-SPCMS-Windows64.exe

2. Cree un directorio en el sistema cliente que desea gestionar y copie allí el paquete de instalación.
3. Extraiga el contenido del archivo del paquete de instalación.
  - En sistemas cliente Linux, lleve a cabo los siguientes pasos:
    - a. Ejecute el siguiente mandato para cambiar un archivo en un archivo ejecutable:
 

```
chmod +x 8.1.x.000-IBM-SPCMS-Linuxx64.bin
```
    - b. Emita el mandato siguiente:
 

```
./8.1.x.000-IBM-SPCMS-Linuxx64.bin
```
  - En sistemas cliente de Windows, haga doble clic en el nombre del paquete de instalación en Windows Explorer.  
Consejo: Si anteriormente ha instalado y desinstalado el paquete, seleccione All cuando se le solicite que sustituya los archivos de instalación existentes.
4. Ejecute el archivo de proceso por lotes de instalación desde el directorio donde ha extraído los archivos de instalación y los archivos asociados. Este es el directorio que ha creado en el paso 2.
  - En los sistemas cliente Linux, emita el mandato siguiente:
 

```
./install.sh
```
  - En sistemas cliente Windows, efectúe una doble pulsación en install.bat.
5. Para instalar el servicio de gestión de clientes, siga las instrucciones del asistente de IBM Installation Manager.




Si IBM Installation Manager aún no está instalado en el sistema cliente, tiene que seleccionar IBM Installation Manager e IBM Spectrum Protect Client Management Services.

Consejo: Puede aceptar las ubicaciones predeterminadas para el directorio de recursos compartidos y el directorio de instalación para IBM Installation Manager.

## Qué hacer a continuación

---

Siga las instrucciones de Verificación de que el servicio de gestión de clientes está instalado correctamente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Instalación de servicio de gestión de clientes en modalidad silenciosa

---

Puede instalar el servicio de gestión de clientes en modalidad silenciosa. Cuando se utiliza la modalidad silenciosa, se proporcionan los valores de instalación en un archivo de respuestas y, a continuación, se ejecuta un mandato de instalación.

### Antes de empezar

---

Revise Requisitos y limitaciones para servicios de gestión de cliente de IBM Spectrum Protect.

Extraiga el paquete de instalación siguiendo las instrucciones de Instalación de servicio de gestión de clientes utilizando el asistente gráfico.

### Acerca de esta tarea

---

Debe instalar el servicio de gestión de clientes en el mismo sistema que el cliente de archivado y copia de seguridad.

El directorio input, que está en el directorio donde se ha extraído el paquete de instalación, contiene el siguiente archivo de respuestas de ejemplo:

install\_response\_sample.xml

Puede utilizar el archivo de ejemplo con los valores predeterminados o puede personalizarlo.

Consejo: Si desea personalizar el archivo de ejemplo, cree una copia del archivo de ejemplo, cámbiele el nombre y edite la copia.

### Procedimiento

---

1. Cree un archivo de respuestas basado en el archivo de ejemplo o utilice el archivo de ejemplo, install\_response\_sample.xml. En cualquiera de los casos, asegúrese de que el archivo de respuestas especifica el número de puerto para el servicio de gestión de clientes. El puerto predeterminado es 9028. Por ejemplo:

```
<variable name='port' value='9028' />
```

2. Ejecute el mandato para instalar el servicio de gestión de clientes y acepte la licencia. Desde el directorio en donde se extrae el archivo del paquete de instalación, emita el siguiente mandato, donde *archivo\_respuestas* representa la vía de acceso del archivo de respuesta, incluyendo el nombre de archivo:

En un sistema cliente Linux:

```
./install.sh -s -input response_file -acceptLicense
```

Por ejemplo:

```
./install.sh -s -input /cms_install/input/install_response.xml -acceptLicense
```

En un sistema cliente Windows:

```
install.bat -s -input response_file -acceptLicense
```




Por ejemplo:

```
install.bat -s -input c:\cms_install\input\install_response.xml -acceptLicense
```

## Qué hacer a continuación

---

Siga las instrucciones de Verificación de que el servicio de gestión de clientes está instalado correctamente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

# Verificación de que el servicio de gestión de clientes está instalado correctamente

Antes de utilizar el servicio de gestión de clientes para recopilar información de diagnóstico acerca de un cliente de archivado y copia de seguridad, puede verificar que el servicio de gestión de clientes esté instalado y configurado correctamente.

## Procedimiento

En el sistema cliente, en la línea de mandatos, ejecute los mandatos siguientes para ver la configuración del servicio de gestión de clientes:

- En los sistemas cliente Linux, emita el mandato siguiente:

```
dir_instalación_cliente/cms/bin/CmsConfig.sh list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
/opt/tivoli/tsm/cms/bin/CmsConfig.sh list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
```

```
Capabilities: [LOG_QUERY]
```

```
Opt Path: /opt/tivoli/tsm/client/ba/bin/dsm.sys
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmerror.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

```
Log File: /opt/tivoli/tsm/client/ba/bin/dsmsched.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

- En los sistemas cliente Windows, emita el mandato siguiente:

```
dir_instalación_cliente\cms\bin\CmsConfig.bat list
```

donde *dir\_instalación\_cliente* es el directorio donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, en el caso de la instalación de cliente predeterminada, ejecute el siguiente mandato:

```
C:\"Archivos de programa"\Tivoli\TSM\cms\bin\CmsConfig.bat list
```

La salida es similar al texto siguiente:

```
Listado de la configuración de CMS
```

```
server1.example.com:1500 NO_SSL HOSTNAME
```

```
Capabilities: [LOG_QUERY]
```

```
Opt Path: C:\Program Files\Tivoli\TSM\baclient\dsm.opt
```

```
Log File: C:\Program Files\Tivoli\TSM\baclient\dsmerror.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

```
Log File: C:\Program Files\Tivoli\TSM\baclient\dsmsched.log  
en_US MM/dd/aaaa HH:mm:ss Windows-1252
```

Si el servicio de gestión de clientes se ha instalado y configurado correctamente, la salida visualiza la ubicación del archivo de registro de errores.

El texto de salida se extrae del siguiente archivo de configuración:

- En sistemas cliente de Linux:




```
client_install_dir/cms/Liberty/usr/servers/cmsServer/client-configuration.xml
```

- En sistemas cliente de Windows:

```
client_install_dir\cms\Liberty\usr\servers\cmsServer\client-configuration.xml
```

Si la salida no contiene ninguna entrada, debe configurar el archivo `client-configuration.xml`. Para obtener instrucciones sobre cómo configurar este archivo, consulte Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas. Puede

utilizar el mandato CmsConfig verify para verificar que se ha creado correctamente una definición de nodo en el archivo client-configuration.xml.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Configuración del Centro de operaciones para utilizar el servicio de gestión de clientes

Si no ha utilizado la configuración predeterminada para el servicio de gestión de clientes, debe configurar el Centro de operaciones para acceder al servicio de gestión de clientes.

### Antes de empezar

Asegúrese de que el servicio de gestión de clientes se ha instalado e iniciado en el sistema cliente.

Verifique si se ha utilizado la configuración predeterminada. La configuración predeterminada no se utiliza si se cumple alguna de las condiciones siguientes:

- El servicio de gestión de clientes no utiliza el número de puerto predeterminado, 9028.
- Al cliente de archivado y copia de seguridad no se accede mediante la misma dirección IP que al sistema cliente donde está instalado el cliente de archivado y copia de seguridad. Por ejemplo, es posible que se utilice una dirección IP diferente en las situaciones siguientes:
  - El sistema tiene dos tarjetas de red. El cliente de archivado y copia de seguridad está configurado para comunicarse en una red, mientras que el servicio de gestión de clientes se comunica en la otra red.
  - El sistema cliente se ha configurado con el DHCP (Dynamic Host Configuration Protocol - Protocolo de configuración dinámica de host). Como resultado, al sistema cliente se le asigna dinámicamente una dirección IP, que se guarda en el servidor de IBM Spectrum Protect durante la operación de cliente de archivado y copia de seguridad anterior. Cuando se reinicia el sistema cliente, se le puede asignar una dirección IP diferente. Para asegurarse de que el Centro de operaciones puede encontrar siempre el sistema cliente, especifique un nombre de dominio completo.

### Procedimiento

Para configurar el Centro de operaciones para utilizar el servicio de gestión de clientes, realice los pasos siguientes:

1. En la página Clientes del Centro de operaciones, seleccione el cliente.
2. Pulse Detalles.
3. Pulse el separador Propiedades.
4. En el campo URL de diagnóstico remoto de la sección General, especifique el URL para el servicio de gestión de clientes en el sistema cliente.



La dirección debe empezar con `https`. La tabla siguiente muestra ejemplos del URL de diagnóstico remoto.

Tipo de URL	Ejemplo
Con nombre de host de DNS y puerto predeterminado, 9028	<code>https://server.example.com</code>
Con el nombre de host de DNS y puerto no predeterminado	<code>https://server.example.com:1599</code>
Con la dirección IP y puerto no predeterminado	<code>https://192.0.2.0:1599</code>

5. Pulse Guardar.

### Qué hacer a continuación

Puede acceder a la información de diagnóstico de cliente, por ejemplo archivos de registro de cliente, desde el separador Diagnóstico del Centro de operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Inicio y detención del servicio de gestión de clientes

El servicio de gestión de clientes se inicia automáticamente después de instalarse en el sistema cliente. Es posible que necesite detener e iniciar el servicio en determinadas situaciones.




### Procedimiento

- Para detener, iniciar o reiniciar el servicio de gestión de clientes en sistemas cliente Linux, emita los mandatos siguientes:
  - Para detener el servicio:
 

```
service cms.rc stop
```
  - Para iniciar el servicio:
 

```
service cms.rc start
```
  - Para reiniciar el servicio:
 

```
service cms.rc restart
```
- En sistemas cliente Windows, abra la ventana Servicios y detenga, inicie o reinicie el servicio IBM Spectrum Protect Client Management Services.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Desinstalación de servicio de gestión de clientes

Si ya no tiene que recopilar información de diagnóstico de cliente, puede desinstalar el servicio de gestión de clientes del sistema cliente.

### Acerca de esta tarea

Debe utilizar IBM® Installation Manager para desinstalar el servicio de gestión de clientes. Si ya no piensa utilizar IBM Installation Manager, también puede desinstalarlo.

### Procedimiento

1. Desinstale el servicio de gestión de clientes del sistema cliente:
  - a. Abra IBM Installation Manager:
    - En el sistema cliente Linux, en el directorio donde está instalado IBM Installation Manager, vaya al subdirectorío eclipse (por ejemplo /opt/IBM/InstallationManager/eclipse) y emita el mandato siguiente:
 

```
./IBMIM
```
    - En el sistema cliente Windows, abra IBM Installation Manager desde el menú Inicio.
  - b. Pulse en Desinstalar.
  - c. Seleccione IBM Spectrum Protect Client Management Services y pulse Siguiente.
  - d. Pulse Desinstalar y, a continuación, pulse Finalizar.
  - e. Cierre la ventana de IBM Installation Manager.
2. Si ya no necesita IBM Installation Manager, desinstálelo del sistema cliente:
  - a. Abra el asistente de desinstalación de IBM Installation Manager:
    - En el sistema cliente Linux, cambie al directorio de desinstalación de IBM Installation Manager (por ejemplo /var/ibm/InstallationManager/uninstall) y emita el mandato siguiente:
 

```
./uninstall
```
    - En el sistema cliente Windows, pulse Inicio > Panel de control. A continuación, pulse Desinstalar un programa > IBM Installation Manager > Desinstalar.
  - b. En la ventana de IBM Installation Manager, seleccione IBM Installation Manager si aún no está seleccionado y pulse Siguiente.
  - c. Pulse Desinstalar y pulse Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Configuración del servicio de gestión de clientes para instalaciones de cliente personalizadas

El servicio de gestión de clientes utiliza información del archivo de configuración de cliente (client-configuration.xml) para descubrir información de diagnóstico. Si el servicio de gestión de clientes no puede descubrir la ubicación de los archivos de registro, debe ejecutar el programa de utilidad CmsConfig para añadir la ubicación de los archivos de registro al archivo client-configuration.xml.

- Programa de utilidad CmsConfig  
Si no está utilizando la configuración de cliente predeterminada, puede ejecutar el programa de utilidad CmsConfig en el sistema



cliente para descubrir y añadir la ubicación de los archivos de registro de cliente al archivo client-configuration.xml. Después de completar la configuración, el servicio de gestión de clientes puede acceder a los archivos de registro de cliente y dejarlos disponibles para las funciones básicas de diagnóstico en el Centro de operaciones.


 Sistemas operativos AIX  Sistemas operativos Linux

## Resolución de problemas de la instalación de Centro de operaciones

---

Si ocurre un problema con la instalación del Centro de operaciones y no puede resolverlo, puede consultar las descripciones de problemas conocidos para una posible solución.

-  Sistemas operativos AIX El asistente de instalación gráfica no puede iniciarse en un sistema AIX. Está instalando Centro de operaciones en un sistema AIX haciendo uso del asistente gráfico, y el programa de instalación no se inicia.
-  Sistemas operativos Linux Las letras en chino, japonés o coreano se muestran incorrectamente. Las fuentes en chino, japonés o coreano se muestran incorrectamente en Centro de operaciones en Red Hat Enterprise Linux 5.

 Sistemas operativos AIX

## El asistente de instalación gráfica no puede iniciarse en un sistema AIX

---

Está instalando Centro de operaciones en un sistema AIX haciendo uso del asistente gráfico, y el programa de instalación no se inicia.

### Solución

---

Los archivos RPM que aparecen en Instalación de Centro de operaciones utilizando el asistente gráfico deben estar instalados en el sistema. Compruebe que los archivos RPM estén instalados.

 Sistemas operativos Linux

## Las letras en chino, japonés o coreano se muestran incorrectamente

---




Las fuentes en chino, japonés o coreano se muestran incorrectamente en Centro de operaciones en Red Hat Enterprise Linux 5.

### Solución

---

Instale los siguientes paquetes de fuentes, que están disponibles en Red Hat:

- fonts-chinese
- fonts-japanese
- fonts-korean

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Desinstalación de Centro de operaciones

---

Puede desinstalar Centro de operaciones utilizando cualquiera de los siguientes métodos: un asistente gráfico, la línea de mandatos en la modalidad de consola o la modalidad silenciosa.

- Desinstalación de Centro de operaciones utilizando el asistente gráfico  
Puede desinstalar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.
- Desinstalación del Centro de operaciones en modalidad de consola  
Para desinstalar Centro de operaciones mediante el uso de la línea de mandatos, debe ejecutar el programa de desinstalación IBM Installation Manager desde la línea de mandato con el parámetro para la modalidad de consola.
- Desinstalar Centro de operaciones en modalidad silenciosa  
Para desinstalar Centro de operaciones en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM Installation Manager desde la línea de mandatos con los parámetros de la modalidad silenciosa.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Desinstalación de Centro de operaciones utilizando el asistente gráfico



---

Puede desinstalar Centro de operaciones mediante el asistente gráfico de IBM® Installation Manager.


## Procedimiento

---




1. Abra IBM Installation Manager.

 Sistemas operativos AIX  Sistemas operativos Linux En el directorio en el que está instalado IBM Installation Manager, vaya al subdirectorio eclipse (por ejemplo, /opt/IBM/InstallationManager/eclipse), y emita el siguiente mandato:

```
./IBMIM
```

 Sistemas operativos Windows Puede abrir IBM Installation Manager desde el menú Inicio.

2. Pulse en Desinstalar.
3. Seleccione la opción para Centro de operaciones y pulse Siguiente.
4. Pulse en Desinstalar.
5. Pulse en Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows




## Desinstalación del Centro de operaciones en modalidad de consola

---




Para desinstalar Centro de operaciones mediante el uso de la línea de mandatos, debe ejecutar el programa de desinstalación IBM® Installation Manager desde la línea de mandato con el parámetro para la modalidad de consola.




### Procedimiento




---

1. En el directorio en el que está instalado IBM Installation Manager, vaya al siguiente subdirectorio:
  - o  Sistemas operativos AIX  Sistemas operativos Linux eclipse/tools
  - o  Sistemas operativos Windows eclipse\tools

Por ejemplo:

- o  Sistemas operativos AIX  Sistemas operativos Linux /opt/IBM/InstallationManager/eclipse/tools
- o  Sistemas operativos Windows C:\Archivos de programa\IBM\Installation Manager\eclipse\tools

2. Desde el directorio herramientas, emita el siguiente mandato:
  - o  Sistemas operativos AIX  Sistemas operativos Linux ./imcl -c
  - o  Sistemas operativos Windows imcl.exe -c
3. Para desinstalar, escriba 5.
4. Elija desinstalar del grupo de paquetes de IBM Spectrum Protect.
5. Especifique **N** para Siguiente.
6. Elija desinstalar el paquete de Centro de operaciones.
7. Especifique **N** para Siguiente.
8. Escriba **U** para Desinstalar.
9. Escriba **F** para Finalizar.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Desinstalar Centro de operaciones en modalidad silenciosa

---

Para desinstalar Centro de operaciones en modalidad silenciosa, debe ejecutar el programa de desinstalación de IBM® Installation Manager desde la línea de mandatos con los parámetros de la modalidad silenciosa.

### Antes de empezar

---




Puede utilizar un archivo de respuestas para proporcionar entrada de datos a fin de desinstalar de forma silenciosa el servidor de Centro de operaciones. IBM Spectrum Protect incluye un archivo de respuestas de ejemplo, `uninstall_response_sample.xml`, en el directorio `input` donde se extrae el paquete de instalación. Este archivo contiene valores predeterminados para ayudarle a evitar cualquier aviso innecesario.

Para desinstalar el Centro de operaciones, deje establecido `modify="false"` para la entrada del Centro de operaciones en el archivo de respuestas.




Si desea personalizar el archivo de respuestas, puede modificar las opciones que hay en el archivo. Para obtener información sobre los archivos de respuestas, consulte Archivos de respuestas.

## Procedimiento




1. En el directorio en el que está instalado IBM Installation Manager, vaya al siguiente subdirectorio:

-  Sistemas operativos AIX  Sistemas operativos Linux/eclipse/tools
-  Sistemas operativos Windows/eclipse/tools




Por ejemplo:




-  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/InstallationManager/eclipse/tools
-  Sistemas operativos WindowsC:\Archivos de programa\IBM\Installation Manager\eclipse/tools

2. Desde el directorio herramientas, emita el siguiente mandato, donde *response\_file* representa la vía de acceso al archivo de respuesta, incluido el nombre del archivo:

-  Sistemas operativos AIX  Sistemas operativos Linux./imcl -input *archivo\_respuestas* -silent
-  Sistemas operativos Windowsimcl.exe -input *archivo\_respuestas* -silent

El siguiente mandato es un ejemplo:

-  Sistemas operativos AIX  Sistemas operativos Linux./imcl -input /tmp/input/uninstall\_response.xml -silent
-  Sistemas operativos Windowsimcl.exe -input C:\tmp\input\uninstall\_response.xml -silent

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Volver a una versión anterior de Centro de operaciones

De forma predeterminada, IBM® Installation Manager guarda versiones anteriores de un paquete para poder regresar a una versión anterior si experimenta un problema con versiones posteriores de actualizaciones, arreglos o paquetes.

### Antes de empezar

La función de restauración está disponible solo cuando Centro de operaciones está actualizado.

### Acerca de esta tarea

Cuando IBM Installation Manager restaura un paquete a una versión anterior, la versión actual de los archivos del paquete se desinstala, y se vuelve a instalar una versión anterior.

Para restaurar a una versión anterior, IBM Installation Manager debe acceder a los archivos de esa versión. De manera predeterminada, estos archivos se guardan durante cada instalación sucesiva. Debido al número de archivos guardados con cada versión instalada, es posible que quiera eliminar estos archivos del sistema de forma regular. Sin embargo, si elimina los archivos, no puede regresar a la versión anterior.

Para eliminar archivos guardados o para actualizar su preferencia para guardar estos archivos en instalaciones futuras, siga estos pasos:

1. En IBM Installation Manager, pulse Archivo > Preferencias.
2. En la página de Preferencias, pulse Archivos a restaurar y especifique su preferencia.

## Procedimiento

Para restaurar una versión anterior de Centro de operaciones, use la función Retrotraer de IBM Installation Manager.

## Configuración de servidores

Para completar las tareas de configuración para el servidor de IBM Spectrum Protect, revise la documentación disponible.

### Acerca de esta tarea

Para una solución existente, revise las acciones siguientes.

Para planificar, implementar, supervisar y utilizar una nueva solución, siga las instrucciones de Soluciones de protección de datos de IBM Spectrum Protect.

Consejo: A partir de IBM Spectrum Protect V7.1.3, la *Guía del administrador* ha quedado obsoleta.

Acción	Detalles	Documentación
--------	----------	---------------



Acción	Detalles	Documentación
Supervisión de una solución de almacenamiento	Supervise la solución de almacenamiento para identificar problemas potenciales y existentes. De este modo, puede resolver problemas y optimizar el rendimiento del sistema.	Supervisión de soluciones de almacenamiento
Selección y configuración de almacenamiento	Seleccione el almacenamiento en función de las necesidades de la empresa y realice las tareas de configuración.	Configuración del almacenamiento
Eliminar datos duplicados	<p>Utilice la eliminación de datos duplicados para eliminar datos redundantes en las agrupaciones de almacenamiento. La eliminación de duplicados de datos reduce el almacenamiento necesario para conservar los datos. En una agrupación de almacenamiento cuyos duplicados se han eliminado sólo se conserva una instancia de los datos.</p> <p>Con IBM Spectrum Protect versión 7.1.3 y posteriores, puede utilizar la eliminación de duplicados de datos en línea.</p>	Para obtener más información sobre las diferencias entre la eliminación de duplicados de datos en línea y postproceso, y para configurar la solución de mejores prácticas para la eliminación de duplicados de datos, consulte Opciones de eliminación de datos duplicados.
Replicar datos	Puede replicar datos de nodo de cliente desde un servidor de réplica fuente a un servidor de réplica de destino. Si se produce un desastre y el servidor de origen no está disponible temporalmente, los nodos de cliente pueden recuperar los datos del servidor de réplica de destino.	<p>Para implementar una solución de mejores prácticas que utilice la duplicación y la migración tras error automática IBM Spectrum Protect, consulte el apartado Solución de disco multisitio.</p> <p>Para obtener información general acerca de la réplica, incluidos los pasos de configuración, consulte Réplica de datos de cliente en otro servidor.</p>
Gestionar la base de datos y las anotaciones de recuperación	La base de datos y el registro de recuperación o el inventario del servidor, almacenan información sobre datos de cliente y son esenciales para el funcionamiento del servidor.	<ul style="list-style-type: none"> <li>• Para obtener información general acerca de la base de datos y registro de recuperación, consulte: Gestión de la base de datos y el registro de recuperación (V7.1.1).</li> <li>• Para optimizar la reorganización de índices y tablas de la base de datos del servidor, y evitar y resolver problemas relacionados con el aumento de la base de datos y el rendimiento, consulte nota técnica 1683633.</li> </ul>
Proteger el servidor	Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.	Protección del servidor IBM Spectrum Protect

Acción	Detalles	Documentación
Configure SSL para LDAP (Lightweight Directory Access Protocol)	Puede configurar SSL para los servidores de directorios LDAP y gestionar las contraseñas y los procedimientos de inicio de sesión.	Para obtener información sobre LDAP, consulte: <ul style="list-style-type: none"> <li>• Autenticación de los usuarios mediante un servidor LDAP</li> <li>• Configuración de SSL o TLS para los servidores de directorio LDAP (V7.1.1)</li> </ul>
Obtenga información y configure políticas para la retención de datos	Las políticas de IBM Spectrum Protect definen las reglas para gestionar los datos.	Para actualizar las políticas, utilice el Centro de operaciones.  Para obtener más información sobre las políticas y crear políticas, consulte Personalización de políticas.
Protección del servidor y recuperación después de un desastre	Proteja la infraestructura del sistema y de los datos para que pueda recuperarlos después de un desastre. Utilice las herramientas y procedimientos que proporciona IBM Spectrum Protect para ayudarlo a crear un plan de recuperación tras desastre.	Para obtener información sobre cómo proteger y recuperar el servidor, consulte: <ul style="list-style-type: none"> <li>• Protección de los archivos de configuración de infraestructura y base de datos (V7.1.1)</li> <li>• Utilización del gestor de recuperación ante siniestro para entornos de cinta (V7.1.1)</li> </ul>
Proteger servidores de archivos NAS	Puede planificar, configurar y gestionar un entorno de copia de seguridad que proteja su servidor de archivos de almacenamiento adjunto de red (NAS).	Protección de servidores de archivos NAS
Configurar un entorno en clúster	Configure un entorno en clúster en AIX, Linux, o Windows para garantizar una mayor disponibilidad del servidor y minimizar el tiempo de inactividad.	Configuración de entornos en clúster
Verificación de conformidad de la licencia	Verifique que la solución de IBM Spectrum Protect cumple las condiciones del acuerdo de licencia. Si comprueba el cumplimiento de forma periódica, podrá realizar un seguimiento de las tendencias del crecimiento de los datos o el uso del value unit de procesador (PVU).	Verificación de la conformidad de licencia

- Protección del servidor IBM Spectrum Protect  
Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.
- Réplica de datos de cliente en otro servidor  
El hecho de realizar una réplica de los datos de cliente de un servidor de origen en otro servidor ayuda a garantizar que los datos de cliente copiados están disponibles para su recuperación si el servidor de origen resulta dañado. La réplica realiza una copia incremental de los datos del servidor de origen en el servidor de destino para proporcionar capacidad de migración y recuperación.
- Configuración de entornos en clúster  
Puede configurar el servidor de IBM Spectrum Protect para la agrupación en clúster en sistemas AIX, Linux o Windows.

## Protección del servidor IBM Spectrum Protect

Proteja el servidor IBM Spectrum Protect y los datos controlando el acceso a servidores y nodos de cliente, cifrando datos y manteniendo niveles de acceso seguros y contraseñas.

- **Conceptos sobre la seguridad**  
Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.
- **Gestión de administradores**  
Un administrador con autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas de las tareas debe tener asignados uno o varios niveles de autorización.
- **Cambio de los requisitos de contraseña**  
Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.
- **Protección de IBM Spectrum Protect en el sistema**  
Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.
- **Protección de las comunicaciones**  
Sus datos y contraseñas son más seguros si los protege mediante Secure Sockets Layer (SSL) o Transport Layer Security (TLS), una forma de SSL.
- **Autenticación de los usuarios de IBM Spectrum Protect mediante un servidor LDAP**  
En un sistema IBM Spectrum Protect, los usuarios deben autenticarse en el servidor proporcionando un ID de usuario y contraseña. Si su organización utiliza un servidor LDAP (Lightweight Directory Access Protocol) para gestionar los ID de usuario, puede utilizar el servidor LDAP para autenticar los ID de usuario de IBM Spectrum Protect.

## Conceptos sobre la seguridad

---

Puede proteger IBM Spectrum Protect de riesgos de seguridad utilizando protocolos de comunicación, contraseñas de seguridad y proporcionando diferentes niveles de acceso para administradores.

### Seguridad de la capa de transporte

---

Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores, clientes y agentes de almacenamiento. Si envía datos entre el servidor el cliente y el agente de almacenamiento, utilice SSL o TLS para cifrar los datos.

Consejo: Toda la documentación de IBM Spectrum Protect que indique "SSL" o "seleccionar SSL" se aplica a TLS.

SSL se proporciona mediante el Global Security Kit (GSKit) que se instala con el servidor de IBM Spectrum Protect que utilizan el servidor, el cliente y el agente de almacenamiento.

Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con una instancia de base de datos de DB2 utilizada por cualquier servidor de IBM Spectrum Protect.

Cada servidor, cliente o agente de almacenamiento que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo firmado por una entidad emisora de certificados (CA). Puede utilizar sus propios certificados o adquirir certificados de una CA. Cada certificado debe instalarse y añadirse a la base de datos de claves en el servidor, cliente o agente de almacenamiento de IBM Spectrum Protect. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL. Algunos certificados CA están preinstalados de forma predeterminada en las bases de datos de claves.

SSL se configura de forma independiente en el agente de almacenamiento, el cliente o en el servidor de IBM Spectrum Protect.

### Niveles de autorización

---

En cada servidor de IBM Spectrum Protect, hay diferentes niveles de autorización administrativa disponibles que determinan las tareas que puede llevar a cabo un administrador.

Después de registrarse, el administrador debe tener autorización para que se le asignen uno o más niveles de autoridad administrativa. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor y asignar niveles de autorización a otros administradores utilizando el mandato GRANT AUTHORITY. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

Un administrador puede registrar otros ID de administrador, otorgarles niveles de autoridad, renombrarlos o eliminarlos, y bloquearlos y desbloquearlos del servidor.

Un administrador puede controlar el acceso a nodos de cliente específicos para ID de usuario root e ID de usuario no root. De forma predeterminada, un ID de usuario no root no puede hacer copia de seguridad de los datos en el nodo. Utilice el mandato UPDATE NODE para cambiar los valores de nodo para habilitar la copia de seguridad.

### Contraseñas

---

De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben entrar una contraseña cuando acceden al servidor.

Utilice Lightweight Directory Access Protocol (LDAP) para aplicar requisitos más estrictos para las contraseñas. Para obtener más información, consulte Autenticación de los usuarios mediante un servidor LDAP.

Tabla 1. Características de la autenticación de contraseña

Característica	Más información
Distinción entre mayúsculas y minúsculas	No distingue entre mayúsculas y minúsculas.
Caducidad de la contraseña predeterminada	90 días.  El período de caducidad se inicia cuando un ID de administrador o nodo cliente se inscribe por primera vez en el servidor. Si no se cambia la contraseña dentro de este período, se deberá cambiar la contraseña la próxima vez que el usuario acceda al servidor.
Intentos de contraseña no válidos	Puede establecer un límite de intentos consecutivos no válidos de entrada de contraseña para todos los nodos cliente. Si se supera el límite, el servidor bloquea el nodo.
Longitud de la contraseña	El administrador puede especificar una longitud mínima.

## Seguridad de sesión

La seguridad de sesión es el nivel de seguridad que se utiliza para la comunicación entre los nodos cliente, los clientes administrativos y los servidores de IBM Spectrum Protect y se establece mediante el parámetro SESSIONSECURITY.

El parámetro SESSIONSECURITY se puede establecer en uno de los siguientes valores:

- El valor STRICT aplica el nivel más alto de la seguridad para la comunicación entre servidores, nodos y administradores de IBM Spectrum Protect.
- El valor TRANSITIONAL especifica que se utiliza el protocolo de comunicación existente mientras se actualiza el software IBM Spectrum Protect a la versión V8.1.2 o posterior. Este es el valor predeterminado. Cuando SESSIONSECURITY=TRANSITIONAL, se aplican automáticamente parámetros de seguridad más estrictos si se utilizan versiones superiores del protocolo TLS y se actualiza el software a V8.1.2 o posterior. Después de que un nodo, administrador o servidor cumpla los requisitos del valor STRICT, la seguridad de sesión se actualiza automáticamente al valor STRICT, y la entidad ya no puede autenticarse utilizando una versión anterior del cliente o protocolos TLS anteriores.

Para obtener más información sobre los valores del parámetro SESSIONSECURITY, consulte los siguientes mandatos:

Tabla 2. Mandatos utilizados para definir el parámetro SESSIONSECURITY

Entidad	Mandato
Nodos cliente	<ul style="list-style-type: none"> <li>• REGISTER NODE</li> <li>• UPDATE NODE</li> </ul>
Administradores	<ul style="list-style-type: none"> <li>• REGISTER ADMIN</li> <li>• UPDATE ADMIN</li> </ul>
Servidores	<ul style="list-style-type: none"> <li>• DEFINE SERVER</li> <li>• UPDATE SERVER</li> </ul>

Los administradores que se autentican mediante el mandato DSMADMC, el mandato DSMC o el programa dsm no se pueden autenticar utilizando una versión anterior, una vez que se han autenticado utilizando V8.1.2 o posterior. Para resolver los problemas de autenticación para los administradores, consulte los siguientes consejos:

Sugerencias:

- Asegúrese de que todo el software de IBM Spectrum Protect que utiliza la cuenta de administrador para iniciar sesión esté actualizado a V8.1.2 o posterior. Si una cuenta de administrador inicia sesión desde varios sistemas, asegúrese de que el certificado esté instalado en todos ellos.
- Después de que un administrador se autentique en un servidor V8.1.2 o posterior utilizando un cliente V8.1.2 o posterior, el administrador solo puede autenticarse en clientes o servidores que utilicen V8.1.2 o posterior. Se puede emitir un mandato de administrador desde cualquier sistema.
- En caso necesario, cree otra cuenta de administrador para utilizar solo con clientes y servidores que utilicen software V8.1.1 o anterior.

Aplice el nivel más elevado de seguridad para la comunicación con el servidor de IBM Spectrum Protect, asegurándose de que todos los nodos, administradores y servidores utilicen la seguridad de sesión STRICT. Puede utilizar el mandato SELECT para determinar qué servidores, nodos y administradores están utilizando la seguridad de sesión TRANSITIONAL y deberían actualizarse para utilizar la seguridad de sesión STRICT.

**Referencia relacionada:**

Protección de las comunicaciones  
SELECT (Realizar una consulta SQL de la base de datos)

## Gestión de administradores

Un administrador con autorización del sistema puede completar cualquier tarea con el servidor de IBM Spectrum Protect, incluida la asignación de niveles de autorización a otros administradores. Para completar algunas de las tareas debe tener asignados uno o varios niveles de autorización.

### Procedimiento

Complete las siguientes tareas para modificar los valores de administrador.

Tarea	Procedimiento
Añada un administrador.	<p>Para añadir un administrador, ADMIN1, con autoridad del sistema y especificar una contraseña, lleve a cabo lo siguiente:</p> <ol style="list-style-type: none"> <li>Registre el administrador y especifique Pa\$#\$twO como contraseña ejecutando el siguiente mandato: <pre>register admin admin1 Pa\$#\$twO</pre> </li> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> </li> </ol>
Cambie los permisos del administrador.	<p>Cambie el nivel de autorización de un administrador, ADMIN1.</p> <ul style="list-style-type: none"> <li>Ejecute el siguiente mandato para proporcionar autoridad del sistema al administrador: <pre>grant authority admin1 classes=system</pre> </li> <li>Emita el siguiente mandato para revocar la autoridad del sistema del administrador: <pre>revoke authority admin1 classes=system</pre> </li> </ul>
Elimine administradores.	<p>Ejecute el siguiente mandato para eliminar el acceso del administrador, ADMIN1, al servidor de IBM Spectrum Protect:</p> <pre>remove admin admin1</pre>
Impida el acceso al servidor de forma temporal.	<p>Utilice el mandato LOCK ADMIN o UNLOCK ADMIN para bloquear o desbloquear a un administrador.</p>

## Cambio de los requisitos de contraseña

Puede cambiar el límite mínimo de contraseña, la longitud de la contraseña, la caducidad de la contraseña y habilitar o inhabilitar la autenticación para IBM Spectrum Protect.

### Acerca de esta tarea

Imponiendo la autenticación de contraseña y gestionando las restricciones de contraseña, protege los datos y los servidores de posibles riesgos de seguridad.

### Procedimiento

Complete las siguientes tareas para cambiar los requisitos de contraseña para los servidores IBM Spectrum Protect.

Tabla 1. Tareas de autenticación para servidores IBM Spectrum Protect

Tarea	Procedimiento
Establecer un límite de intentos de contraseña no válidos.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, haga clic en el separador Propiedades.</p> <p>c. Establezca el número de intentos no válidos en el campo Límite de intentos de inicio de sesión no válidos.</p> <p>El valor predeterminado en la instalación es 0.</p>
Establecer una longitud mínima para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establezca el número de caracteres en el campo Longitud mínima de contraseña.</p>
Establecer el período de caducidad para las contraseñas.	<p>a. En la página Servidores del Centro de operaciones, seleccione el servidor.</p> <p>b. Pulse Detalles y, a continuación, pulse el separador Propiedades.</p> <p>c. Establecer el número de días en el campo Caducidad común de la contraseña.</p>
Inhabilitar la autenticación de contraseña.	<p>De forma predeterminada, el servidor utiliza automáticamente la autenticación de contraseña. Con la autenticación de contraseña, todos los usuarios deben escribir una contraseña para acceder al servidor.</p> <p>Sólo se puede inhabilitar la autenticación por contraseña para las contraseñas que se autentican con el servidor (LOCAL). Si se inhabilita la autenticación de contraseña, puede aumentar el riesgo de seguridad para el servidor.</p>
Establecer un método de autenticación predeterminado.	<p>Emita el mandato SET DEFAULTAUTHENTICATION. Por ejemplo, para utilizar el servidor como método de autenticación predeterminado, emita el mandato siguiente:</p> <pre>set defaultauthentication local</pre> <p>Para actualizar un nodo de cliente para que se autentique con el servidor, incluya AUTHENTICATION=LOCAL en el mandato UPDATE NODE:</p> <pre>update node authentication=local</pre>

## Protección de IBM Spectrum Protect en el sistema

Proteja el sistema donde se ejecuta el servidor de IBM Spectrum Protect para evitar el acceso no autorizado.

### Procedimiento

Asegúrese de que los usuarios no autorizados no puedan acceder a los directorios de la base de datos del servidor ni a la instancia de servidor. Mantenga los valores de acceso para estos directorios que ha configurado durante la implementación.

- Restricción del acceso de usuario al servidor  
Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.
- Limitación de acceso a través de restricciones de puerto  
Limite el acceso al servidor aplicando restricciones de puerto.

## Restricción del acceso de usuario al servidor

Los niveles de autorización determinan qué puede hacer un administrador con el servidor de IBM Spectrum Protect. Un administrador con autoridad del sistema puede completar cualquier tarea con el servidor. Los administradores con autoridad de política, almacenamiento u operador pueden completar subconjuntos de tareas.

### Procedimiento

1. Después de registrar un administrador utilizando el mandato REGISTER ADMIN, utilice el mandato GRANT AUTHORITY para establecer el nivel de autorización del administrador. Para obtener detalles sobre cómo establecer y cambiar la autorización, consulte Gestión de administradores.
2. Para controlar la autoridad de un administrador para completar algunas tareas, utilice las dos opciones de servidor siguientes:
  - a. Puede seleccionar el nivel de autorización que debe tener un administrador para emitir los mandatos QUERY y SELECT con la opción de servidor QUERYAUTH. De forma predeterminada, no se requiere ningún nivel de autorización. Puede cambiar el requisito para uno de los niveles de autorización, incluido el sistema.
  - b. Puede especificar que se requiere autoridad del sistema para mandatos que hacen que el servidor se grabe en un archivo externo con la opción de servidor REQSYSAUTHOUTFILE. El valor predeterminado establece que es necesaria la autorización del sistema para esos mandatos.
3. Puede restringir la copia de seguridad de datos en un nodo cliente a sólo los ID de usuario root o usuarios autorizados. Por ejemplo, para limitar copias de seguridad al ID de usuario root, emita el mandato REGISTER NODE o UPDATE NODE y especifique el parámetro BACKUPINITIATION=root:

```
update node backupinitiation=root
```

## Limitación de acceso a través de restricciones de puerto

Limite el acceso al servidor aplicando restricciones de puerto.

### Acerca de esta tarea

Es posible que tenga que restringir el acceso a servidores específicos, en base a los requisitos de seguridad. El servidor IBM Spectrum Protect se puede configurar para que escuche en cuatro puertos TCP/IP: dos que pueden utilizarse para protocolos TCP/IP regulares o protocolos SSL (Secure Sockets Layer)/TLS (Transport Layer Security) y que pueden utilizarse solo para el protocolo SSL/TLS.

### Procedimiento

Puede establecer las opciones de servidor para especificar el puerto que necesita, tal como se enumera en Tabla 1.

Tabla 1. Opciones de servidor y acceso de puerto

Opción de servidor	Acceso de puerto
TCPPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es 1500.
TCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones distintas de las sesiones de cliente. Este puerto realiza escuchas para sesiones habilitadas para TCP/IP y SSL. El valor predeterminado es el valor de TCPPORT.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPORT y SSLTCPPORT.
SSLTCPPORT	Especifica la dirección de puerto SSL TCP/IP para un servidor. Este puerto solo realiza escuchas para sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.
SSLTCPADMINPORT	Especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor espera las solicitudes para las sesiones habilitadas para SSL. Un valor de puerto predeterminado no está disponible.  Utilice esta opción para separar el tráfico de cliente administrativo del tráfico de cliente regular que utiliza las opciones TCPPORT y SSLTCPPORT.

## Protección de las comunicaciones

Sus datos y contraseñas son más seguros si los protege mediante Secure Sockets Layer (SSL) o Transport Layer Security (TLS), una forma de SSL.

SSL y TLS son la tecnología estándar para crear sesiones cifradas entre servidores y clientes. SSL y TLS proporcionan un canal seguro para que los clientes se comuniquen a través de vías de acceso de comunicación abiertas. Con SSL y TLS, la identidad del servidor se verifica mediante el uso de certificados digitales. Los clientes, servidores y agentes de almacenamiento que utilicen el software IBM Spectrum Protect V8.1.2 o posterior para comunicarse se configuran automáticamente para utilizar TLS 1.2.

Para mejorar el rendimiento del sistema, utilice TLS para la autenticación sin cifrar datos de objetos. Para especificar si el servidor utiliza TLS 1.2 para toda la sesión o solo para la autenticación, consulte la opción de cliente SSL para la comunicación de cliente a servidor, y el parámetro SSL en el mandato UPDATE SERVER para la comunicación de servidor a servidor. Si elige utilizar TLS para cifrar datos de objetos, plantéese la posibilidad de añadir recursos de procesador adicionales en el servidor de IBM Spectrum Protect para gestionar el aumento del tráfico de red.

Si autentica las contraseñas con un servidor de directorios LDAP, TLS protege las contraseñas entre el servidor de IBM Spectrum Protect y el servidor LDAP. TLS es necesario para todas las comunicaciones de contraseñas LDAP.

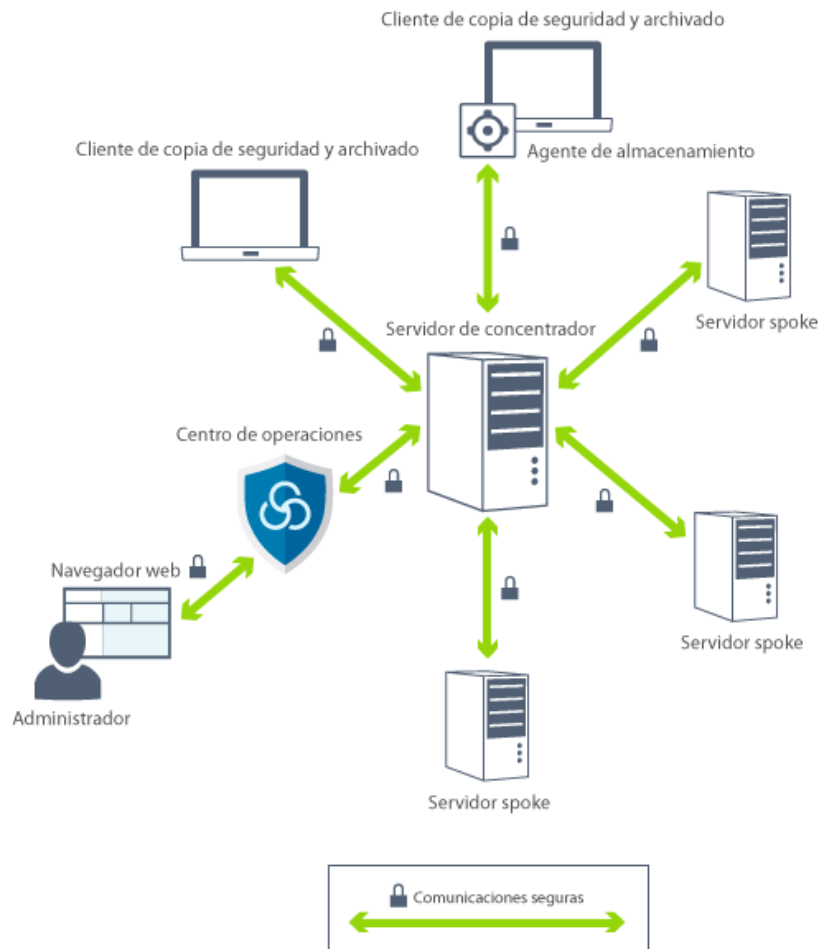
- **Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte**  
Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores de IBM Spectrum Protect, clientes, agentes de almacenamiento y el Centro de operaciones. Si envía datos entre el servidor el cliente y el agente de almacenamiento, se utiliza SSL o TLS para cifrar los datos.
- **Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL**  
Configure la Capa de sockets seguros (SSL) en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad, el agente de almacenamiento y el Centro de operaciones para asegurarse de que los datos están cifrados durante la comunicación.

## Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte

---

Puede utilizar la Capa de sockets seguros (SSL) o el protocolo de Seguridad de la capa de transporte (TLS) para proporcionar seguridad de la capa de transporte para una conexión segura entre servidores de IBM Spectrum Protect, clientes, agentes de almacenamiento y el Centro de operaciones. Si envía datos entre el servidor el cliente y el agente de almacenamiento, se utiliza SSL o TLS para cifrar los datos.





Restricción: No utilice los protocolos SSL o TLS para las comunicaciones con unas instancias de base de datos de IBM DB2 utilizada por el servidor IBM Spectrum Protect.

Cada servidor o agente de almacenamiento tiene una clave privada exclusiva y un certificado firmado exclusivo que se utiliza para permitir conexiones SSL. Si utiliza certificados autofirmados, debe distribuir el certificado autofirmado para cada servidor o agente de almacenamiento para todos los clientes, agentes de almacenamiento y servidores que utilizan TLS para comunicarse con él. Si utiliza certificados firmados por una entidad emisora de certificados, debe distribuir sólo los certificados de entidad emisora de certificados a todos los clientes, agentes de almacenamiento y servidores que utilizan TLS para comunicarse.

Si utiliza un certificado raíz de una entidad emisora de certificados, deberá instalarlo en cada base de datos de claves del cliente, servidor y agente de almacenamiento que inicie la comunicación SSL. Un *certificado raíz* es un certificado que identifica la entidad emisora de certificados raíz. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL.

A partir de IBM Spectrum Protect versión 8.1.2, SSL está habilitado de forma predeterminada para las comunicaciones entre servidores, clientes y agentes de almacenamiento de la versión 8.1.2.

El servidor, cliente o agente de almacenamiento de IBM Spectrum Protect pueden servir como clientes SSL durante la comunicación. Un cliente SSL es el componente que inicia la comunicación y verifica el certificado para un servidor SSL. Por ejemplo, si el cliente de IBM Spectrum Protect inicia la comunicación SSL con el servidor de IBM Spectrum Protect, el cliente de IBM Spectrum Protect es el cliente SSL y el servidor es el servidor SSL.

Tabla 1 enumera los componentes, que pueden ser un cliente SSL o un servidor SSL.

Tabla 1. Servidores y clientes SSL del entorno de IBM Spectrum Protect

Cliente SSL	Servidor SSL	Escenario
Cliente	Servidor	El cliente de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. El cliente verifica el certificado. El servidor proporciona el certificado.
Servidor (por ejemplo, un servidor de origen)	Servidor (por ejemplo, un servidor de destino)	El servidor de origen de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor de destino de IBM Spectrum Protect. El servidor de origen actúa como un cliente SSL y verifica el certificado que proporciona el servidor de destino. Este tipo de comunicación es común durante el proceso de réplica.

Cliente SSL	Servidor SSL	Escenario
Cliente a través de un agente de almacenamiento	Servidor	El cliente comprueba cada certificado cuando inicia la comunicación SSL por separado con el servidor de IBM Spectrum Protect y el agente de almacenamiento.  Cuando el agente de almacenamiento se comunica con el servidor utilizando el protocolo de comunicación SSL, el agente de almacenamiento actúa como un cliente SSL y verifica el certificado que proporciona el servidor.  El agente de almacenamiento puede ser el cliente SSL y el proveedor de SSL al mismo tiempo.
Servidor	Servidor LDAP	El servidor de IBM Spectrum Protect inicia una solicitud de comunicación con el servidor LDAP. El servidor de IBM Spectrum Protect actúa como un cliente SSL y verifica el certificado que proporciona el servidor LDAP.
Centro de operaciones	Servidor	El Centro de operaciones inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. El Centro de operaciones actúa como un cliente SSL y verifica el certificado que proporciona el servidor de IBM Spectrum Protect.
Informes	Servidor	El agente de creación de informes inicia una solicitud de comunicación con el servidor de IBM Spectrum Protect. La función de creación de informes actúa como un cliente SSL y verifica el certificado que proporciona el servidor de IBM Spectrum Protect.

## Configuración de agentes de almacenamiento, servidores, clientes y el Centro de operaciones para conectarse al servidor utilizando SSL

Configure la Capa de sockets seguros (SSL) en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad, el agente de almacenamiento y el Centro de operaciones para asegurarse de que los datos están cifrados durante la comunicación.

Puede utilizar un certificado SSL autofirmado o un certificado firmado por una entidad emisora de certificados (CA) de terceros para verificar una solicitud de comunicación SSL entre el servidor, el cliente y el agente de almacenamiento. Cada servidor, cliente o agente de almacenamiento de IBM Spectrum Protect que habilita SSL debe utilizar un certificado autofirmado de confianza u obtener un certificado exclusivo firmado por una entidad emisora de certificados.

La ventaja de los certificados firmados por una entidad emisora de certificados es que un único certificado firmado por entidad emisora de certificados se puede utilizar para todos los servidores, lo que le permite distribuir un solo certificado a los clientes. Si utiliza un certificado autofirmado, el certificado se crea automáticamente para cada servidor y agente de almacenamiento. Si utiliza un certificado raíz de una entidad emisora de certificados, deberá instalarse en cada base de datos de claves del cliente, servidor y agente de almacenamiento que inicie la comunicación SSL. El certificado se verifica por medio del servidor o cliente de SSL que solicita o inicia la comunicación SSL.

Restricción: Algunas entidades emisoras de certificados utilizan certificados en un formato que no reconoce IBM Spectrum Protect. Es posible que necesite contactar con la entidad emisora de certificados para convertir el certificado a un formato que pueda utilizar con IBM Spectrum Protect.

- Configuración del servidor para aceptar conexiones SSL  
Configure el servidor para que acepte conexiones SSL antes de habilitar la comunicación SSL desde el servidor a un cliente, un agente de almacenamiento u otro servidor.
- Configuración de un agente de almacenamiento para utilizar SSL  
Para asegurarse de que los datos se cifran durante la comunicación entre el agente de almacenamiento y el servidor y el agente de almacenamiento y el cliente, configure los agentes de almacenamiento para la comunicación utilizando el protocolo SSL.
- Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL  
Para proteger los datos que se transmiten entre un cliente y un agente de almacenamiento, configure el cliente para conectarse al agente de almacenamiento mediante el protocolo SSL.

## Configuración del servidor para aceptar conexiones SSL

Configure el servidor para que acepte conexiones SSL antes de habilitar la comunicación SSL desde el servidor a un cliente, un agente de almacenamiento u otro servidor.

### Procedimiento

1. Especifique el puerto en el que el servidor espera comunicaciones de cliente habilitadas para SSL o acepte el número de puerto predeterminado. Opcionalmente, actualice el archivo `dsmserv.opt` en el directorio de instancia del servidor especificando la

opción TCPSPORT o TCPADMINPORT, o ambas. Se pueden utilizar las opciones SSLTCPSPORT y SSLTCPADMINPORT para conexiones SSL solamente.

2. Cree una base de datos de claves de servidor iniciando el servidor. El archivo de base de datos de claves de servidor, cert.kdb, se almacena en el directorio de instancia de servidor, y la etiqueta de certificado predeterminada se define automáticamente como "TSM Server SelfSigned SHA Key". El certificado se exporta al archivo cert256.arm.
3. Si utiliza el certificado autofirmado predeterminado, se requerirá el archivo de certificado autofirmado predeterminado (cert256.arm) cuando se conecte al servidor utilizando TLS.

4. Si está importando un certificado firmado por una entidad emisora de certificados, realice los siguientes pasos:

- a. Importe un certificado exclusivo firmado por una entidad emisora de certificados en cada servidor que habilite SSL. Puede importar un certificado firmado por CA intermediario o raíz. El mismo certificado firmado por CA se utiliza para todos los servidores. Inicie sesión en el sistema del servidor de IBM Spectrum Protect con el ID de usuario de instancia y emita el siguiente mandato de ejemplo desde el directorio de instancia:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -label "CA cert" -file ca.crt
```

- b. Para importar un certificado firmado por entidad emisora de certificados intermedio, emita el siguiente mandato de ejemplo:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed  
-label "Intermediate CA cert" -file intca.crt
```

- c. Se requerirán los certificados intermedio y raíz (ca.crt y intca.crt) cuando se conecte al servidor utilizando TLS.

- d. En el servidor, cree una solicitud de certificado para que lo firme la entidad emisora de certificados emitiendo un mandato similar al siguiente mandato:

```
gsk8capicmd_64 -certreq -create -db cert.kdb -stashed -label "CA cert"  
-sigalg sha256 -size 2048 -ku "digitalSignature,keyEncipherment,keyAgreement "  
-eku "clientAuth,serverAuth" -dn "CN=tucson.example.com,OU=Spectrum Protect,O=IBM"  
-san_dnsname tucson.example.com -san_ipaddr 9.11.0.0 -file cert_request.csr
```

- e. Para recibir el certificado firmado y convertirlo en el certificado predeterminado para la comunicación con los clientes, emita el siguiente mandato de ejemplo:

```
gsk8capicmd_64 -cert -receive -db cert.kdb -stashed -file cert_signed.crt  
-default_cert yes
```

5. Si realiza cambios, reinicie el servidor.

## Qué hacer a continuación

---

Habilite la comunicación SSL desde un cliente, un agente de almacenamiento u otro servidor a este servidor. Para completar las siguientes tareas, debe tener un certificado del servidor y el número de puerto que se define para el servidor.

1. Para habilitar la comunicación SSL desde un cliente a este servidor, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con Secure Sockets Layer.
2. Para habilitar la comunicación SSL desde otro servidor a este servidor, consulte Configuración del servidor para conectarse a otro servidor utilizando SSL.
3. Para habilitar la comunicación SSL desde un agente de almacenamiento a este servidor, consulte Configuración de un agente de almacenamiento para utilizar SSL.
4. Para habilitar la comunicación SSL desde el Centro de operaciones a este servidor, consulte Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL.

- Configuración de clientes para comunicarse con el servidor utilizando SSL  
Para asegurarse de que los datos se cifra durante la comunicación entre clientes y servidor, configure los clientes para la comunicación con el servidor utilizando el protocolo SSL.
- Configuración del servidor para conectarse a otro servidor utilizando SSL  
Para asegurarse de que los datos se cifran durante la comunicación de servidor a servidor, configure los servidores para la comunicación con servidores utilizando el protocolo SSL.
- Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL  
Para asegurarse de que los datos se cifran durante la comunicación entre el Centro de operaciones y el servidor, configure el Centro de operaciones para la comunicación con el servidor utilizando el protocolo SSL.

### Referencia relacionada:

TCPSPORT  
TCPADMINPORT  
QUERY SESSION (Consultar sesiones de cliente)

## Configuración de clientes para comunicarse con el servidor utilizando SSL

---

Para asegurarse de que los datos se cifra durante la comunicación entre clientes y servidor, configure los clientes para la comunicación con el servidor utilizando el protocolo SSL.

## Antes de empezar

---

Debe tener el certificado del servidor y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

## Procedimiento

---

Para habilitar la comunicación SSL entre el servidor y los clientes, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con Secure Sockets Layer.

## Configuración del servidor para conectarse a otro servidor utilizando SSL

---

Para asegurarse de que los datos se cifran durante la comunicación de servidor a servidor, configure los servidores para la comunicación con servidores utilizando el protocolo SSL.

## Antes de empezar

---

Debe tener el certificado y el número de puerto para el servidor al que se va a conectar. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

## Acerca de esta tarea

---

Consejo: Si ambos servidores utilizan el software IBM Spectrum Protect V8.1.2 o posterior, SSL se configura automáticamente. Se recomienda la configuración manual, aunque no es obligatoria. Si el servidor o el agente de almacenamiento están utilizando el software IBM Spectrum Protect de versión anterior a V8.1.2, deberá configurar SSL manualmente.

En el procedimiento, se utilizan las siguientes direcciones de servidor como ejemplos:

- ServerA (el servidor al que se conecta) está en `bfa.tucson.example.com`
- ServerB está en `bfb.tucson.example.com`

## Procedimiento

---

1. Cree una base de datos de claves de servidor iniciando el servidor. El archivo de base de datos de claves del servidor, `cert.kdb`, se almacena en el directorio de instancia del servidor.
2. Para cada servidor, importe los archivos de certificado de entidad emisora de certificados o `cert256.arm` del otro servidor:

```
gsk8capicmd 64 -cert -add -label server_ip_address -db cert.kdb -stashed  
-file cert256.arm
```

Consejo: Utilice la dirección IP del servidor como el nombre de la etiqueta.

3. En cada servidor, puede ver los certificados de la base de datos de claves con el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

4. Reinicie los servidores.
5. Emita el mandato DEFINE SERVER.
  - a. Para ServerA, emita el siguiente mandato:

```
DEFINE SERVER BFB hla=bfb.tucson.example.com lla=1542  
serverpa=passwordforbfb SSL=YES
```

- b. Para ServerB, emita el siguiente mandato:

```
DEFINE SERVER BFA hla=bfa.tucson.example.com lla=1542  
serverpa=passwordforbfa SSL=YES
```

### Referencia relacionada:

QUERY SESSION (Consultar sesiones de cliente)

TCPPORT

TCPADMINPORT

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

## Configuración del centro de operaciones para conectarse al servidor concentrador utilizando SSL

---

Para asegurarse de que los datos se cifran durante la comunicación entre el Centro de operaciones y el servidor, configure el Centro de operaciones para la comunicación con el servidor utilizando el protocolo SSL.

### Antes de empezar

---

Debe tener el certificado del servidor concentrador y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

### Procedimiento

---

Para configurar las comunicaciones SSL con el Centro de operaciones, consulte Protección de las comunicaciones entre el Centro de operaciones y el servidor concentrador.

## Configuración de un agente de almacenamiento para utilizar SSL

---

Para asegurarse de que los datos se cifran durante la comunicación entre el agente de almacenamiento y el servidor y el agente de almacenamiento y el cliente, configure los agentes de almacenamiento para la comunicación utilizando el protocolo SSL.

### Antes de empezar

---

Debe tener el certificado del servidor y el número de puerto que utiliza el servidor. Para obtener más información, consulte Configuración del servidor para aceptar conexiones SSL.

### Procedimiento

---

1. Inicialice el agente de almacenamiento y añada información de comunicación al archivo de configuración de dispositivo y al archivo de opciones del agente de almacenamiento `dsmsta.opt`, emitiendo el mandato `DSMSTA SETSTORAGESERVER`. Debe especificar los parámetros `SSL=YES` y `STAKEYDBPW=password` para crear el archivo de base de datos de claves en `dsmsta.opt`. Todas las contraseñas se cifran en `dsmsta.opt`.

```
dsmsta setstorageserver myname=storage_agent_name mypa=sta_password  
myhla=ip_address servername=server_name serverpa=server_password hla=ip_address lla=ssl_port  
STAKEYDBPW=password ssl=yes
```

2. Cree el certificado de la base de datos de claves y los certificados predeterminados iniciando el agente de almacenamiento.
3. Para el agente de almacenamiento y el servidor, importe los archivos de certificado de entidad emisora de certificados o `cert256.arm` de la otra parte:

```
gsk8capicmd 64 -cert -add -label ip_address -db cert.kdb -stashed  
-file cert256.arm
```

Consejo: Utilice la dirección IP como el nombre de la etiqueta.

4. Puede ver los certificados en la base de datos de claves emitiendo el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

5. Reinicie el agente de almacenamiento y el servidor.
6. Establezca la comunicación entre el servidor y el agente de almacenamiento, emitiendo el mandato siguiente:

```
define server sta hla=ip_address lla=port serverpa=password ssl=yes
```

#### Referencia relacionada:

QUERY SESSION (Consultar sesiones de cliente)

TCPPORT

TCPADMINPORT

DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

## Configuración del cliente para conectarse a un agente de almacenamiento utilizando SSL

---

Para proteger los datos que se transmiten entre un cliente y un agente de almacenamiento, configure el cliente para conectarse al agente de almacenamiento mediante el protocolo SSL.

## Antes de empezar

---

Debe tener el certificado y el número de puerto para el agente de almacenamiento.

## Acerca de esta tarea

---

Después de configurar un agente de almacenamiento para aceptar conexiones SSL, configure los clientes para que se conecten al agente de almacenamiento utilizando SSL.

## Procedimiento

---

Para habilitar la comunicación SSL entre los clientes y el agente de almacenamiento, consulte Configuración de la comunicación entre cliente y servidor de IBM Spectrum Protect con Secure Sockets Layer.

**Referencia relacionada:**

TCPPOPT

TCPADMINPORT

## Autenticación de los usuarios de IBM Spectrum Protect mediante un servidor LDAP

---

En un sistema IBM Spectrum Protect, los usuarios deben autenticarse en el servidor proporcionando un ID de usuario y contraseña. Si su organización utiliza un servidor LDAP (Lightweight Directory Access Protocol) para gestionar los ID de usuario, puede utilizar el servidor LDAP para autenticar los ID de usuario de IBM Spectrum Protect.

Puede utilizar uno de los siguientes métodos para autenticar a los usuarios con un servidor LDAP:

Método preferido para los servidores de IBM Spectrum Protect V7.1.7 y posteriores

Para utilizar este método, que a veces se conoce como *modo integrado*, los ID de usuarios deben registrarse en la base de datos de Active Directory en un servidor LDAP. A continuación, registre los mismos usuarios con el servidor de IBM Spectrum Protect. Cuando un ID de usuario registrado accede al servidor de IBM Spectrum Protect, se autentica las credenciales en la base de datos de Active Directory.

Para utilizar este método, siga las instrucciones de la sección Autenticación de los usuarios mediante una base de datos de Active Directory.

Método utilizado para los servidores anteriores a V7.1.7, y por los usuarios de IBM® Security Directory Server

Para utilizar este método, los ID de usuario deben estar registrados en una base de datos de Active Directory en un servidor LDAP. De forma alternativa, se pueden registrar los ID de usuario en una base de datos de IBM Security Directory Server (anteriormente IBM Tivoli Directory Server) de un servidor LDAP. Con este método, no puede utilizar las cuentas de usuario estándar registradas en el servidor LDAP. Debe crear cuentas de usuario separados que estén asociadas a una unidad organizativa específica. Para utilizar este método, siga las instrucciones de la sección Gestión de contraseñas y procedimientos de inicio de sesión (V7.1.1).

- Autenticación de los usuarios mediante una base de datos de Active Directory  
Puede autenticar a los usuarios de IBM Spectrum Protect mediante una base de datos de Active Directory en un servidor LDAP (Lightweight Directory Access Protocol). Con este método, utilice las cuentas de usuario estándar registradas en el servidor LDAP. Se puede utilizar el mismo ID de usuario para la autenticación en el servidor de IBM Spectrum Protect y en el servidor LDAP.

## Réplica de datos de cliente en otro servidor

---

El hecho de realizar una réplica de los datos de cliente de un servidor de origen en otro servidor ayuda a garantizar que los datos de cliente copiados están disponibles para su recuperación si el servidor de origen resulta dañado. La réplica realiza una copia incremental de los datos del servidor de origen en el servidor de destino para proporcionar capacidad de migración y recuperación.

## Acerca de esta tarea

---

Si se produce un siniestro y el servidor de origen no está disponible temporalmente, los nodos de cliente pueden recuperar los datos del servidor de destino. Si no se puede recuperar el servidor de origen, puede cambiar las configuraciones de los nodos de cliente para almacenar los datos en el servidor de destino. Cuando se produce una parada, el servidor de origen puede migrar los datos automáticamente a un servidor de destino para la recuperación de datos.

Restricción: Un servidor solo puede replicar datos en un servidor de destino.

Puede replicar los datos que se almacenan en cualquier tipo de agrupación de almacenamiento. El tipo de agrupación de almacenamiento puede ser diferente en el servidor de réplica de origen y el servidor de réplica de destino. Puede controlar la réplica por tipo de datos del nodo de cliente:

- Datos de copia de seguridad activos e inactivos juntos o sólo datos de copia de seguridad activos
- Datos de archivado
- Datos migrados al servidor de origen por clientes de IBM Spectrum Protect for Space Management

Cuando replique datos de agrupaciones de almacenamiento de contenedores de directorios, utilice la protección de la agrupación de almacenamiento para mejorar la eficacia del proceso de réplica y para habilitar la reparación de datos. Cuando utilice el Centro de operaciones para configurar las agrupaciones de almacenamiento, las planificaciones de protección se definen automáticamente de modo que se coordinen con la planificación de la réplica.

## Procedimiento

1. Compruebe que los servidores sean compatibles y tengan los recursos del sistema necesarios para utilizar con éxito la réplica.

Se necesita una mayor cantidad de núcleos de procesador y memoria. La base de datos y sus registros deben tener el tamaño adecuado para garantizar que las transacciones se pueden completar. Se necesita una red dedicada, con el ancho de banda suficiente como para gestionar los datos que se van a replicar.

- a. Verifique de que los servidores de origen y destino son compatibles para la réplica. Consulte el apartado Compatibilidad de réplica.
  - b. Verifique que el servidor tiene los recursos adecuados para obtener un buen rendimiento. Para obtener más información, consulte el apartado Lista de comprobación para la réplica de nodos.
2. Habilite la réplica. Consulte el apartado Habilitación de la réplica de nodo.
  3. Planifique la réplica para el servidor de origen. Para obtener información sobre cómo integrar esta planificación en las planificaciones habituales de mantenimiento del servidor, consulte el apartado Definición de planificaciones para actividades de mantenimiento del servidor.
  4. Planifique la protección de la agrupación de almacenamiento para todas las agrupaciones de almacenamiento de contenedores de directorios en el servidor de origen. Consulte el apartado Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio.
  5. Supervise la réplica mediante el Centro de operaciones. Para obtener más información, consulte el apartado Lista de comprobación de supervisión diaria.

- **Compatibilidad de réplica**  
Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino sean compatibles para la réplica.
- **Habilitación de la réplica de nodo**  
Puede habilitar la réplica de nodo para proteger los datos.
- **Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio**  
Proteja los datos de las agrupaciones de almacenamiento de contenedores de directorio para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedores de directorio.
- **Modificación de los valores de réplica**  
Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.
- **Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino**  
Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

## Compatibilidad de réplica

Antes de configurar operaciones de réplica con IBM Spectrum Protect, debe asegurarse de que los servidores de réplica de origen y destino sean compatibles para la réplica.

Tabla 1. Compatibilidad de réplica de versiones de servidor

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V6.3.0 - V6.3.2	V6.3.0 - V6.3.2
V6.3.3	V6.3.3 o niveles posteriores de V6.3
V6.3.4 o niveles posteriores de V6.3	V6.3.4 o posterior
V7.1	V7.1 o posterior

Versión del servidor de réplica de origen	Versiones compatibles para el servidor de réplica de destino
V7.1.1	V7.1 o posterior
V7.1.3	V7.1.3 o posterior
V7.1.4	V7.1.3 o posterior
V7.1.5	V7.1.3 o posterior
V7.1.6	V7.1.3 o posterior
V7.1.7	V7.1.3 o posterior
V8.1	V7.1.3 o posterior
V8.1.1	V7.1.3 o posterior
V8.1.2	V7.1.3 o posterior

## Habilitación de la réplica de nodo

Puede habilitar la réplica de nodo para proteger los datos.

### Antes de empezar

Asegúrese de que los servidores de origen y destino son compatibles para la réplica.

### Acerca de esta tarea

Replique el nodo de cliente para replicar todos los datos de cliente, incluyendo metadatos. De forma predeterminada, la réplica de nodo está inhabilitada cuando se inicia el servidor por primera vez.

Sugerencias:

- Para reducir el tiempo de proceso de réplica, proteja la agrupación de almacenamiento antes de replicar los nodos de cliente. Cuando se inicia la réplica de nodo, las extensiones de datos que ya se han replicado a través de la protección de agrupación de almacenamiento se omiten.
- La réplica requiere gran cantidad de memoria y ancho de banda suficiente para completar el proceso. Cambie el tamaño de la base de datos y sus registros para garantizar que las transacciones se pueden completar.


### Procedimiento

Para habilitar la réplica de nodo, complete los siguientes pasos en Centro de operaciones:

- En la página Servidores, pulse Detalles.
- En la página Detalles, pulse Propiedades.
- En la sección Réplica, seleccione Habilitada en el campo Réplica de salida.
- Pulse Guardar.

### Qué hacer a continuación

Realice las acciones siguientes:

- Para verificar que la réplica es correcta, revise el apartado Lista de comprobación de supervisión diaria.
-  Sistemas operativos Linux Si el servidor IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Siga las instrucciones del apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

## Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio

Proteja los datos de las agrupaciones de almacenamiento de contenedores de directorio para reducir el tiempo de réplica de nodo y para habilitar la reparación de datos en agrupaciones de almacenamiento de contenedores de directorio.

### Antes de empezar



Asegúrese de que exista al menos una agrupación de contenedores en directorios en el servidor de réplica de destino. Cuando habilita la réplica en el Centro de operaciones, puede planificar la protección de agrupación de almacenamiento. Para configurar la réplica y habilitar la protección de agrupación de almacenamiento, complete los siguientes pasos:

1. En la barra de menús de Centro de operaciones, pase el ratón por encima de Almacenamiento y pulse Réplica.
2. En la página Réplica, pulse Par de servidores.
3. Complete los pasos del asistente Añadir par de servidores.

## Acerca de esta tarea

---

La protección de una agrupación de almacenamiento de contenedores de directorio hace copias de seguridad de extensiones en otra agrupación de almacenamiento y puede mejorar el rendimiento de la réplica de nodos. Cuando se inicia la réplica de nodo, se omiten las extensiones de datos de las que ya se han hecho copias de seguridad a través de la protección de la agrupación de almacenamiento, lo cual reduce el tiempo de proceso de la réplica. Puede planificar la protección de agrupaciones de almacenamiento varias veces al día para estar al día con los cambios realizados en los datos.

Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor. Debe utilizar agrupaciones de almacenamiento de contenedores de directorios si solo desea proteger y realizar la copia de seguridad de la agrupación de almacenamiento.

Estrategia de protección alternativa: Como alternativa al uso de la réplica, puede proteger los datos en agrupaciones de almacenamiento de contenedores de directorios copiando los datos en las agrupaciones de almacenamiento de copia de contenedor. Los datos de las agrupaciones de almacenamiento de copia de contenedor se almacenan en volúmenes de cinta. Las copias de cinta que se almacenan fuera del local proporcionan protección adicional de recuperación ante siniestro en un entorno replicado.

## Procedimiento

---

1. Como alternativa para habilitar la protección de agrupación de almacenamiento, puede utilizar el mandato PROTECT STGPOOL desde el servidor de origen para realizar la copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedores de directorios. Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio denominada POOL1, emita el siguiente mandato:

```
protect stgpool pool1
```

Como parte de la operación del mandato PROTECT STGPOOL, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato AUDIT CONTAINER podría identificar daños en la agrupación de almacenamiento de destino antes de que se emita el mandato PROTECT STGPOOL.

2. Opcional: Si las extensiones dañadas se han reparado en la agrupación de almacenamiento de destino y protege varias agrupaciones de almacenamiento de origen en una agrupación de almacenamiento de destino, siga los pasos siguientes para garantizar una reparación completa:
  - a. Emita el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen para reparar el máximo daño posible.
  - b. Vuelva a emitir el mandato PROTECT STGPOOL para todas las agrupaciones de almacenamiento de origen. Para esta segunda operación, utilice el parámetro FORCERECONCILE=YES. Este paso garantiza que las reparaciones de otras agrupaciones de origen se reconocen correctamente para todas las agrupaciones de almacenamiento de origen.

## Resultados

---


Si una agrupación de almacenamiento de contenedores de directorios está protegida, puede reparar la agrupación de almacenamiento si se producen daños mediante el mandato REPAIR STGPOOL.

Restricción: Si replica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorio, no puede reparar la agrupación de almacenamiento.

## Qué hacer a continuación

---

Realice las acciones siguientes:

1. Para ver el estado de la carga de trabajo de la operación de réplica, siga las instrucciones del apartado Lista de comprobación de supervisión diaria.
2.  Sistemas operativos Linux Si el servidor IBM Spectrum Protect replica nodos en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Siga las instrucciones del apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

**Tareas relacionadas:**

➡ Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta

**Referencia relacionada:**

➡ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

➡ PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)

## Modificación de los valores de réplica

Modificación de los valores de réplica en Centro de operaciones. Cambie valores como el número de sesiones de réplica, reglas de réplica, los datos que desea replicar, la planificación de réplica y la carga de trabajo de réplica.

### Acerca de esta tarea

Es posible que tenga que personalizar los valores de réplica en los siguientes escenarios:

- Cambios en las prioridades de datos
- Cambios en las reglas de réplica
- Requisito para que otro servidor sea el servidor de destino
- Procesos planificados que afectan de forma negativa al rendimiento de servidor

### Procedimiento

Utilice el Centro de operaciones para modificar valores de réplica.

Tarea	Procedimiento
Cambiar una regla de réplica.	a. En la página Servidores, pulse Detalles. b. En la página Detalles, pulse Propiedades. c. En la sección Réplica, elija la regla de réplica que desea aplicar: Regla de archivado predeterminada, Regla de copia de seguridad predeterminada o Regla de gestión de espacio predeterminada. d. Pulse Guardar.
Especifique el tiempo que se retienen los registros de réplica.	a. En la página Servidores, pulse Detalles. b. En la página Detalles, pulse Propiedades. c. En la sección Réplica, entre el número de días que deben retenerse los registros de réplica en el campo Retener historial de réplica. Sino, seleccione la casilla de verificación No retener si no necesita registros de réplica. d. Pulse Guardar.
Especifique un servidor de réplica de destino.	a. En la página Servidores, pulse Detalles. b. En la página Detalles, pulse Propiedades. c. En la sección Réplica, especifique el servidor de destino. d. Pulse Guardar.
Cancele un proceso de réplica.	a. En la página Servidores, pulse Tareas activas. b. Seleccione el proceso o sección que desea cancelar. c. Pulse Cancelar.

## Establecimiento de políticas de retención diferentes para el servidor de origen y el servidor de destino

Puede establecer políticas en el servidor de réplica de destino que gestionan los datos del nodo de cliente replicado de forma diferente que en el servidor de origen. Por ejemplo, puede mantener un número de versiones de archivos distinto en los servidores de origen y de destino.

### Procedimiento

1. Desde el servidor de réplica de origen, valide la configuración de la réplica y verifique que el servidor de réplica de origen se puede comunicar con el servidor de réplica de destino mediante el mandato VALIDATE REPLICATION. Por ejemplo, valide la

configuración utilizando el nombre de un nodo de cliente que se está replicado:

```
validate replication node1 verifyconnection=yes
```

2. Desde el servidor de réplica de origen, emita el mandato VALIDATE REPLPOLICY para revisar las diferencias entre las políticas en los servidores de réplica de origen y de destino. Por ejemplo, para mostrar las diferencias entre las políticas en el servidor de origen y el servidor de destino, CVT\_SRV2, emita el mandato siguiente desde el servidor de origen:

```
validate replpolicy cvt_srv2
```

3. Actualice las políticas en el servidor de destino, si es necesario.

Consejo: Puede utilizar el Centro de operaciones para modificar las políticas en el servidor de destino. Siga las instrucciones de la sección Edición de políticas.

Por ejemplo, para mantener versiones inactivas de archivos durante un periodo de tiempo más corto en el servidor de destino que en el servidor de origen, reduzca el valor de Copias de seguridad en las clases de gestión que se aplican a datos de cliente replicados.





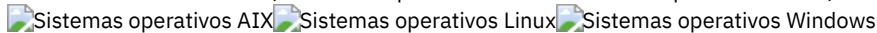

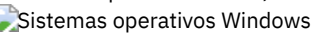
4. Permita al servidor de réplica de destino utilizar sus políticas para gestionar los datos del nodo de cliente replicado emitiendo el mandato SET DISSIMILARPOLICIES en el servidor de origen. Por ejemplo, para habilitar las políticas en el servidor de réplica de destino, CVT\_SRV2, emita el mandato siguiente en el servidor de origen:

```
set dissimilarpolicies cvt_srv2 on
```

La próxima vez que se ejecuta el proceso de réplica, se utilizarán las políticas del servidor de réplica de destino para gestionar los datos del nodo del cliente replicado.

Consejo: Si configura la réplica utilizando el Centro de operaciones y las políticas en los servidores de réplica de origen y destino no coinciden, se aplica la política que se ha especificado para el servidor de réplica de origen. Si ha habilitado las políticas en el servidor de réplica de destino utilizando el mandato SET DISSIMILARPOLICIES, se utiliza la política especificada para el servidor de réplica de destino. Si el servidor de réplica de destino no tiene la política que utiliza el nodo en servidor de réplica de origen, se utiliza la política STANDARD.

#### Referencia relacionada:

-  EXPORT POLICY (Exportar información de políticas)
-  SET DISSIMILARPOLICIES (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)
-  VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)
-  VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Configuración de entornos en clúster

---




Puede configurar el servidor de IBM Spectrum Protect para la agrupación en clúster en sistemas AIX, Linux o Windows.

Puede utilizar un entorno de clúster para los siguientes sistemas operativos:

- IBM® PowerHA SystemMirror para AIX
- IBM Tivoli System Automation for Multiplatforms para AIX y Linux
- Microsoft Failover Cluster para Windows

Puede utilizar otros productos de clúster con IBM Spectrum Protect, aunque no hay documentación disponible y el soporte está limitado. Para obtener la información más reciente sobre el soporte para entornos en clúster, consulte <http://www.ibm.com/support/docview.wss?uid=swg21609772>.




Antes de utilizar otro producto de clúster, verifique que DB2 dé soporte a los sistemas de archivos necesarios. Para obtener más información sobre el nivel de DB2 que está utilizando, consulte la Información del producto DB2 y busque los sistemas de archivos recomendados.

- Visión general del entorno en clúster  
Los *clústeres* están formados por distintos componentes como, por ejemplo, servidores de IBM Spectrum Protect, hardware y software. Puede utilizar la agrupación en clúster para unir dos o más servidores o nodos utilizando un subsistema de disco compartido.
-  Sistemas operativos AIX Configuración de un entorno de AIX para agrupación en clúster  
Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM PowerHA SystemMirror for AIX o IBM Tivoli System Automation for Multiplatforms.
-  Sistemas operativos Linux Configuración de un entorno de Linux para agrupación en clúster  
Puede configurar el servidor Linux de IBM Spectrum Protect en un entorno en clúster utilizando IBM Tivoli System Automation for Multiplatforms Versión 3.2.2.
-  Sistemas operativos Windows Configuración de un entorno en clúster de Windows  
Puede configurar un servidor de IBM Spectrum Protect para Windows en un entorno de clúster de migración tras error de

Microsoft. Los entornos de clúster de Windows están formados por componentes como, por ejemplo, servidores IBM Spectrum Protect, hardware y software. Si estos componentes están conectados al mismo sistema de disco el tiempo de inactividad se minimiza.

#### Información relacionada:

Actualización del servidor en un entorno en clúster

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Visión general del entorno en clúster

---

Los *clústeres* están formados por distintos componentes como, por ejemplo, servidores de IBM Spectrum Protect, hardware y software. Puede utilizar la agrupación en clúster para unir dos o más servidores o nodos utilizando un subsistema de disco compartido.

Esta configuración proporciona a los nodos la capacidad de compartir datos, lo que permite una mayor disponibilidad del servidor y minimiza el tiempo de inactividad. Por ejemplo:


- Puede configurar, supervisar y controlar las aplicaciones y los componentes de hardware que se despliegan en un clúster.
- Puede utilizar una interfaz de clúster de administrador y IBM Spectrum Protect para designar organizaciones de clústeres y definir el patrón de recuperación de errores. El servidor forma parte del clúster, lo que proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.
- Puede aplicar la agrupación en clúster al proceso de réplica de nodo. De esta forma, la disponibilidad del servidor es mayor de lo que debería si se utiliza la réplica de nodo como un proceso por sí mismo. La capacidad del servidor es mayor porque es menos probable que un cliente migre tras error a otro servidor en un entorno en clúster. Si replica datos desde varios servidores de réplica fuente a un servidor de réplica de destino, hay una alta dependencia en el servidor de réplica de destino. Un entorno en clúster facilita la dependencia en el servidor de réplica de destino.

Los componentes de un clúster de servidores se denominan *objetos de clúster*. Los objetos de clúster se asocian con un conjunto de propiedades que tienen valores de datos que describen la identidad y el comportamiento de un objeto en el clúster. Los objetos de clúster pueden incluir los componentes siguientes:

- Nodos
- Almacenamiento
- Servicios y aplicaciones
- Redes

Puede gestionar los objetos de clúster mediante la manipulación de sus propiedades, normalmente, a través de una aplicación de gestión de clústeres.

- Nodos de clúster  
Los nodos de un clúster tienen características similares, lo que les permite trabajar conjuntamente.

 Sistemas operativos AIX

## Configuración de un entorno de AIX para agrupación en clúster

---











Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM® PowerHA SystemMirror for AIX o IBM Tivoli System Automation for Multiplatforms.


PowerHA SystemMirror for AIX y Tivoli System Automation detectan anomalías del sistema y gestionan la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario final. Puede configurar el servidor de IBM Spectrum Protect en un sistema PowerHA o en un clúster de Tivoli System Automation. A continuación, si el sistema falla, el servidor de IBM Spectrum Protect puede iniciarse en otro sistema del clúster.

Tanto en la migración tras error como el restablecimiento, parece que el servidor de IBM Spectrum Protect se detiene y, a continuación, se reinicia. Cualquier transacción que estuviera en curso en el momento del restablecimiento o de la recuperación tras error se retrotrae y todas las transacciones completas siguen estando completas. Los clientes de IBM Spectrum Protect interpretan esto como una anomalía de comunicación e intentan restablecer las conexiones.

Consulte la siguiente información para obtener más detalles sobre estas opciones de agrupación en clúster.

- Configure IBM Spectrum Protect para AIX para utilizar IBM PowerHA SystemMirror for AIX en un entorno en clúster revisando los temas siguientes.
- Configure IBM Spectrum Protect for AIX para utilizar Tivoli System Automation en un entorno de agrupación en clúster revisando la información de <http://www.ibm.com/support/docview.wss?uid=swg27039780>.
- Obtenga más información acerca de Información sobre el producto PowerHA SystemMirror.

- 
**Sistemas operativos AIX Requisitos de un clúster de PowerHA**  
 IBM PowerHA SystemMirror para AIX detecta los errores del sistema y gestiona la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario.
- 
**Sistemas operativos AIX Recuperación de errores y restablecimiento de PowerHA**  
 Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.
- 
**Sistemas operativos AIX Instalación y configuración de PowerHA SystemMirror para AIX**  
 Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM PowerHA tm trademark="SystemMirror" tmttype="reg">SystemMirror para AIX.
- 
**Sistemas operativos AIX Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA**  
 Instale el servidor de IBM Spectrum Protect en un nodo de producción para PowerHA para poder configurar el servidor para la agrupación en clúster.
- 
**Sistemas operativos AIX Instalación del cliente de IBM Spectrum Protect en un nodo de producción para PowerHA**  
 Sólo es necesario instalar el conjunto de archivos del cliente de archivado y copia de seguridad, que contiene los archivos del cliente de archivado y copia de seguridad y el cliente de línea de mandatos administrativos.
- 
**Sistemas operativos AIX Verificación de la configuración del servidor de IBM Spectrum Protect para PowerHA**  
 Cuando haya configurado el servidor de IBM Spectrum Protect para utilizar PowerHA, debe verificar la configuración.
- 
**Sistemas operativos AIX Configuración del nodo de espera para PowerHA**  
 Para PowerHA, asegúrese de que el servidor de IBM Spectrum Protect no se esté ejecutando en el nodo de producción antes de configurar el nodo de espera.
- 
**Sistemas operativos AIX Definición de los dispositivos de almacenamiento de medios extraíbles en AIX para PowerHA**  
 En un sistema operativo AIX, debe definir los dispositivos de almacenamiento de medios extraíbles que utiliza IBM Spectrum Protect en los nodos de producción y espera. El gestor de bibliotecas comprueba que el cartucho que contiene el dispositivo de almacenamiento de soportes extraíble de la unidad está en la unidad correcta.
- 
**Sistemas operativos AIX Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect**  
 Actualice la configuración del gestor del clúster para definir el servidor de IBM Spectrum Protect como una aplicación y un recurso de recuperación de errores del nodo en espera. Esta aplicación es propiedad del nodo de producción.
- 
**Sistemas operativos AIX Resolución de problemas del entorno en clúster de PowerHA**  
 Revise la siguiente lista para obtener información sobre la resolución de problemas habituales. La información que se proporciona para IBM PowerHA SystemMirror para AIX no representa todos los casos posibles.

 Sistemas operativos AIX

## Requisitos de un clúster de PowerHA


---

IBM PowerHA SystemMirror para AIX detecta los errores del sistema y gestiona la recuperación de errores en un procesador de recuperación con una pérdida mínima de tiempo del usuario.

Los requisitos de hardware siguientes son para configurar el servidor de IBM Spectrum Protect:

- Una configuración de hardware que sea adecuada para PowerHA. Los dispositivos de almacenamiento de medios extraíbles del servidor de IBM Spectrum Protect deben estar conectados físicamente a al menos dos nodos del clúster de PowerHA en un bus compartido (incluida una SAN).
- Suficiente espacio de disco compartido para contener la base de datos de IBM Spectrum Protect, las anotaciones de recuperación, el directorio de instancia y las agrupaciones de almacenamiento de disco que se van a utilizar. Consulte Gestión de la capacidad de inventario para determinar cuánto espacio se requiere para el registro de base de datos y recuperación, y para garantizar la disponibilidad del registro de base de datos y recuperación.
- Una red TCP/IP.

Consejo: Si un servidor de IBM Spectrum Protect gestiona dispositivos de almacenamiento de medios extraíbles, puede configurar dos servidores de IBM Spectrum Protect para que se ejecuten en sistemas diferentes en un clúster de PowerHA. Cada sistema puede ejecutar ambos servidores si el otro sistema falla. Para configurar dos servidores de IBM Spectrum Protect para que se ejecuten en sistemas diferentes en un clúster de PowerHA, utilice otro sistema de archivos que sea accesible para ambos servidores.

 Sistemas operativos AIX

## Recuperación de errores y restablecimiento de PowerHA

---

Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.

Los términos *nodo de producción* y *nodo de espera* hacen referencia a los dos nodos PowerHA en los que se ejecuta el servidor de IBM Spectrum Protect.


PowerHA gestiona el control de la dirección TCP/IP y el montaje del sistema de archivos compartidos en el nodo de espera o el nodo de producción, según corresponda.

Cuando se produce una *migración tras error o restablecimiento*, se retrotraen todas las transacciones que se estaban procesando en ese momento. Para los clientes de IBM Spectrum Protect, la *migración tras error* o el *restablecimiento* representan un error en las comunicaciones. Por lo tanto, debe restablecer una conexión basada en los valores de las opciones COMMRESTARTDURATION y COMMRESTARTINTERVAL.

Por lo general, puede reiniciar el cliente de copia de seguridad/archivado desde la última transacción validada. Si se está ejecutando una planificación de cliente cuando se produce la *migración tras error*, es probable que la operación del cliente falle. Si puede reiniciar las operaciones de cliente, debe reiniciarlas desde el inicio del proceso. Las operaciones de clientes y de agente se completan como hacen normalmente si el servidor se ha detenido y reiniciado mientras estaban conectadas. La única diferencia es que el servidor se reinicia físicamente en un hardware diferente.

Si no desea que se produzca un *restablecimiento* automático, puede configurar el recurso como un grupo de recursos en cascada sin *restablecimiento*.





#### Información relacionada:


 Información sobre el producto PowerHA SystemMirror

## Instalación y configuración de PowerHA SystemMirror para AIX

---

Puede configurar el servidor de IBM Spectrum Protect para entornos en clúster de AIX utilizando IBM® PowerHA tm trademark="SystemMirror" tmttype="reg">SystemMirror para AIX.

-  Sistemas operativos AIX Instalación y configuración del clúster de PowerHA  
Puede experimentar errores de proceso si la instalación y la configuración de IBM PowerHA SystemMirror para AIX no se realizan correctamente.
-  Sistemas operativos AIX Configuración del servidor de IBM Spectrum Protect en el nodo primario para PowerHA  
Puede configurar una instancia de servidor IBM Spectrum Protect en el nodo primario.
-  Sistemas operativos AIX Configuración de servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia compartida de DB2  
Si el directorio de instancia de DB2 se comparte entre los nodos del clúster de PowerHA, no necesita crear una instancia de DB2 en el nodo secundario. No ejecute el asistente dsmsicfgx.
-  Sistemas operativos AIX Configuración del servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia de DB2 separada  
Debe crear una instancia de DB2 en cada nodo secundario si el directorio de instancia de DB2, /home/tsminst1/sqllib, no está compartido entre los nodos en el clúster de PowerHA.

 Sistemas operativos AIX

## Instalación y configuración del clúster de PowerHA

---

Puede experimentar errores de proceso si la instalación y la configuración de IBM PowerHA SystemMirror para AIX no se realizan correctamente.

### Procedimiento

---


Siga estos pasos para instalar y configurar el clúster de PowerHA:

1. Defina los sistemas de archivos compartidos y los volúmenes lógicos, cuando sea necesario. Si lo desea, puede colocar los archivos en sistemas de archivos independientes o en discos físicos independientes por motivos de integridad o rendimiento. No ponga el directorio de inicio de la instancia de usuario en un disco compartido. Duplique los volúmenes lógicos para ofrecer la máxima disponibilidad (incluidos los sistemas de archivos subyacentes). Los sistemas de archivos que deben definirse incluyen el directorio de instancia de servidor de IBM Spectrum Protect, los directorios de registro y de base de datos, todos los directorios de agrupación de almacenamiento de disco y los directorios de agrupación de almacenamiento de tipo de dispositivo FILE.
2. Configure PowerHA para que el nodo de producción sea el propietario de los grupos de volúmenes compartidos y el nodo en espera se encargue de los grupos de volúmenes compartidos si el nodo de producción falla.
3. Configure PowerHA para la recuperación de errores de los sistemas de archivos.
4. Configure una dirección IP de servicio para el servidor de IBM Spectrum Protect. La dirección IP de servicio debe ser distinta de la dirección IP de cada host. La IP de servicio se mueve de un host a otro, no la dirección IP de host real.

5. Realice la recuperación de errores de la base de datos compartida y los directorios de anotaciones y de instancias en el nodo en espera del clúster de PowerHA.

## Resultados

Debe configurar los dispositivos de almacenamiento de medios extraíbles para la recuperación de errores y definir el servidor de IBM Spectrum Protect como una aplicación en PowerHA.

 Sistemas operativos AIX

## Configuración del servidor de IBM Spectrum Protect en el nodo primario para PowerHA


Puede configurar una instancia de servidor IBM Spectrum Protect en el nodo primario.

### Procedimiento

1. Revise los temas en la información de configuración del servidor de IBM Spectrum Protect.
2. Después de configurar la instancia del servidor de IBM Spectrum Protect en el nodo primario, puede configurar el servidor de IBM Spectrum Protect en un nodo secundario.

#### Tareas relacionadas:

Configuración de la instancia del servidor de IBM Spectrum Protect

 Sistemas operativos AIX

## Configuración de servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia compartida de DB2

Si el directorio de instancia de DB2 se comparte entre los nodos del clúster de PowerHA, no necesita crear una instancia de DB2 en el nodo secundario. No ejecute el asistente dsmsicfgx.

### Procedimiento

Para configurar una instancia de servidor en el nodo secundario con una instancia de DB2 compartida, siga los siguientes pasos:

1. En cada nodo del clúster, añada el siguiente texto para el script `/opt/tivoli/tsm/server/bin/rc.dsmserv`:

```
DB2NODES_TEMP='/tmp/db2nodes.tmp'
DB2NODES=${homeDir}/sqllib/db2nodes.cfg
# Current hostname
HOSTNAME=$(/bin/hostname)
# hostname saved in db2nodes.cfg
DB2_HOST=$(cat $DB2NODES | cut -d ' ' -f 2)
# if they are different update the file
if [[ "$HOSTNAME" != "$DB2_HOST" ]]
then
  echo "Updating hostname in db2nodes.cfg"
  sed -e s_${DB2_HOST}_${HOSTNAME}_g $DB2NODES > $DB2NODES_TEMP
  cp $DB2NODES_TEMP $DB2NODES
fi
```

Consejo: Si el texto no se incluye en el script puede incluirlo antes de emitir mandatos de `/opt/tivoli/tsm/server/bin/rc.dsmserv`.

2. Traslade todos los recursos compartidos al nodo secundario.
3. Actualice las siguientes variables en el script `/opt/tivoli/tsm/server/bin/startserver`, utilizando los siguientes valores:

Tabla 1. Variables en el script `/opt/tivoli/tsm/server/bin/startserver`

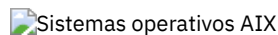
Descripción	Variabl e	Ejemplo
Defina INST_USER en el ID de usuario de instancia.	INST_U SER	INST_USER='tsmuser1'
Defina INST_DIR como la ubicación del directorio de instancia de IBM Spectrum Protect. Este directorio contiene dsmserv.dbid y dsmserv.opt.	INST_DI R	INST_DIR='/home/tsmu ser1/tsminst1'

Descripción	Variabl e	Ejemplo
Seleccione una de las siguientes opciones de inicio:  Opción 1: utilice la instancia \$INST_USER pero ejecute el servidor como raíz (-U)  Opción 2: utilice la instancia \$INST_USER y ejecute el servidor como \$INST_USER (-u)	INST_O PTION	Opción 1:  INST_OPTION='-U \$INST_USER'  Opción 2:  INST_OPTION='-u \$INST_USER'

4. Inicie el servidor emitiendo el script siguiente:

```
/opt/tivoli/tsm/server/bin/startserver
```

5. Cuando se inicie el servidor, emita el mandato BACKUP DB para verificar que se ha realizado la copia de seguridad de los datos correctamente.



## Configuración del servidor de IBM Spectrum Protect en un nodo secundario para PowerHA con una instancia de DB2 separada

Debe crear una instancia de DB2 en cada nodo secundario si el directorio de instancia de DB2, /home/tsminst1/sqllib, no está compartido entre los nodos en el clúster de PowerHA.

### Acerca de esta tarea

Puede configurar el servidor de IBM Spectrum Protect en un nodo secundario utilizando el asistente de dsmsicfgx o de forma manual.

### Procedimiento

- Para crear una instancia de DB2 en un nodo secundario utilizando el asistente de dsmsicfgx, siga estos pasos:
  - Ejecute el asistente de dsmsicfgx.
  - Desde el panel de Directorio de instancia, seleccione la casilla de verificación Seleccionar esto si está configurando la instancia del servidor en un nodo secundario de un clúster de alta disponibilidad.
- Para crear una instancia de DB2 en un nodo secundario de forma manual, siga estos pasos:
  - Traslade todos los recursos compartidos al nodo secundario.
  - Cree una instancia de DB2 emitiendo el siguiente mandato db2icrt:

```
/opt/tivoli/tsm/db2/instance/db2icrt -s ese -u instance_user instance_user
```

donde *instance\_user* es el mismo usuario que posee la instancia de DB2 en el nodo primario.

- Cuando se cree la instancia de DB2, inicie sesión como el usuario de la instancia o emita el mandato su:

```
su - <instance_user>
```

- Como usuario de instancia, emita los siguientes mandatos:

```
db2start
db2 update dbm cfg using DFTDBPATH shared_db_path
db2 catalog db TSMDB1
db2stop
```

donde *shared\_db\_path* es el directorio de base de datos compartido. El directorio de base de datos compartidos es normalmente el directorio de instancia del servidor.

Consejo: Para determinar el valor *shared\_db\_path*, emita el siguiente mandato en el nodo primario:

```
db2 get dbm cfg | grep DFTDBPATH
```

- Actualice las siguientes variables en el script /opt/tivoli/tsm/server/bin/startserver, utilizando los siguientes valores:

Tabla 1. Variables en el script /opt/tivoli/tsm/server/bin/startserver

Descripción	Variabl e	Ejemplo
-------------	--------------	---------

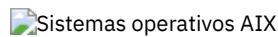


Descripción	Variabl e	Ejemplo
Defina INST_USER en el ID de usuario de instancia.	INST_U SER	INST_USER='tsmuser1 '
Defina INST_DIR como la ubicación del directorio de instancia de IBM Spectrum Protect. Este directorio contiene dsmserv.dbid y dsmserv.opt.	INST_D IR	INST_DIR='/home/tsm user1/tsminst1'
Seleccione una de las siguientes opciones de inicio:  Opción 1: utilice la instancia \$INST_USER pero ejecute el servidor como raíz (-U)  Opción 2: utilice la instancia \$INST_USER y ejecute el servidor como \$INST_USER (-u)	INST_O PTION	Opción 1: INST_OPTION='-U \$INST_USER'  Opción 2: INST_OPTION='-u \$INST_USER'

6. Inicie el servidor emitiendo el script siguiente:

```
/opt/tivoli/tsm/server/bin/startserver
```

7. Cuando se inicie el servidor, emita el mandato BACKUP DB para verificar que se ha realizado la copia de seguridad de los datos correctamente.



Sistemas operativos AIX

## Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA

Instale el servidor de IBM Spectrum Protect en un nodo de producción para PowerHA para poder configurar el servidor para la agrupación en clúster.

### Procedimiento

Complete los pasos siguientes para instalar el servidor de IBM Spectrum Protect en el nodo de producción:

1. Instale IBM Spectrum Protect. Seleccione uno de los siguientes componentes:
  - o El servidor de IBM Spectrum Protect
  - o El controlador de dispositivo de IBM Spectrum Protect, si es necesario
  - o La licencia de IBM Spectrum Protect

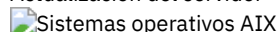
Los archivos ejecutables se instalan normalmente en los discos internos del nodo de producción, no en el espacio de discos de IBM Spectrum Protect compartido. Los archivos ejecutables del servidor de IBM Spectrum Protect se instalan en el directorio /opt/tivoli/tsm/server/bin.

2. Configure IBM Spectrum Protect para utilizar el método de comunicación TCP/IP. Para obtener instrucciones, consulte la información sobre la configuración de una instancia de servidor en AIX: Realización de los primeros pasos después de instalar IBM Spectrum Protect.
3. Defina un nuevo ID de usuario para que sea el propietario de la instancia de servidor de IBM Spectrum Protect o utilice un ID de usuario existente que aún no sea propietario de una instancia de IBM Spectrum Protect. Con la sesión iniciada con el ID de usuario de la instancia, siga estos pasos:
  - a. Crear un directorio de instancia utilizando el mandato mkdir en un sistema de archivos compartidos que puede migrar tras error al sistema en espera. Este disco debe definirse en PowerHA.
  - b. Crear la base de datos y directorios de registro mediante la utilización del mandato mkdir en sistemas de archivos compartidos que se puedan migrar tras error al sistema en espera. Estos discos también deben definirse en PowerHA para la recuperación de errores.
  - c. Complete la configuración utilizando el asistente ds micfgx.

#### Tareas relacionadas:

AIX: Instalación del servidor

Actualización del servidor



Sistemas operativos AIX

# Instalación del cliente de IBM Spectrum Protect en un nodo de producción para PowerHA


Sólo es necesario instalar el conjunto de archivos del cliente de archivado y copia de seguridad, que contiene los archivos del cliente de archivado y copia de seguridad y el cliente de línea de mandatos administrativos.

## Procedimiento

Para obtener instrucciones detalladas sobre la instalación del cliente de IBM Spectrum Protect, consulte la publicación *Instalación de los clientes de copia de seguridad y archivado de IBM Spectrum Protect*.

Complete los pasos siguientes para instalar el cliente de IBM Spectrum Protect en el nodo de producción.

1. Instale los archivos ejecutables del cliente de IBM Spectrum Protect en el directorio `/usr/tivoli/tsm/client/ba/bin`. Estos archivos se instalan normalmente en los discos internos del nodo de producción.
2. Para que el cliente encuentre el servidor, asegúrese de que el archivo de opciones de cliente, `dsm.sys`, apunte al servidor de IBM Spectrum Protect. El nombre de servidor `dsm.sys` se utiliza sólo en el parámetro `-servername` del mandato `dsmadm` para especificar el servidor al que se va a conectar.

 Sistemas operativos AIX

## Verificación de la configuración del servidor de IBM Spectrum Protect para PowerHA

Cuando haya configurado el servidor de IBM Spectrum Protect para utilizar PowerHA, debe verificar la configuración.

### Acerca de esta tarea

Cuando utiliza PowerHA, todos los directorios de base de datos, anotaciones, almacenamiento e instancia deben estar en discos compartidos que estén configurados para que PowerHA pueda ejecutar la recuperación de errores.

## Procedimiento

Para identificar los directorios que están en el disco compartido, siga estos pasos:

1. Inicie una sesión como el usuario de instancia.
2. Ejecute el script `/opt/tivoli/tsm/server/bin/dsmclustfs`.
3. Examine los sistemas de archivos que recoge el script y compruebe que estén en discos compartidos. El siguiente script de ejemplo muestra el tipo de información que debe revisar:

```
> su - tsminst1
$ /opt/tivoli/tsm/server/bin/dsmclustfs
SQL1026N El gestor de base de datos ya está activo.
```

La siguiente información sobre conexión de base de datos se muestra cuando el servidor de IBM Spectrum Protect se conecta a la base de datos de DB2:

```
DB20000I El mandato START DATABASE MANAGER se ha ejecutado correctamente.
```

```
Database Connection Information
```

```
Database server          = DB2/AIX64 11.1.0
SQL authorization ID     = TSMINST1
Local database alias     = TSMDB1
```

```
File systems for the DB2 database: /TSMdbspace2 /TSMdbspace1
File system for Active Log: /TSMalog
File system for Archive Log: /TSMarchlog
Active log mirror not defined for this database
```

Los siguientes sistemas de archivos de DB2 obligatorios están en el script:

```
/TSMdb-1 /TSMalog-1 /TSMarchlog-1
```

```
Checking existing TSM disk-based volumes...
TSM Data is stored in the following file systems: /TSMdisk-1 /TSMfile-1
```

## Configuración del nodo de espera para PowerHA

---

Para PowerHA, asegúrese de que el servidor de IBM Spectrum Protect no se esté ejecutando en el nodo de producción antes de configurar el nodo de espera.

### Procedimiento

---

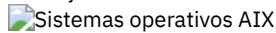
Complete los pasos siguientes para configurar el nodo de espera:

1. En el nodo de espera, abra el grupo de volúmenes compartidos y los sistemas de archivos de IBM Spectrum Protect.
2. En el nodo de espera, instale el código de producto de IBM Spectrum Protect. Para obtener más información, consulte el apartado Instalación del servidor de IBM Spectrum Protect en un nodo de producción para PowerHA. Si los archivos ejecutables se instalan en un espacio de disco compartido, es posible que deba instalarlos en el nodo en espera. Los controladores de dispositivo de IBM Spectrum Protect, los paneles SMIT y otros archivos deben instalarse en directorios del sistema AIX.
3. Abra el asistente dsmicfgx. Siga las instrucciones para completar la configuración. Seleccione el recuadro de selección para indicar que se trata de un nodo secundario del clúster.
4. Inicie el servidor en el nodo de espera. Consulte la base de datos, las anotaciones de recuperación y los volúmenes de agrupaciones de almacenamiento para comprobar que son los mismos que cuando se inició el servidor en el nodo de producción.
5. Instale el cliente en el nodo de espera. Si los archivos ejecutables se instalan en un espacio de disco compartido, es posible que deba instalarlos en el nodo en espera. Los paneles SMIT de IBM Spectrum Protect y otros archivos deben instalarse en directorios del sistema AIX. Utilice el mandato RCP de AIX con la opción -p para copiar el archivo dsm.sys del nodo de producción al nodo en espera. Si el archivo dsm.sys se cambia en un nodo, debe copiarse en el otro.

### Resultados

---

Consejo: Si el archivo dsm.sys se cambia en un nodo, debe copiarlo en el otro.



## Definición de los dispositivos de almacenamiento de medios extraíbles en AIX para PowerHA

---

En un sistema operativo AIX, debe definir los dispositivos de almacenamiento de medios extraíbles que utiliza IBM Spectrum Protect en los nodos de producción y espera. El gestor de bibliotecas comprueba que el cartucho que contiene el dispositivo de almacenamiento de soportes extraíble de la unidad está en la unidad correcta.

### Acerca de esta tarea


---

Requisito previo:

- Si define un servidor de gestor de bibliotecas que no se comparte con el servidor de IBM Spectrum Protect, asegúrese de que el parámetro RESETDRIVES del mandato DEFINE LIBRARY o el mandato UPDATE LIBRARY esté especificado como YES. Si define un servidor de gestor de bibliotecas que no se comparte con el servidor de IBM Spectrum Protect, la opción SANDISCOVERY debe establecerse en ON en el archivo de opciones de servidor de IBM Spectrum Protect dsmserv.opt. De forma predeterminada, esta opción está establecida en OFF.
- Puede emitir el mandato PERFORM LIBACTION desde los tipos de biblioteca SCSI y VTL. Utilice este mandato para definir las unidades y sus vías de acceso para una biblioteca en un paso.

Si su correlación de dispositivos SAN es precisa, continúe con la sección Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect. Si los nombres de dispositivo de los sistemas primario y secundario no son los mismos, debe utilizar el descubrimiento SAN para que el servidor de IBM Spectrum Protect pueda acceder a los dispositivos.

#### Tareas relacionadas:

 Configuración del intercambio de biblioteca (V7.1.1)

#### Referencia relacionada:


DEFINE LIBRARY (Definir una biblioteca)

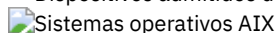
UPDATE LIBRARY (Actualizar una biblioteca)

PERFORM LIBACTION (Definir o suprimir todas las unidades y vías de acceso de una biblioteca)

SANDISCOVERY

#### Información relacionada:

 Dispositivos admitidos de IBM Spectrum Protect






# Cómo completar la configuración del gestor de clúster y IBM Spectrum Protect

Actualice la configuración del gestor del clúster para definir el servidor de IBM Spectrum Protect como una aplicación y un recurso de recuperación de errores del nodo en espera. Esta aplicación es propiedad del nodo de producción.

## Acerca de esta tarea

Puede emitir mandatos de IBM® PowerHA SystemMirror for AIX o Tivoli System Automation para configurar el clúster. Continúe con la configuración del servidor de IBM Spectrum Protect.

### Información relacionada:

-  Información sobre el producto PowerHA SystemMirror
-  Información sobre el producto IBM Tivoli System Automation for Multiplatforms versión 3.2.2
-  Sistemas operativos AIX

## Resolución de problemas del entorno en clúster de PowerHA

Revise la siguiente lista para obtener información sobre la resolución de problemas habituales. La información que se proporciona para IBM® PowerHA SystemMirror para AIX no representa todos los casos posibles.

Mensajes de aviso que se emiten después de ejecutar el programa de utilidad clverify

Puede ejecutar el programa de utilidad de verificación de clúster de PowerHA, clverify, en un nodo para verificar la configuración del clúster y la asignación de los recursos de PowerHA. Si ejecuta el programa de utilidad clverify después de definir el servidor de IBM Spectrum Protect como una aplicación PowerHA, aparecerán mensajes de aviso.

Los mensajes de aviso aparecen porque los scripts de shell que inician y detienen los servidores de IBM Spectrum Protect están en un sistema de archivos compartidos. Los scripts de shell sólo pueden ejecutarse en un nodo cada vez. Por lo tanto, los scripts de shell estarán disponibles en sólo un nodo cada vez. Puede ignorar los mensajes de aviso del programa de utilidad clverify. Si un sistema de archivos compartidos no se puede montar, el servidor de IBM Spectrum Protect no puede iniciarse.

El servidor de IBM Spectrum Protect falla al iniciarse una vez emitido el script startserver

Si utiliza el script de shell startserver y PowerHA falla al iniciar el servidor de IBM Spectrum Protect, inícielo de forma manual en un terminal sin la opción quiet. Si desea ejecutar el servidor con la opción QUIET, emita el mandato dsmserv -q.

Mensajes asociados al mandato tctl

Si emite el mandato tctl -f/dev/rmt2 rewind, es posible que aparezca el siguiente mensaje:

```
/dev/rmt2: Ya hay un dispositivo montado o no se puede desmontar
```

Este mensaje indica que un sistema distinto del sistema donde se ha ejecutado el mandato tctl ha bloqueado con SCSI RESERVE el dispositivo E/S. Si utiliza la reserva persistente, el servidor de IBM Spectrum Protect anticipa una reserva de unidad de forma predeterminada. Si el controlador de dispositivo no utiliza la reserva persistente, el servidor completa un restablecimiento de destino.



Mensaje ANS4329S Server out of data storage space

Si aparece el mensaje ANS4329S Server out of data storage space en el cliente de IBM Spectrum Protect, puede que la licencia del servidor de IBM Spectrum Protect no sea válida. Emita el mandato QUERY LICENSE para mostrar la información de conformidad con la licencia. Si el estado de cumplimiento es válido, utilice el mandato QUERY ACTLOG en el servidor y revise los mensajes que se muestran para identificar el problema.


 Sistemas operativos Linux

## Configuración de un entorno de Linux para agrupación en clúster

Puede configurar el servidor Linux de IBM Spectrum Protect en un entorno en clúster utilizando IBM® Tivoli System Automation for Multiplatforms Versión 3.2.2.

-  Sistemas operativos Linux Descripción general de un clúster de IBM Spectrum Protect de dos nodos utilizando Tivoli System Automation  
Utilice el clúster de Tivoli System Automation para una disponibilidad de base de datos y servidor mayor durante un fallo. Mediante la función de migración tras error de Tivoli System Automation, los componentes de servidor como la base de datos se pueden recuperar automáticamente de una anomalía.
-  Sistemas operativos Linux Configuración de un clúster de IBM Spectrum Protect con Tivoli System Automation  
Debe configurar un clúster de IBM Spectrum Protect para utilizar Tivoli System Automation.

-  Sistemas operativos Linux Requisitos previos para configurar un entorno en clúster de Linux con Tivoli System Automation Antes de instalar y configurar IBM Spectrum Protect en un entorno en clúster con Tivoli System Automation, debe comprobar los requisitos previos.
-  Sistemas operativos Linux Instalación y configuración de componentes de IBM Spectrum Protect en los nodos primario y secundario Debe instalar los componentes de base de datos y servidor de IBM Spectrum Protect en los nodos primario y secundario del clúster. A continuación, configure primero el nodo primario seguido del nodo secundario.
-  Sistemas operativos Linux Instalación de Tivoli System Automation en nodos primario y secundario Después de instalar y configurar IBM Spectrum Protect en los nodos primario y secundario del clúster, debe instalar y configurar Tivoli System Automation en esos nodos. A continuación, debe activar esos nodos para el dominio, configurar los recursos y activar la política base. Finalmente, debe añadir los puntos de montaje para los directorios de IBM Spectrum Protect.
-  Sistemas operativos Linux Configuración de recursos de almacenamiento Utilice la interfaz de usuario de Tivoli System Automation o de la línea de mandatos para añadir o suprimir los recursos de almacenamiento y para suprimir los puntos de montaje que ya no son necesarios. Si añade una agrupación de almacenamiento al clúster, debe añadirla al grupo de recursos. Si elimina una agrupación de almacenamiento del clúster, también debe suprimirla del grupo de recursos.
-  Sistemas operativos Linux Actualización de un servidor configurado con Tivoli System Automation Puede actualizar un servidor configurado con Tivoli System Automation desde la Versión 6.3 o la Versión 7.1.

 Sistemas operativos Linux

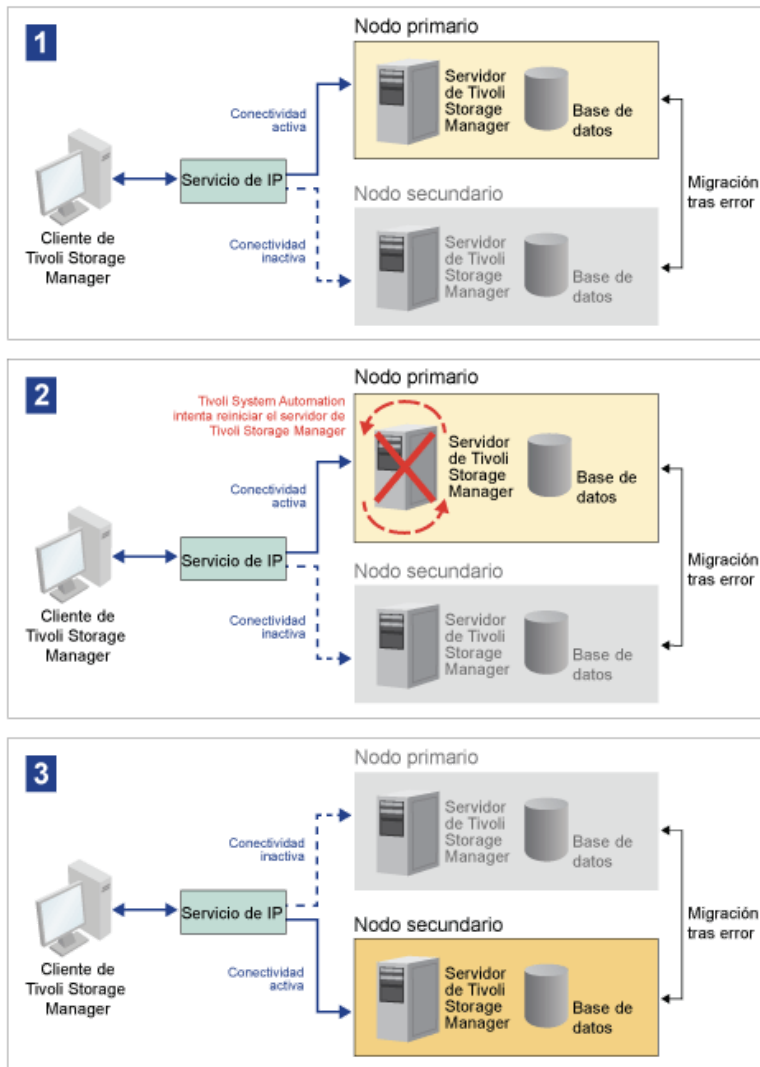
## Descripción general de un clúster de IBM Spectrum Protect de dos nodos utilizando Tivoli System Automation

---

Utilice el clúster de Tivoli System Automation para una disponibilidad de base de datos y servidor mayor durante un fallo. Mediante la función de migración tras error de Tivoli System Automation, los componentes de servidor como la base de datos se pueden recuperar automáticamente de una anomalía.

El servidor de IBM Spectrum Protect y la base de datos DB2 son componentes de servidor subyacentes para este clúster de dos nodos. El servidor es un componente principal. Es responsable de la actividad del servidor y del cliente. La base de datos DB2 es un componente interno que se instala como parte del servidor. El servidor controla toda actividad de la base de datos como el inicio y el cierre. Cuando el servidor detecta un error de componente de base de datos o de servidor, intenta reiniciar la base de datos. Si el reinicio falla, el servidor y la base de datos se cierran automáticamente en el nodo primario y Tivoli System Automation inicia estos componentes en el nodo secundario. Debido a que las funciones de IBM Spectrum Protect se restauran inmediatamente, la disponibilidad del servidor y de la base de datos es mayor.

Figura 1. Función de migración tras error. Los componentes de servidor y de base de datos falla en el nodo primario. Tivoli System Automation inicia estos componentes en el nodo secundario.

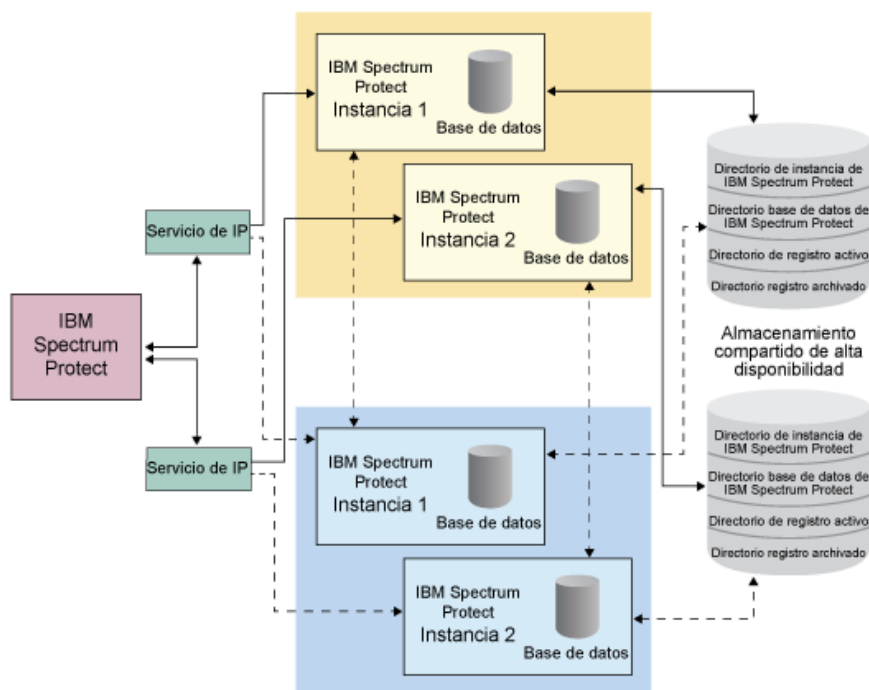




El servidor y la base de datos incluyen los siguientes directorios de registros que se utilizan para el almacenamiento:

- Directorio de instancia de IBM Spectrum Protect
- Directorio de anotaciones activas
- Directorio de anotaciones de archivado
- Directorio de base de datos

Los dos nodos de este clúster de Tivoli System Automation están configurados para acceder a un almacenamiento compartido altamente disponible que protege los datos. Por ejemplo, la topología de dos nodos incluye un nodo primario y un nodo secundario. Estos nodos se ubican en sistemas físicos individuales pero pueden acceder a los mismos datos utilizando la matriz de almacenamiento compartido.

Figura 2. Varias instancias de servidor de IBM Spectrum Protect en nodos separados. Estas instancias de servidor están en sistemas físicos separados. Estas instancias pueden acceder al almacenamiento compartido altamente disponible.



- 
 Sistemas operativos Linux Topología de disco compartido de dos nodos  
 Este clúster utiliza una tipología de disco compartido de dos nodos. Incluye un nodo primario y secundario. El nodo primario aloja el servidor de IBM Spectrum Protect, la base de datos, la instancia de IBM Spectrum Protect y los datos. El nodo secundario es adonde se mueven los recursos de IBM Spectrum Protect si se produce un fallo.
- 
 Sistemas operativos Linux Grupos de recursos de Tivoli System Automation  
 Utilice los grupos de recursos de Tivoli System Automation con políticas de automatización definidas para gestionar los componentes de IBM Spectrum Protect para este clúster. La única excepción es el recurso de instancia de servidor de base de datos gestionada por el servidor de IBM Spectrum Protect.

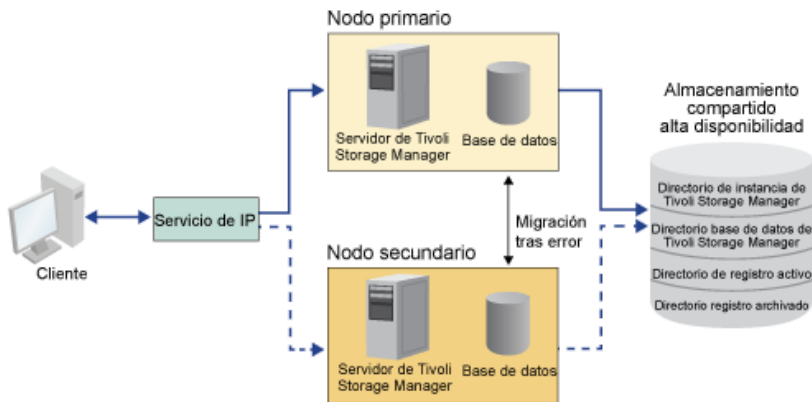
 Sistemas operativos Linux

## Topología de disco compartido de dos nodos

Este clúster utiliza una tipología de disco compartido de dos nodos. Incluye un nodo primario y secundario. El nodo primario aloja el servidor de IBM Spectrum Protect, la base de datos, la instancia de IBM Spectrum Protect y los datos. El nodo secundario es adonde se mueven los recursos de IBM Spectrum Protect si se produce un fallo.

Los dos nodos de este clúster se conectan uno a otro a través de una única red pública y a un sistema de *almacenamiento de disco compartido*, que siempre está disponible. El *almacenamiento de disco compartido* es donde están disponibles uno o más discos para los

odos primario y secundario. Estos discos sólo se montan en un nodo, el nodo primario, a la vez. Un nodo puede tener datos de entrada y de salida que se comparten con los discos de almacenamiento. La siguiente ilustración muestra una topología compartida de dos nodos donde se produce una migración tras error automática al nodo secundario en la instancia de un fallo.



 Sistemas operativos Linux

## Grupos de recursos de Tivoli System Automation

Utilice los grupos de recursos de Tivoli System Automation con políticas de automatización definidas para gestionar los componentes de IBM Spectrum Protect para este clúster. La única excepción es el recurso de instancia de servidor de base de datos gestionada por el servidor de IBM Spectrum Protect.

Los sistemas de archivo compartido y los componentes de IBM Spectrum Protect se definen como recursos. Varios recursos crean un grupo de recursos. Cada recurso del grupo de recursos tiene un tipo de recurso. Cada instancia de IBM Spectrum Protect de un clúster incluye un grupo de recursos. Durante las paradas planificadas, los grupos de recursos se pueden mover manualmente del nodo primario al nodo secundario.

El grupo de recursos de IBM Spectrum Protect incluye los siguientes recursos. El nombre del grupo de recursos de IBM Spectrum Protect es SA-tsm-inst1-rg, donde inst1 es el nombre de instancia. Los recursos siguientes se utilizan para funciones distintas pero obligatorias en este clúster.



## IP de servicio

El recurso de IP de servicio se utiliza para la comunicación. Se denomina tsm-inst1-ip-rs, donde inst1 es el nombre de instancia. La IP de servicio está gestionada por Tivoli System Automation. Esta IP está disponible en el nodo donde se está ejecutando el servidor de IBM Spectrum Protect. Debe crear la interfaz lógica de la IP de servicio en la misma interfaz física que la interfaz de red pública.

## Recurso *almacenamiento de disco compartido*

Un recurso de *almacenamiento de disco compartido* es un dispositivo de almacenamiento físico en el servidor de IBM Spectrum Protect donde están almacenados los datos de aplicación de IBM Spectrum Protect y DB2. Debe crear los siguientes recursos de almacenamiento de disco:

- Directorio de instancia - tsm-inst1-inst1dir-ag
- Directorio de DB2 - tsm-inst1-db2dir-ag
- Directorio de registros activos - tsm-inst1-actlog-ag
- Directorio de registro de archivado - tsm-inst1-archlog-ag

## *Almacenamiento de disco compartido* para agrupaciones de almacenamiento

El recurso de agrupación de almacenamiento incluye dispositivos de almacenamiento físico en el servidor de IBM Spectrum Protect donde se almacenan los datos de cliente.

## Recursos del grupo de volúmenes


Si decide configurar el almacenamiento utilizando grupos de volúmenes, hay un recurso de grupo de volúmenes disponible para los recursos de *almacenamiento de disco compartido* anteriores. Los recursos del grupo de volúmenes se crean automáticamente mediante Tivoli System Automation.

## Recursos de aplicación para la instancia de servidor de IBM Spectrum Protect

El recurso de instancia de servidor de IBM Spectrum Protect es el recurso de servidor que gestiona la aplicación de IBM Spectrum Protect. Este recurso se gestiona a través de scripts de control de Tivoli System Automation.

Tabla 1. Tareas completadas por los scripts de control de Tivoli System Automation

Tareas	Descripción	Mandatos de ejemplo
START	Inicia la instancia de servidor de IBM Spectrum Protect.	El mandato <code>/opt/tivoli/tsm/server/bin/rc.dsmserv -u db2inst1 -i /tsminst1</code> inicia la instancia de servidor con el usuario db2inst1 del directorio /tsminst1.
Detener	Detiene la instancia de servidor de IBM Spectrum Protect.	<code>kill -s SIGURG 345</code> donde 345 es el <i>PID</i> . El <i>PID</i> se puede encontrar en el archivo <code>/tsminst1/dsmserv.v6lock</code> .
Monitor	Comprueba si existe el archivo <code>/tsminst1/dsmserv.v6lock</code> . Utiliza el <i>PID</i> para comprobar si se está ejecutando el proceso.	<code>ps -ef   grep 345</code> donde 345 es el <i>PID</i> .

-  Sistemas operativos Linux Dependencias del grupo de recursos  
Las dependencias del grupo de recursos se crean automáticamente para controlar el orden en el que se inician los recursos. Estas dependencias también controlan qué recursos se deben reiniciar o concluir si falla el recurso específico del que dependen estos recursos.

 Sistemas operativos Linux

# Configuración de un clúster de IBM Spectrum Protect con Tivoli System Automation


Debe configurar un clúster de IBM Spectrum Protect para utilizar Tivoli System Automation.

## Procedimiento

1. Instale y configure los componentes de IBM Spectrum Protect en los nodos primario y secundario.
2. Instale Tivoli System Automation en los nodos primario y secundario.
3. Configure los recursos de almacenamiento.
4. Dependiendo de la versión de IBM Spectrum Protect instalada en el servidor, es posible que tenga que actualizar el servidor de IBM Spectrum Protect para el clúster de Tivoli System Automation.
5. Opcional: Puede establecer la variable `FILE_EXIT` en el script de clúster `tsmservctrl` para direccionar los datos de sucesos de Tivoli System Automation al archivo `FILEEXIT` del servidor de IBM Spectrum Protect.

Por ejemplo, edite el script de clúster de tsmserverctrl en el directorio `<server_install_directory>/tsam/controls` y añada la siguiente línea:

```
FILE_EXIT="fileexittmp"
```

 Sistemas operativos Linux

## Requisitos previos para configurar un entorno en clúster de Linux con Tivoli System Automation

---


Antes de instalar y configurar IBM Spectrum Protect en un entorno en clúster con Tivoli System Automation, debe comprobar los requisitos previos.

Compruebe que se cumplen los siguientes requisitos previos.

- Planifique la instalación del servidor de IBM Spectrum Protect.
- Después de instalar IBM Spectrum Protect, verifique los siguientes elementos:
  - Asegúrese de que la base de datos de DB2 está instalada en el mismo nodo que el servidor.
  - Compruebe que el servidor puede controlar la recuperación de la base de datos de control.
  - Compruebe que están disponibles los volúmenes de almacenamiento compartido. IBM Spectrum Protect requiere dispositivos de almacenamiento compartido de alta disponibilidad para proteger la integridad de datos.
  - Verifique que cada nodo del clúster puede contener varias instancias del servidor.
- Prepare la instalación de Tivoli System Automation. Para obtener instrucciones, vaya a la documentación de producto de Tivoli System Automation. En la *Guía de instalación y configuración*, busque *Preparación para la instalación*.
- Después de instalar Tivoli System Automation, compruebe que Tivoli System Automation puede procesar la migración tras error como migración tras error de la IP y la migración tras error de datos para la base de datos, la instancia de datos, los registros activos y de archivado, y las agrupaciones de almacenamiento.

### Tareas relacionadas:




Planificación para instalar el servidor de IBM Spectrum Protect

 Sistemas operativos Linux

## Instalación y configuración de componentes de IBM Spectrum Protect en los nodos primario y secundario

---

Debe instalar los componentes de base de datos y servidor de IBM Spectrum Protect en los nodos primario y secundario del clúster. A continuación, configure primero el nodo primario seguido del nodo secundario.

-  Instalación de los componentes de servidor de IBM Spectrum Protect  
Después de comprobar y verificar los requisitos previos, debe instalar los componentes requerido en los nodos primario y secundario del sistema.
-  Configuración del nodo primario  
Para establecer la topología de dos nodos, configure los componentes de IBM Spectrum Protect en ambos nodos. En primer lugar, debe configurar la instancia de IBM Spectrum Protect en el nodo primario.
-  Configuración del nodo secundario  
Después de configurar el nodo primario, debe configurar el nodo secundario para que Tivoli System Automation pueda mover los componentes de servidor de IBM Spectrum Protect al nodo secundario si el servidor falla en el nodo primario.

 Sistemas operativos Linux

## Instalación de los componentes de servidor de IBM Spectrum Protect

---

Después de comprobar y verificar los requisitos previos, debe instalar los componentes requerido en los nodos primario y secundario del sistema.


### Procedimiento

---

Revise los temas en la información de configuración de un servidor de IBM Spectrum Protect.

### Tareas relacionadas:

Instalación de los componentes del servidor IBM Spectrum Protect

 Sistemas operativos Linux

## Configuración del nodo primario

---

Para establecer la topología de dos nodos, configure los componentes de IBM Spectrum Protect en ambos nodos. En primer lugar, debe configurar la instancia de IBM Spectrum Protect en el nodo primario.

### Antes de empezar

---

- Instale los componentes del servidor de IBM Spectrum Protect.
- Verifique que el propietario de instancia de IBM Spectrum Protect tiene el mismo ID de grupo y usuario para todos los nodos del dominio de clúster.
- Verifique que el propietario de instancia de IBM Spectrum Protect tiene la misma contraseña para todos los nodos del clúster.

### Procedimiento

---

1. Para obtener instrucciones detalladas sobre cómo crear los directorios y el ID de usuario para la instancia de servidor, consulte Linux: Creación del ID de usuario y los directorios para la instancia de servidor.
2. Verifique que el servidor de IBM Spectrum Protect, la instancia de DB2 y los directorios de registro de archivado y activos se comparten.
3. Defina los puntos de montaje añadiendo entradas al archivo `/etc/fstab`.

Cuando añada puntos de montaje en los nodos de clúster, utilice la opción `noauto` para evitar que los puntos de montaje se monten automáticamente en más de un nodo del clúster.

4. Establezca los siguientes permisos en cada uno de los puntos de montaje:
  - 755. Por ejemplo, el mandato siguiente establece el permiso 755 en el punto de montaje `/tsminst1`.

```
chmod -R 755 /tsminst1
```
  - El propietario de instancia de servidor de IBM Spectrum Protect. Por ejemplo, el mandato siguiente establece los permisos para el propietario de instancia.

```
chown -R tsminst1 /tsminst1
```
  - Grupo de servidores de IBM Spectrum Protect al que pertenece el propietario de instancia. Por ejemplo, el mandato siguiente establece los permisos para el grupo del propietario de instancia.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Para obtener instrucciones detalladas sobre la configuración del servidor de IBM Spectrum Protect utilizando el asistente de configuración, consulte Linux: Configuración de IBM Spectrum Protect mediante el asistente de configuración. Compruebe que todos los directorios compartidos están montados en el nodo primario.
6. Inicie instancia de servidor de IBM Spectrum Protect en el nodo primario utilizando el programa de utilidad DSMSEV. Por ejemplo, el mandato siguiente inicia el servidor para una operación normal.

```
/opt/tivoli/tsm/server/bin/dsmsevr
```

7. Verifique que los componentes de IBM Spectrum Protect se han iniciado sin errores.
8. Cierre el servidor IBM Spectrum Protect.
9. Como usuario `root`, desmonte las unidades compartidas.

 Sistemas operativos Linux

## Configuración del nodo secundario

---

Después de configurar el nodo primario, debe configurar el nodo secundario para que Tivoli System Automation pueda mover los componentes de servidor de IBM Spectrum Protect al nodo secundario si el servidor falla en el nodo primario.

### Procedimiento

---

1. Para crear manualmente los directorios y el ID de usuario para la instancia de servidor, siga las instrucciones de Creación del ID de usuario y los directorios para la instancia de servidor.
2. Verifique que el servidor de IBM Spectrum Protect, la instancia de DB2 y los directorios de registro de archivado y activos se comparten.
3. Defina los puntos de montaje añadiendo entradas al archivo `/etc/fstab`.

Cuando añada puntos de montaje en los nodos de clúster, utilice la opción noauto. Esta opción evita que los puntos de montaje se monten automáticamente en más de un nodo del clúster.

Compruebe que todos los directorios compartidos están montados en el nodo secundario.

4. Establezca los siguientes permisos en cada uno de los puntos de montaje:

- 755. Por ejemplo, el mandato siguiente establece el permiso 755 en el punto de montaje /tsminst1.

```
chmod -R 755 /tsminst1
```

- El propietario de instancia de servidor de IBM Spectrum Protect. Por ejemplo, el mandato siguiente establece los permisos para el propietario de instancia.

```
chown -R tsminst1 /tsminst1
```

- Grupo de servidores de IBM Spectrum Protect al que pertenece el propietario de instancia. Por ejemplo, el mandato siguiente establece los permisos para el grupo del propietario de instancia.

```
chgrp tsmsrv_1_group /tsminst1
```

5. Cree una instancia de servidor de IBM Spectrum Protect emitiendo el mandato db2icrt. Para obtener instrucciones, consulte Creación de la instancia de servidor.

Recuerde: No es necesario que cree un archivo de opciones de servidor porque el nodo secundario utiliza el archivo dsmserv.opt del nodo primario.

Compruebe que todos los directorios compartidos están montados en el nodo secundario.

6. Catalogue la base de datos emitiendo el mandato catalog db. Por ejemplo, el mandato siguiente cataloga la base de datos tsmdb1.

```
db2 catalog db tsmdb1
```

7. Prepare la base de datos para la copia de seguridad. Para obtener instrucciones, consulte Preparación del gestor de bases de datos para la copia de seguridad de base de datos.

8. Inicie el servidor de IBM Spectrum Protect utilizando el programa de utilidad DSMSERV. Por ejemplo, el mandato siguiente inicia el servidor para una operación normal.

```
/opt/tivoli/tsm/server/bin/dsmserv
```








9. Verifique que los componentes de IBM Spectrum Protect se han iniciado sin errores.

10. En los nodos secundarios, cierre el servidor de IBM Spectrum Protect y desmonte los directorios compartidos.

 Sistemas operativos Linux

## Instalación de Tivoli System Automation en nodos primario y secundario

Después de instalar y configurar IBM Spectrum Protect en los nodos primario y secundario del clúster, debe instalar y configurar Tivoli System Automation en esos nodos. A continuación, debe activar esos nodos para el dominio, configurar los recursos y activar la política base. Finalmente, debe añadir los puntos de montaje para los directorios de IBM Spectrum Protect.

-  Sistemas operativos Linux Creación de una etiqueta para los puntos de montaje  
Cree una etiqueta para cada punto de montaje en los nodos primario y secundario del clúster.
-  Sistemas operativos Linux Instalación y configuración de Tivoli System Automation  
Debe instalar IBM Tivoli System Automation for Multiplatforms en los nodos primario y secundario del sistema.
-  Sistemas operativos Linux Preparación para activar los nodos de clúster para el dominio  
Después de instalar Tivoli System Automation en los nodos primario y secundarios del clúster, debe preparar estos nodos para poder activar el clúster e iniciar el dominio de clúster.
-  Sistemas operativos Linux Configuración de recursos del grupo de volúmenes  
Si ha creado grupos de volúmenes para el clúster, debe configurar estos recursos. Tivoli System Automation encuentra y define automáticamente los recursos del volumen de disco compartido.
-  Sistemas operativos Linux Configuración de recursos que no están en un grupo de volúmenes  
Si ha creado los recursos de *almacenamiento de disco compartido* utilizando los tipos de recurso ext2, ext3 o reiserfs en uno de los nodos del clúster, debe configurar estos recursos.
-  Sistemas operativos Linux Activación de la política base  
Después de configurar los recursos, debe activar la política en los nodos primario y secundario para crear los recursos restantes y el grupo de recursos.
-  Sistemas operativos Linux Adición de puntos de montaje a directorios de IBM Spectrum Protect  
Antes de poder iniciar el clúster, debe añadir los puntos de montaje que ha creado para los componentes de IBM Spectrum Protect.

 Sistemas operativos Linux

## Creación de una etiqueta para los puntos de montaje

---

Cree una etiqueta para cada punto de montaje en los nodos primario y secundario del clúster.

### Procedimiento

---

1. Cree una etiqueta para cada uno de los volúmenes que ha creado anteriormente para los puntos de montaje del directorio compartido emitiendo el mandato `e2label`. Por ejemplo, el mandato siguiente crea la etiqueta `/tsminst1` que tiene una partición `/dev/tsmvg1/tsminst1LV`.

```
e2label /dev/tsmvg1/tsminst1LV /tsminst1
```

2. Para cada nodo del clúster, sustituya las entradas para los puntos de montaje que ha creado anteriormente en el archivo `/etc/fstab`. Por ejemplo, para la etiqueta de ejemplo anterior, emita el mandato siguiente:

```
LABEL=/tsminst1 /tsminst1 ext3 defaults 0 0
```

 Sistemas operativos Linux

## Instalación y configuración de Tivoli System Automation

---

Debe instalar IBM® Tivoli System Automation for Multiplatforms en los nodos primario y secundario del sistema.

### Procedimiento

---

1. Para instalar y configurar Tivoli System Automation, existe información detallada en la Tivoli System Automation Guía de instalación y configuración.
2. Descargue el archivo `TSM-25072011-1015.zip` de Integrated Service Management Library. Extraiga el archivo comprimido en cada uno de los nodos de clúster.
3. Después de extraer el archivo comprimido, verifique que el nuevo directorio de Tivoli System Automation creado durante la instalación incluye el directorio `/TSM/HA` y subdirectorios.

#### Información relacionada:

 Información sobre el producto IBM Tivoli System Automation for Multiplatforms versión 3.2.2

 Sistemas operativos Linux

## Preparación para activar los nodos de clúster para el dominio

---

Después de instalar Tivoli System Automation en los nodos primario y secundarios del clúster, debe preparar estos nodos para poder activar el clúster e iniciar el dominio de clúster.

### Procedimiento

---

1. Prepare cada uno de los nodos para el dominio emitiendo el mandato `preprnode`. Emita este mandato para todos los nodos de clúster del dominio. Por ejemplo, el mandato siguiente prepara los nodos `HOST1.ibm.com` y `HOST2.ibm.com`.

```
preprnode HOST1.ibm.com HOST2.ibm.com
```

2. Cree un dominio para cada nodo emitiendo el mandato `mkrpdomain`. Por ejemplo, el mandato siguiente crea `tsm_domain` para los nodos `HOST1.ibm.com` y `HOST2.ibm.com`.

```
mkrpdomain tsm_domain HOST1.ibm.com HOST2.ibm.com
```

3. Inicie el dominio para cada nodo emitiendo el mandato `starttrpdomain`. Por ejemplo, el mandato siguiente inicia `tsm_domain`.

```
starttrpdomain tsm_domain
```

 Sistemas operativos Linux

## Configuración de recursos del grupo de volúmenes

---

Si ha creado grupos de volúmenes para el clúster, debe configurar estos recursos. Tivoli System Automation encuentra y define automáticamente los recursos del volumen de disco compartido.

## Procedimiento

Para configurar los recursos de grupo de volúmenes para los directorios de IBM Spectrum Protect compartidos y montar puntos que ha creado anteriormente, complete los pasos siguientes en el nodo primario.

1. Importe los grupos de volúmenes. Por ejemplo, utilice el mandato `vgimport X` para importar los grupos de volúmenes `X`.
2. Active los grupos de volúmenes. Por ejemplo, utilice el mandato `vgchange -ay X` para activar los grupos de volúmenes `X`.
3. Monte el sistema de archivos emitiendo el mandato `mount`. El ejemplo siguiente monta el sistema de archivos `X`.

```
mount X
```

4. Reinicie el dominio emitiendo los mandatos `stoprpdomain` y `startrpdomain`. Por ejemplo, los mandatos siguientes reinician `tsm_domain`.

```
stoprpdomain tsm_domain  
startrpdomain tsm_domain
```

5. Desmonte el sistema de archivos emitiendo el mandato `umount`. Por ejemplo, utilice el mandato `umount X` para desmontar el sistema de archivos `X`.
6. Desactive los grupos de volúmenes. Por ejemplo, utilice el mandato `vgchange -an X` para desactivar los grupos de volúmenes `X`.
7. Verifique que todos los recursos de almacenamiento IBM®.AgfileSystem se recolectan mediante Tivoli System Automation emitiendo el mandato siguiente:

```
lsrsrc -s "Name=='Resource_Name' && ResourceType=1" IBM.AgFileSystem
```



## Configuración de recursos que no están en un grupo de volúmenes

Si ha creado los recursos de *almacenamiento de disco compartido* utilizando los tipos de recurso `ext2`, `ext3` o `reiserfs` en uno de los nodos del clúster, debe configurar estos recursos.

## Procedimiento

Complete los siguientes pasos en el servidor primario.

1. Monte el sistema de archivos emitiendo el mandato `mount`. Por ejemplo, el mandato siguiente monta el sistema de archivos `X`.

```
mount X
```

2. Reinicie el dominio emitiendo los mandatos `stoprpdomain` y `startrpdomain`. Por ejemplo, el mandato siguiente reinicia `tsm_domain`.

```
stoprpdomain tsm_domain  
startrpdomain tsm_domain
```

3. Desmonte el sistema de archivos emitiendo el mandato `umount`. Por ejemplo, el mandato siguiente desmonta el sistema de archivos `X`.

```
umount X
```

4. Verifique que todos los recursos de almacenamiento IBM®.AgfileSystem se recolectan mediante Tivoli System Automation emitiendo el mandato siguiente:

```
lsrsrc -s "Name=='Resource_Name' && ResourceType=1" IBM.AgFileSystem
```


Por ejemplo, para verificar el recurso `tsmalog`, ejecute el siguiente mandato:

```
lsrsrc -s "Name=='tsmalog' && ResourceType=1" IBM.AgFileSystem  
Resource Persistent Attributes for IBM.AgFileSystem resource 1:  
ResourceHandle= "0x2038 0xffff 0x6ad47197 0x256fc23d 0x9338a9950x263fa510"  
Name           = "tsmalog"  
ResourceType   = 1    <-----  
MountPoint     = ""  
DeviceName     = ""  
Vfs            = "ext3"  
AggregateResource = "0x3fff 0xffff 0x00000000 0x00000000 0x00000000 0x00000000"  
ContainerResource = "0x2036 0xffff 0x6ad47197 0x256fc23d 0x9338a995 0x25ffaa28"  
GhostDevice    = 0  
ResourceId     = "360050768019c021d30000000000005da"  
ProtectionMode = 1
```

```

UserControl          = 0
SysMountPoint       = "/tsmalog"
Label                = "/tsmalog"
FSID                 = "5792f887-8547-4c33-a519-9d0c50ab6882"
PreOnlineMethod     = 0
ContainerResourceId = "360050768019c021d30000000000005da"
AutoMonitor         = 1
Options              = "defaults,noauto"
PreOfflineMethod    = 0
ActivePeerDomain    = "TSM_Domain"
NodeNameList        =
{"tsmlnode01.storage.tucson.ibm.com","tsmlnode02.storage.tucson.ibm.com"}

```

 Sistemas operativos Linux

## Activación de la política base

Después de configurar los recursos, debe activar la política en los nodos primario y secundario para crear los recursos restantes y el grupo de recursos.

### Acerca de esta tarea

Para activar la política base, debe crear el recurso IP de servicio y los recursos de aplicación de IBM Spectrum Protect para los recursos de aplicación de la instancia de servidor de IBM Spectrum Protect. A continuación, debe crear el grupo de recursos y las políticas para gestionar el clúster.

### Procedimiento

Complete los pasos siguientes primero en el nodo primario y, después, en el nodo secundario.

1. Vaya al directorio donde extrajo el contenido del archivo TSM-25072011-1015.zip.
2. Establezca los permisos de archivos en los scripts del directorio bin emitiendo el mandato `chmod`. Por ejemplo, el mandato siguiente establece los permisos de archivo para todos los scripts del directorio bin. XXX es el nombre de la carpeta extraída.

```
chmod 755 /XXX/TSM/HA/bin/*
```

3. Vaya al directorio bin emitiendo el mandato `cd`.
4. Actualice las variables siguientes en el script `base_cluster_variables.sh`:
  - o `NODE1` especifica el nombre de host para el nodo 1 (nodo primario) del clúster.
  - o `NODE2` especifica el nombre de host para el nodo 2 (nodo secundario) del clúster.
  - o `IP_GATEWAY` especifica la pasarela de la IP de servicio.
  - o `SUBNET_MASK` especifica la máscara de subred de la IP de servicio.
  - o `NET_INT` especifica el nombre de la interfaz de red de un nodo específico del clúster. El nombre debe ser el mismo para todos los nodos del clúster.
5. Ejecute el script de configuración de `configureHA.sh` emitiendo el mandato `./configureHA.sh` en todos los nodos del clúster. Si el script `configureHA.sh` falla con el error `-bash: ./configureHA.sh: /bin/bash^M: bad interpreter: No such file or directory`, emita el mandato `dos2unix` en todos los scripts del directorio bin. Por ejemplo, para cada script, ejecute el mandato siguiente:

```
dos2unix -o <filename>
```

6. Verifique que la configuración es un éxito verificando que los scripts de configuración se ejecutan correctamente.
7. Atención: Complete este paso únicamente en el nodo primario. Ejecute el script de configuración emitiendo el mandato `./setup.sh`. Por ejemplo, el mandato siguiente ejecuta el script de configuración en la instancia de servidor de `inst1` IBM Spectrum Protect para el usuario de instancia `dbinst1` del directorio de instancia de servidor `/tsminst1` IBM Spectrum Protect con `9.11.142.129` como IP de servicio.

```
./setup.sh inst1 dbinst1 /tsminst1 9.11.142.129
```

8. Compruebe que está utilizando la IP correcta ejecutando el siguiente mandato:

```
lssam -V
```

9. Repita el paso 5 para todas las instancias de IBM Spectrum Protect que tiene en el entorno de servidor de IBM Spectrum Protect.
10. Complete todos los pasos anteriores en el nodo secundario.

 Sistemas operativos Linux

## Adición de puntos de montaje a directorios de IBM Spectrum Protect

---

Antes de poder iniciar el clúster, debe añadir los puntos de montaje que ha creado para los componentes de IBM Spectrum Protect.

### Procedimiento

---

Para añadir puntos de montaje de disco compartido al grupo de recursos de clúster y poner al clúster en línea, complete los pasos siguientes:

1. Identifique los puntos de montaje para los siguientes directorios:
  - o Instancia
  - o Base de datos
  - o Registro activo
  - o Registro de archivado
  - o Agrupación de almacenamiento
2. Añada recursos a cada punto de montaje:
  - a. Compruebe si el grupo de recursos `tsm-$INST_NAME-rg` está en línea emitiendo el mandato `lssam`.
  - b. Si el grupo de recursos `tsm-$INST_NAME-rg` está en línea, póngalo fuera de línea emitiendo el siguiente mandato:

```
chrg -o offline tsm-$INST_NAME-rg
```
  - c. Vaya al directorio donde extrajo el contenido del archivo `TSM-25072011-1015.zip`.
  - d. Vaya al directorio `bin` emitiendo el mandato `cd`.
  - e. Para añadir recursos de disco compartido a cada punto de montaje, ejecute el script `./update_setup.sh`. Por ejemplo, el mandato siguiente añade el punto de montaje `/tsminst1` a la instancia de servidor `inst1` IBM Spectrum Protect.

```
./update_setup.sh inst1 /tsminst1
```
3. Ponga el grupo de recursos `tsm-$INST_NAME-rg` en línea emitiendo el mandato siguiente:




```
chrg -o online tsm-$INST_NAME-rg
```
4. Conéctese al servidor mediante un IP de pasarela de servicio para comprobar que la configuración es correcta.

 Sistemas operativos Linux

## Configuración de recursos de almacenamiento

---

Utilice la interfaz de usuario de Tivoli System Automation o de la línea de mandatos para añadir o suprimir los recursos de almacenamiento y para suprimir los puntos de montaje que ya no son necesarios. Si añade una agrupación de almacenamiento al clúster, debe añadirla al grupo de recursos. Si elimina una agrupación de almacenamiento del clúster, también debe suprimirla del grupo de recursos.

-  **Sistemas operativos Linux** Adición de una agrupación de almacenamiento a un grupo de recursos  
Si la configuración de IBM Spectrum Protect almacena datos en discos, debe añadir el punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos.
-  **Sistemas operativos Linux** Supresión de una agrupación de almacenamiento de un grupo de recursos  
Puede suprimir una agrupación de almacenamiento que ya no se necesita. Si se elimina una agrupación de almacenamiento de la instancia de servidor de IBM Spectrum Protect, debe suprimirse del grupo de recursos.
-  **Sistemas operativos Linux** Supresión de un punto de montaje de un grupo de recursos  
Puede que desee eliminar un punto de montaje que ya no se necesita.

 Sistemas operativos Linux

## Adición de una agrupación de almacenamiento a un grupo de recursos

---

Si la configuración de IBM Spectrum Protect almacena datos en discos, debe añadir el punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos.

### Procedimiento

---

Para añadir un punto de montaje de disco compartido para la agrupación de almacenamiento al grupo de recursos, complete los pasos siguientes:



1. Bloquee el grupo de recursos emitiendo el mandato `rgreq -o lock`. Por ejemplo, el mandato siguiente bloquea el grupo de recursos `Sample_Resourcegroup_X`.

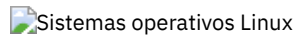
```
rgreq -o lock Sample_Resourcegroup_X
```

2. Vaya al directorio `bin` emitiendo el mandato `cd`.
3. Para añadir un recurso de agrupación de almacenamiento para un grupo de recursos, ejecute el script `update_setup.sh` emitiendo el mandato `./update_setup.sh`. Por ejemplo, el mandato siguiente añade el punto de montaje de la agrupación de almacenamiento `/inst1stg1` a la instancia de servidor `inst1` de IBM Spectrum Protect.

```
./update_setup.sh inst1 /inst1stg1
```

4. Desbloquee el grupo de recursos emitiendo el mandato `rgreq -o unlock`. Por ejemplo, el mandato siguiente desbloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o unlock Sample_Resourcegroup_X
```



Sistemas operativos Linux

## Supresión de una agrupación de almacenamiento de un grupo de recursos

---

Puede suprimir una agrupación de almacenamiento que ya no se necesita. Si se elimina una agrupación de almacenamiento de la instancia de servidor de IBM Spectrum Protect, debe suprimirse del grupo de recursos.

### Procedimiento

---

Para suprimir una agrupación de almacenamiento, complete los pasos siguientes:

1. Bloquee el grupo de recursos emitiendo el mandato `rgreq -o lock`. Por ejemplo, el mandato siguiente bloquea el grupo de recursos `Sample_Resourcegroup_X`.

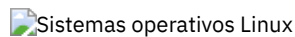
```
rgreq -o lock Sample_Resourcegroup_X
```

2. Vaya al directorio `bin` emitiendo el mandato `cd`.
3. Para suprimir un recurso de agrupación de almacenamiento de un grupo de recursos, ejecute el script `delete_mount.sh` emitiendo el mandato `./delete_mount.sh`. Por ejemplo, el mandato siguiente suprime el punto de montaje `/inst1stg1` de la instancia de servidor `inst1` IBM Spectrum Protect.

```
./delete_mount.sh /inst1stg1 inst1
```

4. Desbloquee el grupo de recursos emitiendo el mandato `rgreq -o unlock`. Por ejemplo, el mandato siguiente desbloquea el grupo de recursos `Sample_Resourcegroup_X`.

```
rgreq -o unlock Sample_Resourcegroup_X
```



Sistemas operativos Linux

## Supresión de un punto de montaje de un grupo de recursos

---

Puede que desee eliminar un punto de montaje que ya no se necesita.

### Procedimiento

---

Para suprimir un punto de montaje, complete los pasos siguientes:

1. Compruebe si el grupo de recursos `tsm-$INST_NAME-rg` está en línea emitiendo el mandato `lssam`.
2. Si el grupo de recursos `tsm-$INST_NAME-rg` está en línea, póngalo fuera de línea emitiendo el siguiente mandato:

```
chrg -o offline tsm-$INST_NAME-rg
```

3. Vaya al directorio `bin` emitiendo el mandato `cd`.
4. Para suprimir un punto de montaje, ejecute el script `delete_mount.sh`. Por ejemplo, el mandato siguiente suprime el punto de montaje `/tsminst1` del grupo de recursos de la instancia de servidor `inst1` IBM Spectrum Protect.

```
./delete_mount.sh /tsminst1 inst1
```

5. Ponga el grupo de recursos `tsm-$INST_NAME-rg` en línea emitiendo el mandato siguiente:

```
chrg -o online tsm-$INST_NAME-rg
```

## Actualización de un servidor configurado con Tivoli System Automation

---

Puede actualizar un servidor configurado con Tivoli System Automation desde la Versión 6.3 o la Versión 7.1.

### Procedimiento

---

Para actualizar el servidor en todos los nodos del clúster, inicie la sesión en el servidor y siga los pasos siguientes. Estos pasos inician la actualización en el nodo primario y, después, la última parte de este procedimiento actualiza el nodo secundario.

1. Detenga los recursos del servidor emitiendo el mandato `chrg -o Offline`. Por ejemplo, el mandato siguiente detiene los recursos del grupo de recursos `tsm-tsminst1-rg`:

```
chrg -o Offline tsm-tsminst1-rg
```

2. Detenga el dominio de Tivoli System Automation emitiendo el mandato `stoprpdomain`. Por ejemplo, el mandato siguiente detiene `tsm_domain`:

```
stoprpdomain tsm_domain
```

3. Monte los puntos de montaje del servidor en el nodo primario.
4. Para actualizar el servidor en el nodo primario, consulte Actualización de IBM Spectrum Protect.
5. Después de que la actualización haya finalizado, complete los pasos posteriores a la actualización para verificar que la actualización se ha realizado correctamente en el nodo primario.
6. Detenga el servidor y desmonte los puntos de montaje del servidor en el nodo primario.
7. Monte los puntos de montaje del servidor en el nodo secundario.
8. Si está actualizando un servidor de la V6 a la V7, realice los pasos siguientes:
  - a. Desinstale el servidor.

Para obtener las instrucciones, consulte Desinstalación del servidor V6.3.

- b. Instale el servidor en el nodo secundario. Siga las instrucciones de Linux: Instalación de los componentes de servidor.

9. Para actualizar el servidor en el nodo secundario, consulte Actualización del servidor.
10. Después de que la actualización haya finalizado, complete los pasos posteriores a la actualización para verificar que la actualización se ha realizado correctamente en el nodo secundario.
11. Desmonte los puntos de montaje del servidor en el nodo secundario.
12. Inicie el dominio de Tivoli System Automation emitiendo el mandato `startrpdomain`. Por ejemplo, el mandato siguiente inicia `tsa_domain`:

```
startrpdomain tsa_domain
```

13. Inicie los recursos del servidor emitiendo el mandato `chrg -o Online`. Por ejemplo, el mandato siguiente inicia los recursos del grupo de recursos `tsm-tsminst1-rg`:

```
chrg -o Online tsm-tsminst1-rg
```


## Configuración de un entorno en clúster de Windows

---





Puede configurar un servidor de IBM Spectrum Protect para Windows en un entorno de clúster de migración tras error de Microsoft. Los entornos de clúster de Windows están formados por componentes como, por ejemplo, servidores IBM Spectrum Protect, hardware y software. Si estos componentes están conectados al mismo sistema de disco el tiempo de inactividad se minimiza.


El software de Microsoft permite configurar, supervisar y controlar componentes de hardware y aplicaciones que están en un clúster de Windows. El administrador utiliza la interfaz del administrador de clústeres de Microsoft y IBM Spectrum Protect para designar organizaciones de clústeres y definir el patrón de recuperación de errores.

IBM Spectrum Protect soporta la migración tras error de cintas para un entorno de clúster utilizando una conexión de fibra o SCSI. Aunque los clústeres de migración tras error de Microsoft no dan soporte a la migración tras error de los dispositivos de cinta, la configuración de la migración tras error puede supervisarse con la interfaz de Microsoft Cluster Administrator después de que se configure en IBM Spectrum Protect.

-  Sistemas operativos Windows Visión general del entorno de Microsoft Failover Cluster  
Con un Microsoft Failover Cluster Manager, puede colocar recursos de un clúster de servidores de IBM Spectrum Protect en un

grupo de clústeres. El grupo de clústeres de IBM Spectrum Protect tiene un nombre de red, una dirección IP, uno o varios discos físicos, un servidor DB2 y un servicio de servidor de IBM Spectrum Protect.

-  Sistemas operativos Windows Recuperación de errores de cinta para los nodos de un clúster  
Los grupos de un clúster pueden transferirse a otros nodos si el nodo que aloja los grupos falla.
-  Sistemas operativos Windows Planificación de un entorno en clúster  
La configuración en un entorno en clúster requiere una planificación para garantizar el rendimiento óptimo del sistema. La decisión de configurar el sistema para incluir clústeres depende de las necesidades de su negocio.
-  Sistemas operativos Windows Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster  
Debe asegurarse de que el clúster esté instalado y configurado correctamente antes de instalar IBM Spectrum Protect.
-  Sistemas operativos Windows Mantenimiento del entorno en clúster  
Después configurar el clúster o los clústeres iniciales, las necesidades de mantenimiento son mínimas.

 Sistemas operativos Windows

## Visión general del entorno de Microsoft Failover Cluster

---

Con un Microsoft Failover Cluster Manager, puede colocar recursos de un clúster de servidores de IBM Spectrum Protect en un grupo de clústeres. El grupo de clústeres de IBM Spectrum Protect tiene un nombre de red, una dirección IP, uno o varios discos físicos, un servidor DB2 y un servicio de servidor de IBM Spectrum Protect.

El nombre de red de la instancia de IBM Spectrum Protect es independiente del nombre del nodo físico en el que se ejecuta el grupo de clústeres de IBM Spectrum Protect y se migra de nodo a nodo. Los clientes se conectan a un servidor de IBM Spectrum Protect utilizando el nombre de red de la instancia, en lugar del nombre de nodo de Windows. El nombre de red de instancia se correlaciona con un nodo primario o de seguridad. La correlación depende del nodo que es propietario del grupo de clústeres. Un cliente que utilice WINS (Windows Internet Name Service) o servicios de directorio para localizar servidores puede realizar automáticamente un seguimiento del servidor en clúster de IBM Spectrum Protect cuando se mueve entre los nodos. Puede realizar automáticamente un seguimiento del servidor en clúster sin modificar o volver a configurar el cliente.

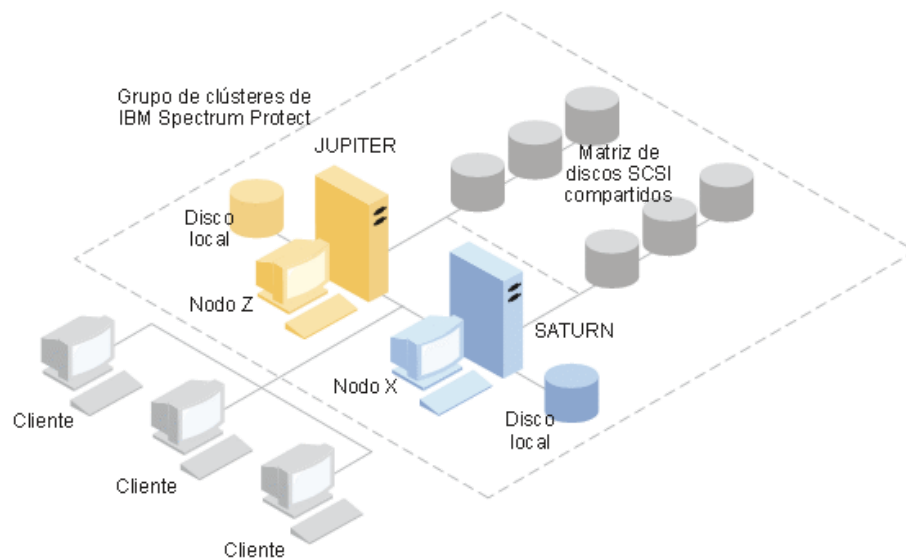
Cada grupo de clústeres de IBM Spectrum Protect tiene su propio disco como parte de un grupo de recursos de clúster. Los grupos de clústeres de IBM Spectrum Protect no pueden compartir datos entre los grupos de clústeres. Cada servidor de IBM Spectrum Protect que se ha configurado en un grupo de clústeres tiene sus propias bases de datos, registros activos, registros de recuperación y conjunto de volúmenes de agrupación de almacenamiento en un disco independiente. Este disco es propiedad del grupo de clústeres donde está configurado el servidor.

Recuerde: Microsoft Failover Cluster Manager sólo da soporte a una dirección IP como recurso. Esto significa que los servidores de IBM Spectrum Protect que se ejecuten en un clúster deben limitar su método de comunicación soportado a sólo TCP/IP. Un cliente que no utilice TCP/IP como método de comunicación no podrá acceder al grupo de clústeres de IBM Spectrum Protect si realiza la migración tras error en el otro nodo de clúster.

El siguiente ejemplo muestra cómo funciona un Microsoft Failover Cluster Manager para un servidor de clúster de IBM Spectrum Protect.

Supongamos que un servidor de IBM Spectrum Protect en clúster denominado JUPITER se ejecuta en el nodo Z y un servidor de IBM Spectrum Protect en clúster denominado SATURN se ejecuta en el nodo X. Los clientes se conectan al servidor de IBM Spectrum Protect JUPITER y al servidor de IBM Spectrum Protect SATURN sin saber qué nodo aloja actualmente su servidor.

Figura 1. Agrupación en clúster con JUPITER como nodo Z y SATURN como nodo X



Cuando falla uno de los recursos de software o de hardware, se produce una recuperación de errores. Los recursos como las aplicaciones, discos y una dirección IP se mueven del nodo con errores al otro nodo. El nodo restante:

- Toma el control del grupo de clústeres de IBM Spectrum Protect
- Pone en línea los recursos de disco, los recursos de red y el recurso de DB2
- Reinicia el servicio de IBM Spectrum Protect

- Proporciona acceso a los administradores y los clientes

Si el nodo X falla, el nodo Z asume el rol de ejecutar SATURN. Para un cliente, es exactamente igual que si se desactiva el nodo X y se vuelve a activar inmediatamente. Los clientes experimentan la pérdida de todas las conexiones con SATURN y todas las transacciones activas se retrotraen al cliente. Los clientes deben volver a conectarse con SATURN una vez perdida la conexión. La ubicación de SATURN no es aparente para el cliente.


 Sistemas operativos Windows

## Recuperación de errores de cinta para los nodos de un clúster

---

Los grupos de un clúster pueden transferirse a otros nodos si el nodo que aloja los grupos falla.

Un nodo puede alojar unidades físicas o lógicas, denominadas recursos. Los administradores organizan estos recursos de clúster en unidades funcionales denominadas grupos y asignan estos grupos a nodos individuales. Si un nodo falla, el clúster de servidores transfiere los grupos alojados en el nodo a otros nodos del clúster. Este proceso de transferencia se denomina *recuperación de errores*. El proceso inverso, el *restablecimiento*, tiene lugar cuando el nodo con errores se vuelve a activar y los grupos en los que se había ejecutado la recuperación de errores se transfieren de nuevo al nodo original.

-  Sistemas operativos Windows Recuperación de errores de cinta de fibra  
IBM Spectrum Protect puede gestionar la recuperación de errores de los dispositivos de cinta y biblioteca con conexión directa de canal de fibra en un sistema Microsoft Windows en un entorno en clúster sin necesidad de hardware adicional.

 Sistemas operativos Windows

## Planificación de un entorno en clúster

---

La configuración en un entorno en clúster requiere una planificación para garantizar el rendimiento óptimo del sistema. La decisión de configurar el sistema para incluir clústeres depende de las necesidades de su negocio.




Planifique una configuración de clústeres que se adapte a su entorno. Además de comprobar que tiene el tipo correcto de hardware y el software aplicable, debe configurar un patrón de migración tras error.

Cuando un nodo falla o necesita ponerse fuera de línea, ¿qué nodo o nodos del clúster continúan con el proceso de las transacciones? En un clúster de dos nodos, se necesita poca planificación. En un clúster más complejo, debe tener en cuenta cómo se maneja mejor el proceso de las transacciones. Es preciso prever algún tipo de equilibrio de carga entre los nodos para mantener un rendimiento óptimo. También es preciso asegurarse de que sus clientes no puedan percibir ningún retraso ni un descenso en la productividad.

Microsoft Cluster Servers y Microsoft Failover Clusters requieren que cada instancia de servidor de IBM Spectrum Protect tenga un conjunto privado de recursos de disco. Aunque los nodos pueden compartir recursos de disco, sólo un nodo puede controlar activamente un disco cada vez.


Atención: Asegúrese de que se haya instalado el mismo nivel de Windows (Windows 2012, Windows 2012 R2 y Windows 2016) en todos los sistemas del clúster.

¿Qué configuración es mejor? Para determinar cuál es la mejor instalación, analice las diferencias de rendimiento y de coste. Supongamos que tiene un clúster de servidores dedicados de IBM Spectrum Protect cuyos nodos tienen una potencia comparable. Durante la migración tras error, el rendimiento de una configuración puede disminuir porque un nodo debe gestionar las dos instancias de clúster de IBM Spectrum Protect. Si cada nodo gestiona 100 clientes en una operación normal, durante una anomalía un nodo gestiona 200 clientes.

-  Sistemas operativos Windows Hoja de trabajo de configuración del clúster  
Registre sus respuestas a las siguientes preguntas de planificación antes de realizar la configuración del clúster.
-  Sistemas operativos Windows Planificación de la configuración de hardware y software del clúster  
La configuración de hardware y software del clúster se determina durante la fase de planificación y antes de la instalación.
-  Sistemas operativos Windows Configuración de IBM Spectrum Protect en Microsoft Failover Cluster  
El procedimiento de configuración de clúster de IBM Spectrum Protect debe completarse en el conjunto de nodos que alojan un grupo de clústeres de IBM Spectrum Protect.

### Información relacionada:

 Sistemas operativos soportados de IBM Spectrum Protect

 Sistemas operativos Windows

## Hoja de trabajo de configuración del clúster

---

Registre sus respuestas a las siguientes preguntas de planificación antes de realizar la configuración del clúster.

1. ¿Qué tipo de solución de clúster se ajusta mejor a las necesidades de su negocio?
2. ¿Qué tipo de patrón de migración tras error necesita?


La utilización del soporte para la recuperación de errores de cinta también afectará a este patrón.

3. ¿Será necesario el soporte de migración tras error de cinta?

Tenga en cuenta cómo se utilizan los dispositivos de cinta en las instancias de clúster de IBM Spectrum Protect. La forma en la que las instancias de clúster utilizan los dispositivos de cinta puede limitar el número de nodos del patrón de migración tras error a dos.

4. ¿Cuáles son los recursos que se dedican a IBM Spectrum Protect?

Tipo de recurso	Nombre de recurso
Grupo de recursos de clúster	
Recursos de disco físico	
Dirección IP	
Máscara de subred	
Red	
Nombre de red (nombre del servidor)	
Nodos	
Recuperación de errores de cinta (opcional): nombre de dispositivo - ambos nodos	

 Sistemas operativos Windows

## Planificación de la configuración de hardware y software del clúster

La configuración de hardware y software del clúster se determina durante la fase de planificación y antes de la instalación.

### Procedimiento


Las siguientes directrices permiten determinar qué recursos son necesarios para que el clúster de IBM Spectrum Protect sea satisfactorio:

1. Decida qué configuración de clúster debe utilizar con los servidores que utilizan dispositivos de disco. Cada instancia de clúster de IBM Spectrum Protect necesita un conjunto aparte de recursos de disco en el subsistema de disco compartido. Es posible que tenga problemas si configura el subsistema de E/S como una matriz de gran tamaño. Por ejemplo, cuando configura un clúster de dos servidores y más adelante decide ampliar a un clúster de cuatro servidores.
2. Identifique los recursos de disco que se van a dedicar a IBM Spectrum Protect. No divida un disco compartido en varias particiones con cada partición asignada a una aplicación diferente y, por lo tanto, a un grupo de clúster diferente.

Por ejemplo, la aplicación A, una aplicación estable, puede verse obligada a una migración tras error debido a un problema de software con la aplicación B. Esta migración tras error se puede producir si ambas aplicaciones utilizan particiones que forman parte del mismo disco físico. Este problema provoca una recuperación de errores de los servicios de clúster en la aplicación B y su recurso de disco de correquisito. Como las particiones están en el mismo disco físico, también se fuerza la recuperación de errores de la aplicación A. Por lo tanto, al instalar y configurar una aplicación de IBM Spectrum Protect, dedique un disco compartido como recurso que se pueda recuperar si es necesario.

3. Asegúrese de tener la dirección IP y el nombre de red de cada una de las instancias del servidor de IBM Spectrum Protect que configure. Para un clúster que implique a dos instancias de clúster de IBM Spectrum Protect, se necesitan dos nombres de red.
4. Cree un grupo de recursos de clúster y traspase los recursos de disco a él. Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster. Inicialmente, el grupo debe contener solamente recursos de disco. O bien, puede optar por cambiar el nombre de un grupo de recursos existente que contenga sólo recursos de disco.
5. IBM Spectrum Protect se instala en un disco local en cada nodo del clúster. Determine el disco que debe utilizarse en cada nodo. Utilice la misma letra de unidad en cada sistema. Cuando el servidor de IBM Spectrum Protect está instalado en un entorno de clúster, la opción SANDISCOVERY debe establecerse en ON. De forma predeterminada, esta opción está establecida en OFF.
6. SI decide no utilizar el soporte de migración tras error de cintas de IBM Spectrum Protect, puede conectar dispositivos de cinta en cualquiera de las configuraciones siguientes:

Configuración	Ventajas e inconvenientes	El espacio de disco necesario	Cómo habilitar la migración	Qué hacer cuando se produce una migración tras error
Conectarlos al nodo en el que la instancia del servidor de IBM Spectrum Protect está activa actualmente.	Esta configuración permite operaciones de copia de seguridad y restauración de alto rendimiento. Sin embargo, no está completamente automatizada porque se necesita la intervención del operador para dar servicio a una recuperación de errores cuando se producen retardos de reparación.	Defina suficiente espacio de volumen para los datos basados en disco para mantener el promedio equivalente a más de dos días de datos.	Establezca una jerarquía de agrupaciones de almacenamiento para mover los datos eficazmente al dispositivo de cinta.	Desconecte manualmente el dispositivo de cinta y vuelva a conectarlo al nodo en el que se ha activado el servidor.
Conectarlos a un tercer sistema sin clúster en el que hay activa una instancia adicional del servidor de IBM Spectrum Protect.	Puede que esta configuración no sea viable en instalaciones con comunicaciones de ancho de banda bajo entre los servidores del clúster y el servidor de controlador de dispositivo de cinta.	Defina suficiente espacio de volumen para los datos basados en disco para mantener el promedio equivalente a más de dos días de datos.	Utilice los volúmenes virtuales para mover los datos de los volúmenes de disco locales al dispositivo de cinta.	No se requiere ninguna acción; el servidor activado continúa utilizando los volúmenes virtuales.

 Sistemas operativos Windows

## Configuración de IBM Spectrum Protect en Microsoft Failover Cluster

El procedimiento de configuración de clúster de IBM Spectrum Protect debe completarse en el conjunto de nodos que alojan un grupo de clústeres de IBM Spectrum Protect.

Los pasos del procedimiento varían dependiendo del nodo donde realice la configuración actualmente. Cuando configura el nodo primario en el conjunto, se crea y se configura la instancia de servidor de IBM Spectrum Protect. Cuando configura los demás nodos del conjunto, cada nodo se actualiza utilizando un método específico. La forma en la que se actualiza el nodo le permite alojar la instancia de servidor de IBM Spectrum Protect creada en el nodo primario. Debe instalarse y configurarse un servidor de IBM Spectrum Protect en el primer nodo del conjunto antes de configurar los demás nodos del conjunto. El incumplimiento de este requisito hará que la configuración falle.

Asegúrese de configurar completamente un grupo de clústeres de IBM Spectrum Protect antes de continuar en el paso siguiente cuando configure varios grupos de clústeres de IBM Spectrum Protect. Como trabaja con direcciones IP y nombres de red diferentes para cada grupo de clústeres de IBM Spectrum Protect, disminuye la posibilidad de errores al configurar cada grupo de clústeres por separado.

 Sistemas operativos Windows

## Configuración de IBM Spectrum Protect en un Microsoft Failover Cluster

Debe asegurarse de que el clúster esté instalado y configurado correctamente antes de instalar IBM Spectrum Protect.


### Procedimiento

Para configurar IBM Spectrum Protect en un Microsoft Failover Cluster, siga estos pasos:

1. Asegúrese de que el sistema operativo de Windows esté instalado en todos los sistemas que formen parte del clúster. Para obtener la información más actual sobre los sistemas operativos Windows soportados, consulte la nota técnica 1243309.
2. Inicie sesión con el ID de usuario de dominio. El usuario de dominio debe estar en el mismo dominio que el servidor de IBM Spectrum Protect.
3. Asegúrese de que el clúster de recuperación de errores esté instalado y configurado para todos los sistemas del clúster. Si tiene previsto instalar el servidor de IBM Spectrum Protect en el sistema operativo Windows Server 2012, instale antes el servidor de automatización de clúster de migración tras error y la interfaz de mandatos de clúster de migración tras error. Para instalar estos componentes, emita los siguientes mandatos desde Windows 2.0 PowerShell:

```
Install-WindowsFeature -Name RSAT-Clustering-AutomationServer
Install-WindowsFeature -Name RSAT-Clustering-CmdInterface
```

4. Compruebe que todos los nodos y discos compartidos del clúster estén operativos.
  5. Asegúrese de que los dispositivos de cinta compartidos estén operativos si se está utilizando el soporte de recuperación de errores de cintas de IBM Spectrum Protect.
-  Sistemas operativos Windows Preparación de un grupo de Microsoft Failover Cluster para un servidor virtual básico  
Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster.
  -  Sistemas operativos Windows Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster  
Instale el servidor de IBM Spectrum Protect en cada nodo del clúster que aloje un servidor en clúster de IBM Spectrum Protect.
  -  Sistemas operativos Windows Inicialización del servidor de IBM Spectrum Protect para un Microsoft Failover Cluster en el nodo primario  
Después de instalar IBM Spectrum Protect en los nodos del clúster, debe inicializar el servidor en el nodo primario.
  -  Sistemas operativos Windows Verificación de la configuración de IBM Spectrum Protect en un Microsoft Failover Cluster  
Cuando termine de configurar IBM Spectrum Protect en un Microsoft Failover Cluster, puede revisar la ventana de resumen de Failover Cluster Manager. Verifique que la agrupación en clúster se haya completado correctamente y que el servidor de IBM Spectrum Protect se haya iniciado.
  -  Sistemas operativos Windows Prueba de recuperación de errores para el clúster  
Después de completar la configuración de clúster, ejecute una prueba de migración tras error para comprobar que los nodos están funcionando correctamente.

 Sistemas operativos Windows

## Preparación de un grupo de Microsoft Failover Cluster para un servidor virtual básico

---

Cada instancia del servidor de IBM Spectrum Protect requiere un grupo de recursos de clúster.

### Antes de empezar

---

Utilice el programa Failover Cluster Manager en el sistema que es propietario del recurso de cinta o disco compartido para preparar su grupo de recursos. Inicialmente, el grupo debe contener solamente recursos de disco. Puede crear un grupo y mover recursos de disco a él. También puede optar por cambiar el nombre de un grupo de recursos existente que contenga sólo recursos de disco.

Cuando construya los grupos de recursos, tenga en cuenta los siguientes elementos:

- Asegúrese de que cada grupo de recursos tenga un nombre distintivo. No cambie los nombres una vez creado el grupo porque puede dañar la configuración.
- Asegúrese de que todos los nodos del clúster se encuentren en línea.
- Asegúrese de que el grupo esté en línea y sea propiedad del nodo donde se ha instalado la instancia de servidor inicial.

### Procedimiento

---

Para preparar un grupo de recursos para la configuración de clúster, realice los siguientes pasos:

1. Abra el programa Failover Cluster Manager. Pulse el botón derecho sobre Servicios y aplicaciones y, a continuación, seleccione Más acciones > Crear aplicación o servicio vacío.
2. Pulse el botón derecho sobre Nuevo servicio o aplicación, seleccione Cambiar el nombre y elija un nombre nuevo para el grupo de recursos, como por ejemplo TSMGROUP.
3. Pulse el botón derecho sobre el grupo de recursos TSMGROUP y seleccione Añadir almacenamiento.
4. En el panel Añadir área de almacenamiento, seleccione el volumen o los volúmenes compartidos para IBM Spectrum Protect y pulse OK. Se muestra el grupo de recursos TSMGROUP, que contiene los volúmenes de disco que ha agregado.

 Sistemas operativos Windows

## Instalación de IBM Spectrum Protect en un Microsoft Failover Cluster

---

Instale el servidor de IBM Spectrum Protect en cada nodo del clúster que aloje un servidor en clúster de IBM Spectrum Protect.


### Procedimiento

---

Siga estos pasos para cada nodo del clúster para instalar el servidor de IBM Spectrum Protect:



1. Inicie sesión con un ID de usuario de dominio o administrador. El usuario de dominio debe ser miembro del grupo de administradores del dominio.
2. Instale el servidor de IBM Spectrum Protect en un disco local en cada nodo. Utilice la misma letra de unidad de disco local para cada nodo.
3. Reinicie el sistema cuando finalice la instalación del servidor.

 Sistemas operativos Windows

## Inicialización del servidor de IBM Spectrum Protect para un Microsoft Failover Cluster en el nodo primario


---

Después de instalar IBM Spectrum Protect en los nodos del clúster, debe inicializar el servidor en el nodo primario.

### Procedimiento

---

1. Asegúrese de que todos los sistemas se reinicien después de la instalación. Compruebe que todos los sistemas se ejecuten correctamente.
2. Inicie sesión con un ID de usuario de dominio o administrador. El usuario de dominio debe estar en el mismo dominio que el servidor de IBM Spectrum Protect.
3. Abra el programa Failover Cluster Manager y verifique que los recursos están en línea y disponibles en el nodo primario.
4. Inicie el proceso de inicialización en el nodo primario del clúster. En el programa Failover Cluster Manager, verifique que el propietario del grupo de recursos sea el nodo primario del clúster.
5. En el menú Inicio, pulse Todos los programas > Servidor de IBM Spectrum Protect > Asistente de configuración.
6. Siga las instrucciones del asistente; pulse Siguiente para seguir los pasos del asistente. Cuando se le solicite el ID de usuario, escriba el nombre de la cuenta de dominio que desee asociar con el clúster.
7. Si se ha completado la inicialización, pulse Finalizado.

 Sistemas operativos Windows

## Verificación de la configuración de IBM Spectrum Protect en un Microsoft Failover Cluster

---

Cuando termine de configurar IBM Spectrum Protect en un Microsoft Failover Cluster, puede revisar la ventana de resumen de Failover Cluster Manager. Verifique que la agrupación en clúster se haya completado correctamente y que el servidor de IBM Spectrum Protect se haya iniciado.

### Procedimiento

---

Para verificar que la instancia del servidor de IBM Spectrum Protect en un Microsoft Failover Cluster se ha creado y configurado correctamente, realice los pasos siguientes:

1. En Failover Cluster Manager, seleccione la instancia del servidor. El nombre de red que ha configurado se muestra en el panel Nombre del servidor.
2. En el panel Otros recursos, confirme que se visualizan la instancia de servidor y el recurso de servidor de IBM® DB2.
3. Pulse con el botón derecho la instancia del servidor de IBM Spectrum Protect y seleccione Colocar este recurso en línea.

 Sistemas operativos Windows

## Prueba de recuperación de errores para el clúster

---

Después de completar la configuración de clúster, ejecute una prueba de migración tras error para comprobar que los nodos están funcionando correctamente.

### Procedimiento

---

1. Abra Failover Cluster Manager. En Other Resources, pulse con el botón derecho el recurso IBM Spectrum Protect Instance(x). Seleccione Bring this resource online.
2. Para probar la recuperación de errores, pulse con el botón derecho el grupo de recursos de clúster de IBM Spectrum Protect y seleccione Move this service or application to another node.
3. Compruebe que la recuperación de errores desde el segundo nodo al primero se realice satisfactoriamente.

## Mantenimiento del entorno en clúster

---

Después configurar el clúster o los clústeres iniciales, las necesidades de mantenimiento son mínimas.

Compruebe regularmente las anotaciones de sucesos de Windows (preferiblemente a diario), para controlar la actividad de los nodos del clúster. Utilice el registro para comprobar si un nodo falla y necesita mantenimiento.

La siguiente lista de temas describe las situaciones que puedan afectar a la configuración o el formato del clúster después de que esté en funcionamiento.

-  **Migración de un servidor de IBM Spectrum Protect existente a un clúster**  
El motivo de mover datos de cliente a un clúster es similar al motivo de agregar un servidor a un clúster. Desea aumentar la disponibilidad y la fiabilidad de los datos para todos los usuarios. Cuando el servidor forma parte del clúster, proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.
-  **Agregación de un servidor de IBM Spectrum Protect con copia de seguridad y restauración**  
Si tiene recursos de hardware limitados, puede agregar un servidor de IBM Spectrum Protect ya existente a un clúster utilizando un procedimiento de copia de seguridad y restauración.
-  **Gestión de un servidor de IBM Spectrum Protect virtual en un clúster**  
Para la mayoría de las tareas, puede administrar un servidor de IBM Spectrum Protect virtual igual que un servidor no de clúster. Para completar tareas como el inicio y detención del servidor o el movimiento de un grupo de recursos a otro nodo para completar el mantenimiento del sistema, debe utilizar la interfaz de Microsoft Cluster Administrator.
-  **Gestión de la recuperación de errores de cinta en un clúster**  
Como parte de las tareas rutinarias, compruebe las anotaciones de sucesos para asegurarse de que la configuración funciona correctamente. Si un servidor falla, se registra el error. La anotación ofrece información sobre el motivo por el que se produjo la anomalía.
-  **Resolución de problemas con las anotaciones de clúster de IBM Spectrum Protect**  
El DLL de recursos de clúster de IBM Spectrum Protect notifica sucesos y errores a las anotaciones de clúster. Las anotaciones de clúster son una herramienta útil de resolución de problemas. Cuando se activan estas anotaciones, registran las acciones de cada componente del servicio de clúster como el resultado de cada acción.

## Migración de un servidor de IBM Spectrum Protect existente a un clúster


---

El motivo de mover datos de cliente a un clúster es similar al motivo de agregar un servidor a un clúster. Desea aumentar la disponibilidad y la fiabilidad de los datos para todos los usuarios. Cuando el servidor forma parte del clúster, proporciona un nivel extra de seguridad al garantizar que ninguna transacción se pierda debido a un servidor anómalo. El patrón de migración tras error establecido previene futuras anomalías.

### Acerca de esta tarea

---

Para migrar un servidor de IBM Spectrum Protect existente a un clúster, puede mover los clientes o realizar un procedimiento de copia de seguridad o restauración. La opción depende principalmente de la disponibilidad y la capacidad de los otros sistemas de servidor IBM Spectrum Protect del sitio y de su familiaridad con el procedimiento de copia de seguridad y restauración.

-  **Movimiento de los clientes**  
Si mueve clientes de un sistema de servidor de IBM Spectrum Protect no de clúster a otro en clúster, tendrá tiempo para migrar gradualmente los usuarios al nuevo sistema y no interrumpir los servicios. No obstante, debe tener el hardware necesario para ejecutar dos servidores de IBM Spectrum Protect simultáneamente.

#### Tareas relacionadas:

Instalación y actualización del servidor

## Agregación de un servidor de IBM Spectrum Protect con copia de seguridad y restauración

---

Si tiene recursos de hardware limitados, puede agregar un servidor de IBM Spectrum Protect ya existente a un clúster utilizando un procedimiento de copia de seguridad y restauración.

## Acerca de esta tarea


---

Por ejemplo, suponga que el único hardware que tiene son los dos sistemas de servidor que se van a agrupar en clúster. Y tiene previsto utilizar el sistema que está ejecutando actualmente el servidor de IBM Spectrum Protect como nodo. Complete este procedimiento para eliminar IBM Spectrum Protect del sistema y volver a instalarlo en el clúster:

## Procedimiento

---

1. Realice una copia de seguridad de todas las agrupaciones de almacenamiento de disco en una agrupación de almacenamiento de copia.
2. Realice una copia de seguridad de la base de datos del servidor de IBM Spectrum Protect existente.
3. Instale y configure el clúster.
4. Restaure la base de datos en el servidor de IBM Spectrum Protect en clúster.
5. Restaure los volúmenes de agrupación de almacenamiento de disco de la agrupación de almacenamiento de copia.
6. Después de comprobar que todos los datos están en el servidor en clúster, elimine el servidor antiguo.

 Sistemas operativos Windows

## Gestión de un servidor de IBM Spectrum Protect virtual en un clúster

---

Para la mayoría de las tareas, puede administrar un servidor de IBM Spectrum Protect virtual igual que un servidor no de clúster. Para completar tareas como el inicio y detención del servidor o el movimiento de un grupo de recursos a otro nodo para completar el mantenimiento del sistema, debe utilizar la interfaz de Microsoft Cluster Administrator.

## Acerca de esta tarea

---

La interfaz de Microsoft Cluster Administrator está disponible a través del grupo de programas Herramientas administrativas. La interfaz es una vista detallada de la configuración del servidor virtual. La configuración del servidor virtual incluye detalles como, por ejemplo, los servidores de Windows físicos que componen el clúster y sus recursos, las conexiones de red y el estado. Visualice los componentes de una configuración de servidor virtual e inicie, detenga o migre tras error un servidor virtual utilizando esta interfaz. Gestione un servidor IBM Spectrum Protect virtual utilizando la interfaz de Microsoft Cluster Administrator para evitar fallos del servidor y mensajes de error. Por ejemplo, si utiliza el gestor de control de servicio de Windows para apagar el servidor, puede recibir mensajes de que el servidor ha fallado.

Es posible que desee mover un servidor IBM Spectrum Protect virtual cuando el servidor de Windows actúa como nodo primario y este servidor requiere mantenimiento de hardware o del sistema. Utilice la interfaz de Microsoft Cluster Administrator para mover la gestión del servidor IBM Spectrum Protect virtual a un nodo secundario hasta que se haya completado el mantenimiento.

 Sistemas operativos Windows

## Gestión de la recuperación de errores de cinta en un clúster

---

Como parte de las tareas rutinarias, compruebe las anotaciones de sucesos para asegurarse de que la configuración funciona correctamente. Si un servidor falla, se registra el error. La anotación ofrece información sobre el motivo por el que se produjo la anomalía.

## Acerca de esta tarea

---

A veces un nodo debe reincorporarse al clúster, por ejemplo:

- Cuando falla un nodo
- Cuando se agrega una nueva tarjeta de fibra de adaptador de bus de host (cambios de equipo)

## Procedimiento

---

Realice las siguientes tareas para asegurarse de que un nodo pueda incorporarse satisfactoriamente al clúster:

- Actualice, si es necesario, la unidad y la biblioteca que utilizan la herramienta de clúster de IBM Spectrum Protect.
- Deje el servidor de IBM Spectrum Protect fuera de línea hasta que el nodo que ha fallado se reincorpore al clúster. Esta acción permite garantizar que el servidor de IBM Spectrum Protect que se ejecuta en el otro nodo no se vea afectado.

 Sistemas operativos Windows

# Resolución de problemas con las anotaciones de clúster de IBM Spectrum Protect

---

El DLL de recursos de clúster de IBM Spectrum Protect notifica sucesos y errores a las anotaciones de clúster. Las anotaciones de clúster son una herramienta útil de resolución de problemas. Cuando se activan estas anotaciones, registran las acciones de cada componente del servicio de clúster como el resultado de cada acción.

En comparación con el registro de sucesos de Microsoft Windows, el registro de clúster es un registro completo de la actividad del clúster. Las anotaciones de clúster registran la actividad del servicio de clúster que se registra en las anotaciones de sucesos. Aunque las anotaciones de sucesos pueden indicarle un problema, las anotaciones de clúster le ayudan a resolverlo.

Las anotaciones de clúster están habilitadas de forma predeterminada en Windows. La salida se imprime como un archivo de registro en %SystemRoot%\Cluster. Para obtener más información, consulte la documentación de ayuda en línea de Windows.

## Configuración de clientes para aplicaciones, máquinas virtuales y sistemas

---

El servidor protege los datos de los clientes, que pueden incluir aplicaciones, máquinas virtuales y sistemas. Para iniciar la protección de datos de cliente, registre el nodo cliente con el servidor y seleccione una planificación de copia de seguridad para proteger los datos de cliente.

- Adición de clientes  
Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.
- Personalización de políticas  
Los objetivos de una empresa en cuanto a la protección y conservación de los datos suelen definirlos los ejecutivos de la empresa, los asesores legales y otros cargos importantes. Las *políticas* son la forma de adaptar el funcionamiento de IBM Spectrum Protect a los objetivos de protección y conservación de datos de su empresa.

## Adición de clientes

---

Después de implementar una solución de protección de datos con IBM Spectrum Protect, puede expandir la solución añadiendo clientes.

### Acerca de esta tarea

---

El procedimiento describe los pasos básicos para añadir un cliente. Para obtener instrucciones más detalladas sobre la configuración de clientes, consulte la documentación del producto que haya instalado en el nodo cliente. Puede tener los siguientes tipos de nodos de cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

## Procedimiento

---

Para añadir un cliente, complete los pasos siguientes:

1. Seleccione el software a instalar en el nodo de cliente y planifique la instalación. Siga las instrucciones de la sección Selección del software de cliente y planificación de la instalación.

2. Especifique cómo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de la sección Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente.
3. Especifique cuándo hacer copia de seguridad y archivado de los datos de cliente. Siga las instrucciones de la sección Planificación de copia de seguridad y operaciones de archivado.
4. Para permitir que el cliente se conecte al servidor, registre el cliente. Siga las instrucciones de la sección Registro de clientes.
5. Para iniciar la protección de un nodo de cliente, instale y configure el software seleccionado en el nodo de cliente. Siga las instrucciones de la sección Instalación y configuración de clientes.

## Selección del software de cliente y planificación de la instalación

Diferentes tipos de datos requieren diferentes tipos de protección. Identifique el tipo de datos que debe proteger y seleccione el software apropiado.

### Acerca de esta tarea

La práctica preferida consiste en instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente, de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM Spectrum Protect for Virtual Environments. Si instala un producto para el cual el aceptador de cliente no ejecuta planificaciones, debe seguir las instrucciones de configuración de la documentación de producto para asegurarse de que se puedan ejecutar operaciones planificadas.

### Procedimiento

En función de su objetivo, seleccione los productos para instalar y revise las instrucciones de instalación.

Consejo: Si instala el software de cliente ahora, también debe completar las tareas de configuración de cliente que se describen en Instalación y configuración de clientes antes de poder utilizar el cliente.

Objetivo	Producto y descripción	Instrucciones de instalación
Proteger un servidor de archivos o una estación de trabajo	El cliente de copia de seguridad y archivado realiza la copia de seguridad y archivado de directorios y archivos desde los servidores de archivos y las estaciones de trabajo al almacenamiento. También puede restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos.	<ul style="list-style-type: none"> <li>• Requisitos del cliente de archivado y copia de seguridad</li> <li>• Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux</li> <li>• Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul>
Proteger aplicaciones con prestaciones de restauración y copia de seguridad de instantáneas	IBM Spectrum Protect Snapshot protege los datos con prestaciones de restauración y copia de seguridad de instantánea conocidas por la aplicación e integradas. Puede proteger datos almacenados por aplicaciones de IBM Software de base de datos de DB2 y SAP, Oracle, Microsoft Exchange y Microsoft SQL Server.	<ul style="list-style-type: none"> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot para VMware</li> <li>• Instalación y actualización de IBM Spectrum Protect Snapshot para Windows</li> </ul>
Proteja una aplicación de correo electrónico en un servidor IBM Domino	IBM Spectrum Protect for Mail: Data Protection para IBM® Domino automatiza la protección de datos, de forma que las copias de seguridad se completen sin tener que concluir los servidores IBM Domino.	<ul style="list-style-type: none"> <li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> </ul>
Proteja una aplicación de correo electrónico en un servidor Microsoft Exchange	IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server automatiza la protección de datos de forma que las copias de seguridad se completen sin tener que concluir los servidores Microsoft Exchange.	Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server

Objetivo	Producto y descripción	Instrucciones de instalación
Proteja una base de datos IBM DB2	La interfaz de programación de aplicaciones (API) del cliente de copia de seguridad y archivado se puede utilizar para realizar la copia de seguridad de los datos de DB2 en el servidor de IBM Spectrum Protect.	Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos IBM Informix	La API del cliente de copia de seguridad y archivado se puede utilizar para hacer una copia de seguridad de los datos de Informix en un servidor IBM Spectrum Protect.	Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)
Proteja una base de datos de Microsoft SQL.	IBM Spectrum Protect para bases de datos: Data Protection for Microsoft SQL Server protege datos de Microsoft SQL.	Instalación de Data Protection para SQL Server en Windows Server Core
Proteger una base de datos Oracle	IBM Spectrum Protect para bases de datos: Data Protection for Oracle protege los datos de Oracle.	Instalación de Data Protection for Oracle
Proteger un entorno SAP	IBM Spectrum Protect for Enterprise Resource Planning: La protección de datos para SAP proporciona protección personalizada para entornos SAP. El producto está diseñado para mejorar la disponibilidad de servidores de bases de datos SAP y reducir la carga de trabajo de administración.	<ul style="list-style-type: none"> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2</li> <li>• Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle</li> </ul>
Proteger una máquina virtual	<p>IBM Spectrum Protect for Virtual Environments proporciona protección que se ha adaptado para los entornos virtuales Microsoft Hyper-V y VMware. Puede utilizar IBM Spectrum Protect for Virtual Environments para crear copias de seguridad siempre incrementales que están almacenadas en un servidor centralizado, para crear políticas de copia de seguridad y para restaurar máquinas virtuales o archivos individuales.</p> <p>Como alternativa, puede utilizar el cliente de copia de seguridad y archivado para hacer copias de seguridad y restaurar una máquina virtual VMware o Microsoft Hyper-V completa. También puede hacer copia de seguridad y restaurar archivos y directorios desde una máquina virtual VMware.</p>	<ul style="list-style-type: none"> <li>• Instalación de protección de datos para Microsoft Hyper-V</li> <li>• Instalación y actualización de Data Protection para VMware</li> <li>• Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)</li> </ul>

Consejo: Para utilizar el cliente para gestionar el espacio, puede instalar IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM for Windows.

## Especificación de reglas para hacer copia de seguridad y archivado de los datos de cliente

Antes de añadir un cliente, asegúrese de que se han especificado las reglas correctas de copia de seguridad y archivado de los datos de cliente. Durante el proceso de registro de cliente, asigne el nodo de cliente a un dominio de políticas, que tenga las reglas que controlan cómo y cuándo se almacenan los datos de cliente.

### Antes de empezar

Determine cómo debe procederse:

- Si está familiarizado con las políticas que están configuradas para la solución y sabe que no requieren cambios, continúe con Planificación de copia de seguridad y operaciones de archivado.
- Si no está familiarizado con las políticas, siga los pasos de este procedimiento.

## Acerca de esta tarea

---

Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y el periodo de tiempo durante el cual los datos se retienen y están disponibles para que los clientes los restauren. Para cumplir los objetivos de protección de datos, puede actualizar la política predeterminada y crear sus propias políticas. Una política incluye las siguientes reglas:

- Cómo y cuándo se hace una copia de seguridad de los archivos y se archivan en el almacenamiento del servidor.
- El número de copias de un archivo y el periodo de tiempo que se mantienen las copias en el almacenamiento del servidor.

Durante el proceso de registro del cliente, puede asignar un cliente a un *dominio de políticas*. La política para un cliente específico la determinan las reglas del dominio de políticas al que está asignado el cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas* activo.

Cuando un cliente realiza una copia de seguridad o de archivado de un archivo, el archivo se enlaza a una clase de gestión del conjunto de políticas activas del dominio de políticas. Una *clase de gestión* es el conjunto principal de las reglas para gestionar datos de cliente. Las operaciones de copia de seguridad y archivado en el cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas a menos que se personalice adicionalmente la política. Una política puede personalizarse definiendo más clases de gestión y asignando su uso a través de las opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo editable local en el sistema cliente y en un conjunto de opciones de cliente del servidor. Las opciones del conjunto de opciones de cliente del servidor pueden sustituir o añadirse a las opciones en el archivo de opciones de cliente local.

## Procedimiento

---

1. Revise las políticas configuradas para su solución siguiendo las instrucciones incluidas en Visualización de políticas.
2. Si necesita realizar cambios poco importantes para adaptarse a los requisitos de retención de datos, siga las instrucciones incluidas en Edición de políticas.
3. Opcional: Si necesita crear dominios de políticas o realizar cambios extensos en las políticas para satisfacer los requisitos de retención de datos, consulte Personalización de políticas.

## Visualización de políticas

---

Vea las políticas para determinar si se deben editar para satisfacer los requisitos.

## Procedimiento

---

1. Para ver el conjunto de políticas activas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
  - b. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.
2. Para ver los conjuntos de políticas inactivas para un dominio de políticas, complete los pasos siguientes:
  - a. En la página Conjuntos de políticas, pulse el conmutador Configurar. Ahora puede ver y editar los conjuntos de políticas que están inactivos.
  - b. Desplácese a través de conjuntos de políticas inactivas utilizando las flechas hacia adelante y atrás. Al visualizar un conjunto de políticas inactivas, los valores que diferencian el conjunto de políticas inactivas del conjunto de políticas activas se resaltan.
  - c. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

## Edición de políticas

---

Para cambiar las reglas que se aplican a un dominio de políticas, edite el conjunto de políticas activas para el dominio de políticas. También puede activar un conjunto de políticas diferente para un dominio.

## Antes de empezar

---

Los cambios en la política pueden afectar a la retención de datos. Asegúrese de que continúa haciendo copia de seguridad de los datos que son esenciales para su organización para que pueda restaurar esos datos si se produce un desastre. Además, asegúrese de que el sistema tiene suficiente espacio de almacenamiento para operaciones de copia de seguridad planificadas.

## Acerca de esta tarea

---

Edite un conjunto de políticas cambiando una o más clases de gestión dentro de un conjunto de políticas. Si edita un conjunto de políticas activas, los cambios no están disponibles para los clientes a menos que reactive el conjunto de políticas. Para hacer que el

conjunto de políticas editado esté disponible para los clientes, active el conjunto de políticas.

Aunque puede definir varios conjuntos de políticas para un dominio de políticas, sólo un conjunto de políticas puede estar activo. Cuando activa un conjunto de políticas diferente, sustituye al conjunto de políticas activo actualmente.

Para obtener información acerca de las prácticas preferidas para definir las políticas, consulte Personalización de políticas.

## Procedimiento

1. En la página Servicios del Centro de operaciones, seleccione un dominio de políticas y pulse Detalles.
2. En la página Resumen del dominio de políticas, pulse el separador Conjuntos de políticas.

La página Conjuntos de políticas indica el nombre del conjunto de políticas activo y lista todas las clases de gestión para ese conjunto de políticas.

3. Pulse el conmutador Configurar. El conjunto de políticas es editable.
4. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
5. Edite el conjunto de políticas completando cualquiera de las siguientes acciones:

Opción	Descripción
<b>Añadir una clase de gestión</b>	<ol style="list-style-type: none"><li>a. En la tabla Conjuntos de políticas, pulse +Clase de gestión.</li><li>b. Para especificar las reglas para los datos de copia de seguridad y archivado, complete los campos de la ventana Añadir clase de gestión.</li><li>c. Para hacer que la clase de gestión sea la clase de gestión predeterminada, seleccione la casilla de verificación Establecer como predeterminada.</li><li>d. Pulse Añadir.</li></ol>
<b>Suprimir una clase de gestión</b>	En la columna Clase de gestión, pulse -. Consejo: Para suprimir la clase de gestión predeterminada, primero debe asignar una clase de gestión diferente como predeterminada.
<b>Establecer una clase de gestión como clase de gestión predeterminada</b>	En la columna Predeterminada para la clase de gestión, pulse el botón de selección. Consejo: La clase de gestión predeterminada gestiona los archivos de cliente cuando no hay asignada otra clase de gestión a, o cuando es adecuada para gestionar un archivo. Para asegurarse de que los clientes siempre pueden hacer copia de seguridad y archivar archivos, elija una clase de gestión que contenga reglas para la copia de seguridad y archivado de archivos.
<b>Modificar una clase de gestión</b>	Para cambiar las propiedades de una clase de gestión, actualice los campos en la tabla.

6. Pulse Guardar.  
Atención: Cuando activa un conjunto de políticas nuevo, es posible que se pierdan datos. Los datos protegidos bajo un conjunto de políticas es posible que no estén protegidos bajo otro conjunto de políticas. Por lo tanto, antes de activar un conjunto de políticas, asegúrese de que las diferencias entre el conjunto de políticas anterior y el nuevo conjunto de políticas no provocan una pérdida de datos.
7. Pulse Activar. Se visualiza un resumen de las diferencias entre el conjunto de políticas activas y el nuevo conjunto de políticas. Asegúrese de que los cambios en el nuevo conjunto de políticas son coherentes con los requisitos de retención de datos completando los pasos siguientes:
  - a. Revise las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a clases de gestión en el conjunto de políticas activas se enlazarán a las clases de gestión con los mismos nombres en el conjunto de políticas nuevo.
  - b. Identifique las clases de gestión en el conjunto de políticas activas que no tienen contrapartidas en el conjunto de políticas nuevo y tenga en cuenta las consecuencias para los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión estarán gestionados por la clase de gestión predeterminada en el conjunto de políticas nuevo.
  - c. Si los cambios que va a implementar el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.

## Planificación de copia de seguridad y operaciones de archivado

Antes de registrar un nuevo cliente en el servidor, asegúrese de que existe una planificación disponible para especificar cuándo tendrán lugar las operaciones de archivado y copia de seguridad. Durante el proceso de registro, asigne una planificación al cliente.

### Antes de empezar

Determine cómo debe procederse:



- Si está familiarizado con las planificaciones que se han configurado para la solución y sabe que no necesitan modificación, continúe con Registro de clientes.
- Si no está familiarizado con las planificaciones o las planificaciones necesitan modificación, siga los pasos de este procedimiento.


## Acerca de esta tarea

Normalmente, las operaciones de seguridad para todos los clientes deben completarse diariamente. Planifique detenidamente las cargas de trabajo de cliente y servidor para lograr el mejor rendimiento para el entorno de almacenamiento. Para evitar el solapamiento de las operaciones de cliente y servidor, planifique las operaciones de archivado y copia de seguridad de cliente para que se ejecuten por la noche. Si las operaciones de cliente y servidor se solapan o no se les da el tiempo y recursos suficientes para procesarse, es posible que experimente una disminución del rendimiento del sistema, operaciones con errores u otros problemas.


## Procedimiento

1. Revise las planificaciones disponibles pasando el cursor sobre Clientes en la barra de menú Centro de operaciones. Pulse Planificaciones.
2. Opcional: Modifique o cree una planificación completando los pasos siguientes:

Opción	Descripción
<b>Modificar una planificación</b>	<ol style="list-style-type: none"> <li>a. En la vista Planificaciones, seleccione la planificación y pulse Detalles.</li> <li>b. En la página Detalles de planificación, vea detalles pulsando las flechas azules al principio de las filas.</li> <li>c. Modifique los valores de la planificación y pulse Guardar.</li> </ol>
<b>Crear una planificación</b>	En la vista Planificaciones, pulse +Planificar y complete los pasos para crear una planificación.

3. Opcional: Para configurar valores de planificación que no están visibles en el Centro de operaciones, utilice un mandato de servidor. Por ejemplo, puede que desee planificar una operación de cliente que realice la copia de seguridad de un directorio específico y lo asigne a una clase de gestión distinta de la predeterminada.
  - a. En la página Visión general del Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.
  - b. Emita el mandato DEFINE SCHEDULE para crear una planificación o el mandato UPDATE SCHEDULE para modificar una planificación. Para obtener detalles sobre los mandatos, consulte DEFINE SCHEDULE (Definir una planificación para un mandato de administración) o UPDATE SCHEDULE (Actualizar una planificación de cliente).

### Tareas relacionadas:

 [Ajuste de la planificación para las operaciones diarias](#)

## Registro de clientes

Registre un cliente para asegurarse de que el cliente se puede conectar al servidor y que el servidor puede proteger los datos del cliente.

### Antes de empezar

Determine si el cliente requiere un ID de usuario de administración con autoridad de propietario de cliente sobre el nodo del cliente. Para determinar qué clientes necesitan un ID de usuario de administración, consulte la nota técnica 7048963.

Restricción: Para algunos clientes, el nombre de nodo del cliente y el ID de usuario de administración deben coincidir. No puede autenticar estos clientes mediante el método de autenticación de protocolo de acceso Lightweight Directory Access Protocol que se introdujo en la versión V7.1.7. Para obtener detalles acerca de este método de autenticación, al que a veces se hace referencia como modo integrado, consulte Autenticación de los usuarios mediante una base de datos de Active Directory.

## Procedimiento

Para registrar un cliente, realice una de las siguientes acciones.

- Si el cliente requiere un ID de usuario de administración, registre al cliente mediante el mandato REGISTER NODE y especifique el parámetro USERID:

```
register node
nombre_nodo contraseña
userid=nombre_nodo
```

donde *nombre\_nodo* especifica el nombre del nodo y la *contraseña* especifica la contraseña del nodo. Si desea obtener más información al respecto, consulte el apartado Registro de un nodo.

- Si el cliente no necesita un ID de usuario de administración, registre al cliente mediante el Centro de operaciones asistente Añadir cliente. Realice los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Clientes.
  - b. En la tabla Clientes, pulse + Cliente.
  - c. Complete los pasos en el asistente Añadir cliente:
    - i. Especifique que los datos redundantes se puedan eliminar en el cliente y en el servidor. En el área de eliminación de deduplicación de datos del lado del cliente, active la casilla de verificación Habilitar.
    - ii. En la ventana Configuración, copie los valores de opción TCPSEVERADDRESS, TCPPORT, NODENAME y DEDUPLICATION.  
Consejo: Anote los valores de opción y guárdelos en un lugar seguro. Después de completar el registro de cliente e instalar el software en el nodo de cliente, utilice los valores para configurar el cliente.
    - iii. Siga las instrucciones del asistente para especificar el dominio de políticas y un conjunto de opciones.
    - iv. Defina cómo se mostrarán los riesgos para el cliente especificando el valor de en riesgo.
    - v. Pulse Añadir cliente.

**Referencia relacionada:**

- [🔗 DECOMMISSION NODE \(Dejar fuera de servicio un nodo de cliente\)](#)
- [🔗 DECOMMISSION VM \(Dejar fuera de servicio una máquina virtual\)](#)
- [🔗 QUERY NODE \(Consultar nodos\)](#)
- [🔗 REMOVE REPLNODE \(Eliminar un nodo de cliente de la réplica\)](#)

## Instalación y configuración de clientes

Para empezar a proteger un nodo cliente, debe instalar y configurar el software seleccionado.

### Procedimiento

Si ya ha instalado el software, comience en el paso 2.

1. Realice una de las siguientes acciones:
  - o Para instalar software en una aplicación de nodo cliente, siga las instrucciones.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"> <li>■ Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux</li> <li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul> Para obtener información sobre el despliegue manual de las actualizaciones de cliente desde el servidor, consulte los documentos siguientes: <ul style="list-style-type: none"> <li>■ Para los servidores IBM Spectrum Protect 8.1.2 o posteriores, consulte la nota técnica 2004596.</li> <li>■ Para los servidores IBM® Tivoli Storage Manager V7.1 y los servidores IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la nota técnica 1673299.</li> </ul>
IBM Spectrum Protect para bases de datos	<ul style="list-style-type: none"> <li>■ Instalación de Data Protection for Oracle</li> <li>■ Instalación de Data Protection para SQL Server en Windows Server Core</li> </ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"> <li>■ Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li> <li>■ Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li> <li>■ Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server</li> </ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot para VMware</li> <li>■ Instalación y actualización de IBM Spectrum Protect Snapshot para Windows</li> </ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2</li> <li>■ Instalación de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle</li> </ul>

- Para instalar software en un nodo cliente de máquina virtual, siga las instrucciones para el tipo de copia de seguridad seleccionada.

Tipo de copia de seguridad	Enlace a instrucciones
Si planea crear copias de seguridad de VMware completas de máquinas virtuales, instale y configure el cliente de archivado y copia de seguridad de IBM Spectrum Protect.	<ul style="list-style-type: none"> <li>■ Instalación de los clientes de copia de seguridad y archivado de UNIX y Linux</li> <li>■ Instalación del cliente de archivado y copia de seguridad de Windows</li> </ul>
Si tiene previsto crear copias de seguridad incrementales siempre completas de máquinas virtuales, instale y configure IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el mismo nodo cliente o en nodos de cliente diferentes.	<ul style="list-style-type: none"> <li>■ Documentación del producto en línea de IBM Spectrum Protect for Virtual Environments</li> </ul> <p>Consejo: Puede obtener el software para IBM Spectrum Protect for Virtual Environments y el cliente de archivado y copia de seguridad en el paquete de instalación de IBM Spectrum Protect for Virtual Environments.</p>

2. Para permitir que el cliente se conecte al servidor, añada o actualice los valores para las opciones TCPSEVERADDRESS, TCPPORT y NODENAME en el archivo de opciones del cliente. Utilice los valores que ha anotado cuando ha registrado el cliente (Registro de clientes).
  - Para los clientes que están instalados en un sistema operativo AIX, Linux, Mac OS X u Oracle Solaris, añada los valores al archivo de opciones de sistema de cliente, dsm.sys.
  - Para los clientes que se han instalado en un sistema operativo Windows, añada los valores al archivo dsm.opt.

De forma predeterminada, los archivos de opciones están en el directorio de instalación.
3. Si ha instalado un cliente de archivado y copia de seguridad en un sistema operativo Linux o Windows, instale el servicio de gestión de cliente en el cliente. Siga las instrucciones del apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes.
4. Configure el cliente para ejecutar las operaciones planificadas. Siga las instrucciones de la sección Configuración del cliente para ejecutar las operaciones planificadas.
5. Opcional: Configure las comunicaciones a través de un cortafuegos. Siga las instrucciones de la sección Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos.
6. Ejecute una copia de seguridad de prueba para verificar que los datos están protegidos según lo planificado. Por ejemplo, para un cliente de archivado y copia de seguridad, complete los pasos siguientes:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente del que desea realizar la copia de seguridad y pulse Copia de seguridad.
  - b. Verifique que la copia de seguridad finalice correctamente y que no hay mensajes de error o de aviso.
7. Supervise los resultados de las operaciones planificadas para el cliente en el Centro de operaciones.

## Qué hacer a continuación

Si necesita cambiar los elementos de los que se está haciendo copia de seguridad del cliente, siga las instrucciones de Modificación del ámbito de una copia de seguridad de cliente.

## Configuración del cliente para ejecutar las operaciones planificadas

Debe configurar e iniciar un planificador de cliente en el nodo cliente. El planificador de cliente habilita la comunicación entre el cliente y el servidor para que se puedan realizar las operaciones planificadas. Por ejemplo, las operaciones planificadas normalmente incluyen la copia de seguridad de archivos desde un cliente.

## Acerca de esta tarea

El método preferido consiste en instalar el cliente de archivado y copia de seguridad en todos los nodos de cliente, de forma que pueda configurar e iniciar el aceptador de cliente en el nodo de cliente. El aceptador de cliente se ha diseñado para ejecutar de forma eficaz operaciones planificadas. El aceptador de cliente gestiona el planificador de cliente para que el planificador de cliente solo se ejecute cuando sea necesario:

- Cuando es el momento de consultar al servidor sobre la siguiente operación planificada
- Cuando es el momento de iniciar la siguiente operación planificada

Mediante el aceptador de cliente, puede reducir el número de procesos de fondo en el cliente y ayudar a evitar problemas de retención de memoria.

El aceptador de cliente ejecuta planificaciones para los productos siguientes: el cliente de archivado y copia de seguridad, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect for Enterprise Resource Planning, IBM Spectrum Protect for Mail y IBM

Spectrum Protect for Virtual Environments. Si ha instalado un producto para el cual el aceptador de cliente no ejecuta planificaciones, siga las instrucciones de configuración en la documentación de producto para garantizar que se puedan ejecutar operaciones planificadas.

Si la empresa utiliza una herramienta de planificación de otro proveedor como práctica estándar, puede utilizar dicha herramienta de planificación como alternativa al aceptador de cliente. Por lo general, las herramientas de planificación de terceros inician los programas de cliente directamente utilizando mandatos de sistema operativo. Para configurar una herramienta de planificación de terceros, consulte la documentación del producto.

## Procedimiento

---

Para configurar e iniciar el planificador de cliente utilizando el aceptador de cliente, siga las instrucciones correspondientes al sistema operativo que está instalado en el nodo cliente.

### AIX y Oracle Solaris

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

- Para permitir que el aceptador de cliente se inicie automáticamente después de un reinicio del sistema, añada la entrada siguiente al archivo de arranque del sistema (normalmente, `/etc/inittab`):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # Daemon de aceptación de clientes
```

### Linux

- Desde la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Pulse la pestaña Cliente web.
- En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de cliente gestione el cliente web, pulse la opción Ambas.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, en el archivo `dsm.sys`, establezca la opción `passwordaccess` en `generate`.
- Para almacenar la contraseña del nodo de cliente, emita el siguiente mandato y entre la contraseña del nodo de cliente cuando se le solicite:

```
dsmc query sess
```

- Inicie el aceptador de cliente iniciando una sesión con el ID de usuario root y emitiendo el mandato siguiente:

```
service dsmcad start
```

- Para permitir que el aceptador de cliente pueda iniciarse automáticamente después de un reinicio del sistema, añada el servicio emitiendo el mandato siguiente en el indicador de shell:

```
# chkconfig --add dsmcad
```

### MAC OS X

- En la GUI del cliente de archivado y copia de seguridad, pulse Editar > Preferencias de cliente.
- Para asegurarse de que el planificador puede iniciarse sin supervisión, pulse Autorización, seleccione Generar contraseña y pulse Aplicar.
- Para especificar cómo se gestionan los servicios, pulse Cliente web, seleccione Planificar, pulse Aplicar, y pulse Aceptar.
- Para asegurarse de que la contraseña generada se guarda, reinicie el cliente de archivado y copia de seguridad.
- Utilice la aplicación de herramientas IBM Spectrum Protect para administradores para iniciar el aceptador de cliente.

### Windows

- a. En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Obtener ayuda para configurar Planificador cliente. Pulse Siguiente.
- b. Consulte la información en la página Asistente del planificador y pulse Siguiente.
- c. En la página Tarea de planificador, seleccione Instalar un planificador nuevo o adicional y pulse Siguiente.
- d. En la página Nombre y ubicación del planificador, especifique un nombre para el planificador de cliente que está añadiendo. A continuación, seleccione Utilizar el daemon de aceptador de cliente (CAD) para gestionar el planificador y pulse Siguiente.
- e. Especifique el nombre que desea asignar a este aceptador de cliente. El nombre predeterminado es Client Acceptor. Pulse Siguiente.
- f. Complete la configuración paso a paso a través del asistente.
- g. Actualice el archivo de opciones de cliente, dsm.opt, y configure la opción passwordaccess como generate.
- h. Para almacenar la contraseña de nodo de cliente, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query sess
```

Entre la contraseña de nodo de cliente cuando se le solicite.

- i. Inicie el servicio aceptador de cliente desde la página Control de servicios. Por ejemplo, si ha utilizado el nombre predeterminado, inicie el servicio Aceptador de cliente. No inicie el servicio de planificador que ha especificado en la página Nombre y ubicación del planificador. El aceptador de cliente inicia y detiene automáticamente el servicio de planificador según sea necesario.

## Configuración de las comunicaciones entre cliente y servidor a través de un cortafuegos

---

Si un cliente debe comunicarse con un servidor a través de un cortafuegos, deberá habilitar las comunicaciones entre cliente y servidor a través del cortafuegos.

### Antes de empezar

---

Si ha utilizado el asistente Añadir cliente para registrar un cliente, busque los valores del archivo de opciones del cliente que ha obtenido durante dicho proceso. Puede utilizar los valores para especificar los puertos.

### Acerca de esta tarea

---

Atención: No configure un cortafuegos de forma que pueda provocar la finalización de sesiones que está utilizando un agente de almacenamiento o servidor. La finalización de una sesión válida puede provocar resultados imprevisibles. Es posible que los procesos y sesiones parece que se detienen debido a errores de entrada y de salida. Para ayudar a excluir sesiones de las restricciones de tiempo de espera, configure puertos conocidos para los componentes de IBM Spectrum Protect. Asegúrese de que la opción de servidor KEEPALIVE permanece establecida en el valor predeterminado de YES. De esta forma, puede asegurarse de que la comunicación entre cliente y servidor no se interrumpe. Para obtener instrucciones sobre la configuración de la opción de servidor KEEPALIVE, consulte KEEPALIVE.

### Procedimiento

---

Abra los siguientes puertos para permitir el acceso a través del cortafuegos:

**Puerto TCP/IP para el cliente de copia de seguridad y archivado, el cliente administrativo de línea de mandatos y el planificador de cliente**

Especifique el puerto utilizando la opción tcpport en el archivo de opciones de cliente. La opción tcpport del archivo de opciones de cliente debe coincidir con la opción TCPPORT en el archivo de opciones del servidor. El valor predeterminado es 1500. Si decide utilizar un valor que no sea el valor predeterminado, especifique un número en el rango 1024 - 32767.

**Puerto HTTP para habilitar la comunicación entre el cliente web y estaciones de trabajo remotas**

Especifique el puerto para la estación de trabajo remota estableciendo la opción httpport en el archivo de opciones de cliente de la estación de trabajo remota. El valor predeterminado es 1581.

**Puertos TCP/IP para la estación de trabajo remota**

El valor predeterminado de 0 (cero) hace que los dos números de puerto libres se asignen aleatoriamente a la estación de trabajo remota. Si no desea que los números de puerto se asignen aleatoriamente, especifique valores estableciendo la opción webports en el archivo de opciones de cliente de la estación de trabajo remota.

**Puerto TCP/IP para sesiones de administración**

Especifique el puerto en el que el servidor espera las solicitudes para sesiones de cliente de administración. El valor de la opción tcpadminport de cliente debe coincidir con el valor de la opción de servidor TCPADMINPORT. De esta forma, puede asegurar las

sesiones administrativas dentro de una red privada.

## Personalización de políticas

---

Los objetivos de una empresa en cuanto a la protección y conservación de los datos suelen definirlos los ejecutivos de la empresa, los asesores legales y otros cargos importantes. Las *políticas* son la forma de adaptar el funcionamiento de IBM Spectrum Protect a los objetivos de protección y conservación de datos de su empresa.

### Acerca de esta tarea

---

Para gestionar de forma automática la protección y conservación de datos, defina políticas, que son las reglas que se configuran en el servidor. Las políticas afectan a la cantidad de datos que se almacenan a lo largo del tiempo y al periodo de tiempo que los datos se retienen y están disponibles para ser restaurados por los clientes. Personalice las políticas para cumplir con los objetivos de protección de datos de su organización.

Puede elegir la política que gestiona los datos de un cliente, asignando al cliente a un dominio de políticas. Los clientes de diferentes tipos tienen diferentes requisitos de retención y normalmente es necesario personalizar y crear políticas.

Cuando se instala un servidor, este tiene de forma predeterminada una política en un dominio de políticas. Puede personalizar la política y crear sus propias políticas.

- **Conceptos de políticas**  
La política de un cliente específico se determina mediante los valores del dominio de políticas al que se ha añadido el cliente.
- **Personalización de una política**  
Puede personalizar las políticas existentes para que cumplan los requisitos de retención de datos nuevos o revisados de la organización. La modificación de un dominio de políticas o la copia de un dominio de políticas existente es una forma habitual de personalizar una política.
- **Creación de una política copiando una política existente**  
Puede crear nuevas políticas copiando una política existente y, a continuación, actualizando las partes que desea cambiar.
- **Creación de un dominio de políticas**  
Es posible que desee crear un nuevo dominio de políticas para cada tipo de cliente que esté protegido mediante el servidor. Es posible que también desee dividir las responsabilidades de los clientes entre varios administradores concediéndoles autorización para dominios de políticas específicos.
- **Control de las operaciones de cliente mediante conjuntos de opciones de cliente**  
Puede utilizar conjuntos de opciones de cliente para controlar de forma centralizada las opciones de proceso que utilizan los clientes para operaciones, tales como una copia de seguridad. Los conjuntos de opciones de cliente garantizan que los datos estén protegidos de forma coherente de acuerdo con sus requisitos. Un conjunto de opciones de cliente pueden reemplazar las opciones en un archivo de opciones de cliente y añadir opciones que podrían no estar en un archivo de opciones del cliente local.

## Conceptos de políticas

---

La política de un cliente específico se determina mediante los valores del dominio de políticas al que se ha añadido el cliente.

Durante el proceso de registro del cliente, puede asignar un cliente a un *dominio de políticas*. La política de cada cliente se determina mediante las reglas del dominio de políticas al que se ha asignado al cliente. En el dominio de políticas, las reglas que están en vigor se encuentran en el *conjunto de políticas* activo.

Cuando un cliente realiza una copia de seguridad o de archivado de un archivo, el archivo se enlaza a una clase de gestión del conjunto de políticas activas del dominio de políticas. Una *clase de gestión* es el conjunto principal de las reglas para gestionar datos de cliente. Las operaciones de copia de seguridad y archivado del cliente utilizan los valores de la clase de gestión predeterminada del dominio de políticas, al menos que personalice la política.

Se puede personalizar una política definiendo más clases de gestión en el conjunto de políticas, activando el conjunto y asignando el uso de las nuevas clases de gestión mediante opciones de cliente.

Las opciones de cliente se pueden especificar en un archivo editable local en el sistema cliente y en un conjunto de opciones de cliente del servidor. Las opciones del conjunto de opciones de cliente del servidor pueden sustituir o añadirse a las opciones en el archivo de opciones de cliente local.

El servidor utiliza la política de las clases de gestión para gestionar los archivos basándose en si hay versiones de archivos activas o inactivas. La copia de seguridad o la copia archivada más reciente de un archivo es la *versión activa*. Las versiones activas no se suprimen nunca del almacenamiento del servidor.

Las versiones de copia de seguridad que no sean la versión más reciente se denominan *versiones inactivas*. Una versión activa de un archivo pasa a estar inactiva cuando se produce uno de los sucesos siguientes:

- Se ha vuelto a realizar una copia de seguridad del archivo, lo que ha creado una versión más reciente del archivo en el almacenamiento del servidor.
- Se ha suprimido el archivo en el almacenamiento del nodo cliente y, a continuación, se ha ejecutado una operación de copia de seguridad incremental. Una *copia de seguridad incremental*, la operación de copia de seguridad más frecuente para un cliente, solo realiza una copia de seguridad de los archivos que se han modificado desde la última copia de seguridad.

Los valores de la clase de gestión que está vinculada a un archivo determinan durante cuánto tiempo y cuántas versiones inactivas de los archivos se conservarán.

El *proceso de caducidad* utiliza políticas para determinar cuándo dejarán de necesitarse los archivos, es decir, cuándo caducarán las versiones. El proceso de caducidad en el servidor aplica las políticas que ha definido para la retención de datos y debe asegurarse de que planifica la caducidad de modo que se ejecute con regularidad. Por ejemplo, si tiene una política que indica que se conserven sólo cuatro versiones de un archivo, caducará la quinta copia, que es la más antigua. Durante el proceso de caducidad, el servidor elimina de la base de datos las entradas de versiones caducadas, lo cual suprime de forma efectiva las versiones del almacenamiento del servidor.

- **Retención y caducidad de las versiones de copia de seguridad**  
Es importante tener varias versiones de las copias de seguridad de archivos ya que los usuarios actualizan de forma continuada los archivos y es posible que necesiten restaurar un archivo en diferentes puntos en el tiempo. Los valores de las políticas controlan las versiones de copia de seguridad que retiene el servidor en el almacenamiento del servidor y afectan a lo que los usuarios pueden restaurar.
- **Activación de las políticas después de las actualizaciones**  
Cuando realiza actualizaciones en la política, las actualizaciones no entran en vigor hasta que activa el conjunto de políticas que ha actualizado.

#### Conceptos relacionados:

 [Copia de seguridad incremental completa y copia de seguridad incremental parcial](#)

## Retención y caducidad de las versiones de copia de seguridad

---

Es importante tener varias versiones de las copias de seguridad de archivos ya que los usuarios actualizan de forma continuada los archivos y es posible que necesiten restaurar un archivo en diferentes puntos en el tiempo. Los valores de las políticas controlan las versiones de copia de seguridad que retiene el servidor en el almacenamiento del servidor y afectan a lo que los usuarios pueden restaurar.

Puede especificar las versiones que retiene el servidor en el almacenamiento del servidor con los valores de la clase de gestión:

- **Especifique el número de días que se conservarán las versiones de copia de seguridad.**  
Especifique el número de días que se han de conservar las versiones de copia de seguridad con valores en el Centro de operaciones:
  - Mantener copias de seguridad extra, que es el número de días que se han de conservar las versiones de copia de seguridad inactivas. Los días se cuentan a partir del día en que las versiones pasan a estar inactivas.  
  
Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro RETEXTRA.
  - Mantener copias de seguridad suprimidas, que es el número de días que se ha de conservar la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente.  
  
Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro RETONLY.
- **Especifique el número de versiones para conservar.**  
Especifique el número de versiones de copia de seguridad para conservar con valores en el Centro de operaciones:
  - Copias de seguridad, que es el número de versiones que se ha de conservar de un archivo que todavía existe en el sistema de archivos del cliente.  
  
Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro VEREXISTS.
  - Copias de seguridad suprimidas, que es el número de versiones para conservar de un archivo que se ha suprimido del sistema de archivos del cliente.  
  
Si utiliza mandatos, utilice el mandato DEFINE COPYGROUP con el parámetro VERDELETED.
- **Especifique una combinación del número de versiones y el número de días que se conservarán.**  
Los valores interactúan para determinar las versiones de copia de seguridad que retiene el servidor. Asegúrese de que comprende qué valores tienen prioridad y qué interacciones se llevan a cabo:
  - Cuando el número de versiones de copia de seguridad inactivas excede el número en los valores Copias de seguridad y Copias de seguridad suprimidas, la versión más antigua caduca y el servidor suprime el archivo de la base de datos la próxima vez que se ejecuta el proceso de caducidad.

- El número de versiones inactivas que el servidor conserva también está afectado por el valor de Mantener copias de seguridad extra. Las versiones inactivas caducan cuando el número de días que han permanecido inactivas excede el valor especificado para retener versiones adicionales, aunque no se supere el número de versiones.
- Caducidad de archivos y procesamiento de la caducidad  
Los archivos caducan cuando superan el criterio de retención que se ha especificado en la política. El proceso de caducidad en el servidor elimina los archivos caducados de la base de datos del servidor y los archivos suprimidos del almacenamiento del servidor.
- Ejemplo: Retención cuando una política utiliza solo controles temporales  
La forma más sencilla de gestionar la retención de datos es utilizar únicamente controles de política basados en el tiempo. Con controles basados en el tiempo únicamente en la política, las versiones de archivos se conservan en función de los días transcurridos desde que las versiones han pasado a estar inactivas.
- Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión  
El uso de los controles de versión y de tiempo en una política ofrece una mayor flexibilidad en la gestión de la retención de datos, pero supone también más complejidad. Para comprender las interacciones entre los controles, revise ejemplos de políticas y sus efectos en la retención de las versiones de copia de seguridad de un archivo durante un mes.
- Interacciones entre configuraciones de política  
Las configuraciones basadas en el tiempo y basadas en las versiones interactúan cuando se utilizan juntas en una clase de gestión de una política. La frecuencia de las copias de seguridad de cliente también afecta a las versiones de copia de seguridad que se almacenan para un cliente.

## Caducidad de archivos y procesamiento de la caducidad

---

Los archivos caducan cuando superan el criterio de retención que se ha especificado en la política. El proceso de caducidad en el servidor elimina los archivos caducados de la base de datos del servidor y los archivos suprimidos del almacenamiento del servidor.

Los archivos caducan en las condiciones siguientes:

- Los usuarios suprimen espacios de archivos de los nodos cliente.
- Los usuarios hacen caducar archivos mediante el mandato EXPIRE en el cliente
- Una versión de copia de seguridad de un archivo supera el criterio de retención de copias de seguridad (el periodo de tiempo en que se conserva un archivo y el número de versiones inactivas de un archivo que se conservan)
- Un archivo de copia archivada supera el criterio de tiempo de retención para los archivos de copia archivada (el periodo de tiempo en que se conservan las copias archivadas).
- Un conjunto de copias de seguridad excede el tiempo de retención que tiene especificado para el conjunto de copias de seguridad.

El servidor suprime los archivos caducados de la base de datos del servidor sólo durante el proceso de caducidad. Una vez que los archivos caducados se suprimen de la base de datos, el servidor puede volver a utilizar el espacio en las agrupaciones de almacenamiento ocupado por los archivos caducados. Asegúrese de que el proceso de caducidad se ejecuta periódicamente para que el servidor pueda volver a utilizar espacio.

## Restricciones relativas al proceso de caducidad

---

El uso de algunas funciones afecta al proceso de caducidad.

### Réplica

Si utiliza políticas distintas en los servidores de origen y de destino, los archivos marcados para una caducidad inmediata en el servidor de réplica fuente no se suprimen hasta que se repliquen al servidor de réplica de destino. Si no utiliza políticas distintas, los archivos marcados para una caducidad inmediata en el servidor de réplica fuente se suprimen inmediatamente.

Para el servidor de réplica de destino, si los archivos se marcan como caducados, se suprimen cuando el servidor de réplica de destino ejecuta el procesamiento de la caducidad.

### Retención basada en sucesos para datos de archivado

Una copia archivada no puede optar a la caducidad si existe una retención de supresión asociada. Si un archivo no está retenido, se gestionará según el proceso de caducidad existente.

### Tareas relacionadas:

 Retención y liberación de la caducidad/supresión

## Ejemplo: Retención cuando una política utiliza solo controles temporales

---

La forma más sencilla de gestionar la retención de datos es utilizar únicamente controles de política basados en el tiempo. Con controles basados en el tiempo únicamente en la política, las versiones de archivos se conservan en función de los días transcurridos



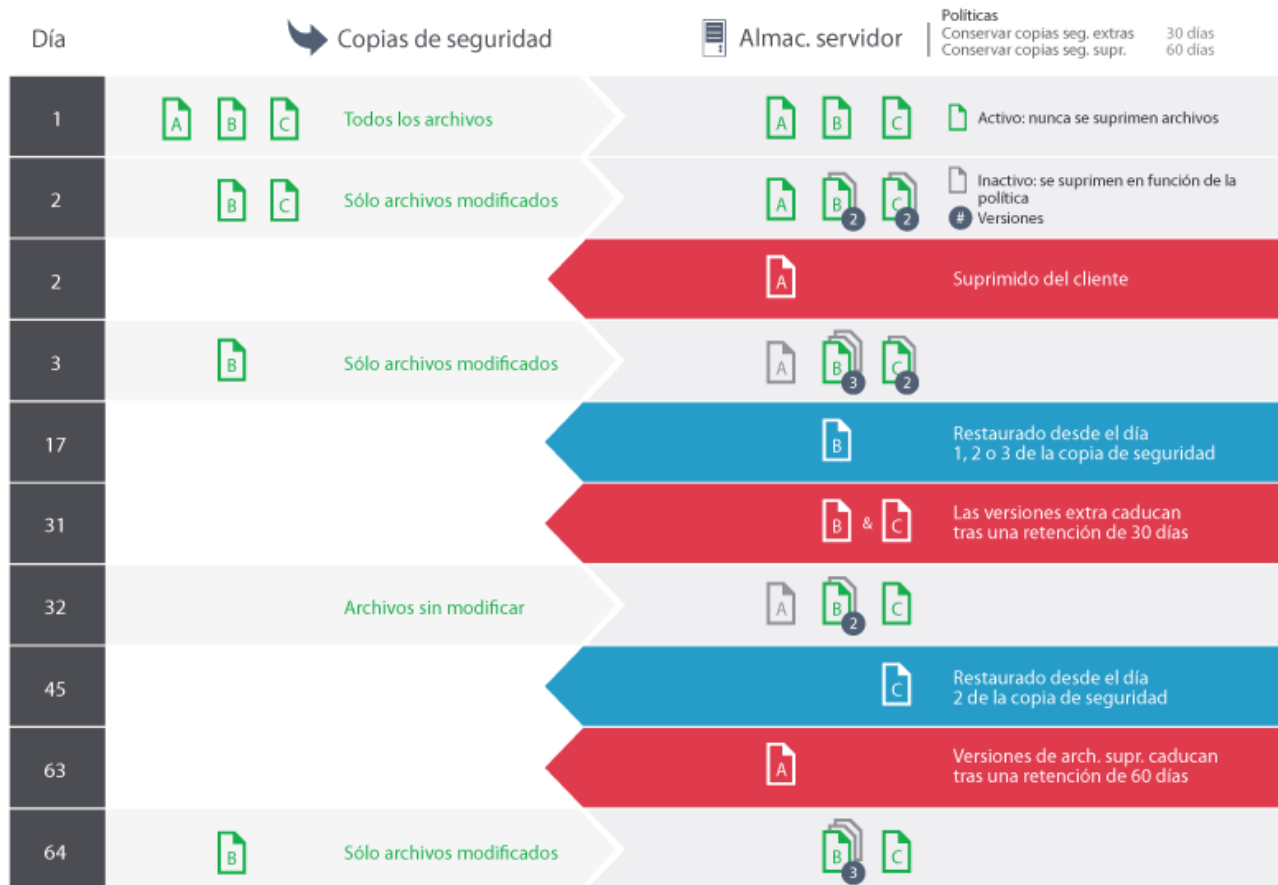
desde que las versiones han pasado a estar inactivas.

En el caso de una política basada únicamente en el tiempo, utilice controles Mantener copias de seguridad extra y Mantener copias de seguridad suprimidas. Este tipo de política no limita el número de versiones de archivos. Si los clientes deben realizar copias de seguridad con frecuencia, asegúrese de que el almacenamiento del servidor pueda manejar el número potencial de versiones de archivos.

La siguiente figura muestra cómo el servidor maneja los archivos a lo largo del tiempo de un cliente que realiza copias de seguridad incrementales diariamente.

En este ejemplo, la política tiene las siguientes características:

- La versión más reciente de un archivo siempre se retiene mientras exista el archivo en el sistema del cliente. La versión más reciente del archivo es la versión activa. Esta característica forma parte de cada política en el servidor.
- Mantener copias de seguridad extra se establece en 30 días. Cuando se realiza una copia de seguridad más reciente, una versión del archivo pasa a estar inactiva y se conserva en el almacenamiento del servidor durante 30 días.
- Mantener copias de seguridad suprimidas se establece en 60 días. Cuando se suprime un archivo del sistema cliente, todas las versiones del archivo que se encuentran en el almacenamiento del servidor pasan a estar inactivas. Estas versiones inactivas se conservan durante 60 días después de que las versiones de archivo pasan a estar inactivas.



## Ejemplo: Retención cuando una política utiliza controles de tiempo y de versión

El uso de los controles de versión y de tiempo en una política ofrece una mayor flexibilidad en la gestión de la retención de datos, pero supone también más complejidad. Para comprender las interacciones entre los controles, revise ejemplos de políticas y sus efectos en la retención de las versiones de copia de seguridad de un archivo durante un mes.

Consulte los apartados Tabla 1 y Figura 1. Un cliente realiza una copia de seguridad del archivo REPORT.TXT cuatro veces en un mes, desde el 23 de marzo hasta el 23 de abril. Los valores del grupo de copias de seguridad de la clase de gestión a la que está enlazado el archivo REPORT.TXT determinan cómo maneja el servidor estas versiones de copia de seguridad. Tabla 2 muestra cómo los diferentes valores de grupo de copia puede afectar a las versiones, a partir del 24 de abril (un día después de la última copia de seguridad).

Tabla 1. Estado de las versiones de copia de seguridad de REPORT.TXT a partir del 24 de abril

Versión	Fecha de creación	Días desde que la versión está inactiva
Activa	23 de abril	(no se aplica)
Inactiva 1	13 de abril	1 (desde el 23 de abril)
Inactiva 2	31 de marzo	11 (desde el 13 de abril)
Inactiva 3	23 de marzo	24 (desde el 31 de marzo)

Figura 1. Versiones activas e inactivas de REPORT.TXT

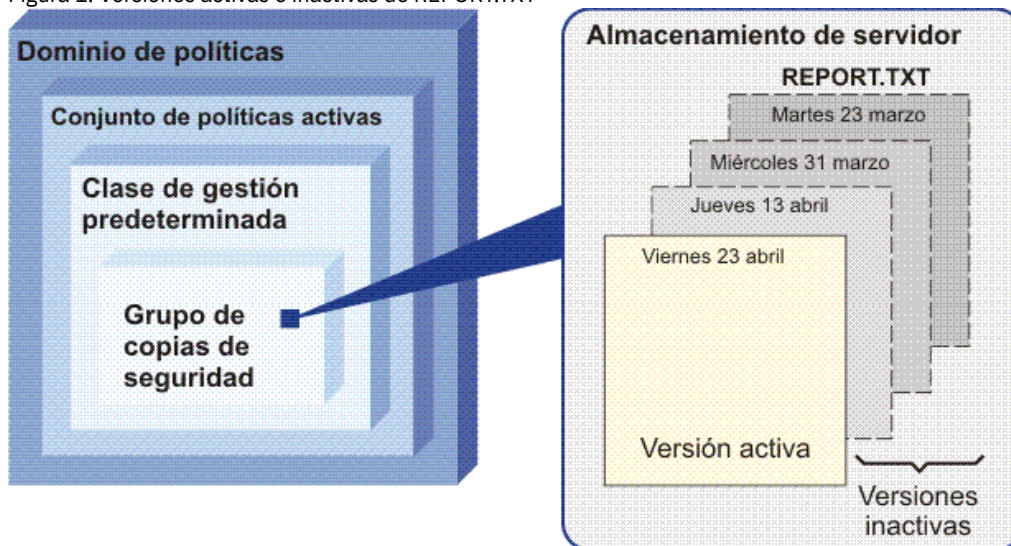


Tabla 2. Efectos de la política sobre la retención de versiones de copia de seguridad de REPORT.TXT a partir del 24 de abril

Copias de seguridad	Copias de seguridad suprimidas	Mantener copias de seguridad extra	Mantener copias de seguridad suprimidas	Resultado
4 versiones	2 versiones	60 días	180 días	<p>Los valores de Copias de seguridad y de Mantener copias de seguridad extra controlan la caducidad de las versiones. La versión creada el 23 de marzo se retiene hasta que se vuelve a realizar una copia de seguridad del archivo (lo que crea una cuarta versión inactiva) o hasta que esta versión permanece inactiva durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el sistema de archivos del cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del cliente. A partir de este punto, los valores de Copias de seguridad suprimidas y de Mantener copias de seguridad suprimidas también tienen un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan). La versión del 13 de abril caduca cuando permanece inactiva durante 60 días (el 23 de junio). El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>

Copias de seguridad	Copias de seguridad suprimidas	Mantener copias de seguridad extra	Mantener copias de seguridad suprimidas	Resultado
Número ilimitado	2 versiones	60 días	180 días	<p>El valor de Mantener copias de seguridad extra controla la caducidad de las versiones. Las versiones inactivas (no la última versión restante) caducan cuando permanecen inactivas durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del cliente. A partir de este punto, los valores de Copias de seguridad suprimidas y de Mantener copias de seguridad suprimidas también tienen un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan) porque sólo se permiten dos versiones. La versión del 13 de abril caduca cuando permanece inactiva durante 60 días (el 22 de junio). El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>
Número ilimitado	Número ilimitado	60 días	180 días	<p>El valor de Mantener copias de seguridad extra controla la caducidad de las versiones. El servidor no hace caducar las versiones inactivas en función del número máximo de copias de seguridad. Las versiones inactivas (no la última versión restante) caducan cuando permanecen inactivas durante 60 días.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del nodo de cliente. A partir de este punto, el valor de Mantener copias de seguridad suprimidas también tiene un efecto sobre la retención. Ahora todas las versiones están inactivas.</p> <p>Tres de las cuatro versiones caducan después de estar inactivas cada una de ellas durante 60 días. El servidor conserva la última versión inactiva restante, la versión del 23 de abril, durante 180 días después de quedar inactiva.</p>
4 versiones	2 versiones	Número ilimitado	Número ilimitado	<p>El valor de Copias de seguridad controla la caducidad de las versiones hasta que un usuario suprime el archivo del nodo cliente. El servidor no caduca las versiones inactivas en función de la antigüedad.</p> <p>Si el usuario suprime el archivo REPORT.TXT en el nodo de cliente, el servidor anota la supresión en la siguiente copia de seguridad incremental completa por parte del nodo de cliente. A partir de este punto, el valor de Copias de seguridad suprimidas controla la caducidad. Ahora todas las versiones están inactivas.</p> <p>Dos de las cuatro versiones caducan de inmediato (las versiones del 23 de marzo y el 31 de marzo caducan) porque sólo se permiten dos versiones. El servidor conserva las dos versiones inactivas restantes de forma indefinida.</p>

**Conceptos relacionados:**

 Copia de seguridad incremental completa y copia de seguridad incremental parcial

## Interacciones entre configuraciones de política

Las configuraciones basadas en el tiempo y basadas en las versiones interactúan cuando se utilizan juntas en una clase de gestión de una política. La frecuencia de las copias de seguridad de cliente también afecta a las versiones de copia de seguridad que se almacenan para un cliente.

Para un sistema cliente que debe realizar una copia de seguridad de dos veces al día, tenga en cuenta los efectos de las siguientes opciones de política en un archivo que cambia frecuentemente:

- Establezca Mantener copias de seguridad extra en 30 días. Establezca Copias de seguridad a Sin límite para que la política no limite el número de versiones. Después de 30 días, el servidor podría tener 60 versiones con copia de seguridad del archivo si este cambia entre cada una de las dos copias de seguridad diarias. El cliente puede elegir restaurar cualquiera de los 60 versiones de los últimos 30 días.

- Establezca Mantener copias de seguridad extra en Sin límite, y Copias de seguridad en 30 versiones. Si el archivo cambia entre cada una de las dos operaciones de copia de seguridad diarias, el servidor tendrá 30 versiones con copia de seguridad después de 15 días. Después de 30 días, el servidor seguirá teniendo solo 30 versiones con copia de seguridad debido al límite del número de versiones. Si el archivo continúa cambiando entre cada una de las dos operaciones de copia de seguridad diarias, las versiones con copia de seguridad pueden ser solo de los últimos 15 días. El cliente puede optar por restaurar una de las 30 versiones, que podrían tener una antigüedad no superior a 15 días.

Los ejemplos muestran que si las versiones con copia de seguridad deben estar disponibles durante un determinado número de días, la forma más sencilla de implementar ese requisito es utilizar una política basada en el tiempo. Establezca Mantener copias de seguridad extra en el número de días específico y Copias de seguridad como Sin límite.

El efecto del valor Sin límite en la configuración de política varía en función de cómo se hayan configurado otros controles de política:

#### Mantener copias de seguridad extra

Si especifica Sin límite, se eliminarán las versiones con copia de seguridad inactivas en función de las configuraciones Copias de seguridad o Copias de seguridad suprimidas.

Para permitir que los nodos de cliente restauren los archivos a un instante específico, establezca Copias de seguridad o Copias de seguridad suprimidas en Número ilimitado. Establezca el valor de Mantener copias de seguridad extra en el número de días que, según sus previsiones, los clientes pueden necesitar que las versiones de los archivos estén disponibles para realizar una posible restauración a un instante específico. Por ejemplo, para permitir que los clientes restauren archivos a partir de un instante específico de 60 días de antigüedad, establezca Mantener copias de seguridad extra en 60.

#### Mantener copias de seguridad suprimidas

Si especifica Sin límite, la última versión se conserva de forma permanente salvo que un usuario o un administrador eliminen el archivo del almacenamiento del servidor.

#### Copias de seguridad

El establecimiento de la configuración como Sin límite puede suponer un incremento del almacenamiento, si bien puede ser necesario especificar este valor en algunas situaciones. Por ejemplo, para permitir que los nodos cliente restauren archivos a un instante específico, establezca el valor de Copias de seguridad en Número ilimitado. Si no establece un límite para las versiones, se asegura de que el servidor retenga las versiones en función del valor de Mantener copias de seguridad extra.

#### Copias de seguridad suprimidas

El establecimiento de la configuración como Sin límite puede suponer un incremento del almacenamiento, si bien puede ser necesario especificar este valor en algunas situaciones. Por ejemplo, establezca el valor de Copias de seguridad suprimidas en Número ilimitado para que los clientes puedan restaurar los archivos en un instante específico. Si no establece un límite para las versiones, se asegura de que el servidor retenga las versiones en función del valor de Mantener copias de seguridad extra.

## Referencia cruzada de los campos y parámetros de mandatos de servidor de Centro de operaciones

La tabla siguiente muestra los campos Centro de operaciones con el parámetro equivalente para utilizar con el mandato `DEFINE COPYGROUP TYPE=BACKUP`.

Nombre de campo en las vistas de Centro de operaciones	Parámetro para utilizar con el mandato <code>DEFINE COPYGROUP TYPE=BACKUP</code>
Mantener copias de seguridad extra	RETEXTRA
Mantener copias de seguridad suprimidas	REONLY
Copias de seguridad	VEREXISTS
Copias de seguridad suprimidas	VERDELETED

## Activación de las políticas después de las actualizaciones

Cuando realiza actualizaciones en la política, las actualizaciones no entran en vigor hasta que activa el conjunto de políticas que ha actualizado.

La activación del conjunto de políticas activa las actualizaciones que ha realizado. Por ejemplo, los siguientes tipos de actualización entran en vigor después de que activa el conjunto de políticas:

- Define un nuevo dominio de políticas con un conjunto de políticas y una o varias clases de gestión

- Añade una clase de gestión a un conjunto de políticas
- Cambia los valores de retención de copias de seguridad en una clase de gestión existente

## Validación del conjunto de políticas antes de la activación

En el Centro de operaciones, la validación no es un paso independiente. Si utiliza mandatos, la validación es un mandato opcional que le permite previsualizar el efecto de activar un conjunto de políticas modificado. Cuando valida un conjunto de políticas, el servidor informa acerca de las condiciones que pueden producir problemas si se activa el conjunto de políticas.

La validación no se puede ejecutar si el conjunto de políticas no contiene una clase de gestión predeterminada. La validación genera mensajes de aviso si existe alguna de las condiciones que se muestran en Tabla 1.

Tabla 1. Condiciones que generan avisos durante la validación de conjuntos de políticas

Condición	Razón del aviso
Los destinos de almacenamiento especificados para las operaciones de copia de seguridad, archivado o migración no están definidos en agrupaciones de almacenamiento.	Debe haber una agrupación de almacenamiento antes de que pueda especificarla como destino.
Un destino de almacenamiento especificado para operaciones de copia de seguridad, archivado o migración es una agrupación de almacenamiento de copias o una agrupación de datos activos.	El destino de almacenamiento debe encontrarse en una agrupación primaria.
La clase de gestión predeterminada no contiene valores de copia de seguridad o archivado.	Si la clase de gestión predeterminada no contiene valores de copias de seguridad o de archivado, no se hará una copia de seguridad ni una copia archivada de los archivos enlazados a la clase de gestión predeterminada.
El conjunto de políticas activas actual da nombre a una clase de gestión que no está definida en el conjunto de políticas que se está validando.	<p>Cuando los usuarios hacen copia de seguridad de archivos que están vinculados con una clase de gestión que ya no existe en el conjunto de políticas activas, las versiones de copia de seguridad se vuelven a vincular con la clase de gestión predeterminada.</p> <p>Cuando la clase de gestión con la que está vinculada una copia archivada ya no existe y la clase de gestión predeterminada no contiene valores de archivado, el servidor utiliza el período de gracia de retención de archivado para gestionar la retención de la copia archivada.</p> <p>El período de gracia de retención de archivado se establece para un dominio de políticas y dicho valor sólo se utiliza cuando ningún otro valor de política está disponible para gestionar una copia archivada.</p>
El conjunto de políticas activas actual contiene los valores de copia que no están definidos en el conjunto de políticas que se está validando.	<p>Cuando un cliente realiza una copia de seguridad de un archivo y la clase de gestión con la que está enlazado el archivo ya no contiene valores de copia de seguridad, las versiones de copia de seguridad las gestiona la clase de gestión predeterminada.</p> <p>Si la clase de gestión predeterminada no contiene ninguna configuración de copia de seguridad, el servidor utiliza el período de gracia de retención de copia de seguridad para gestionar las versiones de archivo. Sin embargo, no se realiza una copia de seguridad del archivo en la siguiente operación de copia de seguridad.</p> <p>El período de gracia de retención de retención se establece para un dominio de políticas y dicho valor sólo se utiliza cuando ningún otro valor de política está disponible para gestionar una versión de copia de seguridad.</p>
Una clase de gestión específica que debe existir una versión de copia de seguridad para poder migrar un archivo de un nodo de cliente, pero la clase de gestión no contiene ningún valor de copia de seguridad.	Este aviso se aplica únicamente si utiliza el producto IBM Spectrum Protect for Space Management. Los conflictos entre clases de gestión pueden causar problemas a los clientes de IBM Spectrum Protect for Space Management.

## Activación de conjunto de políticas

Cuando activa un conjunto de políticas, el servidor valida el contenido del conjunto de políticas y copia el conjunto de políticas para que sea el conjunto de políticas activas. Para modificar posteriormente el contenido del conjunto de políticas activas, debe crear o modificar otro conjunto de políticas y activar dicho conjunto de políticas.

Algunas actualizaciones de políticas tienen un efecto inmediato cuando se activa, pero otras no:

- Las actualizaciones de los valores de Mantener copias de seguridad extra y de Mantener copias de seguridad suprimidas se aplican de forma inmediata a los datos que ya están en el almacenamiento del servidor y a las copias de seguridad futuras.

Si utiliza mandatos, estos valores son los parámetros RETEXTRA y RETONLY para los mandatos DEFINE COPYGROUP o UPDATE COPYGROUP.

- Las actualizaciones de los valores de Copias de seguridad y de Copias de seguridad suprimidas no entran en vigor para los datos del cliente hasta que el cliente completa la siguiente operación de copia de seguridad.

Si utiliza mandatos, estos valores son los parámetros VEREXISTS y VERDELETED para los mandatos DEFINE COPYGROUP o UPDATE COPYGROUP.

## Restricciones de los servidores que utilizan la característica de protección de retención de datos

Si la característica de protección de retención de datos se activa, se aplican más reglas al validar y activar un juego de políticas. La característica de protección de retención de datos se activa utilizando el mandato SET ARCHIVERETENTIONPROTECTION en un servidor que no tiene todavía ningún dato de cliente.

Si la protección de retención de datos se activa para un servidor, deben cumplirse varias reglas para que la política se active:

- Si existe una clase de gestión en el conjunto de políticas activas, debe existir una clase de gestión con el mismo nombre en el conjunto de políticas que se va a activar.
- Todas las clases de gestión del conjunto de políticas que se va a activar deben incluir valores de retención de archivado.
- Si el conjunto de políticas incluye valores de retención de archivado en una clase de gestión, el conjunto de políticas que se va a activar debe tener valores de retención de archivado que sean como mínimo tan grandes como los valores correspondientes del conjunto de políticas activas.

Si el servidor es un servidor gestionado en una configuración empresarial, podría recibir actualizaciones desde el servidor que es el gestor de configuración. Las actualizaciones de política recibidas por el servidor gestionado desde el gestor de configuración deben también cumplir las reglas anteriores.

### Conceptos relacionados:

[Configuración empresarial \(V7.1.1\)](#)

### Referencia relacionada:

SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)

## Personalización de una política

Puede personalizar las políticas existentes para que cumplan los requisitos de retención de datos nuevos o revisados de la organización. La modificación de un dominio de políticas o la copia de un dominio de políticas existente es una forma habitual de personalizar una política.

### Acerca de esta tarea

Los valores de política de claves están en clases de gestión. En las clases de gestión puede controlar tanto el número de versiones de copia de seguridad como el número de días que se conservarán las versiones de copia de seguridad en el almacenamiento del servidor. Cuando se utilizan ambos tipos de control, la política es más compleja. Si se controla solo el número de días que se conservarán las versiones de copia de seguridad, podrá definir de forma más sencilla durante cuánto tiempo se conservarán los datos de copia de seguridad.

Asegúrese de que la clase de gestión predeterminada de un dominio de políticas tenga los valores adecuados para la retención de datos de la mayor parte de los clientes asignados al dominio. Los valores de retención de la clase de gestión predeterminada se aplican a los datos cuando las operaciones del cliente no especifican una clase de gestión.

Puede trabajar en actualizaciones de una política y guardar los cambios para un momento posterior. Cuando esté satisfecho con los cambios del borrador, puede activar el conjunto de políticas actualizadas para aplicar los cambios.

### Procedimiento

1. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
2. Seleccione el dominio de políticas y pulse Aceptar. Pulse Conjuntos de políticas.
3. Pulse el conmutador Configurar para actualizar los valores.
4. Personalice los valores en la clase de gestión.

- a. Realice selecciones para los servicios de copia de seguridad. Por ejemplo, actualice los siguientes elementos para que las versiones de copias de seguridad inactivas de los clientes se conserven durante 30 días:
    - Copias de seguridad: Sin límite
    - Mantener copias de seguridad extra: 30 días
    - Copias de seguridad suprimidas: 1
    - Mantener copias de seguridad suprimidas: Sin límite
  - b. Opcional: Realice selecciones para los servicios de archivado. Por ejemplo, cambie la opción Mantener archivos archivados a 1 año.
  - c. Pulse Guardar.
5. Opcional: Pulse +Clase de gestión para añadir una clase de gestión.
- a. Realice selecciones para los valores básicos y pulse Añadir.
  - b. Personalice más valores en la nueva clase de gestión. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
  - c. Pulse Guardar.
6. En la columna Valor predeterminado, asegúrese de que se ha seleccionado una clase de gestión correcta como predeterminada. Los valores de retención de la clase de gestión predeterminada se aplican cuando las operaciones del cliente no especifican una clase de gestión. Las clases de gestión se pueden especificar al ejecutar una operación de cliente. Una clase de gestión también se puede especificar en un archivo de opciones de cliente que esté en el sistema cliente o en un conjunto de opciones de cliente definido en el servidor.
7. Active el conjunto de políticas pulsando Activar.
8. Asigne nodos cliente al dominio de políticas nuevo actualizando los nodos cliente existentes o inscribiendo nuevos nodos.
- Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
  - Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.
- La retención de datos de cliente que asigne al dominio de políticas ahora se controlará mediante la política.  
 Requisito: Si un cliente está en ejecución cuando se asigna a un nuevo dominio, debe detener y reiniciar el cliente para que el cambio surta efecto.

**Tareas relacionadas:**


Control de las operaciones de cliente mediante conjuntos de opciones de cliente

## Creación de una política copiando una política existente

Puede crear nuevas políticas copiando una política existente y, a continuación, actualizando las partes que desea cambiar.

### Procedimiento

Puede crear una nueva política copiando un dominio de políticas, actualizando las clases de gestión y, a continuación, asignando clientes al nuevo dominio.

1. En la página Visión general del Centro de operaciones, pase el cursor por encima del icono de valores  y pulse Creador de mandatos.
2. Copie un dominio de políticas utilizando el mandato COPY DOMAIN. Por ejemplo, copie el dominio de políticas predeterminadas, STANDARD, en un nuevo dominio de políticas, NEWDOMAIN:

```
copy domain standard newdomain
```

Esta operación copia el dominio de políticas y todos sus conjuntos de políticas y clases de gestión asociados. En este ejemplo, la operación copia los elementos siguientes en el dominio de políticas NEWDOMAIN:

- Un conjunto de políticas denominado STANDARD.
  - La clase de gestión denominada STANDARD, que se encuentra en el conjunto de políticas STANDARD.
  - Los grupos de copia de la clase de gestión STANDARD contienen:
    - El grupo de copias de seguridad denominado STANDARD
    - El grupo de copias archivadas denominado STANDARD
3. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
  4. Seleccione el dominio de políticas nuevo y pulse Aceptar. Pulse Conjuntos de políticas.
  5. Pulse el conmutador Configurar para actualizar los valores.
  6. Personalice los valores en las clases de gestión.
    - a. Realice selecciones para los servicios de copia de seguridad. Por ejemplo, actualice los siguientes elementos para que las versiones de copias de seguridad inactivas de los clientes se conserven durante 30 días:
      - Copias de seguridad: Sin límite
      - Mantener copias de seguridad extra: 30 días

- Copias de seguridad suprimidas: 1
    - Mantener copias de seguridad suprimidas: Sin límite
  - b. Opcional: Realice selecciones para los servicios de archivado. Por ejemplo, cambie la opción Mantener archivos archivados a 1 año.
  - c. Pulse Guardar.
7. Opcional: Realice otras actualizaciones y adiciones, tales como añadir una clase de gestión.
- a. Pulse +Clase de gestión para añadir una clase de gestión. Realice selecciones para los valores básicos y pulse Añadir.
  - b. Personalice más valores en la nueva clase de gestión. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
  - c. Pulse Guardar.
8. Seleccione la clase de gestión que utilizan los clientes, que se indica en la columna Predeterminada. Pulse Guardar. Los valores de retención de la clase de gestión predeterminada se aplican cuando las operaciones del cliente no especifican una clase de gestión. Las clases de gestión se pueden especificar al ejecutar una operación de cliente. Una clase de gestión también se puede especificar en un archivo de opciones de cliente que esté en el sistema cliente o en un conjunto de opciones de cliente definido en el servidor.
9. Active el conjunto de políticas pulsando Activar.
10. Asigne nodos cliente al dominio de políticas nuevo actualizando los nodos cliente existentes o inscribiendo nuevos nodos.
- Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
  - Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.
- La retención de datos de cliente que asigne al dominio de políticas ahora se controlará mediante la política. Por ejemplo, si ha implementado el ejemplo en el paso 6, las versiones de copia de seguridad inactivas de los clientes se conservan durante 30 días de forma predeterminada.
- Requisito: Si un cliente está en ejecución cuando se asigna a un nuevo dominio, debe detener y reiniciar el cliente para que el cambio surta efecto.

#### Tareas relacionadas:

Control de las operaciones de cliente mediante conjuntos de opciones de cliente

## Creación de un dominio de políticas

---

Es posible que desee crear un nuevo dominio de políticas para cada tipo de cliente que esté protegido mediante el servidor. Es posible que también desee dividir las responsabilidades de los clientes entre varios administradores concediéndoles autorización para dominios de políticas específicos.

### Acerca de esta tarea

---


La creación de un dominio de políticas puede ser útil en las siguientes circunstancias:

- Las aplicaciones, sistemas o máquinas virtuales necesitan diferentes valores de retención de datos. Puede crear un dominio de políticas para cada tipo de cliente, con una política predeterminada que sea adecuada para ese tipo.
- Los administradores son responsables de distintos grupos de clientes. Para cada administrador, puede crear un dominio de políticas al que asignará los clientes que va a gestionar ese administrador.

### Procedimiento

---

Los pasos siguientes resumen cómo crear un dominio de políticas.

1. En la página Visión general del Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.
2. Defina un dominio de políticas utilizando el mandato DEFINE DOMAIN.
3. Defina un conjunto de políticas para el dominio utilizando el mandato DEFINE POLICYSET.
4. En la página Visión general de Centro de operaciones, pulse el menú Servicios.
5. Seleccione el dominio de políticas y pulse Aceptar. Pulse Conjuntos de políticas.
6. Pulse el conmutador Configurar para actualizar los valores.
7. Pulse +Clase de gestión para añadir una clase de gestión. Realice selecciones para los valores básicos y pulse Añadir.
8. Opcional: Personalice más valores en la nueva clase de gestión:
  - a. Realice selecciones para los servicios de copia de seguridad en las siguientes columnas: Destino de copia de seguridad, Copias de seguridad, Mantener copias de seguridad extra, Copias de seguridad suprimidas y Mantener copias de seguridad suprimidas.
  - b. Para los servicios de archivado, realice selecciones en las columnas Destino de archivado y Mantener archivados.
  - c. Pulse Guardar.
9. Opcional: Pulse +Clase de gestión para añadir más clases de gestión.



10. En la columna Valor predeterminado, asegúrese de que se ha seleccionado una clase de gestión predeterminada.
11. Active el conjunto de políticas pulsando Activar.
12. Asigne clientes al nuevo dominio de políticas. En la barra de menús del Centro de operaciones, haga clic en Clientes.
  - o Para añadir nuevos clientes al dominio de políticas, pulse +Cliente.
  - o Para mover un cliente existente al dominio de políticas, seleccione el cliente, haga clic en Detalles y, a continuación, en la pestaña Propiedades. Seleccione el dominio de políticas nuevo y pulse Guardar.

**Referencia relacionada:**

DEFINE DOMAIN (Definir un nuevo dominio de políticas)

DEFINE POLICYSET (Definir un juego de políticas)

## Control de las operaciones de cliente mediante conjuntos de opciones de cliente

---

Puede utilizar conjuntos de opciones de cliente para controlar de forma centralizada las opciones de proceso que utilizan los clientes para operaciones, tales como una copia de seguridad. Los conjuntos de opciones de cliente garantizan que los datos estén protegidos de forma coherente de acuerdo con sus requisitos. Un conjunto de opciones de cliente pueden reemplazar las opciones en un archivo de opciones de cliente y añadir opciones que podrían no estar en un archivo de opciones del cliente local.

### Acerca de esta tarea

---

Al crear y asignar conjuntos de opciones de cliente, reduce la necesidad de actualizar archivos de opciones de cliente local y la cantidad de trabajo que deben realizar los usuarios.

Por ejemplo, puede definir un conjunto de opciones de cliente para especificar una lista de inclusión/exclusión que determina qué se incluirá o excluirá de la copia de seguridad y qué clases de gestión se utilizarán para gestionar retenciones de datos. Otras opciones que pueden ser útiles para el control de forma centralizada en un conjunto de opciones de cliente son compression y deduplication.

Puede crear conjuntos de opciones de cliente para clientes que tengan unas necesidades similares, como clientes en el mismo sistema operativo, clientes que utilizan el mismo software o clientes que utiliza un departamento. Por ejemplo, puede crear conjuntos de opciones de cliente para estaciones de trabajo Windows o para el departamento de nóminas. Después de crear el conjunto de opciones de cliente, asigne el conjunto a todos los clientes del mismo tipo.

No todas las opciones de cliente se pueden especificar en un conjunto de opciones de cliente en el servidor. Para obtener información acerca de las opciones de cliente que puede controlar centralmente en un conjunto de opciones de cliente, consulte Las opciones de cliente las puede establecer el servidor.

### Procedimiento

---

1. Defina un conjunto de opciones de cliente utilizando el mandato DEFINE CLOPTSET. Por ejemplo, para definir un conjunto de opciones de cliente con el nombre PAYROLLBACKUP, emita el mandato siguiente:

```
define cloptset payrollbackup description='Opciones de copia de seguridad para el departamento de nóminas'
```

2. Añada opciones de cliente al conjunto de opciones de cliente utilizando el mandato DEFINE CLIENTOPT. Por ejemplo, desea añadir las opciones include y exclude al conjunto de opciones de cliente denominado PAYROLLBACKUP para lograr los objetivos siguientes:

- o Excluir archivos de directorio temporales de internet de las operaciones de copia de seguridad
- o Incluir en la copia de seguridad todos los archivos del directorio C:\Data y sus subdirectorios y asignar los archivos a la clase de gestión PAYCLASS para retención de datos

Emita los siguientes mandatos:

```
define clientopt payrollbackup inclexcl "exclude.dir '*:\..\Archivos temporales de internet"  
define clientopt payrollbackup inclexcl "include C:\Data\..\* payclass"
```

3. Para asignar un conjunto de opciones de cliente a un cliente, siga los pasos siguientes:
  - a. En la página Visión general de Centro de operaciones, pulse Clientes.
  - b. Seleccione un cliente y pulse Detalles.
  - c. Pulse Propiedades.
  - d. En el área General, seleccione un conjunto de opciones y pulse Guardar.

**Referencia relacionada:**

DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)

DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)

- ☞ Opción de cliente de compresión
- ☞ Opción de cliente de eliminación de duplicados

## Configuración del almacenamiento

En función de la funcionalidad de almacenamiento que necesite, elija el tipo correcto de soporte de almacenamiento. Optimice y controle sus agrupaciones de almacenamiento para distintos tipos de datos.

- Tipos de agrupaciones de almacenamiento  
Para ayudarle a determinar qué tipo de agrupación de almacenamiento satisface mejor sus requisitos de almacenamiento, debe evaluar las características de cada tipo de agrupación de almacenamiento.
- Opciones de eliminación de datos duplicados  
Utilice la eliminación de duplicados de datos en línea para eliminar las duplicaciones y escribir los datos en una agrupación de almacenamiento de contenedores al mismo tiempo. Utilice la eliminación de datos duplicados postproceso para eliminar datos duplicados de las agrupaciones de almacenamiento de acceso secuencial (FILE) .
- Configuración de dispositivos de almacenamiento  
Configure dispositivos de almacenamiento conectando dispositivos, configurando controladores de dispositivo y creando los objetos que representan los dispositivos para el servidor.
- Configuración de una agrupación de almacenamiento de contenedores de directorios para almacenamiento de datos  
Puede configurar las agrupaciones de almacenamiento de contenedores de directorios para utilizar la deduplicación de datos en línea y almacenar los datos deduplicados.
- Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos  
Puede almacenar datos duplicados y sin duplicar en una agrupación de almacenamiento de contenedores en la nube y restaurar los datos cuando lo necesite. Puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar uno de los siguientes protocolos y proveedores de servicios: Amazon Web Services (AWS) con Simple Storage Service (S3), IBM® Cloud Object Storage con Swift o S3 (e IBM SoftLayer), Microsoft Azure, y OpenStack con Swift utilizando Keystone versión 1 o versión 2. Las agrupaciones de almacenamiento de contenedores en la nube no se admiten en Linux on System z.
- Optimización de rendimiento para almacenamiento de objetos en la nube  
Puede configurar IBM Spectrum Protect para almacenar datos temporalmente en uno o más directorios de agrupación de almacenamiento local durante la ingestión de datos. Los datos se han movido desde el almacenamiento local a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado.
- Gestión del espacio en las agrupaciones de almacenamiento de contenedor  
Después de configurar IBM Spectrum Protect y añadir almacenamiento, gestione los datos y el espacio de la agrupación de almacenamiento de forma eficaz para asegurarse de que funcione correctamente. Utilice agrupaciones de almacenamiento de contenedores para maximizar el espacio de almacenamiento y el rendimiento del servidor.
- Auditoría de un contenedor de la agrupación de almacenamiento  
Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre la información de base de datos y un contenedor de una agrupación de almacenamiento.
- Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos  
Puede utilizar muchos tipos de almacenamiento para el servidor IBM Spectrum Protect. Si utiliza almacenamiento de disco de bloque, unidades de estado sólido (SSD) o sistemas de archivos conectados a red para el almacenamiento de servidor, asegúrese de que el almacenamiento cumple los requisitos.

## Tipos de agrupaciones de almacenamiento

Para ayudarle a determinar qué tipo de agrupación de almacenamiento satisface mejor sus requisitos de almacenamiento, debe evaluar las características de cada tipo de agrupación de almacenamiento.

Utilice la tabla siguiente para evaluar cada tipo de agrupación de almacenamiento.

Tipo de agrupación de almacenamiento	Descripción	Usos
--------------------------------------	-------------	------

Tipo de agrupación de almacenamiento	Descripción	Usos
Agrupación de almacenamiento de contenedores de directorios	Una agrupación de almacenamiento primaria que utiliza un servidor para almacenar datos. Los datos que se almacenan en las agrupaciones de almacenamiento de contenedores de directorios utilizan la eliminación de duplicados de datos en línea y del lado del cliente.	<p>Utilícelo cuando desee eliminar los duplicados de datos en línea. Al utilizar agrupaciones de almacenamiento de contenedores de directorio, elimina la necesidad de reclamación de volumen, lo que mejora el rendimiento de servidor y reduce el coste del hardware de almacenamiento.</p> <p>No puede utilizar este tipo de agrupación de almacenamiento para operaciones de copia de seguridad, migración, reclamación, importación o exportación de agrupaciones de almacenamiento.</p>
Agrupación de almacenamiento de contenedores en la nube	Una agrupación de almacenamiento primaria que utiliza un servidor para almacenar datos. Utilice las agrupaciones de almacenamiento de contenedores en la nube para almacenar los datos en un proveedor de almacenamiento en la nube basado en almacenamiento de objetos. Los datos que se almacenan en las agrupaciones de almacenamiento de contenedores en la nube utilizan la eliminación de duplicados de datos en línea y del lado del cliente.	<p>Mediante el almacenamiento de datos en agrupaciones de almacenamiento de contenedores en la nube, puede aprovechar las ventajas de coste por unidad que ofrecen las nubes junto con las prestaciones de escalabilidad que proporciona el almacenamiento en nube.</p> <p>No puede utilizar este tipo de agrupación de almacenamiento para operaciones de copia de seguridad, migración, reclamación, cifrado, importación o exportación de agrupaciones de almacenamiento.</p>
Agrupación de almacenamiento de acceso aleatorio	Un conjunto de volúmenes que el servidor utiliza para almacenar las versiones de copia de seguridad de archivos, los archivos que son copias archivadas y los archivos migrados desde nodos cliente. Los archivos se almacenan en dispositivos de disco, DISK.	<p>Utilice este tipo de agrupación de almacenamiento para mantener una copia de los datos en dispositivos de DISCO. Puede migrar datos a estas agrupaciones de almacenamiento y desde las mismas.</p>
Agrupación de almacenamiento de acceso secuencial	Un conjunto de volúmenes que el servidor utiliza para almacenar las versiones de copia de seguridad de archivos, los archivos que son copias archivadas y los archivos migrados desde nodos cliente. Los archivos se almacenan en cinta o en dispositivos FILE. Los datos que se almacenan en las agrupaciones de almacenamiento de contenedores de acceso secuencial utilizan la eliminación de duplicados de datos de postproceso y del lado del cliente.	<p>Utilice este tipo de agrupación de almacenamiento para mantener una copia de los datos en dispositivos de CINTA. Puede migrar datos a este tipo de agrupación de almacenamiento.</p>
Agrupación de almacenamiento de copia	Conjunto de volúmenes que contiene copias de archivos que residen en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copias se utilizan solo para realizar copias de seguridad de datos que están almacenados en agrupaciones de almacenamiento primarias. Una agrupación de almacenamiento de copia no puede ser el destino de un grupo de copia de seguridad, de un grupo de copia archivada ni de una clase de gestión (para archivos bajo gestión de espacio).	<p>Utilice las agrupaciones de almacenamiento de copia para tener una copia de datos activos e inactivos que puede restaurar en una agrupación de almacenamiento primaria después de un desastre o de una parada.</p> <p>No puede utilizar la eliminación de duplicados de datos en línea, la compresión, la réplica o la eliminación de duplicados de datos con este tipo de agrupación de almacenamiento.</p>

Tipo de agrupación de almacenamiento	Descripción	Usos
Agrupación de almacenamiento de copia de contenedor	Un conjunto de volúmenes de cinta que contiene una copia de las extensiones con eliminación de duplicados que residen en una agrupación de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor se utilizan solo para proteger los datos almacenados en las agrupaciones de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor se utilizan para reparar los daños en una agrupación de almacenamiento de contenedores de directorio o para restaurar una agrupación de almacenamiento de contenedores de directorios si se produce un siniestro. Las agrupaciones de almacenamiento de copia de contenedor se almacenan en soporte secuencial.	Utilice las agrupaciones de almacenamiento de copia de contenedor para almacenar copias de agrupaciones de almacenamiento de contenedores de directorios en el local o fuera del local. Los datos dañados en las agrupaciones de almacenamiento de contenedores de directorios se pueden reparar utilizando las extensiones deduplicadas de una agrupación de almacenamiento de copia de contenedor.
Agrupación de almacenamiento de datos activos	Conjunto de volúmenes de agrupación de almacenamiento que contiene sólo versiones activas de datos de copia de seguridad de cliente.	Utilice agrupaciones de almacenamiento de datos activos para restaurar únicamente los datos activos en agrupaciones de almacenamiento primario después de un desastre o una parada. Cuando se restauran datos activos, puede restaurar datos de cliente más rápidamente, a la vez que utiliza menos ancho de banda.  No puede utilizar la eliminación de duplicados de datos en línea, la compresión, la réplica o la eliminación de duplicados de datos con este tipo de agrupación de almacenamiento.

Utilice la tabla siguiente para comparar las posibilidades de las agrupaciones de almacenamiento y elegir la agrupación de almacenamiento que mejor se ajuste a sus necesidades de negocio en función de los requisitos de almacenamiento.

Objetivo del usuario	Agrupación de almacenamiento de contenedores de directorios	Agrupación de almacenamiento de contenedores en la nube	Agrupación de almacenamiento de acceso aleatorio	Agrupación de almacenamiento de acceso secuencial	Agrupación de almacenamiento de copia	Agrupación de almacenamiento de copia de contenedor	Agrupación de almacenamiento de datos activos
Proteja los datos de la agrupación de almacenamiento o mediante la réplica de nodos.	✓		✓	✓	✓		✓
Reduzca las necesidades de almacenamiento o mediante la compresión en línea.	✓	✓					

Objetivo del usuario	Agrupación de almacenamiento de contenedores de directorios	Agrupación de almacenamiento de contenedores en la nube	Agrupación de almacenamiento de acceso aleatorio	Agrupación de almacenamiento de acceso secuencial	Agrupación de almacenamiento de copia	Agrupación de almacenamiento de copia de contenedor	Agrupación de almacenamiento de datos activos
Reduzca las necesidades de almacenamiento o utilizando la eliminación de duplicados de datos en línea.	✓	✓					
Reduzca las necesidades de almacenamiento o utilizando la eliminación de duplicados de datos del lado del cliente.	✓	✓		✓			
Reduzca las necesidades de almacenamiento o utilizando la eliminación de duplicados de datos de postproceso.				✓			
Proteja los datos de la agrupación de almacenamiento o mediante la protección de agrupaciones de almacenamiento.	✓					✓	
Realice una copia de seguridad de los datos de la agrupación de almacenamiento o utilizando las agrupaciones de almacenamiento de copia en disco o cinta.			✓	✓			
Almacene datos en la nube.		✓					

## Opciones de eliminación de datos duplicados

Utilice la eliminación de duplicados de datos en línea para eliminar las duplicaciones y escribir los datos en una agrupación de almacenamiento de contenedores al mismo tiempo. Utilice la eliminación de datos duplicados postproceso para eliminar datos duplicados de las agrupaciones de almacenamiento de acceso secuencial (FILE) .

Debe utilizar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de contenedores en la nube para la eliminación de duplicados de datos en línea. Si utiliza agrupaciones de almacenamiento de contenedores de directorio o de contenedor en la nube, reducirá la necesidad de realizar una reorganización fuera de línea y, de esta forma, se mejorará el rendimiento de servidor y se reducirá el coste del hardware de almacenamiento. No utilice clases de dispositivo o volúmenes con estos tipos de agrupación de almacenamiento.

Mediante la eliminación de datos duplicados postproceso, el servidor identifica en primer lugar los datos y después elimina los datos duplicados de la agrupación de almacenamiento. En el soporte de almacenamiento solo se conserva una instancia de los datos. Otras instancias de los mismos datos se sustituyen por un puntero a la instancia retenida. Cuando elimine datos duplicados, podrá reclamar espacio en la agrupación de almacenamiento.

Para obtener más información sobre la eliminación de datos duplicados postproceso, consulte el Eliminación de datos duplicados (V7.1.1).

En la eliminación de datos duplicados del lado del cliente, solo se envían al servidor datos deduplicados y comprimidos. El proceso se distribuye entre el servidor y el cliente durante un proceso de copia de seguridad.

Utilice la tabla siguiente para comparar opciones de deduplicación de datos.

Tipo de deduplicación de datos	Ventajas	Inconvenientes
Postproceso Restricción: Puede utilizar la deduplicación de datos postproceso para eliminar solo las agrupaciones de almacenamiento de acceso secuencial (FILE).	<ul style="list-style-type: none"> <li>Tras la deduplicación de datos, puede reclamar la agrupación de almacenamiento.</li> </ul>	<ul style="list-style-type: none"> <li>Tiempos de proceso más largos, porque los datos se deben identificar para poder eliminar los datos duplicados de la agrupación de almacenamiento.</li> </ul>
En línea Restricción: Solo puede utilizar la deduplicación de datos en línea con las agrupaciones de almacenamiento de contenedores de directorio y de contenedores en la nube.	<ul style="list-style-type: none"> <li>Deduplica los datos a medida que se escriben en una agrupación de almacenamiento de contenedores.</li> <li>Reduce la necesidad de reorganización fuera de línea, lo que mejora el rendimiento del servidor.</li> <li>Menor coste del hardware de almacenamiento.</li> </ul>	<ul style="list-style-type: none"> <li>Mayor grado de utilización de procesador por parte del servidor.</li> </ul>
En el lado del cliente	<ul style="list-style-type: none"> <li>El proceso se distribuye entre el servidor y el cliente durante un proceso de copia de seguridad.</li> </ul>	<ul style="list-style-type: none"> <li>Mayor grado de utilización de procesador por parte del cliente.</li> <li>Las operaciones del cliente tales como copias de seguridad tardan más tiempo en efectuarse.</li> <li>Sólo los datos comprimidos y deduplicados se envían al servidor.</li> </ul>

**Tareas relacionadas:**




- Configuración de eliminación de duplicados de datos (solución de disco multisitio)
- Configuración de eliminación de duplicados de datos (solución de disco de un solo sitio)
- Comparación de agrupaciones de almacenamiento

## Configuración de dispositivos de almacenamiento

Configure dispositivos de almacenamiento conectando dispositivos, configurando controladores de dispositivo y creando los objetos que representan los dispositivos para el servidor.

### Acerca de esta tarea

Si no va a utilizar la solución de disco de sitio único o de sitio múltiple, configure y gestione dispositivos de almacenamiento siguiendo las instrucciones de la documentación relativa a la V7.1.1:

-  Sistemas operativos AIX  Sistemas operativos Linux Configuración y gestión de los dispositivos de almacenamiento
-  Sistemas operativos Windows Configuración y gestión de los dispositivos de almacenamiento

# Configuración de una agrupación de almacenamiento de contenedores de directorios para almacenamiento de datos

Puede configurar las agrupaciones de almacenamiento de contenedores de directorios para utilizar la deduplicación de datos en línea y almacenar los datos deduplicados.


## Procedimiento

Para almacenar datos en una agrupación de almacenamiento de contenedores de directorios, complete los pasos siguientes:

1. Para crear una agrupación de almacenamiento de contenedores de directorios, siga estos pasos:
  - a. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
  - b. En la página Agrupaciones de almacenamiento, pulse + Agrupación de almacenamiento.
  - c. Realice los pasos del asistente Añadir agrupación de almacenamiento. Seleccione Directorio como tipo de almacenamiento basado en contenedor.
2. Cuando el asistente haya creado la agrupación de almacenamiento, actualice las clases de gestión y los conjuntos de políticas para que se utilice la nueva agrupación. Para actualizar una clase de gestión para utilizar la nueva agrupación, complete los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Servicios.
  - b. En la página Políticas, seleccione un dominio de políticas y pulse Detalles.
  - c. En la página Detalles, pulse la pestaña Conjunto de políticas.
  - d. Pulse el conmutador Configurar. Los conjuntos de políticas se pueden editar.
  - e. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
  - f. Actualice una o más clases de gestión para utilizar la nueva agrupación editando el campo Destino de copia de seguridad de la tabla.
  - g. Pulse Guardar.
3. Active el conjunto de políticas cambiado completando los pasos siguientes:
  - a. Pulse Activar. Como cambiar el conjunto de políticas activo puede provocar la pérdida de datos, se muestra un resumen de las diferencias entre el conjunto de políticas activo y el nuevo conjunto de políticas.
  - b. Mire las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a las clases de gestión del conjunto de políticas actualmente activo se enlazan, después de la activación, a las clases de gestión con los mismos nombres del nuevo conjunto de políticas.
  - c. Identifique las clases de gestión del conjunto de políticas actualmente activo que no tiene contrapartidas en el nuevo conjunto de políticas, y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a estas clases de gestión los gestiona, después de la activación, la clase de gestión predeterminada en el nuevo conjunto de políticas.
  - d. Si los cambios implementados por el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.
4. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.

## Qué hacer a continuación

Para proteger una agrupación de almacenamiento de contenedores de directorio, utilice el mandato PROTECT STGPOOL. Para obtener las instrucciones, consulte la sección PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento) y la sección Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta.

 Sistemas operativos Linux Si está protegiendo una agrupación de almacenamiento de contenedores de directorios copiando los datos en un servidor remoto y tiene problemas de red, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

- Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta  
Puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios copiando los datos a agrupaciones de almacenamiento de copia de contenedor, que se representan mediante volúmenes de cinta. La copia de cinta se utiliza para reparar daños en una agrupación de almacenamiento de contenedores de directorios.
- Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado  
Si su solución de almacenamiento incluye agrupaciones de almacenamiento de copias de contenedores que se representan por medio de volúmenes de cinta, pero no ha configurado la función del gestor de recuperación tras desastre (DRM), puede seguir un procedimiento manual para rotar los volúmenes de cinta fuera del local. Al mantener copias de los datos en volúmenes de cinta fuera del local, puede restaurar los datos si se produce un siniestro en el local.
- Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor  
De forma predeterminada, la reclamación de volumen de cinta está habilitada para las agrupaciones de almacenamiento de

copia de contenedor. Para asegurarse de que los volúmenes de cinta se utilizan de forma eficaz, puede cambiar el umbral para la reclamación de volumen.

- Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor  
Puede reclamar los volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor sin ejecutar ninguna operación de protección cuando no tenga tiempo para permitir operaciones de protección y reclamación.
- Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro  
Determine si las agrupaciones de almacenamiento de copia de contenedor cumplen los requisitos de protección frente a siniestro.

## Copia de agrupaciones de almacenamiento de contenedores de directorios en cinta

---

Puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios copiando los datos a agrupaciones de almacenamiento de copia de contenedor, que se representan mediante volúmenes de cinta. La copia de cinta se utiliza para reparar daños en una agrupación de almacenamiento de contenedores de directorios.

### Antes de empezar

---

Defina como mínimo una biblioteca de cintas en el servidor con el mandato DEFINE LIBRARY. Suministre suficientes unidades de cintas y volúmenes reutilizables para satisfacer los requisitos de almacenamiento. Para obtener más información sobre cómo gestionar los soportes de copia de seguridad y configurar el gestor de recuperación ante siniestro (DRM), consulte Gestor de recuperación ante siniestro (V7.1.1).

### Acerca de esta tarea

---

Para copiar los datos de las agrupaciones de almacenamiento de contenedores de directorio en cinta, el Centro de operaciones crea una planificación para ejecutar el mandato PROTECT STGPOOL. Cuando se ejecuta la planificación de protección, se crea una copia de cinta. Al menos debe estar disponible un volumen cuando se ejecuta la planificación de protección. De lo contrario, la operación no será satisfactoria.

Puede crear hasta dos copias de cinta, pero debe utilizar la interfaz de línea de mandatos para crear una segunda agrupación de almacenamiento de copia de contenedor. Una copia de cinta se puede llevar a una ubicación de recuperación ante siniestro fuera del local. La otra copia puede conservarse en el local para facilitar la recuperación de anomalías menos críticas.

Restricciones:

- Las bibliotecas de cintas virtuales no están soportadas, independientemente del tipo de biblioteca que se defina. Solo recibe soporte la cinta física.
- Las agrupaciones de almacenamiento de copia de contenedor se pueden utilizar para reparar daños menos a moderados de la agrupación de almacenamiento, lo que incluye contenedores o directorios dañados. Las agrupaciones de almacenamiento de copia de contenedor también se pueden utilizar para la protección frente a siniestro, pero debe asegurarse de que los tiempos de recuperación cumplan sus requisitos. Para obtener más información, consulte Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro.
- No puede utilizar la réplica para dirigirse a una agrupación de almacenamiento de copia de contenedor.  
Consejo: Puede crear una copia de cinta de los datos de agrupación de almacenamiento de contenedores del directorio en un sitio de recuperación tras desastre mediante un procedimiento para crear una agrupación de almacenamiento de copia de contenedor en el servidor de réplica de destino. Después, programe los mandatos PROTECT STGPOOL y REPLICATE NODE para ejecutarlo en el servidor de réplica fuente para proteger sus datos en el servidor de réplica de destino.
- No puede utilizar el procedimiento siguiente si la agrupación de almacenamiento de contenedores de directorios ya tiene una agrupación de almacenamiento de copia de contenedor asociada. Para crear una segunda agrupación de almacenamiento de copia de contenedor, siga las instrucciones del paso 5.

Si ha creado una agrupación de almacenamiento de copia de contenedor como parte del asistente Añadir agrupación de almacenamiento, no es necesario que utilice este procedimiento. Cuando haya completado el asistente, el Centro de operaciones habrá configurado la agrupación de almacenamiento de copia de contenedor y una planificación de protección.

### Procedimiento

---

Para configurar la protección de la agrupación de almacenamiento para una agrupación de almacenamiento de contenedores de directorio, siga estos pasos:

1. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
2. En la página Agrupaciones de almacenamiento, seleccione la agrupación de almacenamiento de contenedores de directorio que desea proteger en cinta.



3. Pulse Más > Añadir agrupación de copia de contenedor.
4. Siga las instrucciones de la ventana Añadir agrupación de copia de contenedor para planificar la protección en cinta.
5. Después de completar los pasos anteriores, puede añadir una segunda agrupación de almacenamiento de copia de contenedor utilizando la interfaz de línea de mandatos. Opcionalmente, siga los pasos siguientes para añadir una agrupación de almacenamiento de copia de contenedor:
  - a. Cree una agrupación de almacenamiento de copia de contenedor emitiendo el mandato DEFINE STGPOOL.
  - b. Asigne la agrupación de almacenamiento de copia de contenedor a la agrupación de almacenamiento de contenedores de directorio emitiendo el mandato UPDATE STGPOOL para la agrupación de contenedor de directorio.

## Resultados

---

Después de completar la configuración, los datos de la agrupación de almacenamiento de contenedores de directorios se copiará a una agrupación de almacenamiento de copia de contenedor basada en la planificación de protección definida.

## Qué hacer a continuación

---

1. Si ha creado una copia de cinta para el almacenaje externo, habilite la agrupación de almacenamiento externa de copia de contenedor para operaciones DRM emitiendo el mandato SET DRMCOPYCONTAINERSTGPOOL. Asegúrese de que los volúmenes de cinta se añadan a las planificaciones de rotación de cintas externas. Si no se ha configurado DRM, deberá hacerlo o utilizar un método alternativo para rotar las cintas fuera del local. Para obtener instrucciones sobre el método alternativo, consulte Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado. Para verificar que las agrupaciones de copia de contenedor fuera del local están habilitadas para DRM, utilice el mandato QUERY DRMSTATUS.

Para obtener las instrucciones acerca de cómo configurar DRM, consulte Disaster Recovery Manager (V7.1.1).

2. Confirme que el umbral de reclamación para la agrupación de almacenamiento de copia de contenedor cumpla con sus requisitos.

De forma predeterminada, la reclamación de volumen de cinta está habilitada para nuevas agrupaciones de almacenamiento de copia de contenedor que se crean utilizando el Centro de operaciones. La reclamación de volúmenes se lleva a cabo cuando el umbral de reclamación de la agrupación de almacenamiento de copia de contenedor está por debajo del 100%. Sin embargo, los volúmenes de cinta no son candidatos para la reclamación hasta que están llenos en un 75%. Tenga cuidado cuando utilice la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para la reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Para evitar que se sobrescriban los volúmenes inmediatamente después de que hayan sido suprimidas todas las extensiones, utilice el parámetro REUSEDelay para especificar un valor mayor que 0. El Centro de operaciones establece el umbral de reclamación en 60 % para las agrupaciones de almacenamiento de copia de contenedor locales.

Para obtener instrucciones sobre cómo cambiar el umbral de reclamación, consulte Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor.

3. Proteja los metadatos para la agrupación de almacenamiento de copia de contenedor.

Cuando se ejecute la planificación de protección, las extensiones de datos de las agrupaciones de almacenamiento de copia de contenedor se copian en los volúmenes de cinta sin los metadatos asociados. Estos metadatos son necesarios para restaurar las copias de cinta. Para proteger los metadatos, debe realizar por separado la copia de seguridad de la base de datos del servidor, junto con su historial de volúmenes, las opciones de servidor y los archivos de configuración de los dispositivos. Si utiliza la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes de cinta fuera del local, asegúrese de que se cumplan los requisitos siguientes para proporcionar la protección de recuperación ante siniestro:

  - Las operaciones de copia de seguridad de base de datos se ejecutan después de que estén finalizadas las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM.
  - Todos los volúmenes de copia de seguridad de base de datos y los volúmenes de DRM se trasladan fuera del local conjuntamente.

Para obtener las instrucciones acerca de cómo realizar la copia de seguridad de la base de datos del servidor y los archivos relacionados, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

4. Opcionalmente, cambie la planificación de protección para una agrupación de almacenamiento de contenedores de directorios que tiene una o más agrupaciones de almacenamiento de copia de contenedor asociadas utilizando el mandato UPDATE SCHEDULE. La planificación creada por el Centro de operaciones se denomina CONTAINER\_COPY.

### Conceptos relacionados:

Almacenamiento de datos en agrupaciones de almacenamiento de copia de contenedor

### Tareas relacionadas:

Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

**Referencia relacionada:**

DEFINE LIBRARY (Definir una biblioteca)

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

UPDATE SCHEDULE (Actualizar una planificación de administración)

QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)

## Rotación de volúmenes de cinta fuera del local cuando DRM no está configurado

---

Si su solución de almacenamiento incluye agrupaciones de almacenamiento de copias de contenedores que se representan por medio de volúmenes de cinta, pero no ha configurado la función del gestor de recuperación tras desastre (DRM), puede seguir un procedimiento manual para rotar los volúmenes de cinta fuera del local. Al mantener copias de los datos en volúmenes de cinta fuera del local, puede restaurar los datos si se produce un siniestro en el local.

### Procedimiento

---

1. Compruebe el volumen de almacenamiento que debe rotarse fuera del local utilizando el mandato CHECKOUT LIBVOLUME.
2. Actualice el volumen para indicar que se mueve fuera del local utilizando el mandato UPDATE VOLUME y especificando ACCESS=UNAVAILABLE. Opcionalmente, indique la ubicación fuera del local utilizando el parámetro LOCATION. Por ejemplo, especifique LOCATION=SITE1.
3. Reclame espacio realizando una de las siguientes acciones:
  - o Para reclamar espacio sin proteger la agrupación de almacenamiento, ejecute el mandato PROTECT STGPOOL y especifique TYPE=LOCAL y RECLAIM=ONLY.
  - o Para reclamar espacio protegiendo la agrupación de almacenamiento, ejecute el mandato PROTECT STGPOOL sin especificar RECLAIM=ONLY.
4. Supervise el volumen utilizando el mandato QUERY VOLUME. Si el volumen se muestra no disponibles y vacío, devuelva el volumen en el sitio e incorpórelo a la biblioteca utilizando el mandato CHECKIN LIBVOLUME.
5. Actualice el mandato utilizando el mandato UPDATE VOLUME y especificando ACCESS=READWRITE.

**Referencia relacionada:**

CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

## Cambiar el umbral de reclamación de volumen para agrupaciones de almacenamiento de copia de contenedor

---

De forma predeterminada, la reclamación de volumen de cinta está habilitada para las agrupaciones de almacenamiento de copia de contenedor. Para asegurarse de que los volúmenes de cinta se utilizan de forma eficaz, puede cambiar el umbral para la reclamación de volumen.

### Procedimiento

---

1. En la página Centro de operaciones Visión general, pulse Almacenamiento > Agrupaciones de almacenamiento.
2. Seleccione la agrupación de almacenamiento y pulse Detalles y, a continuación, Propiedades.
3. En la sección Reclamación, establezca el porcentaje de reclamación y pulse Guardar.  
Consejo: De forma alternativa, cambie el umbral de reclamación emitiendo el mandato UPDATE STGPOOL con el parámetro RECLAIM. Para obtener más detalles sobre el parámetro RECLAIM, consulte los mandatos para definir y actualizar las agrupaciones de almacenamiento de copia de contenedor.  
Restricción: No puede utilizar el mandato RECLAIM STGPOOL para reclamar volúmenes en las agrupaciones de almacenamiento de copia de contenedor. Para obtener detalles sobre cómo reclamar volúmenes en las agrupaciones de almacenamiento de copia de contenedor, consulte el parámetro RECLAIM en el mandato PROTECT STGPOOL.

## Reclamación de volúmenes de cinta volúmenes en agrupaciones de almacenamiento de copia de contenedor

---

Puede reclamar los volúmenes de cinta en agrupaciones de almacenamiento de copia de contenedor sin ejecutar ninguna operación de protección cuando no tenga tiempo para permitir operaciones de protección y reclamación.

### Acerca de esta tarea

---

Cuando emite el mandato PROTECT STGPOOL y la agrupación de almacenamiento de destino es una agrupación de almacenamiento de contenedor, las operaciones de protección y reclamación se ejecutan de forma predeterminada. La práctica preferida es permitir las operaciones de protección y reclamación que se desean ejecutar. Sin embargo, para ahorrar tiempo puede ejecutar únicamente la operación de protección de agrupación de almacenamiento o sólo reclamación, o puede limitar el número de volúmenes de cinta que están reclamados. Utilice este procedimiento sólo cuando tenga que reclamar volúmenes de cinta rápidamente tiempo o cuando tenga que reclamar un número limitado de volúmenes de cinta.

## Procedimiento

---

Para reclamar volúmenes de cinta que ejecutan la operación de protección de agrupación de almacenamiento, realice los pasos siguientes:

1. Opcional: Para maximizar la cantidad de espacio que se reclama, inicie el proceso de caducidad de inventario con el mandato EXPIRE INVENTORY.
2. Determine si desea que la reclamación se ejecute hasta su finalización o si desea limitar el número de volúmenes de cinta reclamados.
3. Para ejecutar la reclamación hasta su finalización, emite el mandato PROTECT STGPOOL y especifique los parámetros TYPE=LOCAL y RECLAIM=ONLY. Por ejemplo, para reclamar espacio en una agrupación de almacenamiento de copia de contenedor local que esté definido como protección de destino para SPOOL1, emita el mandato siguiente:

```
protect stgpool spool1 type=local reclaim=only
```

4. Para reclamar un número limitado de volúmenes, realice los pasos siguientes:
  - a. Defina un límite de reclamaciones para la agrupación de almacenamiento de copia de contenedor emitiendo el mandato UPDATE STGPOOL y especificando el parámetro RECLAIMLIMIT. Este parámetro limita al número de volúmenes de la agrupación de almacenamiento de copia de contenedor reclamados.
  - b. Emita el mandato PROTECT STGPOOL y especifique el parámetro TYPE=LOCAL con el parámetro RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED.

Consejo: Si especifica RECLAIM=YESLIMITED, las operaciones de reclamación y de protección de la agrupación de almacenamiento se ejecutan cuando se emite el mandato PROTECT STGPOOL. Si especifica RECLAIM=ONLYLIMITED, la reclamación es la única operación que se ejecuta. Si especifica cualquiera de estos valores, la reclamación sólo se ejecuta hasta que alcanza el límite de reclamaciones definido para la agrupación de almacenamiento de copia de contenedores. El límite de reclamación se define con el parámetro RECLAIMLIMIT en el mandato DEFINE STGPOOL o UPDATE STGPOOL.

Por ejemplo, reclamar un límite para cinco volúmenes de cinta en una agrupación de almacenamiento de copia de contenedor que se llama CCPOOL1 sin ejecutar una operación de protección en la agrupación de almacenamiento de contenedores del directorio de origen que recibe el nombre de SPOOL1, emita los siguientes mandatos:

```
actualizar stgpool ccpool1 reclaimlimit=5  
protect stgpool spool1 type=local reclaim=onlylimited
```

For example, para proteger una agrupación de almacenamiento con el nombre SPOOL1 y reclamar un máximo de 10 volúmenes de cinta en la agrupación de almacenamiento, emita los siguientes mandatos:

```
update stgpool spool1 reclaimlimit=10  
protect stgpool spool1 type=local reclaim=yeslimited
```

## Resultados

---

Se ha completado el procesamiento de la reclamación de la agrupación de almacenamiento. La operación de protección de la agrupación de almacenamiento no se ha ejecutado, por lo que los datos de la agrupación de almacenamiento del contenedor de directorios que se ha actualizado desde la última operación de protección no están protegidos.

## Qué hacer a continuación

---

1. Proteja los datos de la agrupación de almacenamiento de copia de contenedor emitiendo el mandato PROTECT STGPOOL y especificando el parámetro TYPE=LOCAL. El proceso de protección se ejecuta con el parámetro RECLAIM=YES predeterminado. La operación de protección lleva menos tiempo porque la reclamación ya se ha ejecutado. Por ejemplo, para proteger los datos de una agrupación de almacenamiento de copia de contenedor que se llama SPOOL1, emita el siguiente mandato:

```
protect stgpool spool1 type=local
```

También puede proteger los datos de una agrupación de almacenamiento de contenedores de directorios que se llama SPOOL1 sin ejecutar la reclamación emitiendo el siguiente mandato:

```
protect stgpool spool1 type=local reclaim=no
```

2. Realice una copia de seguridad de la base de datos del servidor y ejecute las operaciones planificadas de mantenimiento. Para obtener instrucciones, consulte Definición de planificaciones para actividades de mantenimiento del servidor.

**Referencia relacionada:**

- PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)
- DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia de contenedor)
- UPDATE STGPOOL (Definir agrupación de almacenamiento de copia de contenedor)
- EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)

## Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

Determine si las agrupaciones de almacenamiento de copia de contenedor cumplen los requisitos de protección frente a siniestro.

### Acerca de esta tarea

Puede crear una copia externa de la agrupación de almacenamiento de copia de contenedor para la protección de recuperación ante siniestro o para satisfacer los requisitos empresariales y reglamentarios para las copias de cinta externas. Antes de decidirse por utilizar copias de cintas externas para la protección frente a siniestro, plantéese seriamente si la solución cumple con el objetivo de tiempo de recuperación.

El uso de agrupaciones de almacenamiento de copia de contenedor para la recuperación frente a siniestro es apropiado cuando la cantidad de datos del entorno es igual o menor que los valores siguientes:

- 200 TB de total de datos gestionados
- 50 TB de datos de fondo
- 37 TB de datos frontales

**Total de datos gestionados**

Todos los datos almacenados en la agrupación de almacenamiento de contenedores de directorios en el servidor. Esto incluye las versiones activas e inactivas de los datos. El número de versiones está determinado por las políticas de retención.

**Datos de fondo**

Todos los datos almacenados en la agrupación de almacenamiento de copia de contenedor.

**Datos frontales**

Los datos activos actuales almacenados en la agrupación de almacenamiento de copia de contenedor. Estos son los datos activos que se utilizan para restaurar datos en los nodos cliente. En caso de que se produzca un siniestro, serán necesarios todo o parte de los datos frontales para restablecer la producción. Los datos frontales son un porcentaje del total de los datos gestionados y son menores o iguales al total de datos gestionados, en función de los valores de política en uso.

Para recuperarse de un siniestro dentro de 48 horas, el entorno del sistema en el sitio de recuperación debe cumplir los requisitos de hardware mínimos para las acciones de la tabla siguiente.

Acción	Tiempo requerido	Requisitos mínimos
Configure un servidor nuevo de IBM Spectrum Protect en un sitio de recuperación frente a siniestros. Para configurar el nuevo servidor, debe completar los pasos siguientes: <ol style="list-style-type: none"> <li>1. Suministrar discos para el servidor.</li> <li>2. Restaurar el servidor desde la copia de seguridad.</li> <li>3. Iniciar el servidor.</li> <li>4. Actualizar las configuraciones de dispositivos y de almacenamiento.</li> </ol>	Tiempo para restaurar el servidor: 6 horas	Utilice una unidad de estado sólido (SSD) para la base de datos del servidor, con los requisitos siguientes: <ul style="list-style-type: none"> <li>• Un mínimo de 100 MB por segundo de rendimiento de lectura/escritura promedio combinado</li> <li>• Un mínimo de 12.862 de operaciones de entrada/salida promedio por segundo (IOPS)</li> </ul>

Acción	Tiempo requerido	Requisitos mínimos
Auditar la agrupación de almacenamiento de contenedores de directorios y reparar los datos desde la cinta. Consejo: Si el sistema cumple los requisitos mínimos de hardware, puede reparar un máximo de 50 TB de datos de fondo dentro de 48 horas.	Tiempo para auditar la agrupación de almacenamiento: 2 horas  Tiempo para reparar la agrupación de almacenamiento utilizando una copia de cinta: 28 horas  Nota: La estimación de tiempo se aplica si tiene un máximo de 200 TB del total de datos gestionados en la agrupación de almacenamiento.	Utilice unidades de Nearline SAS (NL-SAS), como en una configuración del servidor de blueprint media, con un mínimo de 700 MB por segundo de rendimiento de grabación para el disco de la agrupación de almacenamiento.  Utilice la nueva generación de tecnología de cinta como, por ejemplo, LTO-7 o mejor, con un mínimo de seis unidades para permitir las operaciones de lectura simultáneas desde los volúmenes de cinta.
Restablezca datos en los nodos de cliente. Consejo: Si el sistema cumple los requisitos mínimos de hardware, puede restaurar un máximo de 37 TB de datos frontales dentro de 48 horas.	Tiempo para realizar las operaciones de restauración del cliente: 12 horas	Utilice unidades NL-SAS, como en una configuración del servidor de blueprint medio, con un mínimo de 10 sesiones de restauración que consiguen 3102 GB por hora.

## Procedimiento

1. El tipo de recuperación frente a siniestro estimado para el entorno utilizando la tabla siguiente. Determine si el tiempo de recuperación cumple los requisitos.

Tabla 1. Estimación de tiempo de recuperación para diferentes cantidades del total de datos gestionados

Objetivo de tiempo de recuperación	Total de datos gestionados (TB)	Número de horas para reparar una agrupación de almacenamiento de contenedores de directorios (First Byte Restored)	Horas hasta que se restauren los nodos de cliente (Disaster Recovery completo)
Hasta 1 al día	25	10	12
	50	13	16
	75	17	22
Hasta 2 días	100	20	26
	200	34	46
Hasta 4 días	300	48	66
	400	62	86
Más de 4 días	500	76	106

Notas:

- o Las frecuencias alcanzables dependen en gran medida de la carga de trabajo y del entorno configurado.
  - o El porcentaje de datos frontales es relativo al total de datos gestionados. Aumentar la cantidad de datos frontales aumenta el total del tiempo de recuperación. La reducción de la cantidad de datos frontales disminuye el total del tiempo de recuperación.
2. Calcule el tiempo de recuperación para el entorno mediante las fórmulas siguientes:
    - o Estime el valor **Horas hasta que se repare la agrupación de almacenamiento de contenedores de directorios (First Byte Restored)**:

Time to Client First Byte Restore =  
6 hours + 14 hours for every 100 TB of Total Managed Data

- o Estime el valor **Horas hasta que se restauren los nodos de cliente (Disaster Recovery completo)**:

Time to Client Restore Complete =  
Time to Client First Byte Restore + ((Total Managed Data \* Front-End Data) / Restore Rate)

**Tasa de restauración:** La velocidad a la que los clientes pueden restaurar datos desde el servidor de nuevo a su sistema local o dispositivo de almacenamiento.

3. Complete los procedimientos de prueba para la recuperación frente a siniestro para asegurarse de que las agrupaciones de almacenamiento de copia de contenedor se puedan utilizar para restaurar el entorno en un intervalo de tiempo que se ajuste a sus requisitos.

**Referencia relacionada:**

Reparación de agrupaciones de almacenamiento después de un siniestro

## Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos

---

Puede almacenar datos duplicados y sin duplicar en una agrupación de almacenamiento de contenedores en la nube y restaurar los datos cuando lo necesite. Puede configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar uno de los siguientes protocolos y proveedores de servicios: Amazon Web Services (AWS) con Simple Storage Service (S3), IBM® Cloud Object Storage con Swift o S3 (e IBM SoftLayer), Microsoft Azure, y OpenStack con Swift utilizando Keystone versión 1 o versión 2. Las agrupaciones de almacenamiento de contenedores en la nube no se admiten en Linux on System z.

### Antes de empezar

---

Realice los pasos siguientes:

1. Obtenga la información de configuración del proveedor de servicios en la nube:
  - o Amazon con S3 (fuera del local)
  - o Microsoft Azure
  - o IBM Cloud Object Storage con S3 (fuera del local, con IBM SoftLayer)
  - o IBM Cloud Object Storage con Swift (fuera del local, con IBM SoftLayer)
  - o IBM Cloud Object Storage con S3 (en local)
  - o OpenStack con Swift (dentro o fuera del local)
2. Especifique una clase de dispositivo que se utilizará para las operaciones de copia de seguridad de base de datos. Cuando utiliza el cifrado para las agrupaciones de almacenamiento de contenedores en la nube, la clave de cifrado maestra se utiliza para proteger la clave de cifrado de la nube en una copia de seguridad de base de datos.
  - a. En la barra de menús de Centro de operaciones, seleccione Servidores.
  - b. Seleccione una fila del servidor y pulse Hacer copia de seguridad.
  - c. Seleccione una clase de dispositivo que se utilizará para las operaciones de copia de seguridad de base de datos y pulse Hacer copia de seguridad.

Consejo: Como alternativa, utilice el mandato SET DBRECOVERY para especificar una clase de dispositivos para la copia de seguridad de base de datos.

### Procedimiento

---

Para almacenar datos en una agrupación de almacenamiento de contenedores en la nube, complete los pasos siguientes:

1. Cree una agrupación de almacenamiento de contenedores en la nube. Debe proporcionar información de configuración que identifique el servicio en la nube.
  - a. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
  - b. En la página Agrupaciones de almacenamiento, pulse + Agrupación de almacenamiento.
  - c. Realice los pasos del asistente Añadir agrupación de almacenamiento. Seleccione Nube en local o Nube fuera de local para el tipo de almacenamiento basado en contenedor.
2. Actualice las clases de gestión y los conjuntos de políticas para que se utilice la nueva agrupación de almacenamiento. Para actualizar una clase de gestión para utilizar la nueva agrupación de almacenamiento, complete los pasos siguientes:
  - a. En la barra de menús de Centro de operaciones, pulse Servicios.
  - b. En la página Políticas, seleccione un dominio de políticas y pulse Detalles.
  - c. En la página Detalles, pulse la pestaña Conjunto de políticas.
  - d. Pulse el conmutador Configurar. Los conjuntos de políticas se pueden editar.
  - e. Opcional: Para editar un conjunto de políticas que no está activo, pulse las flechas hacia adelante y hacia atrás para ubicar el conjunto de políticas.
  - f. Actualice una o más clases de gestión para utilizar la nueva agrupación de almacenamiento editando el campo Destino de copia de seguridad de la tabla.
  - g. Pulse Guardar.
3. Active el conjunto de políticas cambiado completando los pasos siguientes:
  - a. Pulse Activar. Como cambiar el conjunto de políticas activo puede provocar la pérdida de datos, se muestra un resumen de las diferencias entre el conjunto de políticas activo y el nuevo conjunto de políticas.
  - b. Mire las diferencias entre las clases de gestión correspondientes en los dos conjuntos de políticas y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están enlazados a las clases de gestión del conjunto de políticas actualmente activo se enlazan, después de la activación, a las clases de gestión con los mismos nombres del nuevo conjunto de políticas.
  - c. Identifique las clases de gestión del conjunto de políticas actualmente activo que no tiene contrapartidas en el nuevo conjunto de políticas, y tenga en cuenta las consecuencias en los archivos cliente. Los archivos cliente que están

- enlazados a estas clases de gestión los gestiona, después de la activación, la clase de gestión predeterminada en el nuevo conjunto de políticas.
- d. Si los cambios implementados por el conjunto de políticas son aceptables, seleccione la casilla de verificación Entiendo que estas actualizaciones pueden provocar pérdida de datos y pulse Activar.
4. Pulse el conmutador Configurar. Los conjuntos de políticas ya no se pueden editar.
5. Para aprovechar el almacenamiento local, cree un directorio de agrupación de almacenamiento para esta agrupación de almacenamiento utilizando el mandato DEFINE STGPOOLDIRECTORY. Para obtener más información, consulte Optimización de rendimiento para almacenamiento de objetos en la nube.

**Tareas relacionadas:**

- Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS con S3
- Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (en local)
- Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (fuera del local)
- Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con Swift (fuera del local)
- Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack con Swift
- Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube
- Optimización de rendimiento para almacenamiento de objetos en la nube

**Referencia relacionada:**

SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)

## Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS con S3

---

Antes de configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar Amazon Web Services (AWS) fuera del local con el protocolo Simple Storage Service (S3), debe obtener información de Amazon que necesitará para el proceso de configuración.

### Acerca de esta tarea

---

Las credenciales de cuenta de AWS son distintas de las credenciales de cuenta de Amazon. Utilice las credenciales de su cuenta de AWS cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o mediante el mandato DEFINE STGPOOL.

AWS utiliza *grupos* para almacenar datos. Los grupos de AWS se utilizan de la misma manera que los contenedores de una agrupación de almacenamiento de contenedores en la nube. IBM Spectrum Protect crea automáticamente un grupo en Amazon para una instancia de IBM Spectrum Protect y todas las agrupaciones correspondientes a esta instancia comparten dicho grupo.

Restricción: Edite un grupo de AWS solo con IBM Spectrum Protect y no modifique los datos del grupo ni edite los valores de configuración del mismo.

### Procedimiento

---

- Para registrar una cuenta de AWS, vaya a la página de Amazon S3 y pulse Crear una cuenta de AWS.
- Obtenga las credenciales de AWS:
  - Vaya a la página de Amazon S3 y pulse Registrarse en la consola.
  - Seleccione su nombre y seleccione Credenciales de seguridad.
  - Vaya a la sección Claves de acceso para localizar los campos ID de clave de acceso y Clave de acceso secreta. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
- Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
  - Tipo de nube: `Amazon - S3 API`
  - ID de clave de acceso: `id_clave_acceso`
  - Clave de acceso secreta: `clave_acceso_secreta`
  - Región: Seleccione el punto final de la región que mejor se ajuste a su ubicación, que encontrará en la página Regiones y puntos finales de Amazon AWS. Si selecciona `Otros`, especifique un URL de punto final de región en el campo URL e incluya el protocolo, que suele ser `https://`. Normalmente, puede utilizar la región más cercana a su ubicación física para el parámetro Región. Puesto que un grupo de Amazon solo existe en una región, solo puede especificar un URL de punto final para una región. Si necesita una región GovCloud, especifique un URL de la página Puntos finales de AWS GovCloud (Estados Unidos).

Aviso: Asegúrese que utiliza únicamente el URL de punto final de AWS para el valor de la región, como `https://s3-us-west-1.amazonaws.com`. No utilice el sitio web estático que aloja el URL para este valor.

- Nombre de grupo: Utilice el nombre de grupo predeterminado generado por el servidor, o especifique un nuevo nombre de grupo.
4. Para definir la agrupación de almacenamiento de contenedores en la nube, emita el mandato DEFINE STGPOOL con los siguientes valores:
- CLOUDTYPE: S3
  - IDENTITY: *id\_clave\_acceso*
  - PASSWORD: *clave\_acceso\_secreta*
  - CLOUDURL: especifique el URL de punto final de región que mejor se ajuste a su ubicación, que encontrará en la página Regiones y puntos finales de AWS.

Normalmente, puede utilizar la región más cercana a su ubicación física para el parámetro CLOUDURL. Si necesita una región GovCloud, especifique un URL de la página Puntos finales de AWS GovCloud (Estados Unidos).

Aviso: Asegúrese que utiliza únicamente el URL de punto final de AWS para el valor de CLOUDURL, como `https://s3-us-west-1.amazonaws.com`. No utilice el sitio web estático que aloja el URL para este valor.

---

## Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para AWS, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

---

## Configuración de un dispositivo compatible con Amazon S3 como agrupación de almacenamiento de contenedores en la nube

Puede configurar un dispositivo de almacenamiento que sea compatible con el protocolo Simple Storage Service (S3) de Amazon de forma que el dispositivo se pueda utilizar como una agrupación de almacenamiento IBM Spectrum Protect de contenedor en la nube.

---

## Acerca de esta tarea

Amazon S3 utiliza *grupos* para almacenar datos. Debe crear un grupo en el dispositivo de almacenamiento compatible con S3 para que lo utilice un servidor de IBM Spectrum Protect. Después de crear el grupo, utilice las credenciales de la cuenta en el dispositivo de almacenamiento de objetos en nube compatible con Amazon S3 al configurar agrupaciones de almacenamiento con el mandato DEFINE STGPOOL.

Restricción: No cambie los datos del grupo ni edite los valores de configuración para el grupo.

---

## Procedimiento

1. Cree un grupo en el dispositivo de almacenamiento de objetos en la nube. Siga las instrucciones de la documentación del dispositivo.
2. Cree una cuenta de usuario en el dispositivo de almacenamiento de objetos en la nube. La cuenta es utilizada por IBM Spectrum Protect para acceder al dispositivo utilizando el ID de clave de acceso y la clave de acceso secreta. Asegúrese de que la cuenta tenga permisos para almacenar datos y suprimir datos del grupo que ha creado en el paso 1. Tome nota de los valores de ID de clave de acceso y clave de acceso secreta para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Identifique el valor de URL que utilizará IBM Spectrum Protect para acceder al dispositivo de almacenamiento de objetos en la nube. Para obtener instrucciones, consulte la documentación de su dispositivo de almacenamiento de objetos en la nube.
4. Para definir la agrupación de almacenamiento de contenedores en la nube, emita el mandato DEFINE STGPOOL con los siguientes valores:

- CLOUDTYPE: S3
- IDENTITY: *id\_clave\_acceso*
- PASSWORD: *clave\_acceso\_secreta*
- CLOUDURL: `http://dirección_IP_punto_final_almacenamiento_objeto_nube` o `https://dirección_IP_punto_final_almacenamiento_objetos_nube`. Si utiliza más de un punto final, liste las direcciones IP de puntos finales separados por una barra vertical (|), sin espacios, como se muestra en el siguiente ejemplo:

```
CLOUDURL=endpoint_URL1|endpoint_URL2|endpoint_URL3
```

- BUCKETNAME: *nombre\_de\_grupo\_en\_dispositivo*

Para optimizar el rendimiento, utilice varios puntos finales o un equilibrador de carga.

---

## Qué hacer a continuación



Configure las agrupaciones de almacenamiento de contenedores en la nube del mismo modo que configuraría una agrupación de almacenamiento de contenedores en la nube para IBM Cloud Object Storage siguiendo las instrucciones descritas en Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

## Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para Microsoft Azure (fuera del local)

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar el sistema informático en nube Microsoft Azure, debe obtener de Microsoft la información para el proceso de configuración.

### Acerca de esta tarea

IBM Spectrum Protect admite los siguientes niveles de almacenamiento de Azure:

- *Nivel de almacenamiento dinámico* para los datos a los que se accede con frecuencia
- *Nivel de almacenamiento estático* para los datos a los que se accede con menos frecuencia

Puede utilizar un nivel de almacenamiento estático para obtener un almacenamiento a largo plazo rentable. Sin embargo, es más costoso restaurar datos de un nivel de almacenamiento estático que de un nivel de almacenamiento dinámico.

### Procedimiento

1. Regístrese en una cuenta de Microsoft Azure en el portal de Azure y creando una cuenta.
2. Cree una cuenta de almacenamiento. Normalmente, seleccione la ubicación más cercana al servidor de IBM Spectrum Protect más para la ubicación de la cuenta de almacenamiento.
3. Obtenga las credenciales de Azure:
  - a. Vaya al portal de Azure y pulse Cuentas de almacenamiento.
  - b. Abra una nueva cuenta de almacenamiento, vaya a la sección del contenedor del panel Blob Service y anote el valor de punto final de servicio blob para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. El punto final de servicio blob tiene un aspecto similar a estos ejemplos: `https://nombre.blob.core.windows.net` y `http://nombre.blob.core.windows.net`.
  - c. Cree una señal de firma de acceso compartido (SAS) abriendo el separador Firma de acceso compartido y complete los campos. Asegúrese de que la sección Servicios permitidos incluya Blob y que la sección Tipos de recurso permitidos incluya Contenedor y Objeto. Asegúrese de que la señal de SAS tenga permisos para leer, grabar, suprimir, listar, añadir y crear. Pulse Generar SAS.
  - d. Tome nota del valor de señal SAS para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. IBM Spectrum Protect no supervisa la fecha de caducidad de señal de SAS, por lo tanto, asegúrese de que selecciona la fecha que se adapte mejor a sus necesidades. Si la señal caduca, el servidor IBM Spectrum Protect pierde acceso a la cuenta de almacenamiento hasta que proporcione una nueva señal SAS.  
Consejo: Si desea actualizar con menos frecuencia la señal SAS, establezca la fecha de caducidad dentro de unos cuantos años. Además, asegúrese de verificar los campos de fecha y hora de inicio.
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
  - Tipo de nube: `Azure`
  - Señal SAS: `valor_señal_SAS`. Busque una cadena similar al ejemplo siguiente:

```
?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
  - Punto final de servicio Blob: especifique el punto final de servicio blob desde la cuenta de almacenamiento de Azure, por ejemplo, `https://nombre.blob.core.windows.net` o `http://nombre.blob.core.windows.net`.
5. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
  - CLOUDTYPE: `Azure`
  - PASSWORD: `valor_señal_SAS`. Busque una cadena similar al ejemplo siguiente:

```
?sv=2016-05-31&ss=b&srt=sco&sp=rwdlac&se=2017-04-05T18:26:12Z&st=2017-04-05T10:26:12Z&spr=https&sig=XUangS%2FcXXXXXXXXXXXXXXXXXXXXXXXXXXXXXELsuWp106Cmq7o%3D
```
  - CLOUDURL: especifique el punto final de servicio blob desde la cuenta de almacenamiento de Azure, por ejemplo, `https://nombre.blob.core.windows.net` o `http://nombre.blob.core.windows.net`.

### Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para Azure, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

## Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con Swift (fuera del local)

---

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar IBM® Cloud Object Storage y IBM SoftLayer fuera del local utilizando Swift, debe obtener la información de configuración de la página de SoftLayer Object Storage.

### Acerca de esta tarea

---

Utilice las credenciales de su cuenta de IBM SoftLayer cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL.

### Procedimiento

---

1. Cree una cuenta de SoftLayer siguiendo las instrucciones de la documentación de SoftLayer.
2. Obtenga las credenciales de SoftLayer:
  - a. Vaya a la página de SoftLayer Object Storage e inicie sesión con los credenciales de su cuenta.
  - b. Seleccione la cuenta y el clúster que desea configurar.
  - c. En la sección Cuenta, pulse Ver credenciales
  - d. En la sección Credenciales de cuenta, localice los campos Punto final de autenticación pública, Nombre de usuario y Clave de API. Tome nota de los valores de esos campos para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
  - o Tipo de nube: IBM Cloud Object Storage - Swift API (SoftLayer)
  - o Nombre de usuario: *nombre\_usuario*
  - o Contraseña: *clave\_API*
  - o URL: *punto\_final\_autenticación\_pública*
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
  - o CLOUDTYPE: SOFTLAYER
  - o IDENTITY: *nombre\_usuario*
  - o PASSWORD: *clave\_API*
  - o CLOUDURL: *punto\_final\_público\_autenticación*

### Qué hacer a continuación

---

Configure las agrupaciones de almacenamiento de contenedores en la nube para IBM SoftLayer siguiendo las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

## reparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (fuera del local)

---

Puede configurar agrupaciones de almacenamiento en la nube para utilizar IBM® Cloud Object Storage fuera del local con el protocolo Simple Storage Service (S3).

### Acerca de esta tarea

---

La implementación fuera del local de IBM Cloud Object Storage está gestionada a través de IBM SoftLayer o IBM Bluemix. En esta configuración, solo el propietario de la cuenta de Bluemix o SoftLayer puede crear grupos y administradores

Utilice las credenciales de su cuenta de IBM SoftLayer o IBM Bluemix cuando configure las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL. Para obtener más información, consulte la página de SoftLayer Object Storage. Para utilizar esta configuración, seleccione Cloud Object Storage - S3 API en la página de SoftLayer Order Object Storage.

## Procedimiento

---

1. Inicie sesión en el portal de clientes de SoftLayer.
2. Pulse el menú Almacenamiento y seleccione Almacenamiento de objetos.
3. Desde la página de almacenamiento de objetos, seleccione una cuenta S3.
4. Desde la página de almacenamiento de objetos en la nube, pulse Gestionar grupos y, continuación, el símbolo + para crear el grupo que desea utilizar con la nueva agrupación de almacenamiento de contenedores en la nube.
5. Pulse Mostrar credenciales para crear las credenciales de administrador para el nuevo grupo.
6. Pulse Añadir credencial.
7. Localice el ID de clave de acceso, la Clave de acceso secreta y el Punto final de autenticación pública. Tome nota de los valores de esos campos para que pueda utilizarlos al configurar las agrupaciones de almacenamiento. Si se encuentra dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.
8. Para configurar agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento en Centro de operaciones, seleccione Nube externa. Utilice los siguientes valores para los parámetros:
  - o Tipo de nube: *IBM Cloud Object Storage - S3 API (SoftLayer)*
  - o ID de clave de acceso: *id\_clave\_acceso*
  - o Clave de acceso secreta: *clave\_acceso\_secreta*
  - o Nombre de grupo: *nombre\_grupo* (desde el paso 4)
  - o URL: *punto\_final\_autenticación\_us-geo*  
Nota: Solo se necesita un punto final de proveedor de nube con esta configuración. Si todos sus servidores están dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.
9. Si configura agrupaciones de almacenamiento utilizando el mandato DEFINE STGPOOL, utilice los siguientes valores para los parámetros de mandato:
  - o CLOUDTYPE: *S3*
  - o IDENTITY: *ID\_clave\_acceso*
  - o BUCKETNAME: *nombre\_grupo* (del paso 4)
  - o PASSWORD: *clave\_acceso\_secreta*
  - o CLOUDURL: *punto\_final\_autenticación\_us-geo*  
Nota: Solo se necesita un punto final de proveedor de nube con esta configuración. Si todos sus servidores están dentro de la red de SoftLayer, puede utilizar un punto final de autenticación privada.

## Qué hacer a continuación

---

Configure las agrupaciones de almacenamiento de contenedores en la nube para IBM SoftLayer Cloud Object Storage siguiendo las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

## Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage con S3 (en local)

---

Antes de configurar agrupaciones de almacenamiento de contenedores en la nube para utilizar IBM® Cloud Object Storage en local con S3, debe configurar una plantilla de caja fuerte IBM Cloud Object Storage y una cuenta de usuario de IBM Cloud Object Storage y, después, obtener la información de configuración.

## Acerca de esta tarea

---

Las cajas fuertes de IBM Cloud Object Storage se utilizan de la misma manera que los contenedores de una agrupación de almacenamiento de contenedores en la nube. Configure una plantilla de caja fuerte para crear rápidamente cajas fuertes con sus valores preferidos.

Después de crear una plantilla de caja fuerte, utilice las credenciales de la cuenta de usuario de IBM Cloud Object Storage para configurar las agrupaciones de almacenamiento en el Centro de operaciones o con el mandato DEFINE STGPOOL. IBM Spectrum Protect utiliza el protocolo de servicio de almacenamiento simple (S3) para comunicarse con IBM Cloud Object Storage.

Consejo: Puede omitir los cuatro primeros pasos siguientes si desea configurar una caja fuerte que ya existe utilizando el parámetro BUCKETNAME en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

## Procedimiento

---

1. Crear una plantilla de caja fuerte:
  - a. Inicie sesión en IBM Cloud Object Storage y pulse el separador Configurar.
  - b. En el panel de navegación dsNet, expanda Agrupaciones de almacenamiento.
  - c. Seleccione la agrupación de almacenamiento de IBM Cloud Object Storage donde desea crear la plantilla de caja fuerte y pulse el enlace Agrupación de almacenamiento en la sección General.

- d. En la sección Plantillas de caja fuerte, pulse Crear plantilla de caja fuerte.
  - e. Seleccione los valores para la plantilla de caja fuerte predeterminada. Es posible que pueda optimizar el rendimiento si no selecciona las opciones Habilitar tecnología SecureSlice o Índice de nombres habilitado y si selecciona la opción Listado de recuperación habilitado.
  - f. En la sección Despliegue, seleccione la agrupación o agrupaciones de acceso que desea utilizar para la plantilla y pulse Guardar.
2. Establezca la plantilla de caja fuerte como predeterminada para el IBM Cloud Object Storage dsNet:
    - a. Pulse la pestaña Configurar.
    - b. En la sección Configuración de plantilla de caja fuerte predeterminada, pulse Configurar.
    - c. Seleccione una plantilla de caja fuerte para utilizar como predeterminada, y pulse Actualizar para establecer dicha plantilla como la predeterminada.
  3. Si esta es la primera vez que configura una plantilla de caja fuerte, habilite el rol de suministro de caja de fuerte para poder crear nuevas cajas fuertes:
    - a. Pulse la pestaña Administración.
    - b. En la sección Configuración de la API de suministro, pulse Configurar.
    - c. Seleccione Crear solo o Crear y suprimir para que los usuarios puedan crear nuevas cajas fuertes mediante la API de suministro.
    - d. Pulse Actualizar para guardar los valores.
  4. Utilice una cuenta de IBM Cloud Object Storage con la autoridad de administración para crear una cuenta de usuario en la instancia de IBM Cloud Object Storage en el entorno. Asegúrese de que la cuenta de usuario nueva tiene el rol de Suministrador de cuenta caja fuerte.
  5. Pulse la pestaña Seguridad y seleccione la cuenta de usuario nueva.
  6. Genere una clave de acceso para el usuario nuevo:
    - a. En la sección Autenticación de clave de acceso, pulse Cambiar claves.
    - b. En la página Editar claves de acceso, pulse Generar clave de acceso nueva.
    - c. Pulse Atrás.
  7. En la sección Autenticación de clave de acceso, localice los valores de ID de clave de acceso y Clave de acceso secreto. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
  8. Localice el valor del URL:
    - a. Pulse la pestaña Configurar.
    - b. En el panel de navegación dsNet, expanda las secciones Dispositivos y Aplicación de accesos.
    - c. Seleccione la aplicación de acceso IBM Cloud Object Storage. Verifique que la aplicación de acceso pertenece a una agrupación de acceso en la cual se ha desplegado la plantilla de caja fuerte predeterminada.
    - d. En la sección Configuración de dispositivo del dispositivo de acceso, anote el valor de Dirección IP para que pueda utilizarlo al configurar las agrupaciones de almacenamiento. Utilice `http://` delante del valor de dirección IP para impedir errores de seguridad de certificado.
  9. Si configura las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
    - o Tipo de cloud: `IBM Cloud Object Storage - S3 API`
    - o ID de clave de acceso: `id_clave_acceso`
    - o Clave de acceso secreta: `clave_acceso_secreta`
    - o Nombre de grupo: Utilice el nombre de grupo predeterminado generado por el servidor, o especifique un nuevo nombre de grupo.
    - o URL: `http://dirección_IP_acceso_almacenamiento_objetos_nube`  
 Importante: Si utiliza más de una aplicación de acceso, teclee la dirección IP de la aplicación de accesos y, a continuación, pulse Intro para añadir direcciones IP adicionales. Utilice varias aplicaciones de acceso o un equilibrador de carga para obtener un rendimiento óptimo.
  10. Si configura las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
    - o CLOUDTYPE: `S3`
    - o IDENTITY: `ID_clave_acceso`
    - o PASSWORD: `clave_acceso_secreta`
    - o CLOUDURL: `http://dirección_IP_acceso_Cloud_Object_Store`  
 Importante: Si utiliza más de una aplicación de accesos, liste las direcciones IP de acceso separadas por una barra vertical (`|`), sin espacios, como por ejemplo `CLOUDURL=<URL1_acceso>|<URL2_acceso>|<URL3_acceso>`. Utilice varias aplicaciones de acceso o un equilibrador de carga para un rendimiento óptimo.

## Qué hacer a continuación

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para IBM Cloud Object Storage, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

# Preparación para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack con Swift

---

Antes de configurar las agrupaciones de almacenamiento de contenedores en la nube para utilizar OpenStack en local o fuera del local con Swift, debe obtener la información de configuración del sistema OpenStack Swift.

## Acerca de esta tarea

---

Utilice las credenciales de su cuenta de OpenStack Swift al configurar las agrupaciones de almacenamiento mediante Centro de operaciones o el mandato DEFINE STGPOOL.

## Procedimiento

---

1. Cree una cuenta de OpenStack Swift siguiendo las instrucciones de la documentación de OpenStack Swift.
2. Obtenga las credenciales de OpenStack Swift:
  - a. En el sistema OpenStack Swift, escriba el siguiente mandato:

```
swift auth -v
```
  - b. En la salida, localice los valores de `OS_AUTH_URL`, el `OS_TENANT_NAME`, el `OS_USERNAME` y la `OS_PASSWORD`. Tome nota de los valores para que pueda utilizarlos al configurar las agrupaciones de almacenamiento.
3. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el asistente Añadir agrupación de almacenamiento del Centro de operaciones, utilice los valores siguientes para los parámetros:
  - o Tipo de nube: `OpenStack Swift`
  - o Nombre de usuario: `OS_TENANT_NAME:OS_USERNAME`
  - o Contraseña: `OS_PASSWORD`
  - o URL: `OS_AUTH_URL`
4. Si tiene previsto configurar las agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOL, utilice los valores siguientes para los parámetros de mandato:
  - o `CLOUDTYPE: SWIFT` o `V1SWIFT`
  - o `IDENTITY: OS_TENANT_NAME:OS_USERNAME`
  - o `PASSWORD: OS_PASSWORD`
  - o `CLOUDURL: URL_AUT_SO`
5. Si tiene previsto utilizar un arrendatario o un nombre de usuario específicos, anote los valores en el formato siguiente: `NOMBRE_ARRENDATARIO:NOMBRE_USUARIO`.
6. Para evitar la pérdida de datos, configure OpenStack Swift para crear réplicas de los datos que se graban en el almacén de objetos. Para obtener más información, consulte la documentación de OpenStack Swift.

## Qué hacer a continuación

---

Para configurar las agrupaciones de almacenamiento de contenedores en la nube para OpenStack Swift, siga las instrucciones de Configuración de una agrupación de almacenamiento de contenedores en la nube para almacenamiento de datos.

## Cifrado de datos para agrupaciones de almacenamiento de contenedores en la nube

---

Los datos almacenados en agrupaciones de contenedor en la nube fuera de las instalaciones están cifradas de forma predeterminada. Puede cifrar datos opcionalmente en agrupaciones de almacenamiento de contenedores en la nube fuera de las instalaciones.

## Acerca de esta tarea

---

Para obtener información sobre el cifrado de datos de la agrupación de almacenamiento de contenedores en la nube y para consideraciones de rendimiento relacionadas con el cifrado de datos, consulte la nota técnica 1963635.

## Optimización de rendimiento para almacenamiento de objetos en la nube

---

Puede configurar IBM Spectrum Protect para almacenar datos temporalmente en uno o más directorios de agrupación de almacenamiento local durante la ingestión de datos. Los datos se han movido desde el almacenamiento local a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado.

## Antes de empezar

---

Para optimizar el rendimiento de la copia de seguridad y el archivado, asegúrese de que esté instalada la IBM Spectrum Protect Versión 8.1.

## Acerca de esta tarea

---

Después de definir un directorio de agrupaciones de almacenamiento, el servidor de IBM Spectrum Protect utilizará dicho directorio como un área de entrada temporal para los datos que está transfiriendo al almacenamiento de objetos de nube. El servidor utiliza un proceso en segundo plano automatizado para transferir datos del almacenamiento local en el directorio al almacenamiento de objetos de nube. No tendrá que realizar ningún paso adicional para iniciar ni gestionar este proceso de transferencia. Después de que el servidor haya movido satisfactoriamente los datos desde el almacenamiento local al almacenamiento en nube, el servidor suprimirá los datos del directorio y liberará espacio para obtener más datos entrantes.

Si los directorios de agrupaciones de almacenamiento no tienen más espacio libre, las operaciones de copia de seguridad se detendrán prematuramente. Para evitar la situación puede asignar más directorios de agrupación de almacenamiento. También puede esperar a que los datos se eliminen automáticamente de los directorios locales después de mover los datos a la nube. El número requerido de directorios de agrupaciones de almacenamiento que necesita para definir depende de la configuración de su disco en el servidor. Cuando se produzcan las copias de seguridad iniciales, el servidor distribuirá los datos en todos los directorios que haya definido.

La cantidad de espacio que necesita para el almacenamiento local se basa en la cantidad de datos que espera para realizar una copia de seguridad cada día después de la deduplicación y la compresión de datos. Si tiene una conexión de red estable al almacenamiento de objetos de nube, la cantidad de espacio necesario es similar al necesario para una copia de seguridad diaria.

Para obtener información de planificación adicional, consulte el tema para su sistema operativo:

- AIX: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube
- Linux: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube
- Windows: Planificación para las agrupaciones de almacenamiento de contenedores de directorios y de contenedor en la nube




## Procedimiento

---

1. Cree una agrupación de almacenamiento de contenedores en la nube mediante el asistente Añadir agrupación de almacenamiento en el Centro de operaciones. De forma alternativa, cree una agrupación mediante el mandato DEFINE STGPOOL.
2. Defina uno o más directorios de agrupaciones de almacenamiento mediante el mandato DEFINE STGPOOLDIRECTORY. Asegúrese de que cada directorio de agrupación de almacenamiento tiene su propio sistema de archivos. En sistemas Linux, utilice xfs o ext4 como sistema de archivos en lugar de ext3, porque la supresión de archivos grandes tarda más tiempo con ext3. Asegúrese de que los nuevos directorios de agrupaciones de almacenamiento no compartan el sistema de archivos raíz, ni los mismos sistemas de archivos que utilizan otros recursos de IBM Spectrum Protect, como por ejemplo la base de datos o los registros.

### Referencia relacionada:

DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Gestión del espacio en las agrupaciones de almacenamiento de contenedor

---

Después de configurar IBM Spectrum Protect y añadir almacenamiento, gestione los datos y el espacio de la agrupación de almacenamiento de forma eficaz para asegurarse de que funcione correctamente. Utilice agrupaciones de almacenamiento de contenedores para maximizar el espacio de almacenamiento y el rendimiento del servidor.

## Acerca de esta tarea

---

Las agrupaciones de almacenamiento de contenedores son agrupaciones de almacenamiento primario que se utilizan para la deduplicación de datos en línea, la compresión en línea y el almacenamiento en la nube.

Restricción: No puede utilizar ninguna de las siguientes funciones con agrupaciones de almacenamiento de contenedor:

- Migración
- Reclamación
- Agregación
- Proximidad
- Exportar
- Importación
- Grabación simultánea

- Copia de seguridad de agrupaciones de almacenamiento
- Volúmenes virtuales




## Procedimiento

1. Para crear una agrupación de almacenamiento de contenedores de directorios, siga estos pasos:
  - a. Abra el Centro de operaciones.
  - b. En la barra de menús de Centro de operaciones, pulse Almacenamiento > Agrupaciones de almacenamiento.
  - c. Pulse +Agrupación de almacenamiento.
  - d. Complete los pasos del asistente Añadir agrupación de almacenamiento:
    - Para utilizar la deduplicación de datos en línea, seleccione una agrupación de almacenamiento de Directorio bajo el almacenamiento basado en contenedor.
    - Cuando configure directorios para la agrupación de almacenamiento de contenedores de directorio, especifique las vías de acceso de directorio que ha creado para el almacenamiento durante la configuración del sistema.
  - e. Después de configurar la nueva agrupación de almacenamiento de contenedores de directorio, pulse Cerrar y ver políticas para actualizar una clase de gestión y empezar a utilizar la agrupación de almacenamiento.
2. Para obtener un rendimiento óptimo de las agrupaciones de almacenamiento de contenedor, lleve a cabo las siguientes tareas:

Tarea	Procedimiento	Más información
Proteger la agrupación de almacenamiento	<p>Cuando se crea una agrupación de almacenamiento de contenedores de directorio en el Centro de operaciones, puede configurar la protección de la agrupación de almacenamiento en la planificación que se asigna a la agrupación de almacenamiento.</p> <p>Como alternativa, utilice el mandato PROTECT STGPOOL desde el servidor de origen para hacer una copia de seguridad de las extensiones de datos en una agrupación de almacenamiento de contenedores de directorio.</p> <p>Al proteger una agrupación de almacenamiento, no utilice recursos que repliquen datos y metadatos existentes, lo que mejora el rendimiento del servidor.</p>	<ul style="list-style-type: none"> <li>○ Protección de los datos de las agrupaciones de almacenamiento de contenedores de directorio</li> <li>○ PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)</li> </ul>
Reparar una agrupación de almacenamiento	<p>Cuando una agrupación de almacenamiento está protegida, puede utilizar el mandato REPAIR STGPOOL para reparar extensiones de datos dañadas. Utilice el mandato REPAIR STGPOOL para reparar una agrupación de almacenamiento de contenedores de directorio.</p> <p>Restricción: Si replica nodos de cliente, pero no protege la agrupación de almacenamiento del contenedor de directorio, no puede reparar la agrupación de almacenamiento.</p>	<ul style="list-style-type: none"> <li>○ Reparación de agrupaciones de almacenamiento</li> <li>○ REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)</li> </ul>
Suprimir contenedores	<p>Los contenedores se suprimen en el inventario a medida que los datos de archivo se eliminan o caducan.</p> <p>Utilice el mandato DEFINE STGPOOL y especifique el parámetro REUSEDELAY para controlar el tiempo que las extensiones duplicadas están asociadas a una agrupación de almacenamiento de contenedores de directorio después de que se deja de hacer referencia a la misma.</p>	<ul style="list-style-type: none"> <li>○ DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores de directorio)</li> <li>○ AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)</li> </ul>

	Si un contenedor está dañado, utilice el mandato AUDIT CONTAINER para recuperar o eliminar datos.	
Convierta una agrupación de almacenamiento primario que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL)	Puede convertir una agrupación de almacenamiento existente en una agrupación de almacenamiento de contenedores de directorio siguiendo los pasos del apartado Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor. Restricción: No puede convertir los siguientes tipos de agrupación de almacenamiento: <ul style="list-style-type: none"> <li>○ Agrupaciones de almacenamiento primario que utilizan clases de dispositivo de acceso aleatorio (DISK)</li> <li>○ Agrupaciones de almacenamiento de copia</li> <li>○ Agrupaciones de almacenamiento de datos activos</li> </ul>	<ul style="list-style-type: none"> <li>○ CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)</li> </ul>
Supervisar la ocupación de la agrupación de almacenamiento de contenedor	Supervise la solución de almacenamiento para identificar problemas potenciales y existentes. Para obtener más información, consulte el apartado Supervisión de soluciones de almacenamiento.	

- Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor  
Conversión de una agrupación de almacenamiento primaria que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL) en una agrupación de almacenamiento de contenedores. Los datos que se almacenan en una agrupación de almacenamiento de contenedores pueden utilizar tanto la deduplicación de datos en línea como la compresión en línea.
- Limpieza de los datos de una agrupación de almacenamiento de origen  
Para convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio, es posible que tenga que limpiar los datos o archivos dañados que están en la agrupación de almacenamiento de origen.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Conversión de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de contenedor

Conversión de una agrupación de almacenamiento primaria que utiliza una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca de cinta virtual (VTL) en una agrupación de almacenamiento de contenedores. Los datos que se almacenan en una agrupación de almacenamiento de contenedores pueden utilizar tanto la deduplicación de datos en línea como la compresión en línea.

### Antes de empezar

Para asegurarse de que los volúmenes de una agrupación de almacenamiento y las agrupaciones de almacenamiento de copia asociadas no se reutilicen durante el proceso de conversión, especifique un valor para el parámetro REUSEDELAY en el mandato UPDATE STGPOOL. Especifique un valor para el parámetro REUSEDELAY que sea mayor que la duración de la conversión. Es posible que deba retardar la reutilización de los volúmenes por los siguientes motivos:

- Ha suprimido accidentalmente los datos durante la conversión de una agrupación de almacenamiento.
- Necesita funcionalidades de la agrupación de almacenamiento que no están disponibles en agrupaciones de almacenamiento de contenedor.

Consejo: Cuando especifica el parámetro REUSEDELAY y hay una operación de conversión en curso, hay un espacio de almacenamiento que no está disponible en la agrupación de almacenamiento de origen hasta que caduca el valor del parámetro.

Para crear una agrupación de almacenamiento de contenedores donde se traspasarán los datos, siga estos pasos:

1. En la página Agrupaciones de almacenamiento del Centro de operaciones, pulse + Agrupación de almacenamiento.



2. Realice los pasos del asistente Añadir agrupación de almacenamiento. Debe seleccionar el tipo de almacenamiento basado en contenedor que necesite.

## Acerca de esta tarea

---

Al convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedor, elimina la necesidad de la reclamación del volumen. La omisión de las operaciones de reclamación de volúmenes puede ayudar a mejorar el rendimiento del servidor y a reducir la cantidad de hardware de almacenamiento necesario.

A medida que los archivos se convierten, las copias almacenadas en las agrupaciones de copia o en las agrupaciones de datos activos se van suprimiendo.

Restricciones:

- Si la agrupación de origen está definida como un destino de copia de seguridad, archivado o migración en un juego de políticas activo que tiene cambios pendientes, debe activar esos cambios para poder convertir la agrupación.
- Para asegurarse de que el destino especifica una agrupación de almacenamiento que no se convierte o que está llevando a cabo la conversión, debe actualizar todas las políticas que hacen referencia a la agrupación de almacenamiento de origen.
- Si la agrupación de almacenamiento de origen se ha especificado como siguiente agrupación de almacenamiento, debe actualizar el parámetro NEXTSTGPOOL del comando UPDATE STGPOOL para especificar una agrupación de almacenamiento de acceso aleatorio o secuencial que no se esté convirtiendo.
- Los tipos de datos siguientes no son elegibles para la conversión: copias de seguridad de tablas de contenido (TOC), volúmenes virtuales y datos de NDMP (Protocolo de gestión de datos de redes). Antes de iniciar el proceso de conversión, suprima manualmente estos tipos de datos de la agrupación de almacenamiento, mueva los tipos de datos a otra agrupación de almacenamiento primaria, o permita que los tipos de datos caduquen en función de los valores de política.
- Al convertir una agrupación de almacenamiento con una clase de dispositivo FILE a una agrupación de contenedor de directorios, la agrupación de almacenamiento de destino debería ser aproximadamente un 30 % más grande que la agrupación de almacenamiento de origen. Normalmente no es necesario espacio adicional al convertir otros tipos de agrupaciones de almacenamiento.

Para obtener más información sobre las mejores prácticas de la conversión de agrupación de almacenamiento, consulte Mejores prácticas para la conversión de agrupación de almacenamiento de IBM Spectrum Protect.

- Si la agrupación de almacenamiento de origen se utiliza para almacenar copias de seguridad de TOC, asegúrese de que haya disponible otra agrupación de almacenamiento primaria para almacenar nuevas copias de seguridad de TOC. Las copias de seguridad existentes de la TOC no se mueven durante la conversión.

La agrupación de TOC debe utilizar un formato de datos NATIVE o NONBLOCK y una clase de dispositivo que no sea Centera. Para evitar que se produzcan retardos de montaje, utilice una clase de dispositivo DISK o FILE.

## Procedimiento

---

1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione una agrupación de almacenamiento que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta, o VTL.
2. Pulse Más > Convertir y siga los pasos del asistente para Convertir agrupación de almacenamiento.  
Consejo: Planifique la conversión durante al menos 2 horas para una agrupación de almacenamiento que utiliza una clase de dispositivo FILE y un mínimo de 4 horas para VTL.




## Qué hacer a continuación

---

Cuando finalice el proceso de conversión, la agrupación de almacenamiento de origen puede contener datos dañados o datos que sean incompatibles con las agrupaciones de almacenamiento de contenedores. Para limpiar la agrupación de almacenamiento de origen, siga los pasos del apartado Limpieza de objetos tras la conversión de la agrupación de almacenamiento.

### Tareas relacionadas:

Restauración de la base de datos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Limpieza de los datos de una agrupación de almacenamiento de origen

---

Para convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio, es posible que tenga que limpiar los datos o archivos dañados que están en la agrupación de almacenamiento de origen.

## Procedimiento

---

Utilice las opciones siguientes para recuperar o reparar datos dañados:

- Para recuperar una versión no dañada de los datos de una copia o agrupación de almacenamiento de datos activos, utilice el mandato RESTORE STGPOOL.
- Para recuperar una versión no dañada de los datos de un servidor de réplica de destino, emita el mandato REPLICATE NODE y especifique el parámetro RECOVERDAMAGED=YES.
- Elimine los datos que no se pueden reparar después de la conversión de la agrupación de almacenamiento mediante el mandato REMOVE DAMAGED.

Es posible que el mandato REMOVE DAMAGED no elimine volúmenes que estén marcados como destruidos en la agrupación de almacenamiento de origen. Para eliminar estos volúmenes, siga estos pasos:

- a. Emita el mandato DELETE VOLUME y especifique el parámetro DISCARDATA=YES.
  - b. Emita el mandato CONVERT STGPOOL para convertir la agrupación de almacenamiento de nuevo.
  - c. Si los datos dañados se identifican durante la conversión de la agrupación de almacenamiento, vuelva a emitir el mandato REMOVE DAMAGED.
- Lleve a cabo las tareas de análisis que se describen en la nota técnica 1666371.

## Qué hacer a continuación

Tras recuperar o reparar los datos dañados, vuelva a intentar la conversión emitiendo el mandato CONVERT STGPOOL.

Para ver información sobre los archivos dañados que permanecen en la agrupación de almacenamiento de origen, emita el mandato QUERY CLEANUP.

Consejo: Si se muestra un estado Limpieza para una agrupación de almacenamiento que no contiene datos, puede suprimirla mediante el mandato DELETE STGPOOL.

### Referencia relacionada:

DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)

REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)

REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)

RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)

## Auditoría de un contenedor de la agrupación de almacenamiento

Audite un contenedor de agrupación de almacenamiento para comprobar si hay incoherencias entre la información de base de datos y un contenedor de una agrupación de almacenamiento.

### Acerca de esta tarea

Audita un contenedor de la agrupación de almacenamiento en las siguientes situaciones:

- Cuando emite el mandato QUERY DAMAGED y se detecta un problema.
- Cuando el servidor muestra mensajes sobre extensiones de datos dañadas.
- El hardware informa de un problema y se visualizan mensajes de error asociados con el contenedor de la agrupación de almacenamiento.

### Procedimiento

1. Para auditar un contenedor de la agrupación de almacenamiento, emita el mandato AUDIT CONTAINER. Por ejemplo, emita el siguiente mandato para auditar un contenedor, 00000000000076c.dcf:

```
audit container c:\tsm-storage\07\00000000000076c.dcf
```

2. Revise la salida del mensaje ANR4891I para obtener información sobre cualquier extensión de datos dañada.

## Qué hacer a continuación

Si detecta problemas con el contenedor de la agrupación de almacenamiento, puede restaurar datos basándose en la configuración.

Puede reparar el contenido de la agrupación de almacenamiento utilizando el mandato REPAIR STGPOOL.

Restricción: Solo puede reparar el contenido de la agrupación de almacenamiento si ha protegido dicha agrupación de almacenamiento mediante el mandato PROTECT STGPOOL.

### Referencia relacionada:

🔗 AUDIT CONTAINER (Verificar la coherencia de la información de base de datos para una agrupación de almacenamiento de contenedores de directorio)

🔗 QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)

# Requisitos de sistema de almacenamiento y reducción del riesgo de corrupción de datos

---

Puede utilizar muchos tipos de almacenamiento para el servidor IBM Spectrum Protect. Si utiliza almacenamiento de disco de bloque, unidades de estado sólido (SSD) o sistemas de archivos conectados a red para el almacenamiento de servidor, asegúrese de que el almacenamiento cumple los requisitos.

Se aplican los siguientes requisitos al almacenamiento para la base de datos de servidor, el registro activo y el registro de archivado, para agrupaciones de almacenamiento que utilizan clases de dispositivo DISK o FILE y para agrupaciones de almacenamiento de contenedores de directorios.

El almacenamiento se puede conectar al sistema servidor mediante cualquier método que sea válido para el sistema operativo. Por ejemplo, el almacenamiento se puede conectar directamente o utilizando la tecnología de canal de fibra o iSCSI.

Debido a la variedad de sistemas de almacenamiento que pueden cumplir los requisitos del almacenamiento de servidor, no hay disponible ninguna lista de dichos dispositivos. Póngase en contacto con el proveedor si tiene preguntas sobre si un sistema cumple los requisitos de IBM Spectrum Protect.

Para obtener detalles sobre los requisitos de sistema de archivos, consulte la nota técnica 1902417. Para obtener detalles sobre los requisitos de Network File System (NFS), consulte la nota técnica 1470193.

Los sistemas de almacenamiento y de archivos deben informar sobre los resultados de confirmación y grabación de forma síncrona y precisa en el servidor de IBM Spectrum Protect. Los errores de grabación de los que no se informa o de los que se informa de forma asíncrona que hacen que los datos no se confirmen de manera permanente en el sistema de almacenamiento pueden producir corrupción de datos. La corrupción de datos puede producir anomalías operativas, incluyendo la imposibilidad de iniciar el servidor, y normalmente es necesario recuperar los datos.

Puede reducir el riesgo de corrupción de datos siguiendo las siguientes sugerencias:

## Memoria caché de escritura

Los sistemas de disco utilizan memoria caché de escritura para mejorar el rendimiento del sistema. Para reducir el riesgo de corrupción de datos, el sistema de almacenamiento debe confirmar de forma fiable los datos de la memoria caché de escritura en el almacenamiento permanente.

Normalmente la memoria caché de escritura tiene una batería para evitar la pérdida de datos de la memoria caché durante cortas paradas de suministro eléctrico. Para sistemas críticos, tenga en cuenta la posibilidad de utilizar fuentes de alimentación de seguridad para proteger la memoria caché de paradas de suministro eléctrico prolongadas.

## E/S directa

La E/S directa satisface la necesidad del servidor de creación de informes síncronos y precios sobre las operaciones de escritura y confirmación de datos.

Atención: No inhabilite la E/S directa en situaciones donde el método de almacenamiento en memoria caché de escritura tiene potencial para causar la pérdida de datos. Si se inhabilita la E/S directa, pueden aumentar significativamente las probabilidades de pérdida de datos dado que el sistema de archivos, además del sistema de disco, almacena en memoria caché más datos.

## Réplica de almacenamiento

Los entornos que replican el almacenamiento de IBM Spectrum Protect deben utilizar características como mantenimiento de orden de escritura entre el origen (servidor local) y el destino (servidor remoto). La base de datos, el registro activo, los registros de archivado y las agrupaciones de almacenamiento deben formar parte de un grupo de consistencia. Un grupo de consistencia mantiene relaciones entre volúmenes para conservar el orden de escritura para que se puedan recuperar. Las E/S de los miembros del grupo de consistencia de destino deben escribirse en el mismo orden que en el origen y mantener las mismas características de volatilidad.

Para mantener la sincronización entre servidores de IBM Spectrum Protect en los sitios local y remoto, no inicie un servidor en el sitio remoto, excepto en una situación de migración tras error. Supervise la sincronización de datos en las ubicaciones local y remota. Si se pierde la sincronización, debe restaurar el servidor en la ubicación remota utilizando mandatos de restauración de IBM Spectrum Protect para la base de datos y las agrupaciones de almacenamiento.

## Sugerencias para la configuración de almacenamiento

---

Si desea ver sugerencias para la configuración de almacenamiento a fin de optimizar el rendimiento, consulte los temas siguientes en la documentación de producto de la V7.1.1. La información de las listas de comprobación se puede aplicar a releases posteriores.

- Lista de comprobación de los discos de base de datos del servidor
- Lista de comprobación de los discos de registro de recuperación
- Lista de comprobación para agrupaciones de almacenamiento que utilizan clases de dispositivo DISK o FILE

## Supervisión de soluciones de almacenamiento

---

Después de implementar una solución de IBM Spectrum Protect, supervise la solución para asegurarse de que funciona correctamente. Si supervisa la solución a diario y de forma periódica, podrá identificar problemas potenciales y existentes. La información recopilada se puede utilizar para resolver problemas y optimizar el rendimiento del sistema.

### Acerca de esta tarea

---

El método preferido para supervisar una solución es utilizar el Centro de operaciones, que proporciona el estado general y detallado del sistema en una interfaz gráfica de usuario. Además, puede configurar el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema.

### Procedimiento

---


1. Complete las tareas de supervisión diarias. Para obtener instrucciones, consulte Lista de comprobación de supervisiones diarias.
2. Complete las tareas de supervisión periódicas. Para obtener instrucciones, consulte Lista de comprobación de supervisiones periódicas.
3. Para verificar que el sistema cumple con los requisitos de licencia, siga las instrucciones del apartado Verificación de la conformidad de licencia.
4. Opcional: Configure los informes de correo electrónico del estado del sistema. Para obtener instrucciones, consulte el apartado Seguimiento del estado del sistema mediante informes de correo electrónico
5. Opcional: En algunos casos, es posible que desee utilizar las herramientas de supervisión avanzada para completar tareas de supervisión específicas o resolver problemas. Para seleccionar y configurar herramientas de supervisión avanzadas, consulte Selección, configuración y uso de herramientas de supervisión.

### Qué hacer a continuación


---

Para ayudarle a diagnosticar problemas con clientes de archivado y copia de seguridad, instale servicios de gestión de cliente de IBM Spectrum Protect en cada sistema cliente de archivado y copia de seguridad que lo acepte. Cuando el servicio de gestión de cliente está instalado en un sistema, en el Centro de operaciones puede pulsar Diagnosticar para obtener ayuda para diagnosticar problemas con el cliente de archivado y copia de seguridad. Para instalar el servicio de gestión de cliente, siga las instrucciones del apartado Recopilación de información de diagnóstico con servicios de gestión de cliente de IBM Spectrum Protect .

**Conceptos relacionados:**

 Rendimiento

**Tareas relacionadas:**

 Resolución de problemas

## Lista de comprobación de supervisión diaria


---

Revise la lista de comprobación para asegurarse de que realiza las tareas de supervisión diaria importantes.

Complete las tareas de supervisión diariamente desde la página Centro de operaciones Descripción general. Puede acceder a la página Descripción general abriendo Centro de operaciones y pulsando Descripciones generales.

La siguiente figura muestra la ubicación para completar cada una de las tareas.









Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.



La tabla siguiente lista las tareas de supervisión diarias y proporciona instrucciones para completar cada tarea.

Tabla 1. Tareas de supervisión diarias



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>1</b> Determine si los clientes corren riesgo de estar desprotegidos debido a operaciones de seguridad que han fallado o que se han perdido.</p>	<p>Para verificar si los clientes están en riesgo, en el área Clientes, busque una notificación En riesgo. Para ver detalles, pulse el área Clientes. Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede ver y analizar los registros de planificación y errores de cliente completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Clientes, seleccione el cliente y pulse Detalles.</li> <li>2. Para diagnosticar un problema, pulse Diagnóstico.</li> </ol>	<p>Para clientes que no tienen instalado el servicio de gestión de cliente, acceda al sistema de cliente para revisar los registros de error de cliente.</p>
<p><b>2</b> Determine si los errores relacionados con el cliente o relacionados con el servidor requieren atención.</p>	<p>Para determinar la gravedad de cualquier alerta notificada, en el área Alertas, pase el ratón por encima de las columnas.</p>	<p>Para ver información adicional sobre alertas, siga los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Alertas.</li> <li>2. En la tabla Alertas, seleccione una alerta.</li> <li>3. En el panel Registro de actividades, revise los mensajes. El panel muestra los mensajes relaciones que se han emitido antes y después de que se produjera la alerta seleccionada.</li> </ol>
<p><b>3</b> Determine si los servidores gestionados por Centro de operaciones están disponibles para proporcionar servicios de protección de datos a los clientes.</p>	<ol style="list-style-type: none"> <li>1. Para verificar si los clientes están en riesgo, en el área Servicios, busque una notificación No disponible.</li> <li>2. Para ver información adicional, pulse el área Servidores.</li> <li>3. Seleccione un servidor en la tabla Servidores y pulse Detalles.</li> </ol>	<p>Consejo: Si detecta un problema relacionado con las propiedades de servidor, actualice las propiedades de servidor:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione un servidor y pulse Detalles.</li> <li>2. Para actualizar las propiedades de servidor, pulse Propiedades.</li> </ol>


Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>4 Determine si hay suficiente espacio disponible para el inventario del servidor, que consta de la base de datos del servidor, del registro activo y del registro de archivado.</p>	<ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la columna Estado de la tabla, consulte el estado del servidor y resuelva los problemas que puedan surgir: <ul style="list-style-type: none"> <li>o Normal  Hay suficiente espacio para la base de datos de servidor, el registro activo y el registro de archivado.</li> <li>o Crítico  No hay suficiente espacio para la base de datos de servidor, el registro activo o el registro de archivado. Debe añadir espacio inmediatamente o se interrumpirán los servicios de protección de datos proporcionados por el servidor.</li> <li>o Aviso  La base de datos de servidor, el registro activo o el registro de archivado se están quedando sin espacio. Si esta condición persiste, deberá añadir espacio.</li> <li>o No disponible  No se puede obtener el estado. Asegúrese de que el servidor se está ejecutando y de que no hay problemas de red. Este estado se muestra también si el ID de administrador de supervisión está bloqueado o, por el contrario, no disponible en el servidor. Este ID se llama nombre_servidor_concentrador_IBM-OC.</li> <li>o No supervisado  Los servidores no supervisados se definen para el servidor concentrador, pero no están configurados para la gestión por parte de Centro de operaciones. Para configurar un servidor sin supervisar, selecciónelo, y pulse Supervisar servidor de radio.</li> </ul> </li> </ol>	<p>También puede buscar alertas relacionadas en la página Alertas. Para obtener instrucciones adicionales sobre la resolución de problemas, consulte Resolución de problemas del servidor.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>5</b> Verifique las operaciones de seguridad de la base de datos del servidor.</p>	<p>Para determinar la última vez que se hizo copia de seguridad del servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse el área Servidores.</li> <li>2. En la tabla Servidores, revise la columna Última copia de seguridad de base de datos.</li> </ol>	<p>Para obtener información más detallada sobre operaciones de copia de seguridad, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la tabla Servidores, seleccione una fila y pulse Detalles.</li> <li>2. En el área de copia de seguridad de base de datos, pase el ratón por encima de las marcas de selección para revisar la información sobre las operaciones de copia de seguridad.</li> </ol> <p>Si no se ha hecho copia de seguridad de la base de datos recientemente (por ejemplo, en las últimas 24 horas), puede iniciar una operación de seguridad:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Servidores.</li> <li>2. En la tabla, seleccione un servidor y pulse Hacer copia de seguridad.</li> </ol> <p>Para determinar si la base de datos del servidor se ha configurado para operaciones de copia de seguridad automáticas, realice los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY DB: <pre>query db f=d</pre> </li> <li>3. En la salida, revise el campo Nombre de clase de dispositivo completo. Si se especifica una clase de dispositivo, el servidor se configura para copias de seguridad de base de datos automáticas.</li> </ol>
<p><b>6</b> Supervise otras tareas de mantenimiento del servidor. Las tareas de mantenimiento del servidor pueden incluir planificaciones de mandatos administrativos en ejecución, scripts de mantenimiento y mandatos relacionados.</p>	<p>Para buscar información sobre los procesos que han fallado debido a problemas de servidor, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Pulse Servidores &gt; Mantenimiento.</li> <li>2. Para obtener el historial de dos semanas de un proceso, visualice la columna Historial.</li> <li>3. Para obtener más información sobre un proceso planificado, pase el ratón por encima de la casilla de verificación asociada al proceso.</li> </ol>	<p>Para obtener información sobre la supervisión de procesos y la resolución de problemas, consulte la ayuda en línea de Centro de operaciones.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>7</b> Verifique que la cantidad de datos que se ha enviado recientemente a y desde los servidores está dentro del rango esperado.</p>	<ul style="list-style-type: none"> <li>• Para obtener una descripción general de una actividad en las últimas 24 horas, vea el área Actividad.</li> <li>• Para comparar la actividad en las últimas 24 horas con la actividad de las últimas 24 horas, revise las cifras en las áreas Actuales y Anteriores.</li> </ul>	<ul style="list-style-type: none"> <li>• Si se han enviado más datos al servidor de los que esperaba, determine qué clientes están haciendo copia de seguridad de más datos e investigue la causa. Es posible que la deduplicación de datos del lado del cliente no esté funcionando correctamente.</li> <li>• Si se han enviado al servidor menos datos de los que esperaba, investigue si las operaciones de seguridad del cliente están procediendo tal como estaba planificado.</li> </ul>
<p><b>8</b> Verifique que las agrupaciones de almacenamiento están disponibles para hacer copia de seguridad de los datos de cliente.</p>	<ol style="list-style-type: none"> <li>1. Si se indican problemas en el área Almacenamiento &amp; Disponibilidad de datos, pulse Agrupaciones para ver los detalles: <ul style="list-style-type: none"> <li>◦ Si se visualiza un estado Crítico , se muestra el estado, no hay suficiente espacio disponible en la agrupación de almacenamiento o el estado de acceso no está disponible.</li> <li>◦ Si se visualiza un estado de Aviso , se muestra el estado, la agrupación de almacenamiento se está quedando sin espacio o su estado de acceso es de solo lectura.</li> </ul> </li> <li>2. Para ver el espacio utilizado, libre y total para la agrupación de almacenamiento seleccionada, pase el cursor por encima de las entradas de la columna Capacidad utilizada.</li> </ol>	<p>Para ver la capacidad de la agrupación de almacenamiento que se ha utilizado en las dos últimas semanas, seleccione una fila en la tabla Agrupaciones de almacenamiento y pulse Detalles.</p>



Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p>9 Verifique que los dispositivos de almacenamiento están disponibles para operaciones de seguridad.</p>	<p>En el área Almacenamiento &amp; Disponibilidad de datos, en la sección Volúmenes, en las barras de capacidad, revise el estado del que se ha informado junto a los Dispositivos. Si se visualiza un estado Crítico  o Aviso  el estado se muestra para cualquier dispositivo, investigue el problema. Para ver detalles, pulse Dispositivos.</p>	<p>Los dispositivos de disco pueden tener un estado crítico o de aviso por los siguientes motivos:</p> <ul style="list-style-type: none"> <li>• En las clases de dispositivo DISK, es posible que los volúmenes estén fuera de línea o tengan un estado de acceso de solo lectura. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los volúmenes.</li> <li>• En las clases de dispositivo FILE no compartidas, es posible que los directorios estén fuera de línea. Además, puede que no haya suficiente espacio libre disponible para asignar volúmenes reutilizables. La columna Almacenamiento de disco de la tabla Dispositivos de disco muestra el estado de los directorios.</li> <li>• Para las clases de dispositivos FILE que se comparten, es posible que las unidades no estén disponibles. Una unidad no está disponible si está fuera de línea, si ha dejado de responder al servidor o si su vía de acceso está fuera de línea. Otras columnas de la tabla Dispositivos de disco muestran el estado de las unidades y de las vías de acceso.</li> </ul> <p>Es posible que los dispositivos de cinta tengan un estado de aviso o muy grave si las unidades no están disponibles. Una unidad no está disponible si está fuera de línea, si ha dejado de responder al servidor o si su vía de acceso está fuera de línea. Es posible que un dispositivo de cinta también tenga un estado muy grave si la biblioteca está fuera de línea. Otras columnas de la tabla Dispositivos de cinta muestran el estado de la robótica de biblioteca, unidades y vías de acceso.</p> <p>Para las operaciones de copia de seguridad de cinta, compruebe que haya disponible suficientes cintas reutilizables. Si no está seguro de si el número de cintas reutilizables es suficiente, abra el cuaderno de detalles para ver el uso de cintas y una estimación de la disponibilidad de cintas reutilizables. Para abrir el cuaderno de detalles, seleccione una biblioteca en la tabla y pulse Detalles.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados e información sobre solución de problemas
<p><b>10</b> Supervise los procesos de réplica de nodo.</p>	<ol style="list-style-type: none"> <li>1. Para obtener el estado global de los procesos de réplica de nodo, vea el área Réplica en la página Centro de operaciones Descripción general.</li> <li>2. Para ver información sobre cada par de servidores replicados, pulse el área de réplica.</li> <li>3. Para ver la cantidad de datos que se ha duplicado durante las dos últimas semanas y la velocidad de la duplicación, seleccione un par de servidores y pulse Detalles.</li> <li>4. Para ver la información de réplica para un cliente, en la página Centro de operaciones Descripción general, pulse Clientes. Vea la información en la columna Carga de trabajo de réplica.</li> </ol>	<p>Para la supervisión avanzadas, vea la información sobre cómo ejecutar y finalizar procesos de réplica de nodos utilizando mandatos:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general del Centro de operaciones, pase el ratón sobre el icono de configuración  y pulse Creador de mandatos.</li> <li>2. Emita el mandato QUERY REPLICATION. Para obtener instrucciones, consulte QUERY REPLICATION (Consultar los procesos de réplica de nodos). Si la operación de réplica se ha completado satisfactoriamente, el valor de Total de archivos a replicar coincide con el valor de Total de archivos replicados.</li> </ol> <p>Para mostrar mensajes que están relacionados con el proceso de réplica de un nodo en un servidor de réplica de origen o destino, siga los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Visión general del Centro de operaciones pulse Servidores.</li> <li>2. Seleccione el servidor de réplica de origen o destino y pulse Detalles: <ul style="list-style-type: none"> <li>o Para ver las tareas activas, pulse Tareas activas, seleccione la tarea y verifique que se muestra el estado En ejecución. Para obtener detalles, consulte los registros de actividad relacionados.</li> <li>o Para ver las tareas completadas, pulse Tareas completadas, seleccione la tarea y asegúrese de que se visualiza el estado Completado. Para obtener detalles, consulte los registros de actividad relacionados.</li> </ul> </li> </ol>

## Lista de comprobación de supervisión periódica

Para asegurarse de que las operaciones se ejecutan correctamente, lleve a cabo las tareas de la lista de comprobación de supervisión periódica. Planifique las tareas periódicas con la suficiente frecuencia para que pueda detectar problemas potenciales antes de que se conviertan en problemáticos.










Consejo: Para ejecutar mandatos administrativos para tareas de supervisión avanzadas, utilice el creador de mandatos de Centro de operaciones. El creador de mandatos proporciona una función anticipada para guiarle cuando entra mandatos. Para abrir el creador de mandatos, vaya a la página Centro de operaciones Descripción general. En la barra de menús, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.

Tabla 1. Tareas de supervisión periódicas

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
-------	------------------------	--


Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el rendimiento del sistema.</p>	<p>Determine la longitud de tiempo necesaria para las operaciones de copia de seguridad de cliente:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>. Busque el servidor asociado al cliente.</li> <li>2. Pulse <i>Servidores</i>. Seleccione el servidor y pulse <i>Detalles</i>.</li> <li>3. Para ver la duración de las tareas completadas en las últimas 24 hora, pulse <i>Tareas completadas</i>.</li> <li>4. Para ver la duración de las tareas completadas hace más de 24 horas, utilice el mandato QUERY ACTLOG. Siga las instrucciones en QUERY ACTLOG (Consultar las anotaciones de actividades).</li> <li>5. Si la duración de las operaciones de copia de seguridad de cliente está aumentando y los motivos no están claros, investigue la causa.</li> </ol> <p>Si ha instalado el servicio de gestión de cliente en un cliente de archivado y copia de seguridad, puede diagnosticar problemas de rendimiento para el cliente de archivado y copia de seguridad completando los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página de Centro de operaciones <i>Visión general</i>, pulse <i>Cientes</i>.</li> <li>2. Seleccione un cliente de archivado y copia de seguridad y pulse <i>Detalles</i>.</li> <li>3. Para recuperar registros de cliente, pulse <i>Diagnóstico</i>.</li> </ol>	<p>Para obtener instrucciones sobre la reducción del tiempo que tarda el cliente en hacer copia de seguridad de los datos en el servidor, consulte <i>Resolución de problemas de rendimiento del cliente comunes</i>.</p> <p>Busque cuellos de botella de rendimiento. Para ver instrucciones, consulte <i>Identificación de cuellos de botella de rendimiento</i>.</p> <p>Para obtener información sobre la identificación y resolución de otros problemas de rendimiento, consulte <i>Rendimiento</i>.</p>
<p>Determine el ahorro de disco proporcionado por la deduplicación de datos.</p>	<ol style="list-style-type: none"> <li>1. En la página <i>Centro de operaciones Descripción general</i>, pulse <i>Agrupaciones</i>.</li> <li>2. Seleccione una agrupación y pulse <i>Vista rápida</i>.</li> <li>3. En el área <i>Optimización de almacenamiento de datos</i>, vea la fila <i>Espacio guardado</i>.</li> </ol>	<p>En la supervisión avanzada, para obtener estadísticas detalladas sobre el proceso de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o agrupación de almacenamiento de contenedores en la nube específica, complete los siguientes pasos:</p> <ol style="list-style-type: none"> <li>1. En la página <i>Descripción general de Centro de operaciones</i>, pase el ratón sobre el icono de valores  y pulse <i>Creador de mandatos</i>.</li> <li>2. Obtenga un informe estadístico emitiendo el mandato GENERATE DEDUPSTATS. Siga las instrucciones en GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos para una agrupación de almacenamiento de contenedores de directorios).</li> <li>3. Vea el informe estadístico emitiendo el mandato QUERY DEDUPSTATS. Siga las instrucciones de QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos).</li> </ol>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Verifique que se han guardado los archivos de copia de seguridad actuales para la configuración del dispositivo y la información del historial de volumen.</p>	<p>Acceda a las ubicaciones de almacenamiento para asegurarse de que hay archivos disponibles. El método preferido es guardar los archivos de copia de seguridad en dos ubicaciones. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.</li> <li>2. Para ubicar los archivos de historial de volumen y de configuración de dispositivo, emita los siguientes mandatos: <pre>query option volhistory  query option devconfig</pre> </li> <li>3. En la salida, revise la columna Valor de opción para encontrar las ubicaciones de archivo.</li> </ol> <p>Si se produce un desastre, se necesita el archivo de historial de volumen y el archivo de configuración de dispositivo para restaurar la base de datos del servidor.</p>	

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Determinar si hay suficiente espacio disponible para el sistema de archivos del directorio de instancia.</p>	<p>Verifique que al menos el 20% de espacio libre está disponible en el sistema de archivos del directorio de instancia. Realice la acción adecuada para el sistema operativo:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -g instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Linux Para ver el espacio disponible en el sistema de archivos, en la línea de mandatos del sistema operativo emita el siguiente mandato: <pre>df -h instance_directory</pre> donde <i>instance_directory</i> especifica el directorio de instancia.</li> <li>•  Sistemas operativos Windows En el programa Windows Explorer, pulse el botón derecho del ratón en el sistema de archivos y, después, Propiedades. Vea la información de capacidad.</li> </ul> <p>La ubicación preferida del directorio de instancia depende del sistema operativo donde está instalado el servidor:</p> <ul style="list-style-type: none"> <li>•  Sistemas operativos AIX</li> <li>•  Sistemas operativos Linux /home/tsminst1/tsminst1</li> <li>•  Sistemas operativos Windows C:\tsminst1</li> </ul> <p>Consejo: Si ha completado una hora de trabajo de planificación, la ubicación del directorio de instancia se registra en la hoja de trabajo.</p>	

<b>Tarea</b>	<b>Procedimientos básicos</b>	<b>Procedimientos avanzados y solución de problemas</b>
<p>Identifique la actividad de cliente inesperada.</p>	<p>Para supervisar la actividad de cliente para determinar si los volúmenes de datos superan la cantidad esperada, complete los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Clientes.</li> <li>2. Para ver la actividad durante las dos últimas semanas, efectúe una doble pulsación en cualquier cliente.</li> <li>3. Para ver el número de bytes enviados al cliente, pulse la pestaña Propiedades.</li> <li>4. En el área Última sesión, visualice la fila Enviado a cliente.</li> </ol>	<p>Cuando efectúe doble pulsación en un cliente en la tabla Clientes, el área Actividad durante dos semanas muestra la cantidad de datos que el cliente ha enviado al servidor cada día.</p>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Supervise el crecimiento de la agrupación de almacenamiento a lo largo del tiempo.</p>	<ol style="list-style-type: none"> <li>1. En la página Centro de operaciones Descripción general, pulse el área Agrupaciones.</li> <li>2. Para ver la capacidad utilizada durante las dos últimas semanas, seleccione una agrupación y pulse Detalles.</li> </ol>	<p>Sugerencias:</p> <ul style="list-style-type: none"> <li>• Para especificar el periodo de tiempo que debe transcurrir antes de que se eliminen todas las extensiones deduplicadas de una agrupación de almacenamiento de contenedores de directorios o de la agrupación de almacenamiento del contenedor de nube, después de que el inventario haya dejado de hacer referencia a las mismas, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> <li>3. Especifique la duración en el campo <code>Período de retardo para la reutilización del contenedor</code>.</li> </ol> </li> <li>• Para determinar el rendimiento de deduplicación de datos para las agrupaciones de almacenamiento del contenedor de la nube y del contenedor del directorio, utilice el mandato <code>GENERATE DEDUPSTATS</code>.</li> <li>• Para ver las estadísticas de deduplicación de datos para una agrupación de almacenamiento, siga estos pasos: <ol style="list-style-type: none"> <li>1. En la página Agrupaciones de almacenamiento del Centro de operaciones, seleccione la agrupación de almacenamiento.</li> <li>2. Pulse Detalles &gt; Propiedades.</li> </ol> </li> </ul> <p>De forma alternativa, utilice el mandato <code>QUERY EXTENTUPDATES</code> para visualizar información sobre las actualizaciones en las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio o contenedores en la nube. La salida del mandato puede ayudarle a determinar qué extensiones de datos ya no están referenciadas y cuáles son elegibles para suprimirse del sistema. En la salida, supervise el número de extensiones de datos elegibles para suprimirse del sistema. Esta métrica tiene una correlación directa con la cantidad de espacio libre que estará disponible dentro de la agrupación de almacenamiento de contenedores.</p> <ul style="list-style-type: none"> <li>• Para mostrar la cantidad de espacio físico ocupado por un espacio de archivos tras la eliminación del ahorro de deduplicación de datos, utilice el mandato <code>select * from occupancy</code>. La salida del mandato incluye el valor <code>LOGICAL_MB</code>. <code>LOGICAL_MB</code> es la cantidad de espacio utilizado por el espacio de archivos.</li> </ul>

Tarea	Procedimientos básicos	Procedimientos avanzados y solución de problemas
<p>Evalúe la temporización de las planificaciones de cliente. Asegúrese de que las horas de inicio y finalización de las planificaciones de cliente cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Clientes &gt; Planificaciones.</p> <p>En la tabla Planificaciones, la columna Inicio muestra la hora de inicio configurada para la operación planificada. Para ver cuándo se ha iniciado la operación más reciente, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Puede recibir un mensaje de aviso si una operación de cliente ejecutan más tiempo de lo esperado. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón por encima de Clientes y pulse Planificaciones.</li> <li>2. Seleccione una planificación y pulse Detalles.</li> <li>3. Vea los detalles de una planificación pulsando la flecha azul al lado de la fila.</li> <li>4. En el campo Ejecutar alerta de hora, especifique la hora a la que se emitirá un mensaje de aviso si la operación planificada no se ha completado.</li> <li>5. Pulse Guardar.</li> </ol>
<p>Evalúe la temporización de las tareas de mantenimiento. Asegúrese de que las horas de inicio y finalización de las tareas de mantenimiento cumplen las necesidades de negocio.</p>	<p>En la página Centro de operaciones Descripción general, pulse Servidores &gt; Mantenimiento.</p> <p>En la tabla Mantenimiento, revise la información en la columna Hora de la última ejecución. Para ver cuándo se ha iniciado la última tarea de mantenimiento, pase el ratón por encima del icono de reloj.</p>	<p>Consejo: Si una tarea de mantenimiento está en ejecución demasiado tiempo, cambie la hora de inicio o el tiempo de ejecución máximo. Realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. En la página Descripción general de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Creador de mandatos.</li> <li>2. Para cambiar la hora de inicio o el tiempo de ejecución máximo de una tarea, emita el mandato UPDATE SCHEDULE. Para obtener instrucciones, consulte UPDATE SCHEDULE (Actualizar una planificación de cliente).</li> </ol>

**Referencia relacionada:**

QUERY ACTLOG (Consultar las anotaciones de actividades)

➔ UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

➔ QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)

## Verificación de la conformidad de licencia

Verifique que la solución de IBM Spectrum Protect cumple las condiciones del acuerdo de licencia. Si comprueba el cumplimiento de forma periódica, podrá realizar un seguimiento de las tendencias del crecimiento de los datos o el uso de la unidad de valor de procesador (PVU). Utilice esta información para planificar una compra de licencia futura.

### Acerca de esta tarea

El método que utilice para verificar que la solución cumple con los términos de la licencia variará según las disposiciones de su acuerdo de licencia de IBM Spectrum Protect.

**Licencia de capacidad frontal**

El modelo frontal determina los requisitos de licencia basados en la cantidad de datos primarios de los que se informa que los clientes están haciendo copia de seguridad. Los clientes incluyen aplicaciones, máquinas virtuales y sistemas.

**Licencia de capacidad de programa de fondo**

El modelo de programa de fondo determina los requisitos de sistema basados en los terabytes de datos almacenados en agrupaciones de almacenamiento primarias y repositorios.

Sugerencias:

- Para garantizar la precisión de las estimaciones de capacidad frontal y de programa de fondo, instale la versión más reciente del software de cliente en cada nodo de cliente.
- La información sobre la capacidad frontal y de fondo en el Centro de operaciones es para fines de planificación y estimación.

**Licencia de PVU**

El modelo de PVU se basa en el uso de PVU por parte de los dispositivos de servidor.





Importante: Los cálculos de PVU que proporciona IBM Spectrum Protect se consideran estimaciones y no son jurídicamente vinculantes. La información de licencias de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

Para obtener la información más reciente sobre los modelos de licencia, consulte la información sobre detalles de producto y licencias en el sitio web de la familia de productos de IBM Spectrum Protect. Si tiene preguntas o dudas sobre los requisitos de licencia, póngase en contacto con el proveedor de software de IBM Spectrum Protect.

## Procedimiento

Para supervisar la conformidad de licencia, complete los pasos que corresponden a las provisiones del acuerdo de licencia. Consejo: El Centro de operaciones proporciona un informe de correo electrónico que resume el uso de capacidad frontal y de fondo. Pueden enviarse informes automáticamente a uno o más destinatarios regularmente. Para configurar y gestionar informes de correo electrónico, pulse Informes en la barra de menús del Centro de operaciones.

Opción	Descripción
<b>Modelo frontal</b>	<p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Licencias.</p> <p>La estimación de capacidad frontal se visualiza en la página Uso frontal.</p> <p>b. Si se visualiza un valor en la columna Sin informes, pulse el número para identificar clientes que no han informado del uso de capacidad.</p> <p>c. Para calcular la capacidad para clientes que no han informado del uso de capacidad, vaya al siguiente sitio FTP, que proporciona instrucciones y herramientas de medidas:</p> <p><code>ftp://public.dhe.ibm.com/storage/tivoli-storage-management/front_end_capacity_measurement_tools</code></p> <p>Para medir la capacidad frontal mediante un script, siga las instrucciones de la guía de licencias más reciente disponible.</p> <p>d. Añada la estimación de Centro de operaciones y las estimaciones obtenidas utilizando un script.</p> <p>e. Verifique que la capacidad estimada cumple con el acuerdo de licencia.</p>
<b>Modelo suplementario</b>	<p>Restricción: Si los servidores de réplica de origen y destino no utilizan la misma configuración de política, no podrá utilizar el Centro de operaciones para supervisar el uso de la capacidad de programa de fondo para los clientes replicados. Para obtener información sobre cómo estimar el uso de capacidad para estos clientes, consulte nota técnica 1656476.</p> <p>a. En la barra de menús de Centro de operaciones, pase el ratón sobre el icono de valores  y pulse Licencias.</p> <p>b. Pulse la pestaña Suplementario.</p> <p>c. Verifique que la cantidad de datos estimada cumple con el acuerdo de licencia.</p>
<b>Modelo de PVU</b>	<p>Para obtener información sobre cómo evaluar el cumplimiento con los términos de la licencia de PVU, consulte Evaluación de conformidad con el modelo de licencias de PVU.</p>

- Evaluación de conformidad con el modelo de licencias de PVU  
Si ha adquirido IBM Spectrum Protect según el modelo de licencias de unidades de valor de procesador, asegúrese que su solución cumple con los términos de licencia. Revise las estimaciones de PVU periódicamente para planificar futuras compras de licencia. Por ejemplo, si las estimaciones de PVU aumentan o tiene previsto instalar más servidores, puede adquirir más licencias.

## Seguimiento del estado del sistema mediante informes de correo electrónico

Configure el Centro de operaciones para generar informes de correo electrónico que resuman el estado del sistema. Puede configurar una conexión con el servidor de correo, cambiar valores de informe y, opcionalmente, crear informes SQL personalizados.

### Antes de empezar

Antes de configurar los informes de correo electrónico, asegúrese de que se cumplen los siguientes requisitos:

- Un servidor de host del protocolo simple de transferencia de correo (SMTP) está disponible para enviar y recibir informes por correo electrónico. El servidor SMTP debe configurarse como un relé de correo abierto. También debe asegurarse de que el servidor IBM Spectrum Protect que envía mensajes de correo electrónico tiene acceso al servidor SMTP. Si el Centro de operaciones está instalado en un sistema independiente, el sistema no requiere acceso al servidor SMTP.
- Para configurar los informes de correo electrónico, debe tener privilegios del sistema para el servidor.
- Para especificar los destinatarios, puede entrar una o más direcciones de correo electrónico o ID de administrador. Si planea entrar un ID de administrador, el ID debe estar registrado en el servidor concentrador y debe tener una dirección de correo electrónico asociada con él. Para especificar una dirección de correo electrónico para un administrador, utilice el parámetro EMAILADDRESS del mandato UPDATE ADMIN.

## Acerca de esta tarea

Puede configurar el Centro de operaciones para enviar un informe de operaciones general, un informe de verificación de licencia y uno o más informes personalizados, todos los cuales utilizarán sentencia SELECT SQL para consultar servidores gestionados.

## Procedimiento

Para configurar y gestionar los informes de correo electrónico, complete los pasos siguientes:

1. En la barra de menús del Centro de operaciones, pulse Informes.
2. Si aún no se ha configurado ninguna conexión con el servidor de correo electrónico, pulse Configurar servidor de correo y complete los campos. Después de configurar el servidor de correo, se habilitan el informe de operaciones general y el informe de verificación de licencia.
3. Para cambiar los valores de un informe, seleccione dicho informe, pulse Detalles y actualice el formulario.
4. Opcional: Para añadir un informe SQL personalizado, pulse + Informe y complete los campos.  
Consejo: Para ejecutar un informe y enviarlo de inmediato, seleccione el informe y pulse Enviar.

## Resultados

Los informes habilitados se envían según los valores especificados.

### Referencia relacionada:

[UPDATE ADMIN \(Actualizar un administrador\)](#)

### Información relacionada:

[Ejemplos de informes personalizados](#)

## Selección, configuración y uso de herramientas de supervisión

Utilice el Centro de operaciones para obtener una visión general del estado del sistema y para profundizar para obtener información más detallada. En algunos casos, es posible que desee utilizar herramientas avanzadas para recopilar información de supervisión específica.





## Procedimiento

Seleccione y configure las herramientas de supervisión que son adecuadas para la solución.

Tabla 1. Herramientas de supervisión

Tipo de herramienta	Casos de uso	Enlaces a más información
---------------------	--------------	---------------------------

Tipo de herramienta	Casos de uso	Enlaces a más información
Centro de operaciones	<ul style="list-style-type: none"> <li>• Utilice la interfaz gráfica de usuario para revisar el estado del sistema y diagnosticar problemas.</li> <li>• Configure el Centro de operaciones para enviar informes de resumen de correo electrónico diarios.</li> <li>• Opcional: Personalice las alertas que se visualizan en Centro de operaciones y configure las notificaciones por correo electrónico sobre las alertas.</li> <li>• Opcional: Supervise el entorno de almacenamiento de forma remota visualizando la página Visión general en el navegador web de un dispositivo móvil. Por ejemplo, puede utilizar el navegador web Safari de Apple en el dispositivo iPad de Apple. También se pueden utilizar otros dispositivos móviles.</li> </ul> <p>Consejo: Si instala servicios de gestión de cliente de IBM Spectrum Protect en un cliente de archivado y copia de seguridad, puede utilizar Centro de operaciones para obtener información sobre resolución de problemas para el cliente de archivado y copia de seguridad. El servicio de gestión de cliente se puede instalar únicamente en sistemas operativos Linux o Windows.</p>	
Mandatos administrativos de IBM Spectrum Protect	<p>Revise la información detallada. Utilice el método adecuado para la solución:</p> <ul style="list-style-type: none"> <li>• Para visualizar los mensajes generados por el servidor y el cliente, utilice el mandato QUERY ACTLOG. Consejo: Puede ejecutar mandatos administrativos desde el creador de mandatos Centro de operaciones.</li> <li>• Para supervisar actividades como la migración de servidor y los inicios de sesión de cliente, utilice el cliente administrativo en la modalidad de consola. Ejecute el mandato dsmadmc - consolemode.</li> </ul>	<ul style="list-style-type: none"> <li>• mandatos de administración.</li> <li>• QUERY ACTLOG (Consultar las anotaciones de actividades)</li> <li>• Supervisión de actividades del servidor desde el cliente de administración</li> <li>• Opciones de cliente de administración</li> </ul>

Tipo de herramienta	Casos de uso	Enlaces a más información
Registro de sucesos	Registre los mensajes de servidor y la mayoría de los mensajes de cliente como sucesos para uno o más repositorios denominados receptores.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Para obtener instrucciones sobre el uso del registro de sucesos para supervisar una solución, consulte Registro de sucesos de IBM Spectrum Protect en receptores (V7.1.1).   Sistemas operativos Linux Para obtener instrucciones sobre el registro de sucesos en un registro del sistema de Linux, consulte Registro de sucesos en el registro del sistema Linux (V7.1.4).
Consultas SQL	<p>Cree y dé formato a consultas personalizadas de la base de datos del servidor.</p> <p>Por ejemplo, puede consultar la tabla de resumen de actividad SQL para ver estadísticas sobre operaciones de cliente y procesos de servidor. Para visualizar toda la información en la tabla resumen, emita el siguiente mandato desde el cliente administrativo:</p> <pre>select * from summary</pre>	Utilización de mandatos SELECT (V7.1.1)
Herramientas del sistema operativo	Supervise y pruebe el rendimiento del sistema.	
Herramientas de supervisión de dispositivos	Supervise los dispositivos para disponibilidad, capacidad y rendimiento. Por ejemplo, utilice IBM Spectrum Control o las herramientas que se incluyen en los paquetes de hardware de dispositivo.	<p>Para supervisar el estado general de dispositivo utilizando IBM Spectrum Control, siga las instrucciones de Supervisión del estado y la condición de los recursos.</p> <p>Para supervisar el rendimiento utilizando IBM Spectrum Control, siga las instrucciones de Supervisión del rendimiento de los recursos.</p>
IBM® Tivoli Monitoring para Tivoli Storage Manager	<p>Supervise los servidores de IBM Spectrum Protect y produzca informes históricos sobre las actividades de cliente y servidor.</p> <p>Consejo: El Centro de operaciones es la herramienta preferida para la supervisión. Sin embargo, Tivoli Monitoring para Tivoli Storage Manager es útil para generar informes históricos que estén basados en tecnología de IBM Cognos Business Intelligence.</p>	Tivoli Monitoring para Tivoli Storage Manager

## Gestión de operaciones

Gestionando con eficacia las operaciones de cliente y servidor, puede optimizar el rendimiento de su entorno de almacenamiento. Para empezar, supervise el entorno mediante el Centro de operaciones. A continuación, tome medidas para evitar problemas potenciales y aumentar el rendimiento.

### Acerca de esta tarea

- Gestión de operaciones del servidor  
Puede iniciar y detener el servidor, gestionar la capacidad de inventario y gestionar el uso de memoria y procesador. También puede optimizar la transferencia de datos entre servidores, actualizar el servidor y ajustar las actividades planificadas.
- Gestión de operaciones de cliente  
Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones,

que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

- **Gestión del Centro de operaciones**

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect.

Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

## Gestión de operaciones del servidor

---

Puede iniciar y detener el servidor, gestionar la capacidad de inventario y gestionar el uso de memoria y procesador. También puede optimizar la transferencia de datos entre servidores, actualizar el servidor y ajustar las actividades planificadas.

- **Detención e inicio del servidor**

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

- **Gestión de la capacidad de inventario**

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

- **Gestión del uso de la memoria y del procesador**

Asegúrese de que gestiona los requisitos de memoria y el uso de procesador para garantizar que el servidor pueda completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

- **Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema**

Si el servidor IBM Spectrum Protect replica nodos o protege agrupaciones de almacenamiento en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Antes de habilitar la tecnología Aspera FASP, debe obtener las licencias adecuadas. Dispone de licencias tanto de evaluación como completa.

- **Planificación de la actualización del servidor**

Cuando esté disponible un fixpack o arreglo temporal, puede actualizar el servidor de IBM Spectrum Protect para beneficiarse de las mejoras del producto. Los clientes y servidores se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

- **Ajuste de actividades planificadas**

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Mediante el ajuste de la solución, maximice los recursos del servidor y utilice de forma efectiva diferentes funciones disponibles dentro de la solución.

## Detención e inicio del servidor

---

Antes de completar las tareas de mantenimiento o reconfiguración, detenga el servidor. A continuación, inicie el servidor en modalidad de mantenimiento. Cuando haya terminado con las tareas de mantenimiento o reconfiguración, reinicie el servidor en modo de producción.

### Antes de empezar

---

Debe tener privilegio de sistema o de operador para detener e iniciar el servidor de IBM Spectrum Protect.

- **Detención del servidor**

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

- **Inicio del servidor para tareas de mantenimiento o reconfiguración**

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento.

Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

## Detención del servidor

---

Antes de detener el servidor, prepare el sistema asegurándose de que todas las operaciones de copia de seguridad de base de datos se han completado y que los demás procesos y sesiones han finalizado. De esta forma, puede concluir el servidor de forma segura y garantizar que los datos están protegidos.

### Acerca de esta tarea

---

Cuando emite el mandato HALT para detener el servidor, se produce lo siguiente:

- Todos los procesos y sesiones de nodo cliente se cancelan.
- Todas las transacciones actuales se detienen. (Las transacciones se retrotraerán cuando el servidor se reinicia.)

## Procedimiento

---

Para preparar el sistema y detener el servidor, complete los pasos siguientes:

1. Impida que se inicien nuevas sesiones de nodo cliente emitiendo el mandato DISABLE SESSIONS:

```
disable sessions all
```

2. Determine si hay sesiones de nodo de cliente o procesos en curso realizando los pasos siguientes:

- a. En la página Visión general de Centro de operaciones, en el área Actividades, consulte el número total de procesos y sesiones que están activos actualmente. Si el número es muy diferente al número habitual de usuarios que se muestra durante la rutina diaria de gestión del almacenamiento, observe otros indicadores de estado en el Centro de operaciones para comprobar si existe un problema.

- b. Visualice el gráfico en el área Actividad para comparar la cantidad de tráfico de red durante los periodos siguientes:

- El periodo actual, es decir, el periodo más reciente de 24 horas
- El periodo anterior, es decir, 24 horas antes del periodo actual

Si el gráfico del periodo anterior representa la cantidad de tráfico prevista, es posible que las diferencias del gráfico del periodo actual indiquen la existencia de un problema.

- c. En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles. Si el servidor no está registrado como un servidor concentrador o como un servidor spoke en el Centro de operaciones, obtenga información acerca de los procesos utilizando los mandatos administrativos. Emita el mandato QUERY PROCESS para consultar los procesos y obtenga información acerca de las sesiones mediante el mandato QUERY SESSION.

3. Espere a que se completen las sesiones de nodo cliente o cancele las sesiones. Para cancelar los procesos y las sesiones, realice los pasos siguientes:

- En la página Servidores, seleccione un servidor para el que desee ver los procesos y las sesiones y pulse Detalles.
- Pulse el separador Tareas activas y seleccione uno o más procesos, sesiones o una combinación de ambos que desee cancelar.
- Pulse Cancelar.
- Si el servidor no está registrado como un servidor concentrador o como un servidor spoke en el Centro de operaciones, cancele las sesiones utilizando los mandatos administrativos. Emita el mandato CANCEL SESSION para cancelar una sesión y cancele los procesos mediante el mandato CANCEL PROCESS.  
Consejo: Si un proceso que desea cancelar está esperando a que se monte un volumen de cinta, la solicitud de montaje se cancela. Por ejemplo, si emite un mandato EXPORT, IMPORT o MOVE DATA, el mandato puede iniciar un proceso que requiere que el volumen de cinta se monte. Sin embargo, si una biblioteca automatizada está montando un volumen de cinta, la operación de cancelación es posible que no entre en vigor hasta que se complete el proceso de montaje. Dependiendo del entorno del sistema, esto puede tardar varios minutos.

4. Detenga el servidor emitiendo el mandato HALT:

```
halt
```

## Inicio del servidor para tareas de mantenimiento o reconfiguración

---

Antes de comenzar con las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento. Cuando inicia el servidor en modalidad de mantenimiento, inhabilita operaciones que pueden afectar a las tareas de mantenimiento o reconfiguración.

### Acerca de esta tarea

---

Inicie el servidor en modalidad de mantenimiento ejecutando el programa de utilidad DSMSERV con el parámetro MAINTENANCE.

Las siguientes operaciones están inhabilitadas en la modalidad de mantenimiento:

- Planificaciones de mandatos de administración
- Planificaciones de cliente
- Reclamación del espacio de almacenamiento en el servidor
- Caducidad de inventario
- Migración de agrupaciones de almacenamiento

Además, se impide a los clientes iniciar sesiones con el servidor.

Sugerencias:

- No tiene que editar el archivo de opciones de servidor, `dsmserv.opt`, para iniciar el servidor en modalidad de mantenimiento.
- Cuando el servidor se ejecuta en modalidad de mantenimiento, puede iniciar manualmente la reclamación de espacio de almacenamiento, la caducidad de inventario y los procesos de migración de la agrupación de almacenamiento.

## Procedimiento

---

Para iniciar el servidor en modalidad de mantenimiento, emita el siguiente mandato:

```
dsmserv maintenance
```

Consejo: Para ver un vídeo acerca de cómo iniciar el servidor en modalidad de mantenimiento, vea Inicio de un servidor en modalidad de mantenimiento.




## Qué hacer a continuación

---

Para reanudar las operaciones en modo de producción, complete los pasos siguientes:

1. Concluya el servidor emitiendo el mandato `HALT`:

```
halt
```

2. Inicie el servidor utilizando el método que utiliza en el modo de producción. Siga las instrucciones para el sistema operativo:
  -  Sistemas operativos AIX Inicio de la instancia de servidor
  -  Sistemas operativos Linux Inicio de la instancia de servidor
  -  Sistemas operativos Windows Inicio de la instancia de servidor

Las operaciones que se han inhabilitado durante la modalidad de mantenimiento se vuelven a habilitar.

## Gestión de la capacidad de inventario

---

Gestione la capacidad de la base de datos, del registro activo y de los registros de archivado para asegurarse de que el inventario se dimensiona para las tareas, basándose en el estado de los registros.

## Antes de empezar

---

Los registros activos y de archivado tienen las siguientes características:

- El registro activo puede tener un tamaño máximo de 512 GB. Para obtener más información sobre el dimensionamiento del registro activo para su sistema, consulte Planificación de matrices de almacenamiento.
- El tamaño del registro de archivado está limitado al tamaño del sistema de archivos en el que está instalado. El tamaño del registro de archivado no se mantiene a un tamaño predefinido como el registro activo. Los archivos de registro de archivado se suprimen automáticamente cuando ya no son necesarios.

Como práctica recomendada, puede crear opcionalmente un registro de migración tras error de archivado para almacenar archivos de registro de archivado cuando el directorio de registro de archivado está lleno.

Compruebe Centro de operaciones para determinar el componente del inventario que está lleno. Asegúrese de que detiene el servidor antes de aumentar el tamaño de uno de los componentes de inventario.

## Procedimiento

---

- Para aumentar el tamaño de la base de datos, complete los pasos siguientes:
  - Cree uno o más directorios para la base de datos en unidades o sistemas de archivos individuales.
  - Emita el mandato `EXTEND DBSPACE` para agregar uno o varios directorios a la base de datos. Los directorios deben ser accesibles para el ID de usuario de instancia del gestor de bases de datos. De forma predeterminada, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama el espacio.  
Sugerencias:
    - El tiempo necesario para completar la redistribución de datos y reclamar el espacio es variable, dependiendo del tamaño de la base de datos. Asegúrese de que lo ha planeado adecuadamente.
    - Asegúrese de que los directorios que especifique tienen el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.
  - Detenga y reinicie el servidor para utilizar completamente los nuevos directorios.
  - Reorganice la base de datos si es necesario. La reorganización de los índices y de las tablas de la base de datos del servidor puede contribuir a impedir que la base de datos aumente de forma inesperada o problemas de rendimiento. Para obtener

más información sobre cómo reorganizar la base de datos, consulte nota técnica 1683633.

- Para disminuir el tamaño de la base de datos para servidores V7.1 y posterior, emita los siguientes mandatos de DB2 desde el directorio de instancias de servidor:

Restricción: Los mandatos pueden aumentar la actividad de E/S, y puede afectar al rendimiento del servidor. Para minimizar los problemas de rendimiento, espere hasta que se complete un mandato antes de emitir el siguiente. Los mandatos DB2 se pueden emitir cuando el servidor está en ejecución.

```
db2 connect to tsmdb1
db2 set schema tsmdb1
db2 ALTER TABLESPACE USERSPACE1 REDUCE MAX
db2 ALTER TABLESPACE IDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGEIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE LARGESPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE REPLIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE ARCHOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BACKOBJIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFABFIDXSPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTDATASPACE REDUCE MAX
db2 ALTER TABLESPACE BFBFEXTIDSPACE REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE1 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE2 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE3 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE4 REDUCE MAX
db2 ALTER TABLESPACE DEDUPTBLSPACE5 REDUCE MAX
db2 ALTER TABLESPACE DEDUPIIDXSPACE5 REDUCE MAX
```

- Para aumentar o disminuir el tamaño del registro activo, complete los pasos siguientes:
  1. Asegúrese de que la ubicación de las anotaciones activas tenga espacio suficiente para el tamaño de anotaciones mayor. Si existe una duplicación de anotaciones, su ubicación también debe tener espacio suficiente para el tamaño de anotaciones mayor.
  2. Detenga el servidor.
  3. En el archivo dsmserv.opt, actualice la opción ACTIVELOGSIZE para el nuevo tamaño del registro activo, en megabytes. El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. En la tabla siguiente se muestran las directrices de los requisitos de espacio:

Tabla 1. Cómo calcular el volumen y los requisitos de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio de ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

Para cambiar el registro activo a su tamaño máximo de 512 GB, entre la siguiente opción de servidor:

```
activelogsize 524288
```

4. Si piensa utilizar un nuevo directorio de registro activo, actualice el nombre de directorio especificado en la opción de servidor ACTIVELOGDIRECTORY. El nuevo directorio debe estar vacío y debe ser accesible para el ID de usuario del gestor de base de datos.
  5. Reinicie el servidor.
- Comprima los registros de archivado para reducir la cantidad de espacio necesaria para el almacenamiento. Habilite la compresión dinámica del registro de archivado emitiendo el mandato siguiente:

```
setopt archlogcompress yes
```

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio disponible en el sistema de archivos de registro activos después de habilitar la compresión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de



espacio, se debe inhabilitar la opción del servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

**Referencia relacionada:**

- ➡ ACTIVELOGSIZE, opción de servidor
- ➡ EXTEND DBSPACE (Incrementar el espacio para la base de datos)
- ➡ SETOPT (Establecer una opción de servidor para actualización dinámica)

## Gestión del uso de la memoria y del procesador

---

Asegúrese de que gestiona los requisitos de memoria y el uso de procesador para garantizar que el servidor pueda completar procesos de datos como, por ejemplo, la copia de datos y la deduplicación de datos. Tenga en cuenta el impacto sobre el rendimiento cuando complete determinados procesos.

### Antes de empezar


---

- Asegúrese de que la configuración utiliza el hardware y el software necesarios. Para obtener más información, consulte Sistemas operativos soportados de IBM Spectrum Protect.
- Para obtener más información acerca de la gestión de recursos como la base de datos y registro de recuperación, consulte Planificación de matrices de almacenamiento.
- Añada más memoria del sistema para determinar si hay una mejora de rendimiento. Supervise con regularidad el uso de la memoria para determinar si se necesita más.

### Procedimiento

---

1. Libere memoria de la memoria caché de sistema de archivo donde sea posible.
2. Para gestionar la memoria del sistema utilizada para cada servidor en un sistema, utilice la opción de servidor DBMEMPERCENT. Limite el porcentaje de memoria del sistema que puede utilizar el gestor de bases de datos de cada servidor. Si todos los servidores tienen igual importancia, utilice el mismo valor para cada servidor. Si un servidor es de producción y hay otros de prueba, establezca para el servidor de producción un valor más alto que para los de prueba.
3. Establezca el límite de datos de usuario y la memoria privada para la base de datos para asegurarse de que la memoria privada no se ha agotado. Agotar la memoria privada puede provocar errores e inestabilidad, en lugar de un rendimiento óptimo.

 Sistemas operativos Linux

## Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema

---

Si el servidor IBM Spectrum Protect replica nodos o protege agrupaciones de almacenamiento en un servidor remoto, determine si la tecnología Aspera Fast Adaptive Secure Protocol (FASP) puede mejorar el rendimiento de los datos en el servidor remoto. Antes de habilitar la tecnología Aspera FASP, debe obtener las licencias adecuadas. Dispone de licencias tanto de evaluación como completa.

### Antes de empezar

---

La tecnología Aspera FASP se utiliza para transferir extensiones de datos desde una agrupación de almacenamiento de contenedores a un servidor remoto. Cuando la tecnología Aspera FASP está habilitada, las extensiones de datos se cifran siempre durante la transferencia, independientemente de si el protocolo de Capa de sockets seguros (SSL) está o no habilitado. Sin embargo, si desea proteger la conexión de red, habilite SSL. Para obtener información sobre SSL y cómo habilitarlo, consulte el apartado Comunicación de la Capa de sockets seguros y de la Seguridad de la capa de transporte.

### Acerca de esta tarea

---

Restricciones:

- Utilice la tecnología Aspera FASP cuando la red de área amplia (WAN) muestre signos de alto nivel de pérdida de paquetes, retrasos en la transferencia de datos debidos a problemas en la red o ambos. Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Para habilitar la tecnología de Aspera FASP para las operaciones de réplica de nodos, los datos deben almacenarse en una agrupación de almacenamiento de contenedores de directorios.

### Procedimiento

---

1. Determine si la tecnología Aspera FASP resulta adecuada para el entorno del sistema. Si se produce alguna de las siguientes condiciones, habilite la tecnología Aspera FASP:

- o La media de retrasos en operaciones de transferencia de datos supera los 50 milisegundos.
- o La pérdida de paquetes es superior al 0,01 %.

Las características de red pueden variar ampliamente. Es posible que pueda mejorar el rendimiento de la red mediante la habilitación de la tecnología Aspera FASP, incluso si el retraso en la transferencia de datos es de menos de 50 milisegundos y la pérdida de paquetes es inferior al 0,01 %.

2. Obtenga e instale las licencias adecuadas. Realice una de las siguientes acciones:

Obtenga e instale licencias de evaluación

Para obtener e instalar las licencias de evaluación, que caducan en 30 días, siga estos pasos:

- a. Para solicitar las licencias, envíe un correo electrónico a [alliances@asperasoft.com](mailto:alliances@asperasoft.com):

- Incluya el nombre de su empresa, dirección, número de teléfono y la dirección de correo electrónico del contacto principal de su empresa.
- Indique que desea una licencia de evaluación de 30 días.
- Indique el número de licencias que necesita.

Se necesita una licencia para cada servidor que se utiliza para la transferencia de datos con la tecnología Aspera FASP. Por ejemplo, si va a replicar un nodo de un servidor de origen en un servidor de destino, necesita dos licencias.

Si la solicitud de licencia se aprueba, el contacto principal recibirá un correo electrónico en un plazo de 24 horas. El correo electrónico tendrá archivos adjuntos de licencia que siguen el siguiente convenio de denominación:

xxxxx-ConnectSrv-unlim.eval.aspera-license

donde xxxxx es un número exclusivo.

- b. Copie uno de los archivos de licencia en el directorio bin del servidor de origen. Seleccione un archivo de licencia. De forma predeterminada, el directorio se encuentra en la siguiente ubicación:

```
/opt/tivoli/tsm/server/bin
```

- c. Copie el otro archivo de licencia en el directorio bin del servidor de destino.

- d. En los servidores de origen y de destino, establezca el nivel de permiso de cada archivo de licencia en 755. Por ejemplo, si utiliza el directorio de instalación predeterminado y el número de licencia exclusivo es 47474, emita el siguiente mandato en una sola línea:

```
chmod 755 /opt/tivoli/tsm/server/bin/  
47474-ConnectSrv-unlim.eval.aspera-license
```

Obtenga e instale licencias completas

Para obtener e instalar las licencias completas e ilimitadas, que no caducan, siga estos pasos:

- a. Adquiera el producto Transferencia de datos de datos de velocidad de IBM Spectrum Protect. El número de identificación del producto es 5725-Z10. Puede obtener el producto desde Passport Advantage.

Se necesita una instancia de Transferencia de datos de datos de velocidad de IBM Spectrum Protect para cada servidor que se utilice para transferir los datos con la tecnología Aspera FASP. Por ejemplo, si va a replicar un nodo de un servidor de origen en un servidor de destino, necesita dos licencias de Transferencia de datos de datos de velocidad de IBM Spectrum Protect.

- b. Instale Transferencia de datos de datos de velocidad de IBM Spectrum Protect en cada servidor utilizando el asistente de instalación.

Restricción: Si faltan licencias necesarias o han caducado, las operaciones para replicar nodos y proteger las agrupaciones de almacenamiento mediante la tecnología Aspera FASP fallarán.

3. Opcional: Valide la configuración de Aspera FASP emitiendo el mandato VALIDATE ASPERA. Puede utilizar el mandato VALIDATE ASPERA para verificar que el entorno del sistema se haya configurado correctamente para Aspera FASP y para verificar que se hayan instalado licencias válidas. Además, puede utilizar el mandato para comparar la velocidad de la productividad de la red con Aspera FASP y la tecnología de TCP/IP.

## Qué hacer a continuación

Para habilitar la tecnología Aspera FASP, siga los pasos del apartado Optimización de la transferencia de datos mediante la habilitación de la tecnología Aspera FASP.

- Optimización de la transferencia de datos mediante la habilitación de la tecnología Aspera FASP  
Si utiliza un servidor remoto para la protección de la agrupación de almacenamiento o la réplica de nodos y tiene problemas de red, es posible que desee optimizar la transferencia de datos mediante la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

## Planificación de la actualización del servidor

---

Cuando esté disponible un fixpack o arreglo temporal, puede actualizar el servidor de IBM Spectrum Protect para beneficiarse de las mejoras del producto. Los clientes y servidores se pueden actualizar en momentos diferentes. Asegúrese de que ha completado los pasos de planificación antes de actualizar el servidor.

### Acerca de esta tarea

---

Siga estas directrices:

- El método recomendado consiste en actualizar el servidor utilizando el asistente de instalación. Después de iniciar el asistente, en la ventana IBM Installation Manager, pulse el icono Actualizar; no pulse el icono Instalar o Modificar.
- Si hay actualizaciones disponibles para el componente del servidor y el componente de Centro de operaciones, seleccione las casillas de verificación para actualizar ambos componentes.

### Procedimiento




---

1. Revise la lista de fixpacks y arreglos temporales. Consulte el apartado nota técnica 1239415.
2. Revise las mejoras de producto, que se describen en los archivos léame.  
Consejo: Cuando obtiene el paquete de instalación de Sitio de soporte de IBM Spectrum Protect, también puede acceder al archivo léame.
3. Asegúrese de que la versión a la que actualiza el servidor es compatible con otros componentes como, por ejemplo, clientes de biblioteca y agentes de almacenamiento. Consulte el apartado nota técnica 1302789.
4. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas. Consulte el apartado nota técnica 1053218.
5. Revise las instrucciones de actualización. Asegúrese de que hace copia de seguridad de la base de datos del servidor, la información de configuración del dispositivo y el archivo de historial de volumen.

### Qué hacer a continuación

---

Para instalar un fixpack o arreglo temporal, siga las instrucciones para su sistema operativo:

-  Sistemas operativos AIX Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Linux Instalación de un fixpack del servidor de IBM Spectrum Protect
-  Sistemas operativos Windows Instalación de un fixpack del servidor de IBM Spectrum Protect

## Ajuste de actividades planificadas

---

Planificar tareas de mantenimiento a diario para asegurarse de que su solución funciona correctamente. Mediante el ajuste de la solución, maximice los recursos del servidor y utilice de forma efectiva diferentes funciones disponibles dentro de la solución.

### Procedimiento

---

1. Supervise el rendimiento del sistema de forma periódica para asegurarse de que las tareas de copia de seguridad de cliente y de mantenimiento de servidor se completan satisfactoriamente. Siga las instrucciones de la sección Supervisión de soluciones de almacenamiento.
2. Opcional: Si la información de supervisión muestra que la carga de trabajo del servidor ha aumentado, revise la información de planificación. Revise si la capacidad del sistema es adecuada en los casos siguientes:
  - El número de clientes aumenta.
  - La cantidad de datos de los que se hace copia de seguridad aumenta.
  - La cantidad de tiempo necesaria disponible para realizar copias de seguridad cambia.
3. Determine si la solución está funcionando en el nivel esperado. Revise las planificaciones de cliente para comprobar si las tareas se completan en el intervalo de tiempo planificado:
  - a. En la página Clientes del Centro de operaciones, seleccione el cliente.
  - b. Pulse Detalles.
  - c. Desde la página de Resumen de cliente, revise la actividad de Copia de seguridad y Réplica para identificar los riesgos. Ajuste el tiempo y la frecuencia de las operaciones de copia de seguridad de cliente, si es necesario.

4. Planifique tiempo suficiente para que las siguientes tareas de mantenimiento se completen satisfactoriamente en un periodo de 24 horas:

- a. Proteger agrupaciones de almacenamiento.
- b. Replicar datos de nodo.
- c. Realizar una copia de seguridad de la base de datos.
- d. Ejecutar el proceso de caducidad para eliminar copias de seguridad de cliente y copias de archivo de archivado del almacenamiento de servidor.

Consejo: Planificar que las tareas de mantenimiento se inicien a una hora adecuada y en la secuencia correcta. Por ejemplo, planificar tareas de réplica después de que las copias de seguridad de cliente se completen satisfactoriamente.

- Traslado de clientes de un servidor a otro

Para que no se agote el espacio de un servidor o para resolver problemas de carga de trabajo, es posible que tenga que trasladar los nodos de cliente de un servidor a otro.

**Conceptos relacionados:**

➡ Rendimiento

**Tareas relacionadas:**

➡ Eliminación de datos duplicados (V7.1.1)

## Gestión de operaciones de cliente

---

Puede evaluar y resolver errores relacionados con un cliente de archivado y copia de seguridad utilizando Centro de operaciones, que proporciona sugerencias para resolver errores. Para errores en otros tipos de clientes, debe examinar los registros de errores en el cliente y revisar la documentación del producto.

### Acerca de esta tarea

---

En algunos casos, puede resolver errores de cliente deteniendo e iniciando el aceptador de cliente. Si se han bloqueado los nodos cliente o los ID de administrador, puede solucionar el problema desbloqueando el nodo cliente o el ID de administrador y restableciendo después la contraseña.

Para obtener instrucciones detalladas sobre la identificación y resolución de errores de cliente, consulte Resolución de problemas de cliente.

- **Modificación del ámbito de una copia de seguridad de cliente**  
Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.
- **Evaluación de errores en registros de errores de cliente**  
Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.
- **Detención y reinicio del aceptador de cliente**  
Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.
- **Restablecimiento de contraseñas**  
Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.
- **Poner fuera de servicio un nodo cliente**  
Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor IBM Spectrum Protect, pero ya no se utilizaba la estación de trabajo, puede dejar fuera de servicio la estación de trabajo.
- **Desactivación de datos para liberar espacio de almacenamiento**  
En algunos casos, puede desactivar datos que están almacenados en el servidor IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.
- **Gestión de actualizaciones del cliente**  
Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

## Modificación del ámbito de una copia de seguridad de cliente

---

Al configurar operaciones de copia de seguridad de cliente, se recomienda que excluya los objetos que no necesite. Por ejemplo, normalmente deseará excluir archivos temporales de una operación de copia de seguridad.

## Acerca de esta tarea

---

Al excluir objetos innecesarios de las operaciones de copia de seguridad, puede obtener mejor control de la cantidad de espacio de almacenamiento que se necesita para las operaciones de copia de seguridad y el coste de almacenamiento. En función de su paquete de licencia, también podrá reducir los costes de licencia.

## Procedimiento

---

Cómo modificar el ámbito de las operaciones de copia de seguridad depende del producto que está instalado en el nodo de cliente:

- Para un cliente de archivado y copia de seguridad, puede crear una lista de inclusión-exclusión para incluir o excluir un archivo, grupos de archivos o directorios de las operaciones de copia de seguridad. Para crear una lista de inclusión-exclusión, siga las instrucciones en Creación de una lista de inclusión-exclusión.

Para asegurar la coherencia de uso de una lista de inclusión/exclusión de todos los clientes de un tipo, puede crear un conjunto de opciones de cliente en el servidor que contiene las opciones necesarias. A continuación, asigne el conjunto de opciones de cliente a cada uno de los clientes del mismo tipo. Si desea obtener más información al respecto, consulte el apartado Control de las operaciones de cliente mediante conjuntos de opciones de cliente.

- Para un cliente de archivado y copia de seguridad, puede especificar los objetos que desea incluir en una operación de copia de seguridad incremental utilizando la opción dominio. Siga las instrucciones de Opción de cliente de dominio.
- Para otros productos, para definir qué objetos se incluyen y se excluyen en las operaciones de copia de seguridad, siga las instrucciones de la documentación del producto.

## Evaluación de errores en registros de errores de cliente

---

Puede solucionar errores de cliente obteniendo sugerencias de Centro de operaciones o revisando los registros de errores en el cliente.

## Antes de empezar

---

Para solucionar los errores de un cliente de archivado y copia de seguridad de un sistema operativo Linux o Windows, asegúrese de que servicio de gestión de cliente se haya instalado e iniciado. Para obtener instrucciones de instalación, consulte el apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes.

## Procedimiento

---

Para diagnosticar y resolver errores de cliente, realice una de las siguientes acciones:

- Si servicio de gestión de cliente se ha instalado en el nodo cliente, lleve a cabo los siguientes pasos:
  1. En la página Descripción general de Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Detalles.
  3. En la página Resumen de cliente, pulse la pestaña Diagnóstico.
  4. Revise los mensajes de registro recuperados.

Sugerencias:

    - Para mostrar u ocultar el panel Registros de clientes, efectúe una doble pulsación en la barra Registros de clientes.
    - Para cambiar el panel Registros de clientes, pulse y arrastre la barra Registros de clientes.

Si se muestran sugerencias en la página Diagnóstico, seleccione una sugerencia. En el panel Registros de clientes, los mensajes de registro de clientes con los que se relaciona la sugerencia se resaltan.

5. Utilice las sugerencias cuando resuelva los problemas indicados por los mensajes de error.

Consejo: Solo se proporcionan sugerencias para un subconjunto de mensajes de cliente.
- Si servicio de gestión de cliente no se ha instalado en el nodo cliente, revise los registros de errores del cliente instalado.

## Detención y reinicio del aceptador de cliente

---

Si cambia la configuración de la solución, debe reiniciar el aceptador de cliente en todos los nodos de cliente donde está instalado el cliente de archivado y copia de seguridad.

## Acerca de esta tarea

---

En algunos casos, puede resolver los problemas de planificación de cliente deteniendo y reiniciando el aceptador de cliente. El aceptador de cliente debe estar en ejecución para garantizar las operaciones planificadas se pueden llevar a cabo en el cliente. Por ejemplo, si cambia la dirección IP o el nombre de dominio del servidor, debe reiniciar el aceptador de cliente.

## Procedimiento

---

Siga las instrucciones del sistema operativo que esté instalado en el nodo cliente:

### AIX y Oracle Solaris

- Para detener el aceptador de cliente, siga los pasos siguientes:
  - a. Determine el ID de proceso para el aceptador de cliente emitiendo el mandato siguiente en la línea de mandatos:

```
ps -ef | grep dsmcad
```

Revise la salida. En la salida de ejemplo siguiente, 6764 es el ID de proceso para el aceptador de cliente:

```
root 6764 1 0 16:26:35 ? 0:00 /usr/bin/dsmcad
```

- b. Emita el siguiente mandato en la línea de mandatos:

```
kill -9 PID
```

donde *PID* especifica el ID de proceso para el aceptador de cliente.

- Para iniciar el aceptador de cliente, emita el mandato siguiente en la línea de mandatos:

```
/usr/bin/dsmcad
```

### Linux

- Para detener el aceptador de cliente (y no reiniciarlo), emita el mandato siguiente:

```
# service dsmcad stop
```

- Para detener y reiniciar el aceptador de cliente, emita el mandato siguiente:

```
# service dsmcad restart
```

### MAC OS X

Pulse Aplicaciones > Programas de utilidad > Terminal.

- Para detener el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl unload -w com.ibm.tivoli.dsmcad
```


- Para iniciar el aceptador de cliente, emita el mandato siguiente:

```
/bin/launchctl load -w com.ibm.tivoli.dsmcad
```

### Windows

- Para detener el servicio aceptador de cliente, siga los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Detener y Aceptar.
- Para reiniciar el servicio aceptador de cliente, siga los pasos siguientes:
  - a. Pulse Inicio > Herramientas administrativas > Servicios.
  - b. Efectúe doble pulsación en el servicio aceptador de cliente.
  - c. Pulse Iniciar y Aceptar.

#### Referencia relacionada:

 Resolución de problemas de planificación del cliente

## Restablecimiento de contraseñas

---

Si se pierde la contraseña de un nodo cliente o un ID de administrador, podrá restablecerla. Varios intentos de acceso al sistema con una contraseña incorrecta pueden ocasionar el bloqueo del nodo cliente o del ID de administrador. Puede tomar medidas para resolver el problema.

## Procedimiento

---

Para resolver problemas de contraseña, realice una de las siguientes acciones:

- Si se ha instalado un cliente de archivado y copia de seguridad en un nodo cliente, y se pierde la contraseña o se olvida, realice los siguientes pasos:

1. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nodo cliente y *nueva\_contraseña* especifica la contraseña que asigne.

2. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

- Si se bloquea a un administrador por problemas con la contraseña, realice lo siguiente:

1. Para proporcionar acceso al administrador al servidor, ejecute el mandato UNLOCK ADMIN. Para obtener instrucciones, consulte UNLOCK ADMIN (Desbloquear un administrador).
2. Configure una contraseña nueva utilizando el mandato UPDATE ADMIN:

```
update admin nombre_admin nueva_contraseña forcepwnreset=yes
```

donde *admin* especifica el nombre del administrador y *nueva\_contraseña* especifica la contraseña que asigne.

- Si se bloquea un nodo cliente, lleve a cabo los siguientes pasos:

1. Determine la causa del bloqueo y si es necesario desbloquearlo. Por ejemplo, si el nodo cliente está fuera de servicio, se elimina del entorno de producción. No se puede revertir la operación de fuera de servicio y el nodo cliente permanece bloqueado. También se puede bloquear un nodo cliente si los datos del cliente están sujetos a una investigación judicial.
2. Si necesita desbloquear un nodo cliente, utilice el mandato UNLOCK NODE. Para obtener instrucciones, consulte UNLOCK NODE (Desbloquear un nodo de cliente).
3. Genere una nueva contraseña ejecutando el mandato UPDATE NODE:

```
update node nombre_nodo nueva_contraseña forcepwnreset=yes
```

donde *nombre\_nodo* especifica el nombre del nodo y *nueva\_contraseña* especifica la contraseña que asigne.

4. Informe al propietario del nodo cliente sobre la contraseña modificada. Cuando el propietario del nodo cliente inicie sesión con la contraseña especificado, se generará automáticamente una contraseña nueva. Esta contraseña es desconocida para los usuarios a fin de mejorar la seguridad.

Consejo: La contraseña se genera automáticamente si ha definido previamente la opción `passwordaccess` como `generar` en el archivo de opciones del cliente.

## Poner fuera de servicio un nodo cliente

---

Si ya no se necesita un nodo cliente, puede iniciar un proceso para eliminarlo del entorno de producción. Por ejemplo, si una estación de trabajo estaba haciendo una copia de seguridad de datos en el servidor IBM Spectrum Protect, pero ya no se utilizaba la estación de trabajo, puede dejar fuera de servicio la estación de trabajo.

### Acerca de esta tarea

---

Cuando inicia el proceso para poner el servidor fuera de servicio, éste bloquea el nodo cliente para impedir que acceda al servidor. Los archivos que pertenecen al nodo cliente se suprimen gradualmente y, a continuación, el nodo cliente se suprime. Puede poner fuera de servicio los siguientes tipos de nodo cliente:

#### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen servidores de correo electrónico, bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

#### Nodos de cliente de sistemas

Los nodos de cliente de sistemas incluyen estaciones de trabajo, servidores de archivos de almacenamiento adjunto a red (NAS) y clientes de API.

#### Nodos de cliente de máquina virtual

Los nodos de cliente de máquina virtual constan de un host invitado individual dentro de un hipervisor. Cada máquina virtual se representa como un espacio de archivos.

El método más sencillo para poner fuera de servicio un nodo cliente es utilizar Centro de operaciones. El proceso de poner fuera de servicio se ejecuta en segundo plano. Si el cliente está configurado para replicar datos de cliente, Centro de operaciones elimina automáticamente el cliente de la réplica en los servidores de réplica de origen y de destino antes de que ponga fuera de servicio al cliente.

Consejo: De forma alternativa, puede poner fuera de servicio un nodo cliente emitiendo el mandato DECOMMISSION NODE o DECOMMISSION VM. Es posible que desee utilizar este método en los casos siguientes:

- Para planificar el proceso de poner fuera de servicio en un futuro o para ejecutar una serie de mandatos utilizando un script, especifique el proceso de poner fuera de servicio para ejecutarlo en segundo plano.
- Para supervisar el proceso de poner fuera de servicio para fines de depuración, especifique el proceso de poner fuera de servicio para ejecutarlo en primer plano. Si ejecuta el proceso en primer plano, debe esperar a que se complete el proceso antes de continuar con otras tareas.

## Procedimiento

---

Realice una de las siguientes acciones:

- Para poner fuera de servicio un cliente en segundo plano utilizando Centro de operaciones, complete los pasos siguientes:
  1. En la página Visión general del Centro de operaciones, pulse Clientes y seleccione el cliente.
  2. Pulse Más > Poner fuera de servicio.
- Para poner fuera de servicio un nodo cliente utilizando un mandato administrativo, complete los pasos siguientes:
  1. Determine si el nodo cliente se ha configurado para la réplica de nodo emitiendo el mandato QUERY NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, ejecute el siguiente mandato:

```
query node austin format=detailed
```

Revise el campo de salida de Estado de réplica.

2. Si el nodo cliente se ha configurado para la réplica, elimine el nodo cliente de la réplica emitiendo el mandato REMOVE REPLNODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
remove replnode austin
```

3. Realice una de las siguientes acciones:

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación, emita el mandato DECOMMISSION NODE. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin
```

- Para poner fuera de servicio un nodo cliente del sistema o de la aplicación en primer plano, emita el mandato DECOMMISSION NODE y especifique el parámetro `wait=yes`. Por ejemplo, si el nodo cliente se denomina AUSTIN, emita el siguiente mandato:

```
decommission node austin wait=yes
```

- Para poner fuera de servicio una máquina virtual en segundo plano, emita el mandato DECOMMISSION VM. Por ejemplo, si la máquina virtual se denomina AUSTIN, el espacio de archivos es 7 y el nombre de espacio de archivos se especifica por el ID de espacio de archivos, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid
```

Si el nombre de la máquina virtual incluye uno o varios espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid
```

- Para poner fuera de servicio una máquina virtual en primer plano, emita el mandato DECOMMISSION VM y especifique el parámetro `wait=yes`. Por ejemplo, emita el siguiente mandato:

```
decommission vm austin 7 nametype=fsid wait=yes
```

Si el nombre de la máquina virtual incluye uno o varios espacios, especifique el nombre entre comillas dobles. Por ejemplo:

```
decommission vm "austin 2" 7 nametype=fsid wait=yes
```

## Qué hacer a continuación

---

Vea si aparecen mensajes de error, que se pueden ver en la interfaz de usuario o en la salida del mandato, inmediatamente después de ejecutar el proceso.



Puede verificar que el nodo cliente está fuera de servicio:

1. En la página de Centro de operaciones *Visión general*, pulse *Clientes*.
2. En la tabla *Clientes*, en la columna *En riesgo*, revise el estado:
  - o El estado *FUERA DE SERVICIO* indica que el nodo está fuera de servicio.
  - o Un valor nulo indica que el nodo no está fuera de servicio.
  - o El estado *PENDIENTE* indica que se está realizando el proceso de colocar el nodo fuera de servicio o que dicho proceso ha fallado.

Consejo: Si desea determinar el estado de un proceso de colocación fuera de servicio pendiente, emita el mandato siguiente:

```
query process
```

3. Revise la salida del mandato:
  - o Si se muestra el estado del proceso de servicio de retirada de servicio, significa que el proceso está en curso. Por ejemplo:

```
query process
```

Proceso proceso	Descripción proceso	Estado proceso
----- 3 desactivados	----- NODO FUERA DE SERVICIO	----- Número de objetos de copia de seguridad para el nodo NODE1: 8 objetos desactivados.

- o Si no se muestra el estado del proceso de servicio de retirada de servicio y no ha recibido ningún mensaje de error, significa que el proceso está incompleto. Un proceso puede estar incompleto si los archivos que asociados al nodo aún no se han desactivado. Una vez desactivados los archivos, vuelva a ejecutar el proceso de colocación fuera de servicio.
- o Si no se muestra el estado del proceso de servicio de retirada de servicio y recibe un mensaje de error, significa que el proceso ha fallado. Vuelva a ejecutar el proceso de retirada de servicio.

#### Referencia relacionada:

- ➔ [DECOMMISSION NODE](#) (Dejar fuera de servicio un nodo de cliente)
- ➔ [DECOMMISSION VM](#) (Dejar fuera de servicio una máquina virtual)
- ➔ [QUERY NODE](#) (Consultar nodos)
- ➔ [REMOVE REPLNODE](#) (Eliminar un nodo de cliente de la réplica)

## Desactivación de datos para liberar espacio de almacenamiento

En algunos casos, puede desactivar datos que están almacenados en el servidor IBM Spectrum Protect. Cuando ejecuta el proceso de desactivación, los datos de seguridad almacenados antes de la fecha y hora especificadas se desactivan y se suprimirán cuando caduca. De este modo, puede liberar espacio en el servidor.

### Acerca de esta tarea

Algunos clientes de aplicaciones siempre guardan datos en el servidor como datos de copia de seguridad activos. Puesto que los datos de copia de seguridad activos no están gestionados por las políticas de caducidad de inventario, los datos no se suprimen automáticamente y utilizan el espacio de almacenamiento del servidor de forma indefinida. Para liberar el espacio de almacenamiento utilizado por datos obsoletos, puede desactivar los datos.

Cuando ejecute el proceso de desactivación, todos los datos de copia de seguridad activos almacenados antes de la fecha especificada pasan a inactivos. Los datos se suprimen cuando caducan y no se pueden restaurar. La característica de desactivación se aplica solo a clientes de aplicación que protegen bases de datos de Oracle.

### Procedimiento

1. En la página *Descripción general* de Centro de operaciones, pulse *Clientes*.
2. En la tabla *Clientes*, seleccione uno o más clientes y pulse *Más > Borrar*.  
Método de línea de mandatos: Desactive los datos utilizando el mandato *DEACTIVATE DATA*.

#### Referencia relacionada:

- ➔ [DEACTIVATE DATA](#) (Desactivar datos para un nodo de cliente)

## Gestión de actualizaciones del cliente

Cuando hay disponible un fixpack o arreglo temporal, puede actualizar el servidor para sacar provecho de las mejoras del producto. Los servidores y clientes se pueden actualizar en momentos diferentes y pueden estar a distintos niveles con algunas restricciones.

## Antes de empezar

1. Revise los requisitos de compatibilidad cliente/servidor en nota técnica 1053218. Si la solución incluye servidores o clientes en un nivel anterior a V7.1, revise las directrices para asegurarse de que las operaciones de archivado y copia de seguridad de cliente no se vean afectadas.
2. Verifique los requisitos del sistema para el cliente en Sistemas operativos soportados de IBM Spectrum Protect.
3. Si la solución incluye agentes de almacenamiento o clientes de biblioteca, revise la información sobre la compatibilidad del agente de almacenamiento y el cliente de biblioteca con los servidores configurados como gestores de biblioteca. Consulte el apartado nota técnica 1302789.

Si tiene pensado actualizar un gestor de biblioteca y un cliente de biblioteca, debe actualizar el gestor de biblioteca primero.

## Procedimiento

Para actualizar el software, siga las instrucciones que figuran en la tabla siguiente.

Software	Enlace a instrucciones
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<ul style="list-style-type: none"><li>• Actualización del cliente de archivado y copia de seguridad</li></ul>
IBM Spectrum Protect Snapshot	<ul style="list-style-type: none"><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para UNIX y Linux</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para VMware</li><li>• Instalación y actualización de IBM Spectrum Protect Snapshot para Windows</li></ul>
IBM Spectrum Protect para bases de datos	<ul style="list-style-type: none"><li>• Actualización de Data Protection for SQL Server</li><li>• Instalación de Data Protection for Oracle</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server</li></ul>
IBM Spectrum Protect for Enterprise Resource Planning	<ul style="list-style-type: none"><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para DB2</li><li>• Actualización de IBM Spectrum Protect for Enterprise Resource Planning: Data Protection para SAP para Oracle</li></ul>
IBM Spectrum Protect for Mail	<ul style="list-style-type: none"><li>• Instalación de Data Protection for IBM Domino en un sistema UNIX, AIX o Linux (V7.1.0)</li><li>• Instalación de Data Protection for IBM Domino en un sistema Windows (V7.1.0)</li><li>• Instalación, actualización y migración de IBM Spectrum Protect for Mail: Data Protection para Microsoft Exchange Server</li></ul>
IBM Spectrum Protect for Virtual Environments	<ul style="list-style-type: none"><li>• Instalación y actualización de Data Protection para VMware</li><li>• Instalación de protección de datos para Microsoft Hyper-V</li></ul>

## Gestión del Centro de operaciones

El Centro de operaciones ofrece acceso web y a móvil a la información de estado sobre el entorno de IBM Spectrum Protect. Puede utilizar Centro de operaciones para supervisar varios servidores y para completar algunas tareas administrativas. Centro de operaciones también proporciona acceso web a la línea de mandatos de IBM Spectrum Protect.

- Adición y eliminación de servidores spoke  
En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.
- Inicio y detención del servidor web  
El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.
- Reinicio del asistente de configuración inicial  
Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

- Cambio del servidor concentrador  
Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.
- Restauración de la configuración a un estado de preconfiguración  
Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

## Adición y eliminación de servidores spoke

---

En un entorno de varios servidores, puede conectarse a los demás servidores, llamados *servidores spoke*, al servidor concentrador.

### Acerca de esta tarea

---

Los servidores spoke envían alertas e información de estado al servidor concentrador. El Centro de operaciones le muestra una vista consolidada de alertas e información de estado para el servidor concentrador y los servidores spoke.

- Adición de un servidor de radio  
Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.
- Eliminación de un servidor spoke  
Puede eliminar un servidor spoke del Centro de operaciones.

## Adición de un servidor de radio

---

Después de configurar el servidor concentrador para Centro de operaciones, puede añadir uno o más servidores de radio al servidor concentrador.

### Antes de empezar

---

La comunicación entre el servidor spoke y el servidor concentrador debe protegerse mediante el uso del protocolo de Seguridad de la capa de transporte (Transport Layer Security - TLS). Para proteger las comunicaciones, añada el certificado del servidor spoke al archivo de almacén de confianza del servidor concentrador.

### Procedimiento

---

1. En la barra de menús de Centro de operaciones, pulse Servidores. Se abre la página Servidores.

En la tabla de la página Servidores, un servidor puede tener un estado de "No supervisado." Este estado significa que aunque un administrador haya definido este servidor al servidor concentrador utilizando el mandato DEFINE SERVER, el servidor todavía no está configurado como un servidor de radio.

2. Realice uno de los siguientes pasos:
  - Seleccione el servidor para resaltarlo, y en la tabla de la barra del menú, pulse Supervisar radio.
  - Si el servidor que desea añadir no se muestra en la tabla, y no es necesaria la comunicación segura SSL/TLS, pulse + Servidor de radio en la barra de menús de la tabla.
3. Proporcione la información necesaria y complete los pasos del asistente de configuración del servidor de radio.  
Consejo: Si el periodo de retención del registro de sucesos del servidor es inferior a 14 días, el periodo se restablece automáticamente en 14 días, si configura el servidor como un servidor de radio.

## Eliminación de un servidor spoke

---

Puede eliminar un servidor spoke del Centro de operaciones.

### Acerca de esta tarea

---

Tal vez sea conveniente eliminar un servidor de radio en las situaciones siguientes, por ejemplo:

- Desea mover el servidor spoke de un servidor concentrador a otro servidor concentrador.
- Desea que el servidor spoke quede fuera de servicio.

### Procedimiento

---

Para eliminar el servidor spoke del grupo de servidores que gestiona el servidor concentrador, realice los pasos siguientes:

1. Desde la línea de mandatos de IBM Spectrum Protect, emita el mandato siguiente en el servidor concentrador:

```
QUERY MONITORSETTINGS
```

2. En la salida del mandato, copie el nombre incluido en el campo Grupo supervisado.
3. Emita el mandato siguiente en el servidor concentrador, donde *nombre\_grupo* representa el nombre del grupo supervisado y *nombre\_miembro* representa el nombre del servidor spoke:

```
DELETE GRPMEMBER nombre_grupo nombre_miembro
```

4. Opcional: Si desea mover el servidor de radio de un servidor concentrador a otro servidor concentrador, **no** lleve a cabo este paso. De lo contrario, puede inhabilitar las alertas y la supervisión en el servidor spoke emitiendo los mandatos siguientes en el servidor spoke:

```
SET STATUSMONITOR OFF  
SET ALERTMONITOR OFF
```

5. Opcional: Si la definición del servidor de radio se utiliza para otros fines, como por ejemplo, la configuración empresarial, el direccionamiento de mandatos, el almacenamiento de volúmenes virtuales o la gestión de bibliotecas, **no** lleve a cabo este paso. De lo contrario, puede suprimir la definición del servidor spoke en el servidor concentrador emitiendo el mandato siguiente en el servidor concentrador:

```
DELETE SERVER nombre_servidor_spoke
```

## Inicio y detención del servidor web


---

El servidor web de Centro de operaciones se ejecuta como un servicio y se inicia automáticamente. Podría ser que tuviera que detener e iniciar el servidor web, por ejemplo, para realizar cambios de configuración.


### Procedimiento

---


1. Detener el servidor web.

-  **Sistemas operativos AIX** Desde el directorio */installation\_dir/ui/Utils* donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:


```
./stopserver.sh
```

-  **Sistemas operativos Linux** Emita el mandato siguiente:


```
service opscenter.rc stop
```

-  **Sistemas operativos Windows** Desde la ventana Servicios, detenga el servicio IBM Spectrum Protect Centro de operaciones.

2. Inicie el servidor web.

-  **Sistemas operativos AIX** Desde el directorio */installation\_dir/ui/Utils* donde *installation\_dir* representa el directorio donde está instalado Centro de operaciones, emita los siguientes mandatos:

```
./startserver.sh
```

-  **Sistemas operativos Linux** Emita los mandatos siguientes:

Inicie el servidor:


```
service opscenter.rc start
```

Reinicie el servidor:

```
service opscenter.rc restart
```

Determine si se está ejecutando el servidor:

```
service opscenter.rc status
```

-  **Sistemas operativos Windows** Desde la ventana Servicios, inicie el servicio IBM Spectrum Protect Centro de operaciones.

## Reinicio del asistente de configuración inicial

---

Es posible que tenga que reiniciar el asistente de configuración inicial de Centro de operaciones, por ejemplo, para hacer cambios de configuración.

## Antes de empezar

---

Para cambiar los siguientes valores, utilice la página Valores de Centro de operaciones en lugar de reiniciar el asistente de configuración inicial:

- La frecuencia de actualización de los datos de estado
- El tiempo de duración que las alertas permanecen activas, inactivas o cerradas
- Las condiciones que indican que los clientes están en riesgo

La ayuda de Centro de operaciones incluye más información acerca de cómo cambiar estos valores.







## Acerca de esta tarea

---

Para reiniciar el asistente de configuración inicial, debe suprimir un archivo de propiedades que incluye información acerca de la conexión del servidor concentrador. Sin embargo, no se eliminarán los valores de alerta, supervisión, en riesgo o multiservidor que se hayan configurado para el servidor concentrador. Estos valores se utilizan como valores predeterminados en el asistente de configuración cuando se reinicia el asistente.

## Procedimiento

---

1. Detenga el servidor web de Centro de operaciones.
  2. En el sistema donde está instalado Centro de operaciones, vaya al siguiente directorio, donde *installation\_dir* representa el directorio en el que está instalado Centro de operaciones:
    -  Sistemas operativos AIX  Sistemas operativos Linux *installation\_dir*/ui/Liberty/usr/servers/guiServer
    -  Sistemas operativos Windows *installation\_dir*\ui\Liberty\usr\servers\guiServer
- Por ejemplo:
-  Sistemas operativos AIX  Sistemas operativos Linux/opt/tivoli/tsm/ui/Liberty/usr/servers/guiServer
  -  Sistemas operativos Windows c:\Archivos de programa\Tivoli\TSM\ui\Liberty\usr\servers\guiServer
3. En el directorio guiServer, elimine el archivo serverConnection.properties.
  4. Inicie el servidor web Centro de operaciones.
  5. Abra el Centro de operaciones.
  6. Utilice el asistente de configuración para volver a configurar el Centro de operaciones. Especifique una contraseña nueva para el ID de administración de supervisión.
  7. En cualquier servidor spoke que estuviera conectado anteriormente al servidor concentrador, actualice la contraseña para el ID de administrador de supervisión emitiendo el mandato siguiente desde la interfaz de línea de mandatos de IBM Spectrum Protect:

```
UPDATE ADMIN IBM-OC-hub_server_name new_password
```

Restricción: No cambie ningún valor para el ID de administrador. Después de especificar la contraseña inicial, Centro de operaciones la gestiona automáticamente.

## Cambio del servidor concentrador

---

Puede utilizar el Centro de operaciones para eliminar el servidor concentrador de IBM Spectrum Protect y configurar otro servidor concentrador.

## Procedimiento

---

1. Reinicie el asistente de configuración inicial del Centro de operaciones. Como parte de este procedimiento, suprima la conexión del servidor concentrador existente.
2. Utilice el asistente para configurar el Centro de operaciones para conectarse al nuevo servidor concentrador.

### Tareas relacionadas:

Reinicio del asistente de configuración inicial

## Restauración de la configuración a un estado de preconfiguración

---

Si se producen determinados problemas, es posible que desee restaurar la configuración de Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o spoke.

## Procedimiento

---

Para restaurar la configuración, complete los pasos siguientes:

1. Detenga el servidor web de Centro de operaciones.
2. Para desconfigurar el servidor concentrador, lleve a cabo los siguientes pasos:
  - a. En el servidor concentrador, emita los mandatos siguientes:

```
SET MONITORINGADMIN ""
SET MONITOREDSEVERGROUP ""
SET STATUSMONITOR OFF
SET ALERTMONITOR OFF
REMOVE ADMIN IBM-OC-hub_server_name
```

**Consejo:** *IBM-OC-nombre\_servidor\_concentrador* representa el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. Restablezca la contraseña para el servidor concentrador emitiendo el siguiente mandato en el servidor concentrador:

```
SET SERVERPASSWORD ""
```

**Atención:** No complete este paso si el servidor concentrador está configurado con otros servidores para otros fines como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

3. Desconfigure los servidores spoke completando los pasos siguientes:
  - a. En el servidor concentrador para determinar si algún servidor spoke permanece como miembro del grupo de servidores, emita el siguiente mandato:

```
QUERY SERVERGROUP IBM-OC-nombre_servidor_concentrador
```

**Consejo:** *IBM-OC-nombre\_servidor\_concentrador* representa el nombre del grupo de servidores supervisados que se han creado automáticamente al configurar el primer servidor spoke. Este nombre de grupo de servidores también es el mismo que el ID de administrador de supervisión que se creó automáticamente al configurar inicialmente el servidor concentrador.

- b. En el servidor concentrador, para suprimir servidores spoke del grupo de servidores, emita el siguiente mandato para cada servidor spoke:

```
DELETE GRPMEMBER IBM-OC-nombre_servidor_concentrador nombre_servidor_spoke
```

- c. Después de que todos los servidores spoke se ha suprimido del grupo de servidores, emita los mandatos siguientes en el servidor concentrador:

```
DELETE SERVERGROUP IBM-OC-nombre_servidor_concentrador
SET MONITOREDSEVERGROUP ""
```

- d. En cada servidor spoke, emita los siguientes mandatos:

```
REMOVE ADMIN IBM-OC-hub_server_name
SETOPT PUSHSTATUS NO
SET ALERTMONITOR OFF
SET STATUSMONITOR OFF
```

- e. En cada servidor spoke, elimine la definición del servidor concentrador emitiendo el siguiente mandato:

```
DELETE SERVER nombre_servidor_concentrador
```

**Atención:** No complete este paso si la definición se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

- f. En el servidor concentrador, suprima la definición de cada servidor spoke emitiendo el mandato siguiente:

```
DELETE SERVER nombre_servidor_spoke
```

**Atención:** No complete este paso si la definición de servidor se utiliza para otros fines, como, por ejemplo, para la compartición de bibliotecas, exportación e importación de datos o la réplica de nodos.

4. Restablezca los valores predeterminados en cada uno de los servidores emitiendo los mandatos siguientes:

```
SET STATUSREFRESHINTERVAL 5
SET ALERTUPDATEINTERVAL 10
SET ALERTACTIVEDURATION 480
SET ALERTINACTIVEDURATION 480
SET ALERTCLOSEDDURATION 60
SET STATUSATRISKINTERVAL TYPE=AP INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=VM INTERVAL=24
SET STATUSATRISKINTERVAL TYPE=SY INTERVAL=24
SET STATUSSKIPASFAILURE YES TYPE=ALL
```





5. Reinicie el asistente de configuración inicial del Centro de operaciones.

#### **Tareas relacionadas:**

## Configuración de bibliotecas de cintas virtuales

---

Una biblioteca de cintas virtuales (VTL) no utiliza medios de cinta físicos. Cuando implemente el almacenamiento de VTL, puede superar la capacidad de una biblioteca de cintas físicas. La capacidad para definir varios volúmenes y unidades puede proporcionar mayor flexibilidad al entorno de almacenamiento.

- Consideraciones sobre el uso de las bibliotecas de cintas virtuales  
Existen ciertas consideraciones para la definición de una biblioteca como una biblioteca de cintas virtuales (VTL), incluidas las mejoras en el rendimiento y la configuración de su hardware.
- Agregar una biblioteca de cintas virtuales a su entorno  
Defina una biblioteca de cintas virtuales (VTL) para beneficiarse de las ventajas en el rendimiento del montaje y la escalabilidad.
- Definir todas las unidades y vías de acceso de una biblioteca  
Puede utilizar el mandato PERFORM LIBACTION para configurar una biblioteca SCSI o una biblioteca virtual de cintas (VTL) en un solo paso.
-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad  
Configure una biblioteca VTL o SCSI que contenga dos unidades de cinta LTO.
-  Sistemas operativos AIX  Sistemas operativos Linux Ejemplo: Configure una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad  
Puede configurar una biblioteca con varios tipos de dispositivos de unidad, como por ejemplo, una biblioteca StorageTek L40 que contiene una unidad DLT y una unidad LTO Ultrium.

## Consideraciones sobre el uso de las bibliotecas de cintas virtuales

---

Existen ciertas consideraciones para la definición de una biblioteca como una biblioteca de cintas virtuales (VTL), incluidas las mejoras en el rendimiento y la configuración de su hardware.

### Acerca de esta tarea

---

La definición de una VTL en el servidor de IBM Spectrum Protect puede ayudar a mejorar el rendimiento, ya que el servidor maneja el proceso de puntos de montaje para las VTL de modo diferente que para las bibliotecas de cintas reales. Las limitaciones físicas del hardware de cintas reales no se aplican a una VTL, ofreciendo opciones para una mejor escalabilidad.

Puede utilizar una VTL para cualquier biblioteca de cintas virtuales siempre que se cumplan las siguientes condiciones:

- No hay soportes combinados implicados en la VTL. Sólo se emula en la biblioteca un tipo y una generación de unidades y soportes.
- Cada servidor y agente de almacenamiento con acceso a la VTL tiene vías de acceso definidas para todas las unidades de la biblioteca.

Si no se cumple alguna de estas condiciones, podrá reducirse o anularse cualquier ventaja derivada de definir una biblioteca VTL en el servidor de IBM Spectrum Protect.

Las VTL son compatibles con versiones anteriores tanto de los clientes de biblioteca como de los agentes de almacenamiento. El cliente de biblioteca o el agente de almacenamiento no se ve afectado por el tipo de biblioteca que se utiliza para el almacenamiento. Si las condiciones de las vías de acceso y los soportes combinados se cumplen para una biblioteca SCSI, puede definirse o actualizarse como LIBTYPE=VTL.

- Capacidad de almacenamiento para las bibliotecas de cintas virtuales  
Como las bibliotecas de cintas virtuales (VTL) no tienen las limitaciones físicas que tiene el hardware de cinta real, su capacidad de almacenamiento es más flexible.
- Configuración de unidades para las bibliotecas de cintas virtuales  
La configuración de unidades en una biblioteca de cintas virtual (VTL) es variable, dependiendo de las necesidades del entorno.

## Capacidad de almacenamiento para las bibliotecas de cintas virtuales

---

Como las bibliotecas de cintas virtuales (VTL) no tienen las limitaciones físicas que tiene el hardware de cinta real, su capacidad de almacenamiento es más flexible.

El concepto de capacidad de almacenamiento en una biblioteca de cintas virtual es distinto de la capacidad en un hardware de cinta física. En una biblioteca de cintas física, cada volumen tiene una capacidad definida, y la capacidad de la biblioteca se define en

términos del número total de volúmenes en la biblioteca. Por otro lado, la capacidad de una VTL se define en términos del espacio de disco total disponible. Puede aumentar o disminuir el número y el tamaño de los volúmenes en el disco.

Esta variabilidad afecta a lo que significa quedarse sin espacio en una VTL. Por ejemplo, un volumen en una VTL puede quedarse sin espacio antes de alcanzar su capacidad asignada si el total de discos subyacentes se queda sin espacio. En esta situación, el servidor puede recibir un mensaje de fin de volumen sin otro aviso, lo que provoca errores de copia de seguridad.

Cuando se producen errores de copia de seguridad y falta de espacio, normalmente todavía hay espacio de disco disponible en la VTL. Se oculta en volúmenes que no se están utilizando. Por ejemplo, los volúmenes que se suprimen lógicamente o se devuelven a estado reutilizable en el servidor de IBM Spectrum Protect solo se suprimen en la base de datos del servidor. No se notifica a la VTL, que mantiene el tamaño completo del volumen como asignado en sus cálculos de capacidad.

Para evitar errores de falta de espacio, asegúrese de que toda biblioteca SCSI que actualice a LIBTYPE=VTL se actualice con el parámetro RELABELSCRATCH establecido en YES. La opción RELABELSCRATCH permite al servidor sobrescribir la etiqueta de cualquier volumen que se suprima y devolver el volumen al estado reutilizable en la biblioteca. El parámetro RELABELSCRATCH se establece de forma predeterminada en YES para cualquier biblioteca definida como una VTL.

**Referencia relacionada:**

UPDATE LIBRARY (Actualizar una biblioteca)

## Configuración de unidades para las bibliotecas de cintas virtuales

---

La configuración de unidades en una biblioteca de cintas virtual (VTL) es variable, dependiendo de las necesidades del entorno.

La mayoría de los entornos VTL utilizar tantas unidades como sea posible para maximizar el número de operaciones de cinta simultáneas. Un montaje de cinta individual en un entorno VTL suele ser más rápido que un montaje de cinta física. No obstante, el uso de muchas unidades aumenta la cantidad de tiempo que requiere el servidor de IBM Spectrum Protect cuando se solicita un montaje. El proceso de selección tarda más tiempo, ya que aumenta el número de unidades definidas en un objeto de biblioteca individual en el servidor. Los montajes de cintas virtuales puede tardar el mismo tiempo o más que los montajes de cintas físicas, dependiendo del número de unidades en VTL.

Para obtener mejores resultados al crear unidades, compruebe con el proveedor de VTL las recomendaciones específicas para el dispositivo. Si se requieren más de 300-500 unidades para cada VTL, puede hacer una partición lógica del VTL en varias bibliotecas y asignar unidades a cada biblioteca. Las configuraciones de hardware de SAN y sistema operativo pueden imponer limitaciones en el número de dispositivos que pueden utilizarse en la biblioteca VTL.

## Agregar una biblioteca de cintas virtuales a su entorno

---

Defina una biblioteca de cintas virtuales (VTL) para beneficiarse de las ventajas en el rendimiento del montaje y la escalabilidad.

### Acerca de esta tarea

---

Las VTL se identifican utilizando el mandato DEFINE LIBRARY y especificando el parámetro LIBTYPE=VTL. Dado que una biblioteca VTL funcionalmente interactúa con el servidor igual que una biblioteca SCSI, puede utilizar el mandato UPDATE LIBRARY para cambiar el tipo de biblioteca de una biblioteca SCSI que ya esté definida. No es necesario volver a definir la biblioteca.

### Procedimiento

---

- Añadir una biblioteca VTL nueva. Defina la biblioteca como una VTL en el servidor, como se muestra en el ejemplo siguiente:

```
define library chester libtype=vtl
```

Así se establece la nueva biblioteca VTL y se habilita la opción RELABELSCRATCH para volver a etiquetar los volúmenes que han sido suprimidos y devueltos al estado reutilizable.

- Actualizar una biblioteca SCSI a una VTL. Si dispone de una biblioteca SCSI y desea cambiarla a una VTL, utilice el mandato UPDATE LIBRARY para cambiar el tipo de biblioteca:

```
update library calzone libtype=vtl
```

Solo puede emitir este mandato si la biblioteca que se va a actualizar está definida con el parámetro LIBTYPE=SCSI.

**Referencia relacionada:**

DEFINE LIBRARY (Definir una biblioteca)

UPDATE LIBRARY (Actualizar una biblioteca)



# Definir todas las unidades y vías de acceso de una biblioteca

Puede utilizar el mandato PERFORM LIBACTION para configurar una biblioteca SCSI o una biblioteca virtual de cintas (VTL) en un solo paso.

## Acerca de esta tarea

Si está configurando o modificando el entorno de hardware y debe crear o cambiar un gran número de definiciones de unidades, el mandato PERFORM LIBACTION puede facilitarle mucho esta tarea. Puede definir una nueva biblioteca y, a continuación, definir todas las unidades y vías de acceso a las unidades. O, si dispone de una biblioteca existente que desea suprimir, puede suprimir todas las unidades existentes y sus vías de acceso en un solo paso.

El parámetro PREVIEW le permite ver la salida de los comandos antes de que se procesen para verificar la acción que desea realizar. Si define una biblioteca, ya tiene que haber una vía de acceso a la biblioteca definida si desea especificar el parámetro PREVIEW. No puede utilizar los parámetros PREVIEW y DEVICE de forma conjunta.

El mandato PERFORM LIBACTION solo se puede utilizar para bibliotecas SCSI y VTL. Si está definiendo unidades y vías de acceso a la biblioteca, la opción SANDISCOVERY debe estar admitida y habilitada. La biblioteca de cintas tiene que poder devolver la asociación de dirección del número de serie.


## Procedimiento

Para configurar una biblioteca VTL denominada ODIN, complete estos pasos:

### 1. Defina la biblioteca.

```
define library odin libtype=vtl
```

### 2. Defina dos unidades y sus vías de acceso para la nueva biblioteca, ODIN.

 Sistemas operativos AIX

```
perform libaction odin action=define device=/dev/lb3 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=/dev/
lb3 define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/mt2
```

 Sistemas operativos Linux

```
perform libaction odin action=define device=/dev/tsm SCSI/lb3 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=/dev/tsm SCSI/lb3
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=/dev/tsm SCSI/mt1 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=/dev/tsm SCSI/mt2
```

 Sistemas operativos Windows

```
perform libaction odin action=define device=lb0.0.0.2 prefix=dr
```

El servidor emite a continuación los siguientes comandos:

```
define path tsmserver odin srct=server destt=library device=lb0.0.0.2
define drive odin dr0
define path tsmserver dr0 srct=server destt=drive library=odin
device=mt0.1.0.2 define drive odin dr1
define path tsmserver dr1 srct=server destt=drive library=odin
device=mt0.2.0.2
```

### Referencia relacionada:

DEFINE LIBRARY (Definir una biblioteca)

DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)

## Ejemplo: Configure una biblioteca SCSI o una biblioteca virtual de cintas con un único tipo de dispositivo de unidad

---

Configure una biblioteca VTL o SCSI que contenga dos unidades de cinta LTO.

### Acerca de esta tarea

---

Este procedimiento es un ejemplo de cómo configurar una biblioteca SCSI automatizada que contiene dos unidades en el sistema servidor. La biblioteca no está compartida con otros servidores de IBM Spectrum Protect o con agentes de almacenamiento, y está conectada normalmente al sistema de servidor mediante tablas SCSI.

En esta configuración, ambas unidades de la biblioteca son el mismo tipo de dispositivo. Defina una clase de dispositivo. El procedimiento es el mismo tanto para las bibliotecas SCSI como para las VTL, excepto el paso para definir la biblioteca. En las bibliotecas SCSI, defina la biblioteca con `libtype=scsi`. En las bibliotecas VTL, puede definir la biblioteca con `libtype=vtl`.

### Procedimiento

---


1. Defina una biblioteca SCSI denominada AUTODTLIB.

```
define library autoltolib libtype=scsi
```


Si la biblioteca tiene un lector de código de barras y desea etiquetar cintas automáticamente antes de darlas de alta, puede establecer el parámetro AUTOLABEL en YES. Por ejemplo:

```
define library autoltolib libtype=scsi autolabel=yes
```

2. Defina una vía de acceso desde el servidor a la biblioteca.

 Sistemas operativos AIX

```
define path server1 autoltolib srctype=server desttype=library  
device=/dev/lb3
```

 Sistemas operativos Linux

```
define path server1 autoltolib srctype=server desttype=library  
device=/dev/tmscsi/lb3
```

 Sistemas operativos Windows


```
define path server1 autoltolib srctype=server desttype=library  
device=lb0.0.0.3
```

3. Defina las unidades de la biblioteca. Las dos unidades pertenecen a la biblioteca AUTODTLIB.

```
define drive autoltolib drive01  
define drive autoltolib drive02
```

Consejo: Puede utilizar el mandato PERFORM LIBACTION para definir unidades y vías de acceso para una biblioteca en un paso.

4. Defina una vía de acceso del servidor a cada unidad.

 Sistemas operativos AIX

```
define path server1 drive01 srctype=server desttype=drive  
library=autoltolib device=/dev/mt4  
define path server1 drive02 srctype=server desttype=drive  
library=autoltolib device=/dev/mt5
```

 Sistemas operativos Linux

```
define path server1 drive01 srctype=server desttype=drive  
library=autoltolib device=/dev/tmscsi/mt4  
define path server1 drive02 srctype=server desttype=drive  
library=autoltolib device=/dev/tmscsi/mt5
```

 Sistemas operativos Windows

```
define path server1 drive01 srctype=server desttype=drive  
library=autoltolib device=mt0.0.0.4  
define path server1 drive02 srctype=server desttype=drive  
library=autoltolib device=mt0.0.0.5
```

Si no ha especificado la dirección de elemento al definir la unidad, el servidor consulta ahora la biblioteca para obtener la dirección de elemento predeterminada correspondiente a la unidad.

5. Defina una clase de dispositivo denominada AUTODLT\_CLASS para las dos unidades de la biblioteca AUTODTLIB.

```
define devclass autolto_class library=autodltlib devtype=lto
```

6. Defina una agrupación de almacenamiento denominada AUTOLTO\_POOL asociada a la clase de dispositivo denominada AUTOLTO\_CLASS.

```
define stgpool autolto_pool autolto_class maxscratch=20
```

7. Etiquete y dé de alta todos los volúmenes de biblioteca.

```
label libvolume autoltolib search=yes labelsource=barcode checkin=scratch
```

8. Verifique las definiciones emitiendo los siguientes mandatos:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

**Referencia relacionada:**

DEFINE DEVCLASS (Definir una clase de dispositivo)

DEFINE LIBRARY (Definir una biblioteca)

DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)

## Ejemplo: Configure una SCSI o una biblioteca virtual de cintas SCSI con varios tipos de dispositivos de unidad

---

Puede configurar una biblioteca con varios tipos de dispositivos de unidad, como por ejemplo, una biblioteca StorageTek L40 que contiene una unidad DLT y una unidad LTO Ultrium.

### Acerca de esta tarea

---

Este procedimiento es un ejemplo de cómo configurar una biblioteca SCSI automatizada que contiene dos unidades en el sistema servidor. La biblioteca no está compartida con otros servidores de IBM Spectrum Protect o con agentes de almacenamiento, y está conectada normalmente al sistema de servidor mediante cables SCSI.

En esta configuración, las unidades son tipos de dispositivos distintos. Defina una clase de dispositivo para cada tipo de dispositivo de unidad. Las unidades con tipos de dispositivos distintos están admitidas en una única biblioteca si define una clase de dispositivo para cada tipo de unidad. Si emplea esta configuración, debe incluir el formato específico del tipo de dispositivo de la unidad utilizando el parámetro FORMAT con un valor distinto de DRIVE.

El procedimiento es el mismo tanto para las bibliotecas SCSI como para las VTL, excepto el paso para definir la biblioteca. En las bibliotecas SCSI, defina la biblioteca con libtype=scsi. En las bibliotecas VTL, puede definir la biblioteca con libtype=vtl.


### Procedimiento

---

1. Defina una biblioteca SCSI denominada MIXEDLIB.

```
define library mixedlib libtype=scsi
```

2. Defina una vía de acceso desde el servidor a la biblioteca.

 Sistemas operativos AIX

```
define path server1 mixedlib srctype=server desttype=library
device=/dev/lb3
```

 Sistemas operativos Linux

```
define path server1 mixedlib srctype=server desttype=library
device=/dev/tsm SCSI/lb3
```


 Sistemas operativos Windows

```
define path server1 mixedlib srctype=server desttype=library
device=lb0.0.0.3
```


3. Defina las unidades en la biblioteca. Ambas unidades pertenecen a la biblioteca MIXEDLIB.

```
define drive mixedlib dlt1
define drive mixedlib lto1
```


4. Defina una vía de acceso del servidor a cada unidad. El parámetro DEVICE especifica el nombre del controlador de dispositivo para la unidad, que es el nombre de archivo especial de dispositivo.

 Sistemas operativos AIX

```
define path server1 dlt1 srctype=server desttype=drive
library=mixedlib device=/dev/mt4
define path server1 lto1 srctype=server desttype=drive
library=mixedlib device=/dev/mt5
```

 Sistemas operativos Linux

```
define path server1 dlt1 srctype=server desttype=drive
library=mixedlib device=/dev/tmscsi/mt4
define path server1 lto1 srctype=server desttype=drive
library=mixedlib device=/dev/tmscsi/mt5
```

 Sistemas operativos Windows

```
define path server1 drive01 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.4
define path server1 drive02 srctype=server desttype=drive
library=autoltolib device=mt0.0.0.5
```

Si no ha especificado la dirección de elemento al definir la unidad, el servidor consulta ahora la biblioteca para obtener la dirección de elemento correspondiente a la unidad.

5. Defina clases de dispositivo.

Importante: No utilice el formato DRIVE, que es el valor predeterminado. Como las unidades son de tipos diferentes, el servidor utiliza la especificación de formato para seleccionar una unidad. El uso del formato DRIVE en una biblioteca de medios mixtos puede tener consecuencias imprevisibles.

```
define devclass dlt_class library=mixedlib devtype=dlt format=dlt40
define devclass lto_class library=mixedlib devtype=lto format=ultriumc
```

6. Defina agrupaciones de almacenamiento asociadas a las clases de dispositivo.

```
define stgpool lto_pool lto_class maxscratch=20
define stgpool dlt_pool dlt_class maxscratch=20
```

7. Etiquete y dé de alta todos los volúmenes de biblioteca.

```
label libvolume mixedlib search=yes labelsource=barcode checkin=scratch
```

8. Verifique las definiciones emitiendo los siguientes comandos:

```
query library
query drive
query path
query devclass
query stgpool
query libvolume
```

## Protección de servidores de archivos NAS

Puede configurar y gestionar un entorno de copia de seguridad que proteja su servidor de archivos de almacenamiento adjunto de red (NAS).

Puede utilizar el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad de IBM Spectrum Protect o IBM Spectrum Protect Snapshot para realizar una copia de seguridad y restaurar un servidor de archivos NAS como se describe en la tabla siguiente.

Producto	Descripción
----------	-------------

Producto	Descripción
Servidor de IBM Spectrum Protect	<p>Para realizar una copia de seguridad y restaurar datos del servidor de archivos NAS utilizando el servidor de IBM Spectrum Protect, debe tener instalado IBM Spectrum Protect Extended Edition.</p> <p>Puede configurar el servidor de IBM Spectrum Protect para utilizar el protocolo de gestión de datos de redes (NDMP) para realizar una copia de seguridad y restaurar los datos como se describe en los siguientes temas de esta sección.</p> <p>Para proteger los sistemas de archivos NetApp grandes, también puede configurar IBM Spectrum Protect para que utilice la característica NetApp SnapMirror to Tape (también denominada SMTape). SnapMirror to Tape utiliza una copia de datos a nivel de bloque para la copia de seguridad, que es un método más rápido que una copia de seguridad completa tradicional NDMP y se puede utilizar si las copias de seguridad completas de NDMP no resultan prácticas.</p> <p>Para obtener información sobre el uso de SnapMirror to Tape para realizar una copia de seguridad y restaurar datos, consulte Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape.</p>
Cliente de copia de seguridad/archivado de IBM Spectrum Protect	<p>Puede configurar el cliente de archivado y copia de seguridad para realizar una copia de seguridad y restaurar los datos del servidor de archivos utilizando el protocolo Network File System (NFS) o Common Internet File System (CIFS).</p> <p>Para obtener información sobre cómo utilizar el cliente de archivado y copia de seguridad para realizar una copia de seguridad y restaurar datos, consulte Copia de seguridad y restauración de datos con los clientes de archivado y copia de seguridad.</p>
IBM Spectrum Protect Snapshot	<p>Puede utilizar IBM Spectrum Protect Snapshot para realizar una copia de seguridad y restaurar los datos del servidor de archivos utilizando las tecnologías de instantáneas avanzadas de los sistemas de almacenamiento.</p> <p>Para obtener información sobre cómo utilizar IBM Spectrum Protect Snapshot para hacer una copia de seguridad de los datos y restaurarlos, consulte Visión general de IBM Spectrum Protect Snapshot para UNIX y Linux o bien Visión general de IBM Spectrum Protect Snapshot for VMware.</p>

- **Requisitos de NDMP**  
Para utilizar NDMP para operaciones con servidores de archivos NAS, debe tener instalado IBM Spectrum Protect Extended Edition y el entorno de servidor de archivos debe cumplir determinados requisitos.
- **Gestión de operaciones NDMP**  
Existen diversas actividades de administrador para las operaciones NDMP.
- **Configuración de IBM Spectrum Protect para operaciones NDMP**  
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad y recuperar datos en los servidores de archivos NAS utilizando NDMP. El procedimiento de configuración varía dependiendo de si tiene previsto realizar una copia de seguridad de los datos desde un servidor de archivos NAS en clúster o no de clúster.
- **Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP**  
Después de configurar IBM Spectrum Protect para operaciones NDMP, está listo para empezar a utilizar NDMP.
- **Copia de seguridad y restauración en nivel de archivo para operaciones NDMP**  
Al realizar una copia de seguridad de los datos utilizando NDMP, puede especificar que el servidor de IBM Spectrum Protect recopile y almacene información de nivel de archivo en una tabla de contenido (TOC).
- **Operaciones de copia de seguridad y restauración a nivel de directorio**  
Si tiene un sistema de archivos NAS grande, al iniciar una copia de seguridad a nivel de directorios se reducen los tiempos de copia de seguridad y restauración y se proporciona más flexibilidad en la configuración de copias de seguridad NAS. Al definir los espacios de archivos virtuales, la copia de seguridad del sistema de archivos se debe partir en varias operaciones de copia de seguridad NDMP y varias unidades de cintas. También puede utilizar distintas planificaciones de copia de seguridad con el fin de realizar una copia de seguridad de subárboles de un sistema de archivos.
- **Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape**  
Puede realizar una copia de seguridad de sistemas de archivos NetApp grandes utilizando la característica NetApp SnapMirror to Tape (también denominada SMTape). Si se usa una copia de datos a nivel de bloque para copia de seguridad, el método SnapMirror to Tape es más rápido que una copia de seguridad completa tradicional NDMP y se puede usar si las copias de seguridad completas de NDMP no resultan prácticas.
- **Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra**  
Cuando el servidor de IBM Spectrum Protect inicia una operación de copia de seguridad NDMP en un transportador de datos Celerra, la copia de seguridad de un sistema de archivos grande puede tardar varias horas en realizarse. Sin los puntos de comprobación integrados de Celerra, los cambios que se producen en el sistema de archivos se graban en la imagen de copia de seguridad.
- **Réplica de los nodos NAS**  
Puede replicar un nodo NAS que utiliza NDMP para operaciones de copia de seguridad. Antes de configurar la operación de réplica, revise las restricciones que se aplican.

## Requisitos de NDMP

---

Para utilizar NDMP para operaciones con servidores de archivos NAS, debe tener instalado IBM Spectrum Protect Extended Edition y el entorno de servidor de archivos debe cumplir determinados requisitos.

### servidor de archivos NAS

IBM Spectrum Protect debe admitir el sistema operativo del servidor de archivos. Para obtener información sobre los servidores de archivos de NAS admitidos, consulte nota técnica 1054144.

El servidor de archivos NAS debe admitir la combinación del modelo de servidor de archivos y el sistema operativo. Para obtener información más específica, consulte la documentación del producto para el servidor de archivos de NAS.

### Bibliotecas de cintas

Este requisito sólo es necesario para una copia de seguridad en un dispositivo NAS conectado localmente. El servidor de IBM Spectrum Protect da soporte a los siguientes tipos de bibliotecas para las operaciones que utilizan NDMP:

#### SCSI

Una biblioteca SCSI puede conectarse directamente al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Cuando se conecta la biblioteca directamente al servidor de IBM Spectrum Protect, ese servidor controla las operaciones de la biblioteca pasando los mandatos SCSI directamente a la biblioteca. Cuando se conecta la biblioteca directamente al servidor de archivos NAS, el servidor de IBM Spectrum Protect controla la biblioteca pasando los mandatos SCSI a la biblioteca mediante el servidor de archivos NAS.

#### ACSLs

Una biblioteca ACSLS (software de biblioteca del sistema de cartuchos automatizados) puede conectarse directamente solo al servidor de IBM Spectrum Protect. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud de biblioteca a través de TCP/IP al servidor de control de la biblioteca.

Restricción: El servidor de IBM Spectrum Protect no incluye soporte de biblioteca externa para la biblioteca ACSLS cuando la biblioteca se utiliza para las operaciones NDMP.

#### VTL

Una biblioteca virtual de cintas (VTL) se puede conectar directamente al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Una biblioteca virtual de cintas es esencialmente igual que una biblioteca SCSI, pero mejorada para las características de biblioteca virtual de cintas y con un mejor rendimiento de montaje.

Si está definiendo una VTL, el entorno no puede incluir medios combinados. Las vías de acceso deben estar definidas entre todas las unidades de la biblioteca y todos los servidores definidos incluidos los agentes de almacenamiento que utiliza la biblioteca. Si no se cumplen estas condiciones, el rendimiento general puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad.

#### 349X

Una biblioteca 349X se puede conectar directamente al servidor de IBM Spectrum Protect. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud de biblioteca a través de TCP/IP al gestor de biblioteca.

Compartición de biblioteca: El servidor IBM Spectrum Protect que realiza operaciones NDMP puede ser un gestor de biblioteca, tanto para una biblioteca ACSLS, SCSI, VTL o para una biblioteca 349X, pero no puede ser un cliente de biblioteca. El servidor de IBM Spectrum Protect también puede ser un cliente de biblioteca, en una configuración en la que el servidor de archivos NAS envía datos al servidor mediante TCP/IP, en lugar de a una biblioteca de cintas conectada al servidor de archivos. Si la ejecución de las operaciones de NDMP en el servidor de IBM Spectrum Protect que es un gestor de biblioteca, el servidor de biblioteca que debe controlar directamente y no mediante mandatos pasados a través de un servidor de archivos NAS.

### Unidades de cintas

Una unidad de cintas sólo es necesaria para realizar una copia de seguridad en un dispositivo NAS conectado localmente. El servidor de archivos NAS debe poder acceder a las unidades. Una biblioteca de dispositivos distintos no admite un dispositivo NAS. El servidor de archivos NAS y el sistema operativo deben admitir las unidades para operaciones de copia de seguridad. Para obtener soporte completo de dispositivos para NDMP, consulte la documentación del producto del servidor de archivos NAS.

Compartición de unidades: El servidor de IBM Spectrum Protect y uno o más servidores de archivos NAS pueden compartir unidades de cintas. Asimismo, cuando se conecta una biblioteca SCSI, VTL o 349X al servidor y no al servidor de archivos NAS, las unidades se pueden compartir entre uno o varios servidores de archivos NAS: Las unidades también se pueden compartir por uno o varios clientes de almacenamiento y clientes de biblioteca de IBM Spectrum Protect.

Reservas de unidad: Cuando las unidades de cintas se conectan a dispositivos NAS y se especifica el parámetro RESETPDRIVES=YES para el mandato DEFINE LIBRARY, se aplican las siguientes limitaciones:

- Si un servidor IBM Spectrum Protect y un dispositivo NAS comparten una unidad de cintas, la preferencia de reserva de unidad se soporta cuando el dispositivo NAS soporta la reserva persistente y está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
- Si una unidad está conectada únicamente a un dispositivo NAS y no se comparte con un servidor de IBM Spectrum Protect, no se admite la preferencia de reserva de unidad. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

Consulte con los fabricantes de hardware la compatibilidad de combinaciones específicas de un servidor de archivos NAS con dispositivos de cintas y dispositivos con conexión a la SAN.

Consejo: IBM Spectrum Protect admite NDMP Versión 4 para todas las operaciones NDMP. IBM Spectrum Protect sigue siendo compatible con todas las copias de seguridad NDMP y las operaciones de restauración con un dispositivo NAS que ejecuta NDMP con versión 3. El servidor de IBM Spectrum Protect negocia el nivel de protocolo superior (bien la versión 3 o la versión 4) con el servidor NDMP cuando establece una conexión NDMP. Si experimenta problemas con la versión 4 es posible que desee utilizar la versión 3.

- Interfaces para operaciones NDMP  
Puede usar diversas interfaces para ejecutar operaciones NDMP. Para planificar una operación NDMP, utilice el mandato BACKUP NODE o RESTORE NODE y cree una planificación para procesar el mandato.
- Formatos de datos para operaciones de copia de seguridad NDMP  
Los datos que se copian utilizando NDMP no tienen el mismo formato que los datos que se utilizan para las operaciones de copia de seguridad de IBM Spectrum Protect típicas. El servidor de archivos NAS controla el formato de los datos de copia de seguridad.

## Interfaces para operaciones NDMP

---

Puede usar diversas interfaces para ejecutar operaciones NDMP. Para planificar una operación NDMP, utilice el mandato BACKUP NODE o RESTORE NODE y cree una planificación para procesar el mandato.

Interfaces de cliente:

- Cliente de línea de mandatos de copia de seguridad/archivado (en un sistema Windows, AIX de 64 bits u Oracle Solaris de 64 bits)
- Cliente Web

Interfaces de servidor:

- Consola del servidor
- Línea de mandatos en el cliente de administración  
Consejo: Todos los ejemplos de las operaciones NDMP utilizan mandatos de servidor.

La interfaz de cliente web de IBM Spectrum Protect, disponible con el cliente de copia de seguridad/archivado, muestra gráficamente los sistemas de archivos del servidor de archivos NAS. La función de cliente no es necesaria, pero puede utilizar las interfaces de cliente para operaciones NDMP. La función de cliente es el método preferido para las operaciones de restauración de nivel de archivo. Para obtener más información acerca de las operaciones de restauración, consulte Copia de seguridad y restauración en nivel de archivo para operaciones NDMP.

IBM Spectrum Protect le solicitará un ID de administrador y una contraseña cuando realice funciones NDMP a través de cualquiera de las dos interfaces de cliente. Para obtener más información sobre la instalación y la activación de interfaces de cliente, consulte Instalación de los clientes de copia de seguridad y archivado de IBM Spectrum Protect.

Para poder utilizar el cliente de copia de seguridad/archivado o el cliente web de IBM Spectrum Protect con el fin de realizar operaciones NAS, los nombres del sistema de archivos en el dispositivo NAS deben incorporar una barra inclinada (/) como primer carácter. Esta restricción no afecta a las operaciones NAS que se hayan iniciado desde la línea de mandatos del servidor de IBM Spectrum Protect.

## Formatos de datos para operaciones de copia de seguridad NDMP

---

Los datos que se copian utilizando NDMP no tienen el mismo formato que los datos que se utilizan para las operaciones de copia de seguridad de IBM Spectrum Protect típicas. El servidor de archivos NAS controla el formato de los datos de copia de seguridad.

Los datos que se han copiado en una biblioteca que está directamente conectada al servidor de archivos deben direccionarse a una agrupación de almacenamiento con el formato de datos adecuado. Cuando define una agrupación de almacenamiento para operaciones NDMP, especifique uno de los siguientes formatos de datos:

- NETAPPDUMP, si el servidor de archivos NAS es un dispositivo NetApp o un dispositivo IBM® System Storage de serie N.
- CELERRADUMP, si el servidor de archivos de NAS es un dispositivo EMC Celerra.
- NDMPDUMP para los demás dispositivos.

Los datos que se copian a través de la red en la jerarquía de IBM Spectrum Protect local pueden direccionarse a cualquier agrupación de almacenamiento primario de acceso aleatorio o acceso secuencial. No obstante, el formato de los datos no cambia.

## Gestión de operaciones NDMP

---

Existen diversas actividades de administrador para las operaciones NDMP.

- Gestión de los nodos del servidor de archivos NAS  
Puede consultar, actualizar, renombrar y eliminar nodos de servidor de archivos NAS.
- Gestión de los transportadores de datos utilizados en las operaciones NDMP  
Puede consultar, actualizar y suprimir los transportadores de datos que defina para servidores de archivos NAS.
- Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP  
Si ya utiliza una unidad para operaciones IBM Spectrum Protect, puede dedicar dicha unidad para operaciones NDMP.
- Gestión de agrupaciones de almacenamiento para operaciones NDMP  
Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales.
- Gestión de tablas de contenido  
Puede utilizar diversos mandatos para gestionar diferentes aspectos de sus contenidos de datos.
- Impedir que se cierren las conexiones NDMP de larga ejecución inactivas  
Para impedir que los cortafuegos cierren las conexiones NDMP que son de larga ejecución pero están inactivas, puede habilitar el estado activo de TCP (protocolo de control de transmisiones) en las conexiones de control NDMP.

## Gestión de los nodos del servidor de archivos NAS

---

Puede consultar, actualizar, renombrar y eliminar nodos de servidor de archivos NAS.

### Procedimiento

---

Utilice uno de los siguientes mandatos para gestionar los nodos del servidor de archivos NAS:

mandato	Procedimiento
<b>QUERY NODE</b>	Para consultar un nodo, emita el mandato QUERY NODE con los parámetros adecuados. Por ejemplo, si desea consultar el nodo NAS NASNODE1, emita el siguiente mandato:  <code>query node nasnode1 type=nas</code>
<b>UPDATE NODE</b>	Para actualizar un nodo, emita el mandato UPDATE NODE con los parámetros adecuados. Por ejemplo, si ha creado un nuevo dominio de políticas denominado NASDOMAIN para nodos NAS y desea actualizar el nodo NASNODE1 para incluirlo en el nuevo dominio, emita el siguiente mandato:  <code>update node nasnode1 domain=nasdomain</code>



mandato	Procedimiento
<b>RENAME NODE</b>	<p>Para cambiar el nombre de un nodo NAS, también debe cambiar el nombre del transportador de datos NAS correspondiente; ambos deben tener el mismo nombre.</p> <p>Por ejemplo, para cambiar el nombre NASNODE1 por NAS1, realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>1. Suprima todas las vías de acceso entre el transportador de datos NASNODE1 y las bibliotecas, así como entre el transportador de datos y NASNODE1 y las unidades.</li> <li>2. Suprima el transportador de datos definido para el nodo NAS.</li> <li>3. Para cambiar el nombre NASNODE1 por NAS1, emita el mandato siguiente: <pre>rename node nasnode1 nas1</pre> </li> <li>4. Defina el transportador de datos mediante el nuevo nombre de nodo. En este ejemplo, debe definir un nuevo transportador de datos llamado NAS1 con los mismos parámetros utilizados para definir NASNODE1. <p>Importante: Cuando defina un nuevo transportador de datos para un nodo cuyo nombre ha cambiado, asegúrese de que el nombre del transportador de datos coincida con el nuevo nombre de nodo. Y, además asegúrese de que los parámetros del nuevo transportador de datos sean duplicados de los parámetros del transportador de datos original. Si existen discrepancias entre un nombre de nodo y un nombre de transportador de datos o entre los parámetros del nuevo transportador de datos y los parámetros del transportador de datos original, es posible que no pueda establecer una sesión con el servidor de archivos NAS.</p> </li> <li>5. Para las bibliotecas SCSI o 349X, defina una vía de acceso entre el transportador de datos NAS y una biblioteca sólo si la biblioteca de cintas está conectada física y directamente al servidor de archivos NAS.</li> <li>6. Defina vías de acceso entre el transportador de datos NAS y las unidades utilizadas para operaciones NDMP.</li> </ol>
<b>REMOVE NODE</b>	<p>Para eliminar un nodo, siga estos pasos:</p> <ol style="list-style-type: none"> <li>1. Suprima las definiciones de espacios de archivos virtuales del nodo.</li> <li>2. Suprima todas las vías de acceso entre el transportador de datos y las bibliotecas, así como entre el transportador de datos y las unidades.</li> <li>3. Suprima el nodo. Por ejemplo, si desea eliminar un nodo denominado NAS1, emita el siguiente mandato: <pre>remove node nas1</pre> </li> </ol>

**Referencia relacionada:**

- QUERY NODE (Consultar nodos)
- UPDATE NODE (Actualizar atributos del nodo)
- RENAME NODE (Cambiar el nombre de un nodo)
- REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)

## Gestión de los transportadores de datos utilizados en las operaciones NDMP

Puede consultar, actualizar y suprimir los transportadores de datos que defina para servidores de archivos NAS.

### Procedimiento

Utilice uno de los mandatos siguientes para gestionar los transportadores de datos:

Mandato	Procedimiento
<b>QUERY DATAMOVER</b>	Para consultar un transportador de datos, emita el mandato QUERY DATAMOVER con los parámetros adecuados. Por ejemplo, si desea consultar el transportador de datos NASNODE1, emita el siguiente mandato:  <code>query datamover nasnode1</code>
<b>UPDATE DATAMOVER</b>	Para actualizar un transportador de datos, emita el mandato UPDATE DATAMOVER con los parámetros adecuados. Por ejemplo, si cierra un servidor de archivos NAS para realizar tareas de mantenimiento y desea poner el transportador de datos fuera de línea, emita el siguiente mandato:  <code>update datamover nasnode1 online=no</code>
<b>DELETE DATAMOVER</b>	Para suprimir un transportador de datos, emita el mandato DELETE DATAMOVER. Por ejemplo, si desea suprimir el transportador de datos NASNODE1, emita el siguiente mandato:  <code>delete datamover nasnode1</code>  Restricción: Si el transportador de datos tiene una vía de acceso a una biblioteca y suprime o desactiva el transportador de datos, imposibilitará el acceso a la biblioteca.

**Referencia relacionada:**

QUERY DATAMOVER (visualizar definiciones de un transportador de datos)

UPDATE DATAMOVER (Actualizar un transportador de datos)

DELETE DATAMOVER (Suprimir un transportador de datos)

## Dedicar una unidad de IBM Spectrum Protect a operaciones NDMP

Si ya utiliza una unidad para operaciones IBM Spectrum Protect, puede dedicar dicha unidad para operaciones NDMP.

### Procedimiento

Elimine el acceso al servidor de IBM Spectrum Protect suprimiendo la definición de vía de acceso. Por ejemplo, si el nombre de servidor es SERVER1 y la unidad es NASDRIVE1, emita el siguiente mandato:

```
delete path server1 nasdrive1 srctype=server desttype=drive library=naslib
```

## Gestión de agrupaciones de almacenamiento para operaciones NDMP

Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales.

Se aplican las siguientes directrices y restricciones a las agrupaciones de almacenamiento de tipo NETAPPDUMP, CELERRADUMP, y NDMPDUMP generadas por las operaciones NDMP:

- Puede consultar y actualizar agrupaciones de almacenamiento, pero no puede actualizar el parámetro DATAFORMAT.
- No es posible designar una agrupación de almacenamiento CENTERA, de contenedor de directorios o de contenedor en la nube como agrupación de destino de operaciones NDMP.
- Se recomienda mantener agrupaciones de almacenamiento separadas para datos de proveedores de NAS diferentes, aunque el formato de datos de ambos sea NDMPDUMP.
- Los siguientes parámetros de mandato DEFINE STGPOOL y UPDATE STGPOOL se pasan por alto puesto que no se admiten jerarquías de agrupaciones de almacenamiento ni operaciones de reclamación o migración para estas agrupaciones de almacenamiento:
  - MAXSIZE
  - NEXTSTGPOOL
  - LOWMIG
  - HIGHMIG
  - MIGDELAY
  - MIGCONTINUE

- RECLAIMSTGPOOL
- OVFLLOCATION

Importante: Asegúrese de que no utiliza de forma accidental agrupaciones de almacenamiento definidas para operaciones NDMP en operaciones de IBM Spectrum Protect tradicionales. Sea especialmente precavido cuando asigne al nombre de agrupación de almacenamiento el valor del parámetro DESTINATION del mandato DEFINE COPYGROUP. Si el destino no es una agrupación de almacenamiento con el formato de datos adecuado, la operación de copia de seguridad fallará.

## Gestión de tablas de contenido

---

Puede utilizar diversos mandatos para gestionar diferentes aspectos de sus contenidos de datos.

### Acerca de esta tarea

---

El mandato SET TOCLOADRETENTION puede utilizarse para especificar el número aproximado de minutos que una tabla de contenido sin referencia permanecerá cargada en la base de datos de IBM Spectrum Protect. El valor de retención de TOC en el servidor de IBM Spectrum Protect determina cuánto tiempo se conservará una tabla de contenido cargada en la base de datos tras el último acceso a la información de la tabla de contenido.

Dado que la información de la tabla de contenido (TOC) se carga en tablas de bases de datos temporales, esta información se pierde si se detiene el servidor, aunque no haya transcurrido el período de retención de la tabla de contenido (TOC). Durante la instalación, el tiempo de retención se establece en 120 minutos. Utilice el mandato QUERY STATUS para ver el tiempo de retención de la tabla de contenido.

Emita el mandato QUERY NASBACKUP para visualizar información acerca de los objetos de imagen de sistema de archivos de los que se ha efectuado una copia de seguridad para un nodo NAS y un espacio de archivos específicos. Al emitir el mandato, puede visualizar todas las imágenes de copia de seguridad generadas por NDMP y si cada imagen tiene una TOC correspondiente.

Consejo: El servidor de IBM Spectrum Protect puede almacenar una copia de seguridad completa que exceda el número de versiones especificado si esa copia de seguridad completa tiene copias de seguridad diferenciales dependientes. Las copias de seguridad de NAS completas con copias de seguridad diferenciales dependientes se comportan igual que cualquier otro archivo base con subarchivos dependientes. Debido al tiempo de retención especificado en el valor RETEXTRA, la copia de seguridad completa de NAS no caducará y la versión se mostrará en la salida de un mandato QUERY NASBACKUP. Para obtener información sobre la configuración de las políticas de retención de datos, consulte el apartado Personalización de políticas.

Utilice el mandato QUERY TOC para visualizar archivos y directorios en una imagen de copia de seguridad generada por NDMP. Emitiendo el mandato de servidor QUERY TOC, puede visualizar todos los directorios y archivos de una única tabla de contenido (TOC) especificada. Se accederá a la tabla de contenido (TOC) especificada de una agrupación de almacenamiento cada vez que se emita el mandato QUERY TOC, ya que este mandato no carga la información de la tabla de contenido (TOC) en la base de datos de IBM Spectrum Protect. A continuación, utilice el mandato RESTORE NODE con el parámetro FILELIST para restaurar archivos individuales.

## Impedir que se cierren las conexiones NDMP de larga ejecución inactivas

---

Para impedir que los cortafuegos cierren las conexiones NDMP que son de larga ejecución pero están inactivas, puede habilitar el estado activo de TCP (protocolo de control de transmisiones) en las conexiones de control NDMP.

### Acerca de esta tarea

---

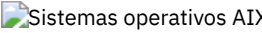
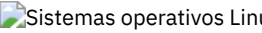
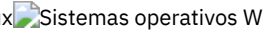
El servidor de IBM Spectrum Protect inicia las conexiones de control para dispositivos de NAS durante las operaciones NDMP de copia de seguridad o restauración. Estas conexiones de control pueden permanecer abiertas e inactivas durante un largo período de tiempo. Por ejemplo, supongamos que el mismo dispositivo NAS pone en marcha dos operaciones NDMP. La conexión de control para una operación NDMP puede permanecer abierta, pero inactiva, si la operación requiere un recurso, por ejemplo, una unidad de cintas o volumen secuencial, que está siendo utilizado por la otra operación NDMP.

Algún software de cortafuegos se configura para cerrar automáticamente conexiones de red que llevan inactivas un período específico de tiempo. Si existe un cortafuegos entre un servidor de IBM Spectrum Protect y un dispositivo NAS, es posible que el cortafuegos pueda cerrar las conexiones de control NDMP inesperadamente y provocar que la operación NDMP falle.

El servidor de IBM Spectrum Protect proporciona un mecanismo, el estado activo de TCP, que se puede habilitar para impedir que las conexiones de larga ejecución inactivas se cierren. Si el estado activo de TCP está habilitado, los paquetes pequeños se envían a través de la red, a intervalos predefinidos, al socio de conexión.

Restricción: Para evitar errores, no habilite el estado activo TCP en determinados tipos de entornos. Un ejemplo son los entornos en los que no existen cortafuegos entre el servidor de IBM Spectrum Protect y un dispositivo NAS. Otro ejemplo son los entornos con cortafuegos que toleran conexiones inactivas de larga ejecución. Habilitar el estado activo de TCP en este tipo de entornos puede

causar que una conexión inactiva se cierre por error si el socio de conexión no responde temporalmente a los paquetes de estado activo de TCP.

- **Habilitar el estado activo de TCP**  
Para habilitar el estado activo de TCP, que mantiene abiertas las conexiones NDMP, utilice la opción de servidor NDMPENABLEKEEPALIVE.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Windows** Especificar tiempo de inactividad de conexión para el estado activo de TCP  
Para especificar el período de tiempo de inactividad de la conexión, en minutos, antes de que se envíe el primer paquete de estado activo de TCP, utilice la opción del servidor NDMPKEEPIDLEMINUTES.

## Habilitar el estado activo de TCP

---

Para habilitar el estado activo de TCP, que mantiene abiertas las conexiones NDMP, utilice la opción de servidor NDMPENABLEKEEPALIVE.

### Procedimiento

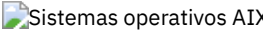
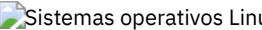
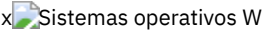
---

Agregue la opción al archivo de opciones del servidor dsmserv.opt:

```
ndmpenablekeepalive yes
```

**Referencia relacionada:**

NDMPENABLEKEEPALIVE

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Windows**

## Especificar tiempo de inactividad de conexión para el estado activo de TCP

---

Para especificar el período de tiempo de inactividad de la conexión, en minutos, antes de que se envíe el primer paquete de estado activo de TCP, utilice la opción del servidor NDMPKEEPIDLEMINUTES.

### Procedimiento

---

Agregue la opción al archivo de opciones del servidor dsmserv.opt:

```
ndmpkeepidleminutes minutes
```

**Referencia relacionada:**

NDMPKEEPIDLEMINUTES

## Configuración de IBM Spectrum Protect para operaciones NDMP

---

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad y recuperar datos en los servidores de archivos NAS utilizando NDMP. El procedimiento de configuración varía dependiendo de si tiene previsto realizar una copia de seguridad de los datos desde un servidor de archivos NAS en clúster o no de clúster.

- **Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster**  
Antes de configurar IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster, registre la licencia necesaria.
- **Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno en clúster de NetApp**  
Puede realizar una copia de seguridad de los datos de un clúster de NetApp en un dispositivo de cinta conectado directamente o en servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Puede realizar una copia de seguridad del clúster completo en un único nodo de IBM Spectrum Protect o de partes del clúster en varios nodos.

## Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster

---



Antes de configurar IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster, registre la licencia necesaria.


### Procedimiento

---

1. Configure la biblioteca de cintas y los medios. Consulte el apartado Configuración de una biblioteca de cintas para operaciones NDMP, donde los pasos siguientes se describen con más información.

- a. Conecte la SCSI o la biblioteca virtual de cintas (VTL) al servidor de archivos de NAS o al servidor de IBM Spectrum Protect, o conecte la biblioteca ACSLS o la biblioteca 349X al servidor de IBM Spectrum Protect.
  - b. Defina la biblioteca con un tipo de biblioteca SCSI, VTL, ACSLS o 349X.
  - c. Defina una clase de dispositivo para unidades de cintas.
  - d. Defina una agrupación de almacenamiento para medios de copia de seguridad NAS.
  - e. Opcional: Defina una agrupación de almacenamiento para almacenar una tabla de contenido.
2. Configure la política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Consulte el apartado Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
  3. Registre un nodo de servidor de archivos NAS con el servidor de IBM Spectrum Protect. Consulte el apartado Registro de nodos NAS con el servidor de IBM Spectrum Protect.
  4. Defina un transportador de datos para el servidor de archivos NAS. Consulte el apartado Definición de un transportador de datos para un servidor de archivos de NAS.
  5. Defina una vía de acceso desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS a la biblioteca. Consulte el apartado Definición de vías de acceso a bibliotecas para operaciones NDMP.
  6. Defina las unidades de cintas en IBM Spectrum Protect y defina las vías de acceso a dichas unidades desde el servidor de archivos NAS y, opcionalmente, desde el servidor de IBM Spectrum Protect. Consulte el apartado Definición de vías de acceso para operaciones NDMP.
  7. Dé de alta las cintas en la biblioteca y etiquételas.

 Sistemas operativos AIX  Sistemas operativos Linux Los volúmenes de cinta deben estar etiquetados antes de que el servidor pueda utilizarlos. Puede utilizar el mandato LABEL LIBVOLUME, o puede utilizar el parámetro AUTOLABEL con los mandatos DEFINE LIBRARY y UPDATE LIBRARY.

 Sistemas operativos Windows Todos los medios deben estar etiquetados. El etiquetado de medios con una biblioteca automatizada requiere que los medios se den de alta en la biblioteca. Para etiquetar volúmenes con el mandato LABEL LIBVOLUME, especifique el parámetro CHECKIN. Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los mandatos DEFINE LIBRARY y UPDATE LIBRARY.

Para obtener instrucciones, consulte LABEL LIBVOLUME, DEFINE LIBRARY y UPDATE LIBRARY.

8. Opcional: Configure las copias de seguridad planificadas para servidores de archivos NAS. Consulte el apartado Planificación de operaciones NDMP.
  9. Opcional: Defina un nombre del espacio de archivos virtual. Consulte el apartado Definición de espacios de archivos virtuales.
  10. Opcional: Configure la copia de cinta a cinta para que realice la copia de seguridad de los datos. Consulte el apartado Copia de seguridad de datos mediante la función de cinta a cinta.
  11. Opcional: Configure la copia de cinta a cinta para que traspase los datos a otra tecnología de cinta. Consulte el apartado Traslado de datos con la función de copia de cinta a cinta.
- Configuración de una política de IBM Spectrum Protect para operaciones NDMP  
Con las políticas, puede gestionar el número y el período de retención de versiones de copia de seguridad de imágenes NDMP.
  - Bibliotecas y unidades de cintas para operaciones NDMP  
La mayor parte de la planificación necesaria para implementar operaciones de copia de seguridad y recuperación que utilizan NDMP está relacionada con la configuración de los dispositivos. Puede elegir cómo conectar las bibliotecas y las unidades.
  - Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS  
Si tiene previsto realizar una copia de seguridad de datos de NAS en una biblioteca directamente conectada al dispositivo NAS y utilizar una biblioteca de cintas SCSI, debe determinar dónde se debe conectar la biblioteca.
  - Registro de nodos NAS con el servidor de IBM Spectrum Protect  
Registre el servidor de archivos NAS como nodo de IBM Spectrum Protect, especificando TYPE=NAS. Este nombre de nodo sirve para realizar un seguimiento de las copias de seguridad de imagen para el servidor de archivos NAS.
  - Definición de un transportador de datos para un servidor de archivos de NAS  
Defina un transportador de datos para cada servidor de archivos NAS utilizando las operaciones NDMP en el entorno. El nombre del transportador de datos debe coincidir con el nombre de nodo especificado al inscribir el nodo NAS en el servidor de IBM Spectrum Protect.
  - Definición de vías de acceso para operaciones NDMP  
Para operaciones NDMP, se crean vías de acceso a unidades y a bibliotecas.
  - Planificación de operaciones NDMP  
Puede programar operaciones de copia de seguridad o restauración de las imágenes generadas por las operaciones NDMP. Utilice las planificaciones de administración que procesan los mandatos de administración BACKUP NODE o RESTORE NODE.
  - Definición de espacios de archivos virtuales  
Utilice una definición de espacio de archivos virtual para realizar copias de seguridad a nivel de directorios NAS. Para reducir el tiempo de copia de seguridad y restauración para sistemas de archivos grandes, correlacione una vía de acceso de directorios desde un servidor de archivos de NAS a un nombre del espacio de archivos virtual en el servidor de IBM Spectrum Protect.
  - Copia de seguridad de datos mediante la función de cinta a cinta  
Cuando utilice la función de cinta a cinta de NDMP para realizar la copia de seguridad de los datos, el tipo de biblioteca puede ser SCSI, 349X o ACSLS (software de biblioteca del sistema de cartuchos automatizados). Las unidades se pueden compartir entre los dispositivos NAS y el servidor de IBM Spectrum Protect.

- Traslado de datos con la función de copia de cinta a cinta  
Para traspasar datos de una tecnología de cinta antigua a otra nueva mediante la operación de copia de cinta a cinta de NDMP, debe realizar los pasos de configuración habituales, así como otros adicionales.

## Configuración de una política de IBM Spectrum Protect para operaciones NDMP

---

Con las políticas, puede gestionar el número y el período de retención de versiones de copia de seguridad de imágenes NDMP.

### Acerca de esta tarea

---

Para obtener más información, consulte el apartado Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect.

### Procedimiento

---

Complete los pasos siguientes para configurar una política para operaciones NDMP:

1. Cree un dominio de políticas para servidores de archivos NAS (almacenamiento adjunto de red). Por ejemplo, para definir un dominio de políticas con el nombre NASDOMAIN, especifique el mandato siguiente:

```
define domain nasdomain description='Dominio de políticas para servidores de
archivos NAS'
```

2. Cree un juego de políticas en ese dominio. Por ejemplo, para definir un conjunto de políticas denominado STANDARD en el dominio de políticas denominado NASDOMAIN, emita el siguiente mandato:

```
define policyset nasdomain standard
```

3. Defina una clase de gestión y, a continuación, asígnela como clase de gestión predeterminada para el juego de políticas. Por ejemplo, para definir una clase de gestión denominada MC1 en el conjunto de políticas STANDARD y asignarla como clase predeterminada, especifique los mandatos siguientes:

```
define mgmtclass nasdomain standard mc1
assign defmgmtclass nasdomain standard mc1
```

4. Defina un grupo de copia de seguridad en la clase de gestión predeterminada. El destino debe ser la agrupación de almacenamiento creada para las imágenes de copia de seguridad generadas por las operaciones NDMP. Asimismo, puede especificar el número de versiones de copia de seguridad que se deben retener. Por ejemplo, para definir un grupo de copia de seguridad para la clase de gestión MC1, en la que se retienen hasta cuatro versiones de cada sistema de archivos en la agrupación de almacenamiento NASPOOL, emita el mandato siguiente:

```
define copygroup nasdomain standard mc1 destination=naspool verexists=4
```

Si desea crear una tabla de contenido para las copias de seguridad, el parámetro TOCDESTINATION del grupo de copias debe contener el nombre de la agrupación de almacenamiento primario.

```
define copygroup nasdomain standard mc1 destination=naspool
tocdestination=tocpool verexists=4
```

Importante: Cuando define un grupo de copias para una clase de gestión en el que se encontrará una imagen de sistema de archivos producida por NDMP, asegúrese de que el parámetro DESTINATION especifique el nombre de una agrupación de almacenamiento que se haya definido para las operaciones NDMP. Si el parámetro DESTINATION especifica una agrupación de almacenamiento no válida, las copias de seguridad realizadas mediante NDMP fallan.

5. Active el juego de políticas. Por ejemplo, para activar el juego de políticas STANDARD en el dominio de políticas NASDOMAIN, emita el siguiente mandato:

```
activate policyset nasdomain standard
```

El juego de políticas está listo para utilizarlo. Los nodos se asocian a una política cuando se registran. Para obtener más información, consulte el apartado Registro de nodos NAS con el servidor de IBM Spectrum Protect.

- Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect  
Puede registrar un servidor de archivos NAS (almacenamiento adjunto de red) como un nodo utilizando operaciones NDMP (Protocolo de gestión de datos de redes). Con el control del servidor de IBM Spectrum Protect, el servidor de archivos NAS realiza copias de seguridad y restaura imágenes de sistemas de archivos y de directorios en una biblioteca de cintas.

- Políticas para copias de seguridad iniciadas con la interfaz de cliente  
Cuando un cliente inicia una copia de seguridad, el archivo de opciones de ese nodo de cliente influye en la política.
- Determinación de la ubicación de copia de seguridad NAS  
Cuando IBM Spectrum Protect utiliza NDMP para proteger servidores de archivos NAS, el servidor de IBM Spectrum Protect controla las operaciones. Durante este tiempo, el servidor de archivos NAS transfiere los datos a una biblioteca conectada o directamente al servidor de IBM Spectrum Protect.

## Políticas para copias de seguridad iniciadas con un servidor de IBM Spectrum Protect

---

Puede registrar un servidor de archivos NAS (almacenamiento adjunto de red) como un nodo utilizando operaciones NDMP (Protocolo de gestión de datos de redes). Con el control del servidor de IBM Spectrum Protect, el servidor de archivos NAS realiza copias de seguridad y restaura imágenes de sistemas de archivos y de directorios en una biblioteca de cintas.

El servidor de IBM Spectrum Protect inicia la copia de seguridad, asigna una unidad y selecciona y monta los medios. A continuación, el servidor de archivos NAS transfiere los datos a la cinta.

Puesto que el servidor de archivos NAS realiza una copia de seguridad de los datos, estos se almacenan en su propio formato. Para la mayoría de los servidores NAS, los datos se almacenan en formato de datos NDMPDUMP. En los servidores de archivos NetApp, los datos se almacenan en el formato de datos NETAPPDUMP. En el caso de los servidores de archivos EMC, los datos se almacenan con el formato de datos CELERRADUMP. Para gestionar copias de seguridad de imagen del servidor de archivos NAS; los grupos de copia para los nodos NAS deben hacer referencia a una agrupación de almacenamiento que tenga un formato de datos NDMPDUMP, NETAPPDUMP o CELERRADUMP.

Los siguientes atributos de grupo de copia de seguridad se pasan por alto para imágenes NAS:

- Frecuencia
- Modalidad
- Retener única versión
- Serialización
- Versiones si datos suprimidos

Para configurar la política necesaria para los nodos NAS, puede definir un dominio de políticas nuevo y separado.

Cuando el servidor de IBM Spectrum Protect crea una tabla de contenido, puede ver un conjunto de archivos y directorios individuales cuya copia de seguridad se ha realizado mediante NDMP. A continuación, puede seleccionar los archivos y directorios que desea restaurar. Para establecer adónde se enviarán los datos y almacenar la tabla de contenidos, establezca la política de la forma siguiente:

- Asegúrese de que los datos de copia de seguridad de imagen se envían a una agrupación de almacenamiento con un formato NDMPDUMP, NETAPPDUMP o CELERRADUMP.
- Asegúrese de que la tabla de contenidos se envíe a una agrupación de almacenamiento con el formato NATIVE o NONBLOCK.

## Políticas para copias de seguridad iniciadas con la interfaz de cliente

---

Cuando un cliente inicia una copia de seguridad, el archivo de opciones de ese nodo de cliente influye en la política.

Puede controlar las clases de gestión que se aplican a las imágenes de copia de seguridad generadas por las operaciones NDMP (Protocolo de gestión de datos de redes) independientemente del nodo que inicia la copia de seguridad. Puede completar esta tarea creando un conjunto de opciones para que lo utilicen los nodos cliente. El conjunto de opciones puede incluir una sentencia `include.fs.nas` para especificar la clase de gestión para las copias de seguridad del servidor de archivos NAS (almacenamiento adjunto de red).

Consejo: Puede definir un conjunto de opciones utilizando el mandato DEFINE CLOPTSET. A continuación, añada una opción de cliente al conjunto de opciones utilizando el mandato DEFINE CLIENTOPT. Puede asignar un conjunto de opciones a un cliente completando los pasos siguientes:

1. Abra la página Descripción general del Centro de operaciones y haga clic en Clientes.
2. Efectúe una doble pulsación en el cliente y haga clic en Propiedades.
3. En el campo Conjunto de opciones, seleccione un conjunto de opciones y haga clic en Guardar.

Para obtener instrucciones sobre cómo utilizar el mandato DEFINE CLOPTSET, consulte DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente). Para obtener instrucciones sobre cómo utilizar el mandato DEFINE CLIENTOPT, consulte DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones).

## Determinación de la ubicación de copia de seguridad NAS

Cuando IBM Spectrum Protect utiliza NDMP para proteger servidores de archivos NAS, el servidor de IBM Spectrum Protect controla las operaciones. Durante este tiempo, el servidor de archivos NAS transfiere los datos a una biblioteca conectada o directamente al servidor de IBM Spectrum Protect.

También puede utilizar un cliente de copia de seguridad/archivado para realizar la copia de seguridad de un servidor de archivos NAS montando el sistema de archivos NAS en la máquina cliente y realizando la copia de seguridad de la forma usual. Puede utilizar un montaje de sistema de archivos de red (NFS) o una correlación de sistema de archivos de Internet común (CIFS).

Para obtener una descripción de los métodos de copia de seguridad y restauración, consulte Tabla 1.

Consejo: Puede utilizar un único método o una combinación de métodos en su entorno de almacenamiento individual.

Tabla 1. Comparación de métodos de copia de seguridad de los datos NDMP

Propiedad	NDMP: de servidor de archivos a servidor	NDMP: de servidor de archivos a biblioteca conectada	De cliente de copia de seguridad/archivado a servidor
Tráfico de datos en la red	Todos los datos de la copia de seguridad se desplazan por la LAN desde el servidor de archivos NAS hasta el servidor.	El servidor controla remotamente las operaciones, aunque el dispositivo NAS traspasa los datos de forma local.	Todos los datos de copia de seguridad se desplazan por la LAN desde el dispositivo NAS hasta el cliente y desde éste hasta el servidor.
Proceso del servidor de archivos durante la copia de seguridad	Se precisan menos procesos de servidor de archivos, en comparación con el método de cliente de copia de seguridad/archivado, ya que la copia de seguridad no utiliza protocolos de acceso a archivos, como NFS y CIFS.	Se precisan menos procesos de servidor de archivos, en comparación con el método de cliente de copia de seguridad/archivado, ya que la copia de seguridad no utiliza protocolos de acceso a archivos, como NFS y CIFS.	Las operaciones de copia de seguridad de archivos requieren más recursos de proceso de servidor para protocolos de acceso a archivos, como NFS y CIFS.
Distancia entre dispositivos	El servidor de IBM Spectrum Protect debe encontrarse dentro del rango del canal de fibra o SCSI de la biblioteca de cintas.	El servidor de IBM Spectrum Protect puede estar alejado del servidor de archivos NAS y de la biblioteca de cintas.	El servidor de IBM Spectrum Protect debe encontrarse dentro del rango del canal de fibra o SCSI de la biblioteca de cintas.
Consideraciones acerca del cortafuegos	Más estricto que el método de archivador a biblioteca conectada porque las comunicaciones las puede iniciar el servidor de IBM Spectrum Protect o el servidor de archivos NAS.	Menos estricto que el método de archivador a servidor ya que sólo el servidor de IBM Spectrum Protect puede iniciar las comunicaciones.	Los datos y las contraseñas de cliente están cifradas.
Consideraciones de seguridad	Los datos se envían descifrados desde un servidor de archivos NAS a un servidor de IBM Spectrum Protect.	El método debe utilizarse en un entorno de confianza porque los números de puerto no son seguros.	La configuración del número de puerto permite efectuar sesiones de administración seguras en una red privada.
Carga en el servidor de IBM Spectrum Protect	Se necesita una carga de trabajo de CPU superior para gestionar todos los procesos de datos back-end (por ejemplo, migración).	La carga de trabajo de CPU se reduce porque ya no se admiten ni la migración ni la reclamación.	Se necesita una carga de trabajo de CPU superior para gestionar todos los procesos de datos back-end.
Copia de seguridad de las agrupaciones de almacenamiento primarias en las agrupaciones de almacenamiento de copia	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el formato de datos NATIVE.	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el mismo formato de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP).	La copia de seguridad de los datos sólo se puede realizar en las agrupaciones de almacenamiento de copia que tengan el formato de datos NATIVE.



Propiedad	NDMP: de servidor de archivos a servidor	NDMP: de servidor de archivos a biblioteca conectada	De cliente de copia de seguridad/archivado a servidor
Restauración de agrupaciones de almacenamiento primarias y volúmenes desde agrupaciones de almacenamiento de copia	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el formato de datos NATIVE.	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el mismo formato NDMP.	Los datos sólo se pueden restaurar en agrupaciones de almacenamiento y volúmenes que tengan el formato de datos NATIVE.
Traspaso de datos NDMP desde volúmenes de agrupaciones de almacenamiento	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene un formato de datos NATIVE.	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene el mismo formato de datos NDMP.	Los datos sólo se pueden traspasar a otra agrupación de almacenamiento si ésta tiene un formato de datos NATIVE.
Migración de una agrupación de almacenamiento primaria a otra	Permitido	No permitido	Permitido
Reclamación de una agrupación de almacenamiento	Permitido	No permitido	Permitido
Operaciones de grabación simultánea durante las copias de seguridad	No permitido	No permitido	Permitido
Operaciones de exportación e importación	No permitido	No permitido	Permitido
Generación de juegos de copias de seguridad	No permitido	No permitido	Permitido
Comprobación de redundancia cíclica (CRC) cuando los datos se traspasan empleando procesos de IBM Spectrum Protect	Permitido	No permitido	Permitido
Validación mediante mandatos de auditoría de IBM Spectrum Protect	Permitido	No permitido	Permitido
Gestor de recuperación ante siniestro	Permitido	Permitido	Permitido

## Bibliotecas y unidades de cintas para operaciones NDMP

La mayor parte de la planificación necesaria para implementar operaciones de copia de seguridad y recuperación que utilizan NDMP está relacionada con la configuración de los dispositivos. Puede elegir cómo conectar las bibliotecas y las unidades.

Muchas de las opciones de configuración para bibliotecas y unidades se determinan mediante las funciones de hardware de las bibliotecas. Puede configurar operaciones NDMP con bibliotecas y unidades no admitidas. Sin embargo, cuantas más funciones tenga la biblioteca, mayor será la flexibilidad de que dispondrá la implementación.

Puede empezar respondiendo a las preguntas siguientes:

- ¿Qué tipo de biblioteca (SCSI, ACSLS o 349X) utilizará?
- Si utiliza una biblioteca SCSI, ¿desea conectar robots de biblioteca de cintas al servidor de IBM Spectrum Protect o al servidor de archivos NAS (almacenamiento adjunto de red)?
- ¿Deseará trasladar los datos NDMP a cinta?
- ¿Cómo desea utilizar las unidades de cintas en la biblioteca?
  - Dedicará todas las unidades de cintas a operaciones NDMP.
  - Dedicará algunas unidades de cintas a operaciones NDMP y otras unidades a operaciones tradicionales de IBM Spectrum Protect.
  - Compartirá unidades de cintas entre operaciones NDMP y operaciones tradicionales de IBM Spectrum Protect.
- ¿Realizará la copia de seguridad de datos de cinta a cinta para las funciones de recuperación tras siniestro?
- ¿Enviará los datos de copia de seguridad a un único servidor de IBM Spectrum Protect en vez de conectar una biblioteca de cintas a cada dispositivo NAS?
- ¿Desea conservar todo el hardware en el servidor de IBM Spectrum Protect y enviar los datos NDMP por la LAN?

- Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS  
Se pueden utilizar unidades para varios fines debido a las configuraciones flexibles permitidas por IBM Spectrum Protect. Para operaciones NDMP, el servidor de archivos NAS debe tener acceso a la unidad. El servidor de IBM Spectrum Protect también puede tener acceso a la misma unidad, en función de las conexiones y limitaciones de hardware.
- Configuración de una biblioteca de cintas para operaciones NDMP  
Puede configurar una biblioteca de cintas para hacer copia de seguridad de un dispositivo de almacenamiento adjunto de red (NAS) a una cinta.

## Determinar la utilización de las unidades de la biblioteca al hacer copias de seguridad en bibliotecas conectadas a NAS

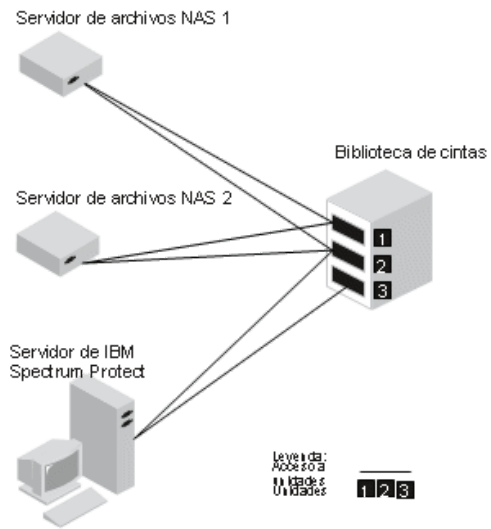
---

Se pueden utilizar unidades para varios fines debido a las configuraciones flexibles permitidas por IBM Spectrum Protect. Para operaciones NDMP, el servidor de archivos NAS debe tener acceso a la unidad. El servidor de IBM Spectrum Protect también puede tener acceso a la misma unidad, en función de las conexiones y limitaciones de hardware.

### Acerca de esta tarea

---

Todas las unidades se definen en el servidor de IBM Spectrum Protect. Sin embargo, se puede definir la misma unidad para las operaciones de IBM Spectrum Protect y las operaciones de NDMP tradicionales. En la Figura 1 se muestra una posible configuración. El servidor de IBM Spectrum Protect tiene acceso a las unidades 2 y 3, y cada servidor de archivos NAS tiene acceso a las unidades 1 y 2. Figura 1. Ejemplo de uso de la unidad de IBM Spectrum Protect



Para crear la configuración que se muestra en Figura 1, complete los pasos siguientes:

## Procedimiento

---

1. Defina las tres unidades en IBM Spectrum Protect.

2. Defina las vías de acceso desde el servidor de IBM Spectrum Protect a las unidades 2 y 3. Puesto que el servidor no accede a la unidad 1, no se define ninguna vía de acceso.
3. Defina cada servidor de archivos NAS como transportador de datos separado.
4. Defina vías de acceso desde cada transportador de datos a las unidades 1 y 2.

## Resultados

---

Para utilizar las operaciones de movimiento de datos de programa de fondo de IBM Spectrum Protect, el servidor de IBM Spectrum Protect necesita dos vías de acceso de unidad disponibles desde un único transportador de datos de NAS. Las unidades pueden estar en bibliotecas diferentes y tener tipos de dispositivos diferentes con soporte de NDMP. Puede realizar copias entre dos diferentes dispositivos de cinta. Por ejemplo, la unidad de cintas de origen puede ser una unidad DLT de una biblioteca y la unidad de destino puede ser una unidad LTO de otra biblioteca.

Durante los movimientos de datos de programa de fondo de IBM Spectrum Protect, el servidor de IBM Spectrum Protect localiza un transportador de datos de NAS que soporte el mismo formato de datos como el de los datos que se deben copiar y que tenga dos puntos de montaje disponibles y vías de acceso a las unidades. Si el servidor de IBM Spectrum Protect no puede localizar un transportador de datos de este tipo, la operación de traspaso de datos solicitada no se llevará a cabo. El número de puntos de montaje y unidades disponibles depende de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento que están implicadas en los movimientos de datos de programa de fondo.

Si la función de movimiento de datos de programa de fondo soporta multiproceso, cada movimiento de datos de programa de fondo de IBM Spectrum Protect simultáneo necesita dos puntos de montaje disponibles y dos unidades disponibles. Para ejecutar dos procesos de IBM Spectrum Protect simultáneamente, debe haber como mínimo cuatro puntos de montaje y cuatro unidades disponibles.

Para obtener más información, consulte Definición de vías de acceso para operaciones NDMP.

## Configuración de una biblioteca de cintas para operaciones NDMP

---

Puede configurar una biblioteca de cintas para hacer copia de seguridad de un dispositivo de almacenamiento adjunto de red (NAS) a una cinta.

## Procedimiento

---

Complete los siguientes pasos para configurar las bibliotecas de cintas para operaciones NDMP:

1. Conecte la biblioteca y las unidades que se van a utilizar para operaciones NDMP.
  - a. Conecte la biblioteca SCSI. Antes de configurar una biblioteca de cintas SCSI para operaciones NDMP, debe haber determinado si desea conectar el control robótico de la biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos de NAS. Consulte el apartado Bibliotecas y unidades de cintas para operaciones NDMP. Conecte el robot de la biblioteca de cintas SCSI al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Consulte la documentación del fabricante del dispositivo para obtener instrucciones.

Si la biblioteca está conectada a IBM Spectrum Protect, establezca una conexión SCSI o de canal de fibra entre el servidor de IBM Spectrum Protect y el puerto de control robótico de la biblioteca. A continuación, conecte el servidor de archivos de NAS a las unidades.

Si la biblioteca está conectada al servidor de archivos NAS, realice una conexión SCSI o de canal de fibra entre el servidor de archivos NAS y las unidades o la robótica de biblioteca.
  - b. Conecte la biblioteca ACSLS. Conecte la biblioteca de cintas ACSLS al servidor de IBM Spectrum Protect.
  - c. Conecte la biblioteca 349X. Conecte la biblioteca de cintas 349X al servidor de IBM Spectrum Protect.
2. Defina una biblioteca para los dispositivos de biblioteca emitiendo el mandato DEFINE LIBRARY. La biblioteca tiene que ser de un solo tipo de dispositivo, no de una mezcla de dispositivos. Emita uno de los mandatos siguientes para definir la biblioteca en función del tipo de dispositivo que esté configurando:

Biblioteca SCSI

```
define library tsmlib libtype=scsi
```

Biblioteca ACSLS

```
define library acslib libtype=acsls acsid=1
```

Biblioteca 349X

```
define library tsmlib libtype=349x
```

3. Defina una clase de dispositivo para el dispositivo NDMP emitiendo el mandato DEFINE DEVCLASS.

Consejo: Una clase de dispositivo que está definida con un tipo de dispositivo de NAS no está asociada explícitamente a un tipo de unidad específico, por ejemplo, LTO. Sin embargo, la práctica recomendada es definir una clase de dispositivo independiente para tipos de unidades diferentes.

En el mandato DEFINE DEVCLASS, utilice los siguientes parámetros y valores:

- Especifique DEVTYPE=NAS.
- Especifique MOUNTRETENTION=0. Es necesario para las operaciones NDMP.
- Especifique un valor para el parámetro ESTCAPACITY.

Por ejemplo, para definir una clase de dispositivo denominada NASCLASS para una biblioteca denominada NASLIB con una capacidad estimada de 40 GB para el soporte, emita el siguiente mandato:

```
define devclass nasclass devtype=nas library=naslib mountretention=0
  estcapacity=40g
```

4. Defina una agrupación de almacenamiento para soportes NDMP emitiendo el mandato DEFINE STGPOOL. Cuando se designa NETAPPDUMP, CELERRADUMP o NDMPDUMP como tipo de agrupación de almacenamiento, la gestión de las agrupaciones de almacenamiento generadas por operaciones de NDMP es diferente de la gestión de agrupaciones de almacenamiento que contienen medios para las copias de seguridad de IBM Spectrum Protect tradicionales. Las operaciones de IBM Spectrum Protect utilizan agrupaciones de almacenamiento definidas con un formato de datos NATIVE o NONBLOCK. Si selecciona NETAPPDUMP, CELERRADUMP o NDMPDUMP, las operaciones NDMP necesitarán agrupaciones de almacenamiento que dispongan de un formato de datos que coincida con el servidor de archivos de NAS y el método de copia de seguridad seleccionado. Se recomienda mantener agrupaciones de almacenamiento separadas para datos de proveedores de NAS diferentes, aunque el formato de datos de ambos sea NDMPDUMP. Por ejemplo, para definir una agrupación de almacenamiento denominada NDMPPool para un servidor de archivos que no sea un servidor de archivos Celerra o NetApp, emita el siguiente mandato:

```
define stgpool ndmppool nasclass maxscratch=10 dataformat=ndmpdump
```

Para definir una agrupación de almacenamiento denominada NASPOOL para un servidor de archivos NetApp, emita el siguiente mandato:

```
define stgpool naspool nasclass maxscratch=10 dataformat=netappdump
```

Para definir una agrupación de almacenamiento denominada CELERRAPOOL para un servidor de archivos EMC Celerra, emita el siguiente mandato:



```
define stgpool celerrapool nasclass maxscratch=10 dataformat=celerradump
```


Atención: Asegúrese de que en las operaciones tradicionales de IBM Spectrum Protect no utilizan por accidente agrupaciones de almacenamiento definidas para operaciones NDMP. Sea especialmente precavido cuando asigne al nombre de agrupación de almacenamiento el valor del parámetro DESTINATION del mandato DEFINE COPYGROUP. Si el destino no es una agrupación de almacenamiento con el formato de datos adecuado, la operación de copia de seguridad fallará.



5. Opcional: Defina una agrupación de almacenamiento para una tabla de contenido. Si tiene previsto crear una tabla de contenido, también debe definir una agrupación de almacenamiento en disco en la que almacenar la tabla de contenido. Debe configurar la política de modo que el servidor de IBM Spectrum Protect almacene la tabla de contenido en una agrupación de almacenamiento distinta de la empleada para almacenar la imagen de copia de seguridad. La tabla de contenido se maneja del mismo modo que cualquier otro objeto de esa agrupación de almacenamiento. Por ejemplo, para definir una agrupación de almacenamiento denominada TOCPool para una clase de dispositivo DISK, emita el siguiente mandato:

```
define stgpool tocpool disk
```

Posteriormente, defina volúmenes para la agrupación de almacenamiento.

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#) Para obtener más información sobre la definición de volúmenes, consulte [Configuración de volúmenes de acceso aleatorio en dispositivos de disco \(V7.1.1\)](#).

 [Sistemas operativos Windows](#) Para obtener más información sobre la definición de volúmenes, consulte [Configuración de volúmenes de acceso aleatorio en dispositivos de disco \(V7.1.1\)](#).

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#) Para obtener más información sobre la configuración de bibliotecas, consulte [Configuración de bibliotecas para su uso por parte de un servidor](#).

**Referencia relacionada:**

DEFINE DEVCLASS (Definir una clase de dispositivo)

## Conexión del robot de la biblioteca de cintas para las bibliotecas conectadas a NAS

Si tiene previsto realizar una copia de seguridad de datos de NAS en una biblioteca directamente conectada al dispositivo NAS y utilizar una biblioteca de cintas SCSI, debe determinar dónde se debe conectar la biblioteca.













## Acerca de esta tarea

Debe determinar si conectará el robot de biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos NAS. Independientemente de dónde conecte el robot de biblioteca, las unidades de cintas siempre deben estar conectadas al servidor de archivos NAS para operaciones NDMP.

Debe tener en cuenta la distancia y las conexiones de hardware disponibles para las bibliotecas SCSI. Si la biblioteca no tiene puertos separados para control robótico y acceso a las unidades, la biblioteca debe estar conectada al servidor de archivos NAS porque el servidor de archivos debe tener acceso a las unidades. Si la biblioteca SCSI tiene puertos separados para el control robótico y el acceso a las unidades, puede elegir conectar el robot de la biblioteca al servidor de IBM Spectrum Protect o al servidor de archivos NAS indistintamente. Si el servidor de archivos NAS tiene una ubicación diferente del servidor de IBM Spectrum Protect, la distancia puede significar que debe conectar la biblioteca al servidor de archivos NAS.

Tanto si utiliza una biblioteca SCSI, ACSLS o 349X, tiene la opción de dedicar la biblioteca a las operaciones NDMP o de utilizar la biblioteca para las operaciones NDMP. También puede utilizar la biblioteca para la mayoría de las operaciones tradicionales de IBM Spectrum Protect.

Tabla 1. Resumen de configuraciones para operaciones NDMP

Configuración	Distancia entre el servidor de IBM Spectrum Protect y la biblioteca	Compartición de biblioteca	Compartición de unidades entre IBM Spectrum Protect y el servidor de archivos NAS	Compartición de unidades entre servidores de archivos NAS	Compartición de unidades entre el agente de almacenamiento y el servidor de archivos NAS
Configuración 1 (biblioteca SCSI conectada al servidor de IBM Spectrum Protect)	Con límite de conexión SCSI o de canal de fibra	Permitido	Permitido	Permitido	Permitido
Configuración 2 (biblioteca SCSI conectada al servidor NAS)	Sin límite	No permitido	Permitido	Permitido	No permitido
Configuración 3 (biblioteca 349X)	Con posible límite de conexión 349X	Permitido	Permitido	Permitido	Permitido
 Sistemas operativos AIX  Sistemas operativos Windows Configuración 4 (biblioteca ACSLS)	 Sistemas operativos AIX  Sistemas operativos Windows Con posible límite de conexión ACSLS	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido	 Sistemas operativos AIX  Sistemas operativos Windows Permitido

- **Configuración 1:** biblioteca SCSI conectada al servidor de IBM Spectrum Protect  
En esta configuración, la biblioteca de cintas debe tener puertos separados para el control robótico y para el acceso a las unidades. Además, la biblioteca debe estar al alcance del canal de fibra o del bus SCSI tanto del servidor de IBM Spectrum Protect como del servidor de archivos NAS.
- **Configuración 2:** biblioteca SCSI conectada al servidor de archivos NAS  
En esta configuración, el robot de la biblioteca y las unidades deben estar conectadas directamente al servidor de archivos NAS. Deben definirse vías de acceso desde el transportador de datos NAS a la biblioteca y a las unidades. No es necesaria ninguna conexión física entre el servidor de IBM Spectrum Protect y la biblioteca SCSI.
- **Configuración 3:** biblioteca 349x conectada al servidor de IBM Spectrum Protect  
Para esta configuración la biblioteca de cintas se conecta al sistema igual que para las operaciones tradicionales.
- **Configuración 4:** biblioteca ACSLS conectada al servidor de IBM Spectrum Protect  
Para esta configuración, conecte la biblioteca de cintas al sistema igual que para las operaciones de IBM Spectrum Protect tradicionales.

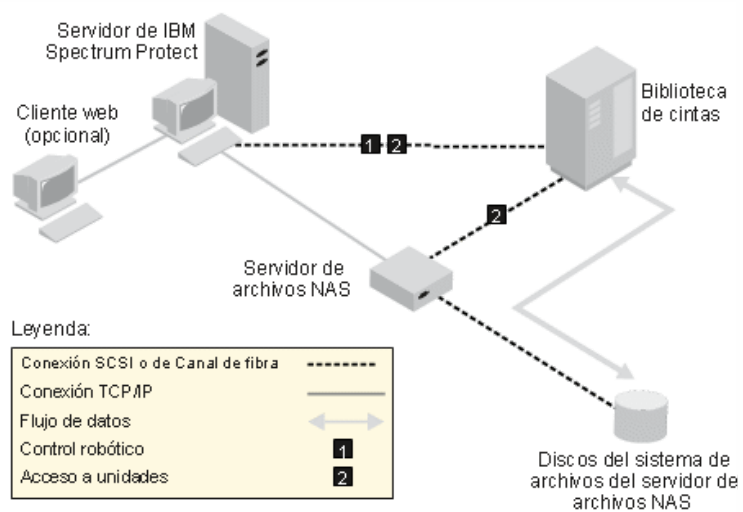
## Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect

En esta configuración, la biblioteca de cintas debe tener puertos separados para el control robótico y para el acceso a las unidades. Además, la biblioteca debe estar al alcance del canal de fibra o del bus SCSI tanto del servidor de IBM Spectrum Protect como del servidor de archivos NAS.

En esta configuración, el servidor de IBM Spectrum Protect controla la biblioteca SCSI mediante una conexión física directa al puerto de control robótico de la biblioteca. Para operaciones NDMP, las unidades de la biblioteca están conectadas directamente al servidor de archivo NAS, y se debe definir la vía de acceso desde el transportador de datos NAS hasta cada una de las unidades que se van a utilizar. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Para utilizar también las unidades para operaciones de IBM Spectrum Protect, conecte el servidor de IBM Spectrum Protect a las unidades de cintas y defina las vías de acceso desde el servidor hasta las unidades de cintas.

Esta configuración también admite un agente de almacenamiento de IBM Spectrum Protect con acceso a las unidades para sus operaciones fuera de la LAN, y el servidor de IBM Spectrum Protect puede ser un gestor de biblioteca.

Figura 1. Configuración 1: biblioteca SCSI conectada al servidor de IBM Spectrum Protect



## Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS

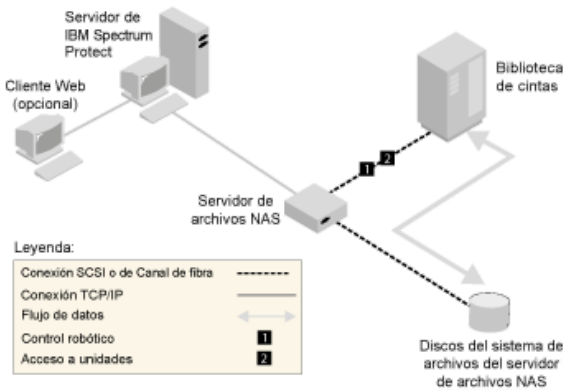
En esta configuración, el robot de la biblioteca y las unidades deben estar conectadas directamente al servidor de archivos NAS. Deben definirse vías de acceso desde el transportador de datos NAS a la biblioteca y a las unidades. No es necesaria ninguna conexión física



entre el servidor de IBM Spectrum Protect y la biblioteca SCSI.

El servidor de IBM Spectrum Protect controla el robot de la biblioteca enviando mandatos de biblioteca al servidor de archivos NAS a través de la red. El servidor de archivos NAS pasa los mandatos a la biblioteca de cintas. Las respuestas que genera la biblioteca se envían al servidor de archivos NAS y se devuelven al servidor de IBM Spectrum Protect a través de la red. Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect está en una ciudad y el servidor de archivos NAS y la biblioteca de cintas está en otra ciudad.

Figura 1. Configuración 2: biblioteca SCSI conectada al servidor de archivos NAS



## Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect

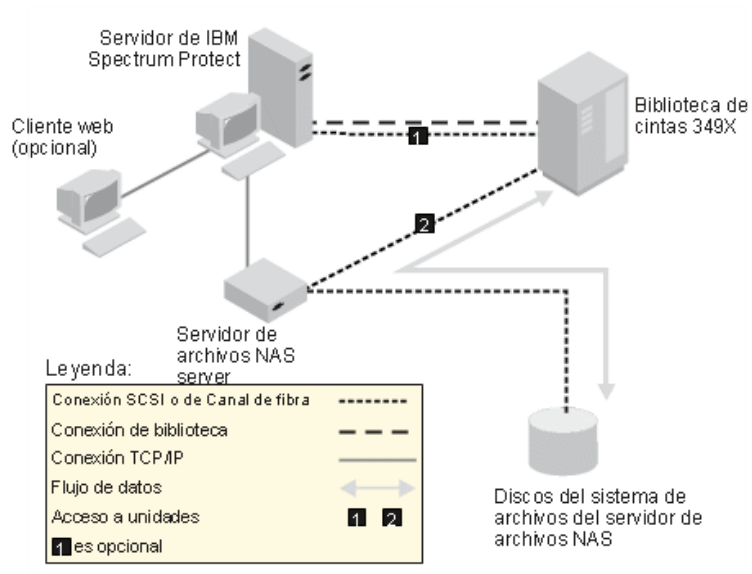
Para esta configuración la biblioteca de cintas se conecta al sistema igual que para las operaciones tradicionales.

En esta configuración, el servidor de IBM Spectrum Protect controla la biblioteca de cintas 349X. El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud al gestor de la biblioteca 349X a través de TCP/IP.

Para completar las operaciones de copia de seguridad o restauración NAS (almacenamiento adjunto de red), el servidor de archivos NAS debe poder acceder a una o varias unidades de cintas de la biblioteca 349X. Todas las unidades de cintas empleadas para las operaciones NAS deben estar conectadas físicamente al servidor de archivos NAS, y deben definirse vías de acceso desde el transportador de datos NAS hasta las unidades. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Siga las instrucciones del fabricante para conectar el dispositivo al sistema servidor.

Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect puede estar en una ciudad y el servidor de archivos NAS y la biblioteca de cintas puede estar en otra.

Figura 1. Configuración 3: biblioteca 349x conectada al servidor de IBM Spectrum Protect



**Tareas relacionadas:**


- [Conexión de dispositivos para el servidor \(V7.1.1\)](#)

## Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect

---

Para esta configuración, conecte la biblioteca de cintas al sistema igual que para las operaciones de IBM Spectrum Protect tradicionales.

El servidor de IBM Spectrum Protect controla la biblioteca de cintas ACSLS (software de biblioteca del sistema de cartuchos automatizado). El servidor de IBM Spectrum Protect controla la biblioteca pasando la solicitud al servidor de la biblioteca ACSLS a través de TCP/IP. La biblioteca ACSLS permite operaciones de compartir bibliotecas y trabajos fuera de la LAN.

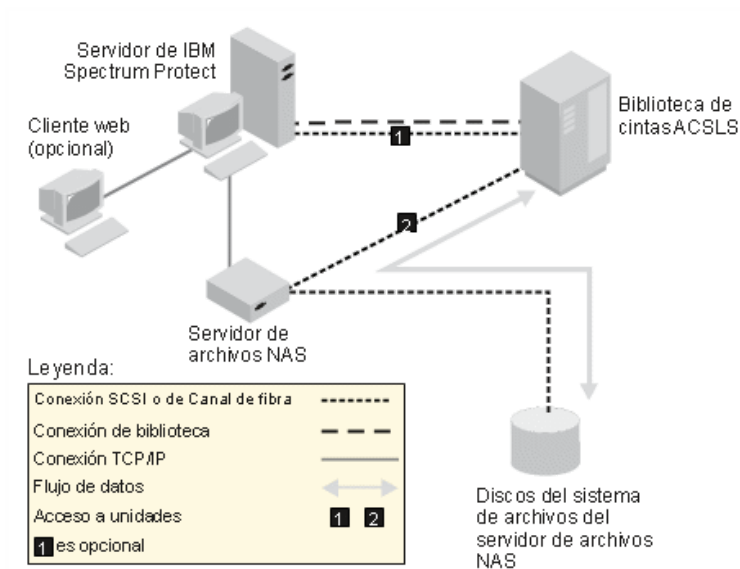
 **Sistemas operativos Windows** Restricción: Para utilizar las funciones ACSLS, debe instalarse el software StorageTek Library Attach. Para obtener más información, consulte Bibliotecas gestionadas mediante ACSLS (V7.1.1).

Para completar las operaciones de copia de seguridad o restauración NAS (almacenamiento adjunto de red), el servidor de archivos NAS debe poder acceder a una o varias unidades de cintas de la biblioteca ACSLS. Todas las unidades de cintas empleadas para las operaciones NAS deben estar conectadas físicamente al servidor de archivos NAS y deben definirse vías de acceso desde el transportador de datos NAS hasta las unidades. El servidor de archivos NAS transfiere datos a la unidad de cintas cuando así lo requiere el servidor de IBM Spectrum Protect. Siga las instrucciones del fabricante para conectar el dispositivo al sistema servidor.

Esta configuración admite un servidor de IBM Spectrum Protect alejado físicamente y un servidor de archivos NAS. Por ejemplo, el servidor de IBM Spectrum Protect puede estar en una ciudad y el servidor de archivos NAS y la biblioteca de cintas pueden estar en otra ciudad.

Para utilizar también las unidades para operaciones de IBM Spectrum Protect, conecte el servidor de IBM Spectrum Protect a las unidades de cintas y defina las vías de acceso desde el servidor de IBM Spectrum Protect hasta las unidades de cintas.

Figura 1. Configuración 4: biblioteca ACSLS conectada al servidor de IBM Spectrum Protect



**Tareas relacionadas:**

- Conexión de dispositivos para el servidor (V7.1.1)

## Registro de nodos NAS con el servidor de IBM Spectrum Protect

Registre el servidor de archivos NAS como nodo de IBM Spectrum Protect, especificando TYPE=NAS. Este nombre de nodo sirve para realizar un seguimiento de las copias de seguridad de imagen para el servidor de archivos NAS.

## Procedimiento

---

Para registrar un sistema de archivos NAS como un nodo denominado NASNODE1, con la contraseña NASPWD1, en un dominio de políticas denominado NASDOMAIN, emita el siguiente mandato de ejemplo:

```
register node nasnode1 naspwd1 domain=nasdomain type=nas
```

Si utiliza un conjunto de opciones de cliente, especifique el conjunto de opciones cuando inscriba el nodo. Puede comprobar que este nodo esté registrado emitiendo el siguiente mandato:

```
query node type=nas
```

Recuerde: Debe especificar TYPE=NAS para que sólo se visualicen los nodos de NAS.

## Definición de un transportador de datos para un servidor de archivos de NAS

---

Defina un transportador de datos para cada servidor de archivos NAS utilizando las operaciones NDMP en el entorno. El nombre del transportador de datos debe coincidir con el nombre de nodo especificado al inscribir el nodo NAS en el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

---

IBM Spectrum Protect admite dos tipos de transportadores de datos:

- Para operaciones NDMP, los transportadores de datos son servidores de archivos NAS. La definición de un transportador de datos de NAS contiene la dirección de red, la autorización y los formatos de datos necesarios para las operaciones NDMP. Un transportador de datos permite la comunicación y garantiza la autorización para operaciones NDMP entre el servidor de IBM Spectrum Protect y el servidor de archivos NAS.
- Para el traspaso de datos fuera del servidor, los transportadores de datos son dispositivos, como por ejemplo IBM® SAN Data Gateway, que traspasa datos entre dispositivos de disco y de cintas en la SAN.

## Procedimiento

---

Para definir un transportador de datos, utilice el mandato DEFINE DATAMOVER.

### Ejemplo

---

Por ejemplo, defina un transportador de datos con estos parámetros:

- El nodo NAS se llama NASNODE1.
- La dirección de alto nivel es una dirección IP del servidor de archivos NAS y puede ser una dirección numérica o un nombre de host.
- La dirección de bajo nivel es el puerto IP de las sesiones NDMP con el servidor de archivos NAS. El valor predeterminado es el número de puerto 10000.
- El ID de usuario es el ID definido en el servidor de archivos NAS que autoriza una sesión de NDMP con el servidor de archivos NAS. Para este ejemplo, el ID de usuario es el ID administrativo para el servidor de archivos NetApp.
- El parámetro de contraseña es una contraseña válida para la autenticación en una sesión NDMP con el servidor de archivos NAS.
- El formato de datos es NETAPPDUMP. Este es el formato de datos que utiliza el servidor de archivos NetApp para realizar copia de seguridad de cinta. Este formato de datos debe coincidir con el formato de datos de la agrupación de almacenamiento de destino.

Entre el mandato siguiente:

```
define datamover nasnode1 type=nas haddress=netapp2 lladdress=10000 userid=root  
password=admin dataformat=netappdump
```

#### Referencia relacionada:

DEFINE DATAMOVER (Definir un transportador de datos)

## Definición de vías de acceso para operaciones NDMP

---

Para operaciones NDMP, se crean vías de acceso a unidades y a bibliotecas.

- Definición de vías de acceso a unidades para operaciones NDMP  
El método elegido para la creación de vías de acceso a unidades depende de si a las unidades accede un servidor de archivos NAS y el servidor de IBM Spectrum Protect, o solo un servidor de archivos NAS.
- Definición de vías de acceso a bibliotecas para operaciones NDMP  
Defina una vía de acceso a la biblioteca SCSI desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS.

## Definición de vías de acceso a unidades para operaciones NDMP

---

El método elegido para la creación de vías de acceso a unidades depende de si a las unidades accede un servidor de archivos NAS y el servidor de IBM Spectrum Protect, o solo un servidor de archivos NAS.

- Definición de vías de acceso a unidades conectadas a un servidor de archivos NAS y al servidor de IBM Spectrum Protect  
Si un servidor de archivos de almacenamiento adjunto de red (NAS) y el servidor IBM Spectrum Protect deben acceder a una unidad de cintas server, debe crear dos vías de acceso. Existe una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Existe otra vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect.
- Definición de vías de acceso a unidades conectadas únicamente a servidores de archivos NAS  
Si solo debe acceder a una unidad de cintas un servidor de archivos NAS y no el servidor IBM Spectrum Protect, solo es necesaria una única vía de acceso entre la unidad de cintas y el servidor de archivos NAS.
- Obtención de nombres para dispositivos conectados a servidores de archivos NAS  
Para vías de acceso procedentes de un transportador de datos NAS, el valor del parámetro DEVICE en el mandato DEFINE PATH es el nombre por el cual el servidor de archivos NAS identifica la biblioteca o la unidad.

## Definición de vías de acceso a unidades conectadas a un servidor de archivos NAS y al servidor de IBM Spectrum Protect

---

Si un servidor de archivos de almacenamiento adjunto de red (NAS) y el servidor IBM Spectrum Protect deben acceder a una unidad de cintas server, debe crear dos vías de acceso. Existe una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Existe otra vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect.

### Procedimiento

---

Realice los pasos siguientes:

1. Si la unidad no está definida para el servidor de IBM Spectrum Protect, cree la definición de unidad. Por ejemplo, para definir una unidad NASDRIVE1 para una biblioteca NASLIB, emita el siguiente mandato:


```
define drive naslib nasdrive1 element=autodetect
```

Recuerde: Si la unidad está conectada al servidor de IBM Spectrum Protect, la dirección de elemento se detecta automáticamente.

2. Correlacione el nombre del dispositivo NAS con la definición de la unidad correspondiente en el servidor de IBM Spectrum Protect:
  - En el servidor IBM Spectrum Protect, emita el mandato QUERY DRIVE FORMAT=DETAILED para obtener el nombre de ámbito mundial (WWN) y el número de serie para la unidad que estará conectada al servidor de archivos NAS.
  - En el dispositivo NAS, obtenga el nombre del dispositivo de cinta, el número de serie y el WWN para la unidad.Si coincide el WWN o el número de serie, una unidad de un servidor de archivos NAS es la misma que la unidad del servidor de IBM Spectrum Protect.
3. Utilizando el nombre del dispositivo, defina una vía de acceso a la unidad desde el servidor de archivos NAS y una vía de acceso a la unidad desde el servidor de IBM Spectrum Protect.
  - Por ejemplo, para definir una vía de acceso entre una unidad de cintas con el nombre de dispositivo rst01 y un servidor de archivos NetApp, emita el siguiente mandato:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive  
library=naslib device=rst01
```


- Para definir una vía de acceso entre la unidad de cintas y el servidor de IBM Spectrum Protect, emita el mandato siguiente:

 Sistemas operativos AIX

```
define path server1 nasdrive1 srctype=server desttype=drive  
library=naslib device=/dev/rmt0
```

 Sistemas operativos Linux

```
define path server1 nasdrive1 srctype=server desttype=drive
library=naslib device=/dev/tsm SCSI/mt0
```

 Sistemas operativos Windows

```
define path server1 nasdrive1 srctype=server desttype=drive
library=naslib device=mt3.0.0.2
```

## Definición de vías de acceso a unidades conectadas únicamente a servidores de archivos NAS

---

Si solo debe acceder a una unidad de cintas un servidor de archivos NAS y no el servidor IBM Spectrum Protect, solo es necesaria una única vía de acceso entre la unidad de cintas y el servidor de archivos NAS.

### Procedimiento




---

Realice los pasos siguientes:

1. Obtenga las direcciones de elementos SCSI, los nombres de ámbito mundial (WWN) y los números de serie para la unidad que se va a conectar al servidor de archivos NAS.

Restricción: Si la unidad SCSI está conectada únicamente a un servidor de archivos NAS, la dirección del elemento no se detecta automáticamente y se debe proporcionar. Si una biblioteca tiene más de una unidad, se debe especificar una dirección de elemento para cada unidad.

Para obtener una dirección de elemento SCSI, vaya a los siguientes sitios web de soporte de dispositivo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

La asignación del número de elemento y las asignaciones de los WWN de dispositivo también están disponibles en los fabricantes de dispositivos de biblioteca de cintas.

2. Cree definiciones de unidades especificando las direcciones de elemento identificadas en el paso precedente. Especifique la dirección de elemento en el parámetro ELEMENT del mandato DEFINE DRIVE. Por ejemplo, para definir una unidad NASDRIVE1 con la dirección de elemento 82 para la biblioteca NASLIB, emita el siguiente mandato:

```
define drive naslib nasdrive1 element=82
```

Atención: Para una unidad conectada sólo al servidor de archivos NAS, no especifique ASNEEDED como valor para el parámetro CLEANFREQUENCY del mandato DEFINE DRIVE.

3. Obtenga el nombre del dispositivo, el número de serie y el WWN para la unidad en el dispositivo NAS.
4. Con la información obtenida en los pasos 1 y 3, correlacione el nombre del dispositivo de NAS con la dirección de elemento en la definición de unidad en el servidor de IBM Spectrum Protect.
5. Defina una vía de acceso entre la unidad de cintas y el servidor de archivos NAS. Por ejemplo, para definir una vía de acceso entre un servidor de archivos NetApp y una unidad de cintas con un nombre de dispositivo rst01, emita el siguiente mandato:

```
define path nasnode1 nasdrive1 srctype=datamover desttype=drive
library=naslib device=rst01
```

## Obtención de nombres para dispositivos conectados a servidores de archivos NAS

---

Para vías de acceso procedentes de un transportador de datos NAS, el valor del parámetro DEVICE en el mandato DEFINE PATH es el nombre por el cual el servidor de archivos NAS identifica la biblioteca o la unidad.

### Acerca de esta tarea

---

Puede obtener estos nombres de dispositivo, también denominados *nombres de archivo especial*, realizando una consulta al servidor de archivos NAS. Para obtener más información sobre cómo obtener nombres para dispositivos conectados al servidor de archivos NAS, consulte la información de producto del servidor de archivos.

### Procedimiento

---

- Para obtener los nombres de dispositivo para bibliotecas de cintas en un servidor de archivos NetApp Release ONTAP 10.0 GX, o posterior, conéctese con el servidor de archivos mediante telnet y emita el mandato SYSTEM HARDWARE TAPE LIBRARY SHOW. Para obtener los nombres de dispositivo para unidades de cintas en un servidor de archivos NetApp Release ONTAP 10.0 GX, o posterior, conéctese con el servidor de archivos mediante telnet y emita el mandato SYSTEM HARDWARE TAPE DRIVE SHOW.

Para obtener más detalles sobre estos mandatos, consulte la documentación de producto del servidor de archivos NetApp ONTAP GX.

- Para los releases anteriores a NetApp Release ONTAP 10.0 GX, continúe utilizando el mandato SYSCONFIG. Por ejemplo, para visualizar los nombres de dispositivo para bibliotecas de cintas, conéctese al servidor de archivos mediante telnet y emita el siguiente mandato:

```
sysconfig -m
```

Para visualizar los nombres de dispositivo para unidades de cintas, emita el siguiente mandato:

```
sysconfig -t
```

- Para las unidades conectadas a canal de fibra y el transportador de datos Celerra, realice los pasos siguientes:
  1. Inicie sesión en la estación de trabajo de control de EMC Celerra utilizando un ID de administración. Emita el mandato siguiente:

```
server_devconfig server_1 -l -s -n
```

Consejo: La opción `-l` enumera únicamente la información de dispositivo que se ha guardado en la base de datos del transportador de datos. El mandato y la opción no muestran los cambios en la configuración del dispositivo que se han producido después de la última actualización de la base de datos en el transportador de datos. Para obtener más detalles sobre cómo obtener la configuración más reciente del dispositivo para su transportador de datos, consulte la documentación de EMC Celerra.

La salida del mandato `server_devconfig` incluye los nombres de dispositivo para los dispositivos conectados al transportador de datos. Los nombres de dispositivo se enumeran en la columna `addr`, por ejemplo:

```
server_1:
Scsi Device Table
name      addr      type      info
tape1     c64t010  tape     IBM ULT3580-TD2 53Y2
ttape1    c96t010  tape     IBM ULT3580-TD2 53Y2
```

2. Correlacione el nombre del dispositivo Celerra con el nombre de ámbito mundial del dispositivo (WWN):
  - a. Para mostrar el WWN, inicie sesión en la estación de trabajo de control de EMC Celerra y emita el siguiente mandato. Recuerde incluir un punto (.) as the first character in this command.

```
.server_config server_# -v "fcplib show"
```

La salida de este mandato incluye el WWN, por ejemplo:

```
Chain 0064: WWN 500507630f418e29 HBA 2 N_PORT Bound
Chain 0096: WWN 500507630f418e18 HBA 2 N_PORT Bound
```

Consejo: El mandato `.server_config` es un mandato no documentado de EMC Celerra. Para obtener más información sobre cómo utilizarlo, póngase en contacto con EMC.

- b. Utilice el número de cadena para identificar el dispositivo de cinta que se mostraba en la salida del mandato `server_devconfig` y que tiene el mismo WWN, por ejemplo:

Nombre del dispositivo de cintas	Número de cadena	WWN
c64t010	0064	500507630f418e29
c96t010	0096	500507630f418e18


Es posible que los mandatos Celerra se comporten de forma diferente en los diferentes sistemas EMC Celerra y niveles del sistema operativo. Para conocer los detalles, consulte la documentación de EMC Celerra o póngase en contacto con EMC.

## Definición de vías de acceso a bibliotecas para operaciones NDMP

Defina una vía de acceso a la biblioteca SCSI desde el servidor de IBM Spectrum Protect o el servidor de archivos NAS.

### Procedimiento

1. Para una biblioteca SCSI conectada a IBM Spectrum Protect, emita el siguiente mandato de ejemplo para definir una vía de acceso desde el servidor, denominado SERVER1, a la biblioteca SCSI denominada TSMLIB:

 Sistemas operativos AIX

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lb1
```

 Sistemas operativos Linux



```
define path server1 tsmlib srctype=server desttype=library
device=/dev/tmsmcsi/lb1
```

#### Sistemas operativos Windows

```
define path server1 tsmlib srctype=server desttype=library
device=lb0.0.0.2
```

2. Para una biblioteca SCSI conectada a un servidor de archivos NAS, emita el siguiente mandato de ejemplo para definir una vía de acceso entre un transportador de datos NetApp NAS denominado NASNODE1 y una biblioteca denominada NASLIB:

```
define path nasnode1 naslib srctype=datamover desttype=library device=mc0
```

3. Para una biblioteca 349X, defina una vía de acceso a la biblioteca desde el servidor de IBM Spectrum Protect. Por ejemplo, emita el siguiente mandato para definir una vía de acceso del servidor, denominado SERVER1, a la biblioteca 349X denominada TSMLIB:

#### Sistemas operativos AIX

```
define path server1 tsmlib srctype=server desttype=library
device=/dev/lmcp0
```

#### Sistemas operativos Linux Sistemas operativos Windows

```
define path server1 tsmlib srctype=server desttype=library
device=library1
```

Consejo: El mandato DEFINE PATH no es necesario para una biblioteca ACSLS (software de biblioteca del sistema de cartuchos automatizados).

## Planificación de operaciones NDMP

---

Puede programar operaciones de copia de seguridad o restauración de las imágenes generadas por las operaciones NDMP. Utilice las planificaciones de administración que procesan los mandatos de administración BACKUP NODE o RESTORE NODE.

### Procedimiento

---


Cree una planificación utilizando el mandato DEFINE SCHEDULE. Por ejemplo, para crear una planificación de administración llamada NASSCHED para hacer una copia de seguridad de todos los sistemas de archivos para el nodo NASNODE1, especifique el siguiente mandato:

```
define schedule nassched type=administrative cmd='backup node nasnode1' active=yes
starttime=20:00 period=1 perunits=days
```

La planificación está activa y se establece para que se ejecute diariamente a las 8 de la tarde.

Restricción: Los mandatos BACKUP NODE y RESTORE NODE solo los pueden los nodos TYPE=NAS.

#### Tareas relacionadas:

 Ajuste de la planificación para las operaciones diarias

#### Referencia relacionada:

BACKUP NODE (Copia de seguridad de un nodo NAS)

RESTORE NODE (Restaurar un nodo NAS)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

## Definición de espacios de archivos virtuales

---

Utilice una definición de espacio de archivos virtual para realizar copias de seguridad a nivel de directorios NAS. Para reducir el tiempo de copia de seguridad y restauración para sistemas de archivos grandes, correlacione una vía de acceso de directorios desde un servidor de archivos de NAS a un nombre del espacio de archivos virtual en el servidor de IBM Spectrum Protect.

### Procedimiento

---

Para crear un nombre de espacio de archivos virtual para la vía de acceso de directorios en el dispositivo NAS, emita el mandato DEFINE VIRTUALFSMAPPING:

```
define virtualfsmapping nas1 /mikesdir /vol/voll /mikes
```

Este mandato define el nombre de espacio de archivos virtual /MIKESDIR en el servidor, que representa la vía de acceso de directorios /VOL/VOL1/MIKES en el servidor de archivos de NAS, representado por el nodo NAS1. Para obtener más información, consulte el

apartado Copia de seguridad y restauración a nivel de directorio para operaciones NDMP.

## Copia de seguridad de datos mediante la función de cinta a cinta

---

Cuando utilice la función de cinta a cinta de NDMP para realizar la copia de seguridad de los datos, el tipo de biblioteca puede ser SCSI, 349X o ACSLS (software de biblioteca del sistema de cartuchos automatizados). Las unidades se pueden compartir entre los dispositivos NAS y el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

---

Cuando se usa la función de copia de cinta a cinta de NDMP, la configuración puede afectar al rendimiento del movimiento de datos de back-end de IBM Spectrum Protect.

### Procedimiento

---

Para tener un dispositivo NAS con vías de acceso a cuatro unidades en una biblioteca, utilice el mandato MOVE DATA tras completar la configuración. De esta manera, los datos del volumen VOL1 se traspasarán como VOL1 a cualquier volumen disponible de la misma agrupación de almacenamiento:

```
move data voll
```

## Traslado de datos con la función de copia de cinta a cinta

---

Para traspasar datos de una tecnología de cinta antigua a otra nueva mediante la operación de copia de cinta a cinta de NDMP, debe realizar los pasos de configuración habituales, así como otros adicionales.

### Acerca de esta tarea

---

Cuando se usa la función de copia de cinta a cinta de NDMP, la configuración puede afectar al rendimiento del movimiento de datos de back-end de IBM Spectrum Protect.

### Procedimiento

---

Además de los pasos habituales de configuración, complete los siguientes pasos:

1. Defina una unidad en la biblioteca, lib1, que tenga tecnología de cinta antigua:

```
define drive lib1 drv1 element=1035
```

2. Defina una unidad de la biblioteca, lib2, que tenga tecnología de cinta nueva:

```
define drive lib2 drv1 element=1036
```

3. Defina las vías de acceso desde el servidor de archivos NAS a cada unidad:

```
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib1 device=rst11  
define path nas1 drv1 sourcetype=datamover desttype=drive library=lib2 device=rst21
```

4. Traspase los datos del volumen vol1 de la agrupación de almacenamiento primaria a los volúmenes de otra agrupación de almacenamiento primaria, nasprimpool2:

```
move data voll stgpool=nasprimpool2
```

## Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno en clúster de NetApp

---

Puede realizar una copia de seguridad de los datos de un clúster de NetApp en un dispositivo de cinta conectado directamente o en servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Puede realizar una copia de seguridad del clúster completo en un único nodo de IBM Spectrum Protect o de partes del clúster en varios nodos.

### Antes de empezar

---

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

## Acerca de esta tarea

Puede realizar una copia de seguridad de los datos de un entorno en clúster de NetApp en los siguientes soportes de almacenamiento:

Un dispositivo de cintas conectado directamente a un servidor de archivos NAS

Puede realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente a un servidor de archivos NAS. Este es el método preferido. Por lo general, es más rápido realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente que en una agrupación de almacenamiento de IBM Spectrum Protect utilizando una conexión de red.

Agrupación de almacenamiento en la jerarquía de IBM Spectrum Protect local

Puede realizar una copia de seguridad de los datos en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento de tipo DISK, FILE o de cinta. El ventaja de almacenar los datos en una agrupación de almacenamiento es que puede replicar los datos para lograr una protección de datos adicional. Puede utilizar las agrupaciones de almacenamiento existentes o crear agrupaciones de almacenamiento. Debe tener una conexión de red entre el servidor de archivos NAS y el servidor de IBM Spectrum Protect. La conexión de red debe tener suficiente ancho de banda para transferir los datos de copia de seguridad de NAS.

Consejo: Este tipo de copia de seguridad se denomina a veces una copia de seguridad de archivador a servidor.

Puede utilizar uno de los siguientes métodos de copia de seguridad:

Copia de seguridad de clúster completo

Cuando aplica este método, los datos de copia de seguridad de todo el clúster son propiedad de un único nodo de IBM Spectrum Protect. Aunque mueva los volúmenes dentro del clúster, las operaciones de copia de seguridad del clúster completo continúan y no es necesario reconfigurar las operaciones de copia de seguridad. Este es el método preferido.

Copia de seguridad de clúster parcial

Cuando aplica este método, especifica una máquina virtual de almacenamiento (SVM) de NetApp, que determina el ámbito de la operación de copia de seguridad. La SVM es un servidor virtual que proporciona acceso a parte de un clúster. Puede especificar que cada SVM en el clúster realice una copia de seguridad de los datos en un nodo de IBM Spectrum Protect diferente. Este método requiere una mayor configuración que el método de copia de seguridad de clúster completo, así como una conexión de red para transferir los datos desde la SVM al nodo de IBM Spectrum Protect.

Restricción: No puede utilizar este método para copiar datos en un dispositivo de cintas, porque las SVM no tienen acceso directo a los dispositivos de cintas.

## Procedimiento

1. Seleccione el soporte de almacenamiento utilizando las siguientes preguntas:

Pregunta	Soporte de almacenamiento
Según sus requisitos de negocio, ¿es necesario realizar una copia de seguridad de los datos en un dispositivo de cintas local?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Su organización requiere operaciones de copia de seguridad de alta velocidad?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Su organización dispone de suficiente ancho de banda de red para los datos de copia de seguridad de NAS?	Si la respuesta es sí, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente.
¿Su organización desea aumentar la protección de datos mediante la réplica?	Si la respuesta es sí, utilice una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.
¿Están los servidores de archivos NAS en ubicaciones remotas sin acceso a las bibliotecas de cintas conectadas directamente?	Si la respuesta es sí, utilice una agrupación de almacenamiento de IBM Spectrum Protect local. Si la respuesta es no, utilice un dispositivo de cintas conectado directamente o una agrupación de almacenamiento de IBM Spectrum Protect local.

2. Seleccione un método de copia de seguridad utilizando las siguientes preguntas:

Pregunta	Método de copia de seguridad
----------	------------------------------

Pregunta	Método de copia de seguridad
Según sus requisitos de negocio, ¿es necesario realizar una copia de seguridad de los datos en un dispositivo de cintas conectado directamente?	Si la respuesta es sí, utilice el método de copia de seguridad completa.  Si la respuesta es no, utilice el método de copia de seguridad completa o parcial.
¿Tiene el sistema suficiente ancho de banda de red para realizar una copia de seguridad de varias SVM sin afectar al rendimiento de red?	Si la respuesta es sí, utilice el método de copia de seguridad completa o parcial.  Si la respuesta es no, utilice el método de copia de seguridad completa. El método de copia de seguridad parcial puede afectar negativamente al rendimiento del sistema.
¿Están las SVM distribuidas en varias organizaciones? Por ejemplo, ¿están las SVM controladas por terceros, por ejemplo, por proveedores de plataformas de nube?	Si la respuesta es sí, utilice el método de copia de seguridad parcial, ya que los propietarios de SVM pueden controlar operaciones de copia de seguridad para SVM individuales. Si un propietario de SVM también es propietario de un servidor de IBM Spectrum Protect, el propietario puede configurar operaciones de copia de seguridad desde la SVM en un nodo de servidor. De este modo, el propietario puede controlar el proceso de extremo a extremo.  Si la respuesta es no, utilice el método de copia de seguridad completa o parcial.

3. Configure el entorno del sistema en función del soporte de almacenamiento y el método de copia de seguridad que elija. Siga las instrucciones para el método seleccionado:

- Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente
- Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect
- Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect

Consejo: Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, se recomienda reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp. Siga las instrucciones de la sección Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster.

- Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente  
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cinta conectado directamente.
- Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect  
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.
- Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect  
Puede configurar IBM Spectrum Protect para realizar una copia de seguridad parcial de un clúster de NetApp. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos.
- Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster  
Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, puede reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp.

## Configuración de copias de seguridad de clúster completo en dispositivos de cinta conectados directamente

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cinta conectado directamente.

### Antes de empezar

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de todos los volúmenes.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

## Acerca de esta tarea

---

El método recomendado es realizar una copia de seguridad del clúster completo utilizando un nodo y un transportador de datos que estén asociados a la red en todo el clúster. De este modo, se asegura de que los datos de la copia de seguridad pertenezcan a un único nodo de IBM Spectrum Protect. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.

## Procedimiento

---

Para configurar operaciones de copias de seguridad de clúster completo en un dispositivo de cinta conectado directamente, siga estos pasos:

1. Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

2. Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
3. En el servidor de archivos de NetApp, habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
  - a. Habilite las operaciones de copia de seguridad de NDMP con ámbito de SVM en el nivel de clúster. De este modo, inhabilita las operaciones de copia de seguridad de NDMP con ámbito de nodo en el servidor de archivos NAS. Asegúrese de que la opción `node-scoped-ndmp` en el servidor de archivos NAS esté establecida en OFF.
  - b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
  - c. Configure una interfaz de red para las conexiones de control NDMP en el nivel de clúster.
4. Registre el nodo de IBM Spectrum Protect que será propietario de todos los datos de la copia de seguridad del clúster. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre\_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio\_nas* especifica el dominio del nodo. Asigne el nodo a un dominio que tenga una política para hacer copia de seguridad de datos en una agrupación de almacenamiento apropiada.

5. Determine la dirección IP de la interfaz de gestión de clústeres de NetApp en el servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida del mandato es necesaria si especifica el parámetro HLADDRESS en el paso 6.

6. Defina un transportador de datos para el nodo de IBM Spectrum Protect que será el propietario de los datos de la copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER en una línea:

```
define datamover nombre_transportador_datos type=nascluster  
hladdress=interfaz_gestión_clúster lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz\_gestión\_clúster* es el valor que ha obtenido en el paso 5 y *nombre\_transportador\_datos* es el nombre de nodo que ha registrado en el paso 4. Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

Consejo: Después de definir el transportador de datos, los transportadores de datos adicionales se definen automáticamente para cada nodo en el clúster. El nombre de cada transportador de datos coincide con el nombre del nodo físico en el clúster. Utilizará estos transportadores de datos cuando defina vías de acceso a unidades de cintas en el paso 3 de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.

## Qué hacer a continuación

---

Para configurar el dispositivo de cinta para la copia de seguridad del clúster completo, siga las instrucciones de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.

- Configuración de dispositivos de cinta para copias de seguridad de clúster completas  
Si tiene previsto realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un dispositivo de cintas conectado directamente, debe configurar el dispositivo de cintas.

**Referencia relacionada:**

REGISTER NODE (Inscribir un nodo)

## Configuración de copias de seguridad de clúster completo en un servidor de IBM Spectrum Protect

---

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad de todos los volúmenes en un clúster de NetApp en un servidor de IBM Spectrum Protect, que almacena los datos en una agrupación de almacenamiento. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.

### Antes de empezar

---

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de todos los volúmenes del clúster. Todos los datos de la copia de seguridad serán propiedad de un único nodo de IBM Spectrum Protect.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

### Procedimiento

---

1. Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

2. Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
3. Habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
  - a. Habilite NetApp SVM para controlar las operaciones de copia de seguridad de NDMP en el nivel de clúster.
  - b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
  - c. Configure una interfaz de red para las conexiones de control NDMP a nivel de clúster.
4. Registre el nodo de IBM Spectrum Protect que será propietario de todos los datos de la copia de seguridad del clúster. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre\_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio\_nas* especifica el dominio del nodo.

5. Determine la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida es necesaria si especifica un valor para el parámetro HLADDRESS en el paso 6.

6. Para definir un transportador de datos para el nodo, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASCLUSTER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nascluster  
hladdress=interfaz_gestión_clúster lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz\_gestión\_clúster* es el valor que ha obtenido en el paso 5 y *nombre\_transportador\_datos* es el nombre de nodo que ha registrado en el paso 4. Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

7. Configure una política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
8. Actualice el nodo de clúster que ha registrado en el paso 4 en el dominio que se ha configurado en el paso 7. En el servidor de IBM Spectrum Protect, emita el mandato UPDATE NODE:

```
update node nombre_nodo domain=nombre_dominio
```

9. Opcional: Identifique los volúmenes en el clúster y planifique las copias de seguridad de los volúmenes:
  - a. En el servidor de archivos de NAS, identifique los volúmenes del clúster emitiendo el siguiente mandato de Data ONTAP:

```
volume show
```
  - b. Planifique las operaciones de copia de seguridad siguiendo las instrucciones de Planificación de operaciones NDMP.

## Qué hacer a continuación

---

Las tareas siguientes son opcionales:

- Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:
  1. En la barra de menús de Centro de operaciones, pulse Clientes.
  2. Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
  3. Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.
- Para configurar agrupaciones de almacenamiento de copias para la protección de datos añadida, configure la función de cinta a cinta para hacer copias de seguridad de datos. Para ver instrucciones, consulte Copia de seguridad de datos mediante la función de cinta a cinta.

### Referencia relacionada:

REGISTER NODE (Inscribir un nodo)

## Configuración de copias de seguridad de clúster parcial en un servidor de IBM Spectrum Protect

---

Puede configurar IBM Spectrum Protect para realizar una copia de seguridad parcial de un clúster de NetApp. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos.

### Antes de empezar

---

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

Si está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, utilice el procedimiento siguiente. Después de configurar el servidor de archivos de NetApp para trabajar con IBM Spectrum Protect, puede utilizar la extensión CAB (Cluster Aware Backup) de NetApp para realizar una copia de seguridad de una parte del clúster. Cuando configura una copia de seguridad de clúster parcial, puede determinar el ámbito de la copia de seguridad especificando un servidor virtual, la máquina virtual de almacenamiento (SVM) de NetApp. La SVM proporciona acceso a parte de un clúster.

Si no está instalado el sistema operativo NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetAPP, haga copia de seguridad de los datos siguiendo las instrucciones de Configuración de IBM Spectrum Protect para operaciones NDMP en un entorno no de clúster.

### Procedimiento

---

1. Verifique que IBM Spectrum Protect Extended Edition esté instalado y que la licencia esté registrada. Si la licencia no está registrada, emita el siguiente mandato de IBM Spectrum Protect:

```
register license file=tsmee.lic
```

2. Obtenga los privilegios de administrador de clústeres para el servidor de archivos de NetApp. Este paso es necesario para acceder a la consola de clústeres.
3. En el servidor de archivos de NetApp, habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice los pasos siguientes:
  - a. Habilite NetApp SVM para controlar las operaciones de copia de seguridad de NDMP.
  - b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
  - c. Configure una interfaz de red para las conexiones de control NDMP en el nivel de SVM.
4. Registre el nodo de IBM Spectrum Protect que será el propietario de los datos de copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre\_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio\_nas* especifica el dominio del nodo.

- Determine la dirección IP numérica o el nombre de dominio de la interfaz de clúster que utiliza SVM. Para determinar el valor, en el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo ONTAP:

```
network interface show -vserver nombre_vserver -role data
```

donde *nombre\_vserver* especifica el nombre de la SVM. El valor obtenido es necesario en el paso 6.

- Para definir un transportador de datos asociado para el nodo de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASVSERVER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nasvserver  
hladdress=interfaz_datos_svm lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz\_datos\_svm* es el valor que ha obtenido en el paso 5 y *nombre\_transportador\_datos* es el nombre del nodo que ha registrado en el paso 4.

Para obtener información sobre cómo especificar otros parámetros, consulte DEFINE DATAMOVER (Definir un transportador de datos).

- Configure una política de IBM Spectrum Protect para gestionar copias de seguridad de imágenes NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
- Actualice el nodo que ha registrado en el paso 4 en el dominio que ha configurado en el paso 7. En el servidor de IBM Spectrum Protect, emita el mandato UPDATE NODE:

```
update node nombre_nodo domain=nombre_dominio
```

- Opcional: identifique los volúmenes en el clúster y planifique las operaciones de copia de seguridad. Realice los pasos siguientes:
  - En el servidor de archivos de NAS, identifique los volúmenes del clúster emitiendo el siguiente mandato de Data ONTAP:

```
volume show -vserver nombre_vserver
```

donde *nombre\_vserver* especifica el nombre de la SVM.

- Planifique las operaciones de copia de seguridad siguiendo las instrucciones de Planificación de operaciones NDMP.

## Qué hacer a continuación

---

Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:

- En la barra de menús de Centro de operaciones, pulse Clientes.
- Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
- Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.

### Referencia relacionada:

REGISTER NODE (Inscribir un nodo)

## Reconfiguración de IBM Spectrum Protect para optimizar las copias de seguridad en clúster

---

Si ha configurado IBM Spectrum Protect para realizar la copia de seguridad de los clústeres de NetApp utilizando NDMP con ámbito de nodo, puede reconfigurar IBM Spectrum Protect para que utilice CAB (Cluster Aware Backup) de NDMP. De este modo, puede optimizar las operaciones de copia de seguridad para los clústeres de NetApp.

## Antes de empezar

---

Para obtener una visión general de la funcionalidad de NDMP en IBM Spectrum Protect y en los servidores de archivos NetApp, consulte la nota técnica 7046965. Esta nota técnica también enumera los requisitos de sistema.

## Acerca de esta tarea

---

Cuando reconfigura IBM Spectrum Protect para utilizar CAB, puede optimizar las operaciones de copia de seguridad de la siguiente manera:



- Puede configurar IBM Spectrum Protect para que realice copias de seguridad de todos los volúmenes de un clúster de NetApp en un dispositivo de cintas conectado directamente o en un servidor de IBM Spectrum Protect. En ambos casos, los datos serán propiedad de un único nodo de IBM Spectrum Protect. Aunque mueva volúmenes dentro del clúster, las operaciones de copia de seguridad continúan y no es necesaria ninguna reconfiguración.
- Puede realizar una copia de seguridad parcial de un clúster de NetApp en un servidor de IBM Spectrum Protect. Este método es muy útil cuando varias organizaciones poseen datos en el clúster. Cada organización puede gestionar operaciones de copia de seguridad de sus datos. Para establecer el ámbito de una copia de seguridad parcial, especifique una máquina virtual de almacenamiento (SVM) de NetApp, que proporciona acceso a parte de un clúster.

Para reconfigurar IBM Spectrum Protect para utilizar CAB, debe definir un nuevo nodo de IBM Spectrum Protect y un nuevo transportador de datos.

## Procedimiento

1. Verifique que se haya instalado NetApp Clustered Data ONTAP 8.2 o posterior, o 9.1 o posterior, en el servidor de archivos de NetApp.
2. Habilite el uso de NDMP siguiendo las instrucciones de la publicación *Clustered Data ONTAP® Data Protection Tape Backup and Recovery Guide*. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

Realice los pasos siguientes:

- a. Habilite las operaciones de copia de seguridad de NDMP con ámbito de SVM en el nivel de clúster. De este modo, inhabilita las operaciones de copia de seguridad de NDMP con ámbito de nodo en el servidor de archivos NAS. Asegúrese de que la opción `node-scoped-ndmp` en el servidor de archivos NAS esté establecida en OFF.
- b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
- c. Configure una interfaz de red para las conexiones de control NDMP a nivel de clúster.

Para una copia de seguridad de clúster parcial

Realice los pasos siguientes:

- a. Habilite NDMP con ámbito de SVM para controlar las operaciones de copia de seguridad de NDMP.
- b. Cree un ID de usuario de copia de seguridad para las operaciones NDMP.
- c. Configure una interfaz de red para las conexiones de control NDMP en el nivel de SVM.

3. Registre el nodo de IBM Spectrum Protect que será el propietario de los datos de copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato REGISTER NODE:

```
register node nombre_nodo contraseña domain=dominio_nas type=nas
```

donde *nombre\_nodo* especifica el nombre del nodo, *contraseña* especifica la contraseña del nodo y *dominio\_nas* especifica el dominio del nodo.

4. Si tiene previsto realizar una copia de seguridad de un clúster completo, determine la dirección IP de la interfaz de gestión de clústeres de NetApp en el servidor de archivos NAS. La interfaz proporciona acceso a todo el clúster. En el servidor de archivos de NAS, emita el siguiente mandato de sistema operativo Data ONTAP:

```
network interface show -role cluster-mgmt
```

La dirección IP que se muestra en la salida es necesaria si especifica el parámetro HLADDRESS en el paso 6.

5. Si va a realizar una copia de seguridad de un clúster parcial, determine la dirección IP numérica o el nombre de dominio de la interfaz de clúster que utiliza SVM. Para determinar el valor, emita el siguiente mandato de sistema operativo Data ONTAP en el servidor de archivos de NAS:

```
network interface show -vserver nombre_vserver -role data
```

donde *nombre\_vserver* especifica el nombre de la SVM. El valor que obtiene es necesario en el paso 6.

6. Defina un transportador de datos para el nodo de IBM Spectrum Protect. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

Defina un transportador de datos para el nodo de IBM Spectrum Protect que será el propietario de los datos de la copia de seguridad. En el servidor de IBM Spectrum Protect, emita el mandato DEFINE DATAMOVER en una línea:

```
define datamover nombre_transportador_datos type=nascluster
hladdress=interfaz_gestión_clúster lladdress=puerto
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz\_gestión\_clúster* es el valor que ha obtenido en el paso 4 y *nombre\_transportador\_datos* es el nombre de nodo que ha registrado en el paso 3.

Consejo: Después de definir el transportador de datos, los transportadores de datos adicionales se definen automáticamente para cada nodo en el clúster. El nombre de cada transportador de datos coincide con el nombre del

nodo físico en el clúster. Utilizará estos transportadores de datos cuando defina vías de acceso a unidades de cintas que están conectadas al clúster.

Para una copia de seguridad de clúster parcial

Para definir un transportador de datos para el nodo, emita el mandato DEFINE DATAMOVER y especifique TYPE=NASVSERVER. En el servidor de IBM Spectrum Protect, emita el mandato siguiente en una línea:

```
define datamover nombre_transportador_datos type=nasvserver  
hladdress=interfaz_datos_svm lladdress=puerto  
USER=nombre_usuario password=contraseña dataformat=netappdump
```

donde *interfaz\_datos\_svm* es el valor que ha obtenido en el paso 5 y *nombre\_transportador\_datos* es el nombre de nodo que ha registrado en el paso 3.

Para obtener información sobre cómo especificar otros parámetros en el mandato DEFINE DATAMOVER, consulte DEFINE DATAMOVER (Definir un transportador de datos).

7. Para realizar una copia de seguridad de los datos en un dispositivo de cinta conectado directamente, para cada unidad de cintas que está conectada al clúster, identifique el nombre de dispositivo y el nodo físico al que está conectada la unidad:
  - a. En el servidor de archivos de NAS, emita el siguiente mandato de Data ONTAP:

```
storage tape show-tape-drive
```

- b. Revise la salida para encontrar el número de serie de la unidad de cintas y el nodo del clúster al que se conecta la unidad.

La misma stanza incluye el nombre de dispositivo, por ejemplo, *st1*, *st2* o *st3*.

8. Para configurar una copia de seguridad de clúster completa en un dispositivo de cinta conectado directamente, siga las instrucciones de Configuración de dispositivos de cinta para copias de seguridad de clúster completas.
9. Para configurar una copia de seguridad de clúster completa o parcial en un servidor de IBM Spectrum Protect, configure una política para gestionar las copias de seguridad de imagen de NAS. Siga las instrucciones de la sección Configuración de una política de IBM Spectrum Protect para operaciones NDMP.
10. Inhabilite las operaciones de copia de seguridad planificadas para todos los nodos que se han utilizado previamente para realizar una copia de seguridad del clúster de NetApp.
11. Identifique los volúmenes en el clúster y, opcionalmente, planifique las operaciones de copia de seguridad de los volúmenes. Realice una de las siguientes acciones:

Para una copia de seguridad de clúster completa

- a. En el servidor de archivos de NAS, identifique los volúmenes del clúster utilizando el siguiente mandato de Data ONTAP:

```
volume show
```

- b. Ejecutar una copia de seguridad completa de todo el clúster.
- c. Opcional: para planificar operaciones de copia de seguridad, siga las instrucciones de Planificación de operaciones NDMP.

Para una copia de seguridad de clúster parcial

- a. En el servidor de archivos de NAS, identifique los volúmenes del clúster utilizando el siguiente mandato de Data ONTAP:

```
volume show -vserver nombre_vserver
```

donde *nombre\_vserver* especifica el nombre de la SVM.

- b. Ejecutar una copia de seguridad completa del clúster parcial.
- c. Opcional: para planificar operaciones de copia de seguridad, siga las instrucciones de Planificación de operaciones NDMP.

## Qué hacer a continuación

---

Para verificar que se realiza la copia de seguridad de los volúmenes en el clúster de NetApp, siga estos pasos:

1. En la barra de menús de Centro de operaciones, pulse Clientes.
2. Efectúe una doble pulsación en un cliente de dispositivo NAS y pulse Volúmenes.
3. Para determinar si ha finalizado la última copia de seguridad completa del volumen, revise la información en la columna Última completa. Para determinar si ha finalizado la copia de seguridad diferencial más reciente, revise la información en la columna Última diferencial.

### Referencia relacionada:

DEFINE DATAMOVER (Definir un transportador de datos)  
DEFINE PATH (Definir una vía de acceso cuando el destino es una unidad)  
REGISTER NODE (Inscribir un nodo)

# Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP

---

Después de configurar IBM Spectrum Protect para operaciones NDMP, está listo para empezar a utilizar NDMP.

## Procedimiento

---

Utilice una interfaz de cliente o una interfaz de administración para realizar una copia de seguridad de imagen del sistema de archivos. Por ejemplo, para utilizar la interfaz de cliente de copia de seguridad/archivado de Windows con el fin de realizar una copia de seguridad de un sistema de archivos denominado /vol/vol1 en un servidor de archivos NAS denominado NAS1, emita el siguiente mandato:

```
dsmc backup nas -nasnodename=nas1 {/vol/vol1}
```

Para obtener más información acerca del mandato, consulte Imagen de copia de seguridad.

Consejo: Cuando utilice la interfaz de cliente, se le solicitará que se autentique como administrador de IBM Spectrum Protect antes de que pueda empezar la operación. El ID de administrador debe tener como mínimo autorización de propietario de cliente para el nodo NAS.

Puede realizar la misma operación de copia de seguridad con una interfaz de servidor. Por ejemplo, desde el cliente de línea de mandatos de administración, haga una copia de seguridad del sistema de archivos denominado /vol/vol1 en un servidor de archivos NAS denominado NAS1, emitiendo el siguiente mandato:

```
backup node nas1 /vol/vol1
```

Restricción: Los mandatos BACKUP NAS y BACKUP NODE no incluyen instantáneas. Para hacer copias de seguridad de instantáneas, consulte el apartado Copia de seguridad y restauración con instantáneas.

Puede restaurar la imagen utilizando cualquiera de las dos interfaces. Las copias de seguridad son idénticas tanto si la copia de seguridad se efectúa con una interfaz de cliente como con una interfaz de servidor. Por ejemplo, supongamos que desea restaurar la imagen de la que ha hecho copia de seguridad en los ejemplos anteriores. En este ejemplo, el sistema de archivos denominado /vol/vol1 se va a restaurar en /vol/vol2. Restaure el sistema de archivos con el mandato siguiente, que emitirá desde una interfaz de cliente de copia de seguridad/archivado Windows:

```
dsmc restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}
```

Puede elegir restaurar el sistema de archivos mediante una interfaz de servidor. Por ejemplo, para restaurar el nombre de sistema de archivos /vol/vol1 en el sistema de archivos /vol/vol2, para un servidor de archivos NAS denominado NAS1, especifique el mandato siguiente:

```
restore node nas1 /vol/vol1 /vol/vol2
```

Puede restaurar datos de un sistema NAS de un proveedor a un sistema NAS de otros proveedores al utilizar el formato de datos NDMPDUMP. Sin embargo, debe verificar la compatibilidad entre sistemas o mantener una agrupación de almacenamiento diferente para cada proveedor de NAS.

- Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único  
Si tiene varios servidores NAS en diversas ubicaciones, es posible que prefiera enviar los datos de la copia de seguridad a un único servidor de IBM Spectrum Protect que conectar una biblioteca de cintas a cada dispositivo NAS.
- Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect  
Puede hacer copias de seguridad de los datos en un único servidor de IBM Spectrum Protect en lugar de conectar una biblioteca de cintas con cada dispositivo NAS.

## Servidores de archivos de NAS: copias de seguridad en un servidor de IBM Spectrum Protect único

---

Si tiene varios servidores NAS en diversas ubicaciones, es posible que prefiera enviar los datos de la copia de seguridad a un único servidor de IBM Spectrum Protect que conectar una biblioteca de cintas a cada dispositivo NAS.

Cuando se almacenan datos de copia de seguridad de NAS en la jerarquía de almacenamiento del servidor de IBM Spectrum Protect, puede aplicar funciones de gestión de datos de programa de fondo de IBM Spectrum Protect. De este modo, puede aprovechar las características de migración, reclamación, recuperación tras desastre y otras.

Para realizar la copia de seguridad de un dispositivo de NAS en una agrupación de almacenamiento nativa de IBM Spectrum Protect, establezca la agrupación de almacenamiento de destino del grupo de copias para que apunte a la agrupación de almacenamiento nativa deseada. Dicha agrupación proporciona información acerca de la biblioteca y las unidades que se utilizan para realizar las operaciones de copia de seguridad y restauración. Asegúrese de que la agrupación de almacenamiento de destino disponga de espacio suficiente

para los datos de NAS, de los que se puede hacer una copia de seguridad en dispositivos de tipo secuencial, de disco o de archivo. No es preciso definir otra clase de dispositivo.

Si va a crear una tabla de contenido, deberá especificar una clase de gestión en el con el parámetro TOCDESTINATION de los mandatos DEFINE y UPDATE COPYGROUP. Al realizar una copia de seguridad del servidor de archivos de NAS en agrupaciones nativas de IBM Spectrum Protect, el TOCDESTINATION puede ser el mismo que el del destino de los datos de los que se hace copia de seguridad utilizando NDMP.

Las consideraciones de cortafuegos son más estrictas que en el caso del método de archivador a biblioteca conectada, ya que tanto el servidor de IBM Spectrum Protect como el servidor de archivos NAS pueden iniciar las comunicaciones. Los servidores de cintas NDMP se ejecutan como hebras dentro del servidor de IBM Spectrum Protect y el servidor de cintas acepta conexiones en el puerto 10001. Este número de puerto se puede cambiar mediante la opción siguiente del archivo de opciones del servidor de IBM Spectrum Protect: NDMPPORTRANGE número\_puerto\_bajo, número\_puerto\_alto.

Durante las operaciones de copia de seguridad de archivador a servidor de NDMP, puede utilizar la opción NDMPPREFDATAINTERFACE para especificar qué interfaz de red utiliza el servidor de IBM Spectrum Protect para recibir datos de copia de seguridad. El valor de esta opción es un nombre de host o una dirección IPV4 que se asocia a una de las interfaces de red activas del sistema en el que se ejecuta el servidor de IBM Spectrum Protect. Esta interfaz debe haberse activado para IPV4.

Antes de usar esta opción, verifique que el dispositivo NAS dé soporte a las operaciones NDMP que usan una interfaz de red distinta para las conexiones de control NDMP y de datos NDMP. IBM Spectrum Protect usa conexiones de control NDMP para autenticar un servidor NDMP y supervisar una operación NDMP, mientras que se usan conexiones de datos NDMP para transmitir y recibir datos de copia de seguridad durante las operaciones NDMP. Aún debe configurar el dispositivo NAS para direccionar los datos de copia de seguridad y restauración a la interfaz de red apropiada.

Cuando se habilita, la opción NDMPPREFDATAINTERFACE afecta a todas las operaciones de gestor de archivos a servidor NDMP posteriores. No afecta a las conexiones de control NDMP, ya que estas usan la interfaz de red predeterminada del sistema. Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Los servidores de archivos NetApp proporcionan una opción NDMP (ndmpd.preferred\_interface) para cambiar la interfaz usada para las conexiones de datos NDMP. Para obtener más información, consulte la documentación del dispositivo NAS.

Para obtener instrucciones sobre cómo realizar operaciones de copia de seguridad de archivador a servidor NDMP, consulte Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect.

Para obtener información sobre las opciones de servidor, consulte Opciones de servidor.

## Copia de seguridad de servidores de archivos NDMP en un servidor de IBM Spectrum Protect

---

Puede hacer copias de seguridad de los datos en un único servidor de IBM Spectrum Protect en lugar de conectar una biblioteca de cintas con cada dispositivo NAS.

### Procedimiento

---

Para realizar copias de seguridad de un servidor en un sistema de archivos NAS, complete los pasos siguientes:

1. Seleccione una agrupación de almacenamiento existente o configure una agrupación de almacenamiento para los datos NAS emitiendo el siguiente mandato:

```
define stgpool naspool disk
```

2. Defina volúmenes para agregarlos a la agrupación de almacenamiento. Por ejemplo, defina un volumen denominado naspool\_volAB:

```
define volume naspool /usr/storage/naspool_volAB formatsize=100
```

3. Establezca el destino de la copia en la agrupación de almacenamiento definida previamente y active el conjunto de políticas asociadas.

```
update copygroup standard standard standard destination=naspool  
tocdestination=naspool  
activate policysset standard standard
```

El destino de los datos NAS está determinado por el destino del grupo de copia. El cálculo del tamaño del almacenamiento en el caso de las copias de seguridad diferenciales NAS emplea la ocupación del espacio de archivos, el mismo valor que se utiliza para realizar una copia de seguridad completa. Puede utilizar este cálculo del tamaño como una de las consideraciones que

deben tenerse en cuenta al elegir una agrupación de almacenamiento. Uno de los atributos de una agrupación de almacenamiento es el valor MAXSIZE, que indica que los datos se envíen a la agrupación de almacenamiento NEXT si el tamaño calculado es superior al valor MAXSIZE. Dado que las copias de seguridad diferenciales NAS a las agrupaciones de almacenamiento nativas de IBM Spectrum Protect utilizan el tamaño de ocupación del espacio del archivo base como cálculo del tamaño del almacenamiento, las copias de seguridad diferenciales acaban en la misma agrupación de almacenamiento que la copia de seguridad completa. Según los valores de proximidad, las copias de seguridad diferenciales pueden acabar en los mismos medios que la copia de seguridad completa.

4. Configure un nodo y un transportador de datos para el dispositivo NAS. El formato de datos significa que las imágenes de copia de seguridad creadas por este dispositivo NAS son un tipo de volcado de la imagen de copia de seguridad en un formato específico de NetApp.

```
register node nas1 nas1 type=nas domain=standard
define datamover nas1 type=nas hla=nas1 user=root
password=***** dataformat=netappdump
```

Ahora ya se puede realizar la copia de seguridad del dispositivo NAS en una agrupación de almacenamiento del servidor de IBM Spectrum Protect. Las vías de acceso se pueden definir en unidades locales, pero el destino especificado mediante la clase de gestión determina la ubicación de destino de esta operación de copia de seguridad.

5. Realice la copia de seguridad del dispositivo NAS en la agrupación de almacenamiento de IBM Spectrum Protect ejecutando el mandato siguiente:

```
backup node nas1 /vol/vol0
```

6. Restaure un dispositivo NAS de la agrupación de almacenamiento de IBM Spectrum Protect ejecutando el mandato siguiente:

```
restore node nas1 /vol/vol0
```

## Copia de seguridad y restauración en nivel de archivo para operaciones NDMP

---

Al realizar una copia de seguridad de los datos utilizando NDMP, puede especificar que el servidor de IBM Spectrum Protect recopile y almacene información de nivel de archivo en una tabla de contenido (TOC).

Si especifica esta opción al realizar la copia de seguridad, posteriormente puede visualizar la TOC de la imagen de copia de seguridad. Mediante el cliente web de archivado y copia de seguridad, puede seleccionar archivos o directorios individuales para restaurarlos directamente de las imágenes de copia de seguridad generadas.

Para recopilar información de nivel de archivo, se necesita tiempo de proceso, recursos de red, espacio de agrupación de almacenamiento y espacio de base de datos temporal extras, así como posiblemente interacción adicional entre dispositivos de almacenamiento. Para obtener instrucciones sobre la configuración de dispositivos de almacenamiento, consulte Configuración de dispositivos de almacenamiento. Considere la posibilidad de destinar más espacio a la base de datos del servidor de IBM Spectrum Protect. Debe configurar la política de modo que el servidor de IBM Spectrum Protect almacene la TOC en una agrupación de almacenamiento distinta de la empleada para almacenar la imagen de copia de seguridad. La TOC se maneja del mismo modo que cualquier otro objeto de esa agrupación de almacenamiento.

También tiene la posibilidad de efectuar una copia de seguridad mediante NDMP sin recopilar información de restauración de nivel de archivo.

Para permitir que se cree una TOC para una copia de seguridad mediante NDMP, debe definir el atributo TOCDESTINATION en el grupo de copias de seguridad para la clase de gestión a la que está vinculada esta imagen de copia de seguridad. No puede especificar una agrupación de almacenamiento de copia ni una agrupación de datos activos como destino. La agrupación de almacenamiento que especifique para el destino de la tabla de contenido debe tener un formato de datos NATIVE o NONBLOCK, por lo tanto no puede ser la agrupación de almacenamiento en cinta empleada para la imagen de copia de seguridad.

Si elige recopilar la información de nivel de archivo, especifique el parámetro TOC en el mandato de servidor BACKUP NODE. O bien, si inicia la copia de seguridad utilizando el cliente, puede especificar la opción TOC en el archivo de opciones de cliente, en el conjunto de opciones de cliente o en la línea de mandatos del cliente. Puede especificar NO, PREFERRED o YES. Si especifica PREFERRED o YES, el servidor de IBM Spectrum Protect almacena la información de archivo de una única copia de seguridad controlada por NDMP en una TOC. La TOC se coloca en una agrupación de almacenamiento. A continuación, el servidor de IBM Spectrum Protect puede acceder a la TOC de modo que el servidor o cliente pueda consultar la información de archivo y directorio. El uso del parámetro TOC permite generar una TOC para unas imágenes y no otras, sin que se necesiten clases de gestión distintas para las imágenes.

Para obtener más información sobre el mandato BACKUP NODE, consulte BACKUP NODE (Copia de seguridad de un nodo NAS).

Para evitar retardos de montaje y asegurarse de que tiene suficiente espacio disponible, utilice agrupaciones de almacenamiento de acceso aleatorio (clase de dispositivo DISK) como destino para la TOC. Para las agrupaciones de almacenamiento de acceso secuencial, no es necesario etiquetar los volúmenes ni realizar ninguna otra tarea de preparación si los volúmenes reutilizables están permitidos.

Para obtener más información, consulte Gestión de tablas de contenido.

- Interfaces para las operaciones de restauración a nivel de archivos  
Al restaurar directorios y archivos individuales, tiene la opción de utilizar una de dos interfaces para iniciar la restauración: el cliente web de archivado y copia de seguridad o la interfaz de servidor.
- Caracteres internacionales para servidores de archivos NetApp  
Todos los sistemas que crean datos en un volumen de servidor de archivos NAS específico, o que acceden a sus datos, deben hacerlo de modo compatible con el valor de idioma del volumen.
- Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio  
Las operaciones de restauración a nivel de archivos se admiten para imágenes de copia de seguridad a nivel de directorio.

## Interfaces para las operaciones de restauración a nivel de archivos

---

Al restaurar directorios y archivos individuales, tiene la opción de utilizar una de dos interfaces para iniciar la restauración: el cliente web de archivado y copia de seguridad o la interfaz de servidor.

Operaciones de restauración mediante el cliente web de copia de seguridad-archivado.

El cliente web del archivado y copia de seguridad requiere que existe una TOC para restaurar archivos y directorios. El cliente web debe estar en un sistema Windows. El servidor de IBM Spectrum Protect accede a la TOC desde la agrupación de almacenamiento y carga la información de la tabla de contenido en una tabla de base de datos temporal. A continuación, puede utilizar el cliente web de archivado y copia de seguridad para examinar los directorios y archivos incluidos en una o varias imágenes de sistemas de archivos, y seleccionar directorios o archivos individuales para restaurarlos directamente a partir de las imágenes de copia de seguridad generadas.

Operaciones de restauración mediante la interfaz de servidor

- Si dispone de una TOC, utilice el mandato QUERY NASBACKUP para visualizar información sobre las imágenes de copia de seguridad generadas por NDMP y para ver qué imágenes tienen su correspondiente TOC. Después, utilice el mandato RESTORE NODE con el parámetro FILELIST.
- Si no ha creado una TOC, el contenido de la imagen de copia de seguridad no podrá visualizarse. Puede restaurar archivos y directorios individuales si sabe el nombre del archivo o directorio y en qué imagen se encuentra la copia de seguridad. Utilice el mandato RESTORE NODE con el parámetro FILELIST.

## Caracteres internacionales para servidores de archivos NetApp

---

Todos los sistemas que crean datos en un volumen de servidor de archivos NAS específico, o que acceden a sus datos, deben hacerlo de modo compatible con el valor de idioma del volumen.

Para obtener plena compatibilidad para los caracteres internacionales en los nombres de archivos y directorios, debe instalar Data ONTAP 6.4.1 o posterior, si está disponible, en el servidor de archivos de NetApp NAS.

Si el nivel de Data ONTAP de que dispone es anterior a 6.4.1, debe tener una de las dos configuraciones siguientes para recopilar y restaurar información de nivel de archivo. El uso de configuraciones distintas a estas dos puede ocasionar resultados imprevisibles. El servidor de IBM Spectrum Protect emitirá un mensaje de aviso (ANR4946W) durante las operaciones de copia de seguridad. El mensaje indica que la codificación de caracteres de los mensajes históricos de archivo NDMP es desconocida y se dará por supuesta la codificación UTF-8 para construir una tabla de contenido. El omitir este mensaje no supone ningún riesgo únicamente en las dos configuraciones siguientes.

- Los datos tienen nombres de archivo y de directorio que contienen caracteres en inglés únicamente (ASCII de 7 bits).
- Los datos tienen nombres de directorio y archivo que contienen caracteres que no están en inglés y el idioma del volumen se ha establecido en la versión de UTF-8 del entorno nacional adecuado (por ejemplo, de UTF-8 para el alemán).

Si el nivel de Data ONTAP de que dispone es 6.4.1 o posterior, debe tener una de las tres configuraciones siguientes para recopilar y restaurar información de nivel de archivo. El uso de configuraciones distintas a estas tres puede ocasionar resultados imprevisibles.

- Los datos tienen nombres de directorio y archivo que contienen caracteres en inglés únicamente (ASCII de 7 bits) y el idioma del volumen no se ha establecido o se ha establecido en uno de estos valores:
  - C (POSIX)
  - en
  - en\_US
  - en.UTF-8
  - en\_US.UTF-8
- Los datos tienen nombres de directorio y archivo que contienen caracteres que no están en inglés y el idioma del volumen se ha establecido en el entorno nacional adecuado (por ejemplo, de UTF-8 o de para el alemán).  
Consejo: El uso de la versión de UTF-8 del valor de idioma del volumen es más eficaz en términos de proceso del servidor de IBM Spectrum Protect y espacio de almacenamiento de la tabla de contenido.

- Utilice CIFS únicamente para crear los datos y acceder a ellos.

## Operaciones de restauración a nivel de archivo desde una imagen de copia de seguridad a nivel de directorio

---

Las operaciones de restauración a nivel de archivos se admiten para imágenes de copia de seguridad a nivel de directorio.

Al igual que con una copia de seguridad de sistema de archivos NAS, se crea una tabla de contenidos durante una acción de copia de seguridad a nivel de directorio, y puede examinar los archivos de la imagen utilizando el cliente web. La forma predeterminada es que los archivos se restauren a la ubicación original. Sin embargo, durante una restauración a nivel de archivos a partir de la copia de seguridad a nivel de directorios, puede seleccionar un sistema de archivos distinto u otro nombre del espacio de archivos virtual como destino.

Para una tabla de contenidos (TOC) de una imagen de copia de seguridad a nivel de directorio, los nombres de vía de acceso para todos los archivos son relativos al directorio especificado en la definición de espacio de archivos virtual, no la raíz del sistema de archivos.

## Operaciones de copia de seguridad y restauración a nivel de directorio

---

Si tiene un sistema de archivos NAS grande, al iniciar una copia de seguridad a nivel de directorios se reducen los tiempos de copia de seguridad y restauración y se proporciona más flexibilidad en la configuración de copias de seguridad NAS. Al definir los espacios de archivos virtuales, la copia de seguridad del sistema de archivos se debe partir en varias operaciones de copia de seguridad NDMP y varias unidades de cintas. También puede utilizar distintas planificaciones de copia de seguridad con el fin de realizar una copia de seguridad de subárboles de un sistema de archivos.

El nombre del espacio de archivos virtual no puede ser idéntico a ningún sistema de archivos en el nodo NAS. Si se crea un sistema de archivos en el dispositivo NAS con el mismo nombre que un sistema de archivos virtual, se producirá un conflicto de nombres en el servidor de IBM Spectrum Protect al realizarse la copia de seguridad del nuevo espacio de archivos. Para obtener instrucciones sobre cómo emitir mandatos de correlación de espacios de archivos virtuales, consulte DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales).

Restricción: Las correlaciones de espacios de archivos virtuales sólo se admiten para nodos NAS.

- Copia de seguridad y restauración a nivel de directorio para operaciones NDMP  
El mandato DEFINE VIRTUALFSMAPPING correlaciona una vía de acceso de directorios de un servidor de archivos NAS con un nombre de espacio de archivos virtual en el servidor de IBM Spectrum Protect. Tras definir la correlación, puede llevar a cabo operaciones NAS como BACKUP NODE y RESTORE NODE utilizando los nombres de espacios de archivos virtuales como si se tratase de espacios de archivos NAS reales.
- Copia de seguridad y restauración con instantáneas  
Las operaciones de copia de seguridad a nivel de directorio NDMP le ofrecen la posibilidad de realizar una copia de seguridad de las instantáneas creadas por el usuario de un sistema de archivos NAS. Estas instantáneas se almacenan como subdirectorios. Las instantáneas se pueden tomar en cualquier momento, y la copia de seguridad se puede aplazar hasta un momento más adecuado.

## Copia de seguridad y restauración a nivel de directorio para operaciones NDMP

---

El mandato DEFINE VIRTUALFSMAPPING correlaciona una vía de acceso de directorios de un servidor de archivos NAS con un nombre de espacio de archivos virtual en el servidor de IBM Spectrum Protect. Tras definir la correlación, puede llevar a cabo operaciones NAS como BACKUP NODE y RESTORE NODE utilizando los nombres de espacios de archivos virtuales como si se tratase de espacios de archivos NAS reales.

Para iniciar una copia de seguridad del directorio, emita el mandato BACKUP NODE y especifique el nombre del espacio de archivos virtual en lugar del nombre de un espacio de archivos. Para restaurar el subárbol de directorios a la ubicación original, ejecute el mandato RESTORE NODE y especifique el nombre del espacio de archivos virtual.

Las definiciones de espacios de archivos virtuales también pueden especificarse como destino en un mandato RESTORE NODE. De esta forma, podrá restaurar imágenes de copia de seguridad (del sistema de archivos o directorio) en un directorio de cualquier sistema de archivos del dispositivo NAS.

Puede utilizar el cliente web para seleccionar archivos con el fin de restaurarlos a partir de una imagen de copia de seguridad de nivel de directorios porque el cliente de IBM Spectrum Protect trata los nombres de espacios de archivos virtuales como espacios de archivos NAS.

## Copia de seguridad y restauración con instantáneas

---

Las operaciones de copia de seguridad a nivel de directorio NDMP le ofrecen la posibilidad de realizar una copia de seguridad de las instantáneas creadas por el usuario de un sistema de archivos NAS. Estas instantáneas se almacenan como subdirectorios. Las instantáneas se pueden tomar en cualquier momento, y la copia de seguridad se puede aplazar hasta un momento más adecuado.

### Procedimiento

---

Por ejemplo, para realizar una copia de seguridad de una instantánea que se ha creado para un sistema de archivos NetApp, complete los pasos siguientes:

1. En la consola del dispositivo NAS, emita el mandato para crear la instantánea. SNAP CREATE es el mandato para un dispositivo NetApp.

```
snap create vol2 february17
```

Este ejemplo creará una instantánea denominada FEBRUARY 17 del sistema de archivos /vol/vol2. La ubicación física para los datos de la instantánea es el directorio /vol/vol2/.snapshot/february17. La ubicación de almacenamiento de los datos de instantánea dependerá de la implementación del proveedor NAS. Para NetApp, se puede utilizar el mandato SNAP LIST para visualizar todas las instantáneas de un determinado sistema de archivos.

2. Defina una definición de correlación de espacios de archivos virtuales en el servidor de IBM Spectrum Protect para los datos de la instantánea creados en el paso anterior.

```
define virtualfsmapping nas1 /feb17snapshot /vol/vol2 /.snapshot/february17
```

Este ejemplo creará una definición de correlación de espacios de archivos virtuales denominada /feb17snapshot.

3. Realice una copia de seguridad de la correlación de espacios de archivos virtuales.

```
backup node nas1 /feb17snapshot mode=full toc=yes
```

4. Tras crear la copia de seguridad, puede restaurar toda la imagen instantánea o un archivo individual. Antes de restaurar los datos, puede crear un nombre de correlación de espacios de archivos virtuales para el directorio de destino. Puede elegir cualquier nombre del sistema de archivos como destino. La ubicación de destino en este ejemplo es el directorio /feb17snaprestore del sistema de archivos /vol/vol1.

```
define virtualfsmapping nas1 /feb17snaprestore /vol/vol1 /feb17snaprestore
```

5. Restaure la imagen de copia de seguridad de instantánea.

```
restore node nas1 /feb17snapshot /feb17snaprestore
```

De esta forma se restaura una copia del sistema de archivos /vol/vol2 en el directorio /vol/vol1/feb17snaprestore en el mismo estado que tenía cuando se creó la instantánea en el primer paso.

## Copia de seguridad y restauración de operaciones utilizando la característica NetApp SnapMirror to Tape

---

Puede realizar una copia de seguridad de sistemas de archivos NetApp grandes utilizando la característica NetApp SnapMirror to Tape (también denominada SMTape). Si se usa una copia de datos a nivel de bloque para copia de seguridad, el método SnapMirror to Tape es más rápido que una copia de seguridad completa tradicional NDMP y se puede usar si las copias de seguridad completas de NDMP no resultan prácticas.

Utilice la característica NDMP SnapMirror to Tape como una opción de recuperación tras desastre para copiar sistemas de archivos NetApp grandes en almacenamiento auxiliar. En la mayoría de los sistemas de archivos NetApp, utilice el método de copia de seguridad diferencial o completa NDMP estándar.

Mediante la especificación de un parámetro en los mandatos BACKUP NODE y RESTORE NODE, puede hacer una copia de seguridad de los sistemas de archivos y restaurarlos utilizando SnapMirror to Tape. Hay diversas limitaciones y restricciones sobre cómo pueden usarse las imágenes de SnapMirror. Tenga en cuenta las siguientes directrices antes de usarlas como un método de copia de seguridad:

- Si ha instalado NetApp ONTAP 8.2 o posterior, debe definir un transportador de datos de tipo NASCLUSTER o NASVSERVER para operaciones de SnapMirror to Tape.
- No puede iniciar una copia de seguridad de SnapMirror to Tape o una operación de restauración desde IBM Spectrum Protect Centro de operaciones, el cliente web o el cliente de línea de mandatos.
- No se pueden realizar copias de seguridad diferenciales de imágenes de SnapMirror.



- No puede realizar una copia de seguridad de nivel de directorio utilizando SnapMirror to Tape. Por consiguiente, IBM Spectrum Protect no permite operaciones de copia de seguridad de SnapMirror to Tape en un espacio de archivos virtual de servidor.
- No se puede realizar una operación de restauración a nivel de archivo NDMP desde imágenes de SnapMirror to Tape. Por lo tanto, nunca se crea una tabla de contenidos durante las copias de seguridad de imágenes de SnapMirror to Tape.
- Al inicio de la operación de copia de SnapMirror to Tape, el servidor de archivos genera una instantánea del sistema de archivos. NetApp proporciona una variable de entorno de NDMP para controlar si esta instantánea se elimina al final de la operación de SnapMirror to Tape. IBM Spectrum Protect siempre establece esta variable para eliminar la instantánea.
- Tras recuperar una imagen de SnapMirror to Tape y copiarla en un sistema de archivos NetApp, el sistema de archivos de destino sigue configurado como socio de SnapMirror. NetApp proporciona una variable de entorno NDMP para controlar si esta relación de SnapMirror se debe romper. IBM Spectrum Protect siempre "rompe" la relación de SnapMirror durante la recuperación. Tras completarse la operación de restauración, el sistema de archivos de destino está en el mismo estado que el sistema de archivos original en el momento de la copia de seguridad.

Para obtener más información sobre la función SnapMirror to Tape, consulte BACKUP NODE (Copia de seguridad de un nodo NAS) y RESTORE NODE (Restaurar un nodo NAS).

## Operaciones de copia de seguridad NDMP usando los puntos de comprobación integrados del servidor de archivos Celerra

---

Cuando el servidor de IBM Spectrum Protect inicia una operación de copia de seguridad NDMP en un transportador de datos Celerra, la copia de seguridad de un sistema de archivos grande puede tardar varias horas en realizarse. Sin los puntos de comprobación integrados de Celerra, los cambios que se producen en el sistema de archivos se graban en la imagen de copia de seguridad.

Como resultado, la imagen de copia de seguridad incluye los cambios realizados en el sistema de archivos durante la operación de copia de seguridad entera. La imagen de copia de seguridad no es una imagen de punto en el tiempo verdadera del sistema de archivos.

Si está realizando operaciones de copia de seguridad de NDMP desde servidores de archivos de Celerra, actualice el sistema operativo del transportador de datos a la versión de servidor de archivos de Celerra T5.5.25.1 o posterior. Esta versión del sistema operativo permite habilitar los puntos de comprobación integrados para todas las operaciones de copia de seguridad NDMP desde Celerra Control Workstation. Al habilitar esta característica se asegura de que los datos de copia de seguridad representen verdaderas imágenes de punto en el tiempo del sistema de archivos del que se hace copia de seguridad.

Para obtener instrucciones sobre cómo habilitar los puntos de comprobación integrados durante todas las operaciones de copia de seguridad de NDMP, consulte la documentación de servidor de archivos de Celerra.

Si la versión del sistema operativo del servidor de archivos Celerra es anterior a la versión T5.5.25.1 y se usa NDMP para la copia de seguridad de los transportadores de datos Celerra, debe generar manualmente una instantánea del sistema de archivos usando la característica de punto de comprobación de la línea de mandatos de Celerra. A continuación, inicie una operación de copia de seguridad de NDMP del sistema de archivos de punto de comprobación en lugar del sistema de archivos original.

Consulte la documentación del servidor de archivos de Celerra para obtener instrucciones sobre la creación y planificación de puntos de control desde la estación de trabajo de control de Celerra.

## Réplica de los nodos NAS

---

Puede replicar un nodo NAS que utiliza NDMP para operaciones de copia de seguridad. Antes de configurar la operación de réplica, revise las restricciones que se aplican.

### Acerca de esta tarea

---

Restricciones:

- Los datos de copia de seguridad deben estar en una agrupación de almacenamiento con el formato de datos NATIVE. No puede replicar datos de copia de seguridad en agrupaciones de almacenamiento que tienen los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Una copia de seguridad diferencial sólo puede replicarse si se replica su copia de seguridad completa.

### Procedimiento

---

1. Habilite el nodo NAS para la réplica emitiendo el mandato UPDATE NODE:

```
update node nombre_nodo replstate=enabled
```

donde *nombre\_nodo* especifica el nombre del nodo NAS.

2. Replique el nodo emitiendo el mandato REPLICATE NODE:

```
replicate node nombre_nodo
```

donde *nombre\_nodo* especifica el nombre del nodo NAS.

3. Para garantizar que los datos replicados puedan restaurarse, defina un transportador de datos en el servidor de destino para el nodo emitiendo el mandato DEFINE DATAMOVER:

```
define datamover nombre_nodo type=nas hladdress=dirección_hl lladdress=dirección_ll  
userid=ID_usuario password=contraseña_usuario dataformat=netappdump
```

donde:

*nombre\_nodo*

Especifica el nombre del nodo NAS.

*dirección\_hl*

Especifica la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS.

*dirección\_ll*

Especifica el número de puerto TCP para acceder al dispositivo NAS para las sesiones NDMP.

*ID\_usuario*

Especifica el ID del usuario autorizado para iniciar una sesión con el servidor de archivos NAS.

*contraseña\_usuario*

Especifica la contraseña del usuario autorizado para iniciar una sesión NDMP con el servidor de archivos NAS.

## Resultados

---

El formato de los datos de copia de seguridad no cambia durante el proceso de réplica. Si los datos de copia de seguridad se replican, la tabla de contenido asociada también se replican.

## Protección de datos utilizando la característica con licencia NetApp SnapLock

---

Puede utilizar la característica con licencia NetApp SnapLock para cumplir los estrictos requisitos normativos. Al habilitar la característica SnapLock, puede utilizar IBM Spectrum Protect para establecer una fecha de retención de los archivos y aplicar un estado WORM (Grabar una vez, leer varias) a un archivo.

Los datos almacenados con una fecha de retención no pueden suprimirse del sistema de archivos antes de que caduque el periodo de retención. La función SnapLock puede utilizarse únicamente con servidores de IBM Spectrum Protect que tengan habilitada la protección de retención de datos.

Los datos archivados por servidores con protección de retención de datos y almacenados en servidores de archivos NetApp NAS se almacenan como volúmenes FILE de IBM Spectrum Protect. Al final de una transacción de grabación, se establece una fecha de retención para el volumen FILE a través de la interfaz SnapLock. Esta fecha se calcula mediante los parámetros RETVER y RETMIN del grupo de copias archivadas utilizado al archivar los datos. Al asociar una fecha de retención con el volumen FILE, este volumen no destruirá ni sobrescribirá los datos hasta que pase la fecha de retención. Este tipo de volúmenes FILE se conocen como volúmenes WORM FILE. Tras establecer una fecha de retención, no se puede suprimir el volumen WORM FILE hasta que haya pasado la fecha de retención. IBM Spectrum Protect para retención de datos combinado con la reclamación de volúmenes WORM FILE garantiza la protección durante el ciclo de vida de los datos.

Las agrupaciones de almacenamiento pueden gestionarse por el umbral o por el periodo de retención de datos. El parámetro de agrupación de almacenamiento RECLAMATIONTYPE indica que una agrupación de almacenamiento está gestionada en función del periodo de retención de datos. Al realizar una consulta a una agrupación de almacenamiento tradicional con el parámetro FORMAT=DETAILED, se muestra la siguiente salida:

```
Tipo de reclamación: THRESHOLD
```

Si un servidor de IBM Spectrum Protect tiene habilitada la protección de retención de datos a través de IBM Spectrum Protect para retención de datos, y el servidor tiene acceso a un archivador NetApp con la característica con licencia SnapLock, puede definir una agrupación de almacenamiento con el parámetro RECLAMATIONTYPE definido en SNAPLOCK. Esto significa que los datos creados en volúmenes de esta agrupación de almacenamiento se gestionan por una fecha de retención. Al realizar una consulta a una agrupación de almacenamiento SnapLock con el parámetro FORMAT=DETAILED, la salida indica que las agrupaciones de almacenamiento están gestionadas por el periodo de retención de datos:

```
Tipo de reclamación: SNAPLOCK
```

Para obtener más información sobre el archivador SnapLock, consulte la documentación de NetApp *Data ONTAP Archive and Compliance Management Guide for 7-Mode*.

Atención: No utilice esta característica para proteger los datos con un periodo de retención inferior a tres meses.

- **Reclamación y la característica SnapLock**  
Para garantizar la protección continua de los datos, establezca el periodo de retención predeterminado de NetApp en 30 días para que coincida con el periodo de reclamación predeterminado del volumen WORM FILE. IBM Spectrum Protect reclama todos los datos restantes en un volumen WORM FILE justo antes de la caducidad de la fecha de retención.
- **Periodos de retención**  
Las políticas de IBM Spectrum Protect gestionan el periodo de retención del volumen WORM FILE. La retención de algunos archivos puede exceder el periodo de retención para el volumen WORM FILE en el que se han almacenado. Es posible que tenga que mover algunos archivos a otro volumen para garantizar que los archivos se almacenen en medios WORM.
- **Configuración de la característica SnapLock para la retención basada en sucesos**  
Los datos almacenados en volúmenes SnapLock gestionados por IBM Spectrum Protect para retención de datos y la retención basada en sucesos pueden provocar una reclamación excesiva, lo que causará una disminución en el rendimiento del servidor.
- **Protección de datos continua con la característica SnapLock**  
Si los datos se almacenan en un volumen con la característica SnapLock habilitada, y los datos se mueven o copian a un volumen que no sea SnapLock, los datos pierden la protección exclusiva por hardware que proporcionan los volúmenes NetApp WORM.
- **Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect**  
Para cumplir los estrictos requisitos de los datos archivados, habilite la característica NetApp SnapLock.

## Reclamación y la característica SnapLock

---

Para garantizar la protección continua de los datos, establezca el periodo de retención predeterminado de NetApp en 30 días para que coincida con el periodo de reclamación predeterminado del volumen WORM FILE. IBM Spectrum Protect reclama todos los datos restantes en un volumen WORM FILE justo antes de la caducidad de la fecha de retención.

La reclamación de un volumen WORM FILE a otro volumen WORM FILE antes de la caducidad de la fecha de retención garantiza que los datos siempre estarán protegidos por la función SnapLock.

Puesto que esta protección se realiza en el nivel de volumen de IBM Spectrum Protect, los datos de los volúmenes pueden ser gestionados por la política de IBM Spectrum Protect independientemente de dónde están almacenados los datos. Los datos almacenados en volúmenes WORM FILE están protegidos tanto por la protección de retención de datos como por el periodo de retención almacenado con el archivo físico en el volumen SnapLock. Si un administrador de IBM Spectrum Protect emite un mandato para suprimir los datos, el mandato falla. Si alguien intenta suprimir el archivo a través de una serie de llamadas del sistema de archivos de red, la función SnapLock impedirá la supresión de los datos.

Durante el proceso de reclamación, si el servidor de IBM Spectrum Protect no puede traspasar datos de un volumen SnapLock a punto de caducar a un nuevo volumen SnapLock, se mostrará un mensaje de aviso.

## Periodos de retención

---

Las políticas de IBM Spectrum Protect gestionan el periodo de retención del volumen WORM FILE. La retención de algunos archivos puede exceder el periodo de retención para el volumen WORM FILE en el que se han almacenado. Es posible que tenga que mover algunos archivos a otro volumen para garantizar que los archivos se almacenen en medios WORM.

Es posible que algunos objetos del volumen se retengan durante más tiempo que otros objetos del volumen por los motivos siguientes:

- Los objetos están vinculados con clases de gestión con distintos periodos de retención.
- Los objetos no pueden eliminarse debido a una espera de supresión.
- Los objetos están esperando que se produzca un suceso antes de caducar.
- El periodo de retención de un grupo de copia se incrementa, lo que requiere un periodo de retención más largo que el especificado en la función SnapLock al confirmar el volumen WORM FILE.

Para gestionar un volumen WORM FILE por tiempo de retención, debe emitir el mandato DEFINE STGPOOL y especificar RECLAMATIONTYPE=SNAPLOCK. De esta forma, puede definir una agrupación de almacenamiento como una agrupación de almacenamiento SnapLock. Después, no puede actualizar el parámetro RECLAMATIONTYPE a un valor de THRESHOLD. Al definir una agrupación de almacenamiento SnapLock, el sistema verifica que los directorios especificados que están en la clase de dispositivo estén en volúmenes SnapLock WORM. Al definir una clase de archivo y crear agrupaciones de almacenamiento con el tipo de reclamación de SNAPLOCK, todos los volúmenes deben ser volúmenes WORM para que la operación se ejecute correctamente. Si se actualiza una clase de dispositivo para que contenga directorios adicionales y se asignan agrupaciones de almacenamiento SnapLock, se realiza la misma comprobación para garantizar que todos los directorios sean volúmenes WORM SnapLock.

Hay tres periodos de retención disponibles para la característica NetApp SnapLock. Los periodos de retención deben estar configurados correctamente para que el servidor de IBM Spectrum Protect pueda gestionar correctamente los datos WORM almacenados en los volúmenes SnapLock. El servidor de IBM Spectrum Protect define el periodo de retención para los datos que se almacenan en los volúmenes SnapLock de NetApp en función de los valores del grupo de copias para los datos que se archivan. El servidor de archivos NetApp no debería entrar en conflicto con la capacidad del servidor de IBM Spectrum Protect para definir el periodo de retención. El método preferido consiste en configurar los siguientes valores para periodos de retención en el servidor de archivos NetApp:

- Periodo de retención mínimo. Defina el valor más alto: entre 30 días o el número mínimo de días especificado por cualquier grupo de copias (utilizando un servidor de archivos SnapLock de NetApp para el almacenamiento WORM FILE) para el periodo de retención de datos. El grupo de copias es el que se utiliza para almacenar datos en los volúmenes SnapLock de NetApp.
- Periodo de retención máximo. Acepte el valor predeterminado de 30 años. Este periodo de retención permite al servidor de IBM Spectrum Protect establecer el periodo de retención real del volumen en función de los valores del grupo de copia archivada.
- Periodo de retención predeterminado. Se establece en 30 días. Si no establece este valor ni el periodo máximo de retención, el periodo de retención de cada volumen se establecerá en 30 años. En este caso, el servidor de IBM Spectrum Protect no puede gestionar la caducidad y reutiliza los volúmenes NetApp SnapLock. Como resultado, no se puede reutilizar ningún volumen en 30 años.

Con los periodos de retención de SnapLock de NetApp definidos, IBM Spectrum Protect puede gestionar los datos de las agrupaciones de almacenamiento SnapLock con la máxima eficacia. IBM Spectrum Protect crea un periodo de reclamación para cada volumen que se encuentra en una agrupación de almacenamiento SNAPLOCK. El periodo de reclamación de IBM Spectrum Protect tiene una fecha de inicio, BEGIN RECLAIM PERIOD, y una fecha de finalización END RECLAIM PERIOD. Puede ver estas fechas ejecutando el mandato QUERY VOLUME con el parámetro FORMAT=DETAILED en un volumen SnapLock. La salida es similar a este ejemplo:

```
Begin Reclaim Period: 09/05/2017
End Reclaim Period: 10/06/2017
```

Cuando IBM Spectrum Protect archiva archivos en un volumen SnapLock, realiza el seguimiento de la fecha de caducidad más lejana de estos archivos y el valor de BEGIN RECLAIM PERIOD se establece en esa fecha de caducidad más lejana. Cuando se agregan más archivos al volumen SnapLock, la fecha de inicio se establece en esa fecha más reciente si existe un archivo con una fecha de caducidad posterior a la que tiene actualmente el volumen. La fecha de inicio se establece en la fecha de caducidad más lejana de cualquier archivo de ese volumen. Se espera que todos los archivos de ese volumen ya deberían haber caducado o que deberían caducar ese día. Al día siguiente, en el volumen no queda ningún dato válido.

El parámetro END RECLAIM PERIOD se define en un mes después que la fecha de BEGIN RECLAIM PERIOD. La fecha de retención establecida en el servidor de archivos NetApp para ese volumen se define en la fecha END RECLAIM PERIOD. El servidor de archivos NetApp impide la supresión de ese volumen hasta que se llegue a la fecha de END RECLAIM PERIOD. Esta fecha es aproximadamente un mes después de la caducidad de los datos en el servidor de IBM Spectrum Protect. Cuando el servidor de IBM Spectrum Protect calcula una fecha de END RECLAIM PERIOD para el volumen, y la fecha es posterior a END RECLAIM PERIOD, la fecha se restablece en el servidor de archivos NetApp para dicho volumen a una fecha posterior. Restablecer los datos a una fecha posterior garantiza que el volumen IBM Spectrum Protect WORM FILE no se suprimirá hasta que los datos del volumen hayan caducado o hasta que los datos se hayan traspasado a otro volumen SnapLock.

El periodo de reclamación de IBM Spectrum Protect es el periodo de tiempo entre la fecha de inicio y la fecha final. Durante el periodo de reclamación, el servidor de IBM Spectrum Protect suprime los volúmenes en los que todos los datos han caducado, o debe traspasar los archivos que todavía no han caducado de volúmenes SnapLock caducados a nuevos volúmenes SnapLock con nuevas fechas. Este mes resulta de gran importancia en cuanto a la seguridad y eficacia con las que el servidor gestiona los datos de volúmenes WORM FILE. Normalmente, los datos de un volumen SnapLock ya han caducado cuando llega la fecha de inicio y el volumen debería estar vacío. Al llegar la fecha final, el volumen puede suprimirse con seguridad del inventario de IBM Spectrum Protect y del servidor de archivos SnapLock.

Sin embargo, algunos sucesos pueden provocar que haya datos válidos en un volumen SnapLock:

- Es posible que el proceso de la caducidad del servidor de IBM Spectrum Protect para ese volumen se haya pospuesto o no haya finalizado.
- Es posible que los parámetros de retención del grupo de copia o de las clases de gestión asociadas se hayan alterado para un archivo después de haberse archivado, y ese archivo no caducará hasta transcurrir un cierto periodo de tiempo.
- Es posible que se haya aplicado una espera de supresión a uno o más archivos del volumen.
- El proceso de reclamación se ha inhabilitado o ha encontrado errores al traspasar datos a los nuevos volúmenes SnapLock de una agrupación de almacenamiento SnapLock.
- Un archivo está esperando que se produzca un suceso para que el servidor de IBM Spectrum Protect pueda iniciar el proceso de caducidad del archivo.

Cuando llega la fecha de inicio y los archivos en un volumen SnapLock no han caducado, los archivos deben traspasarse a un nuevo volumen SnapLock con nuevas fechas de inicio y final. Sin embargo, si se retrasa el procesamiento de la caducidad en el servidor de IBM Spectrum Protect, y dichos archivos caducan cuando se ejecuta el procesamiento de la caducidad en el servidor de IBM Spectrum Protect, no resulta eficaz traspasar esos archivos a un nuevo volumen SnapLock. Para asegurarse de que no se produce ese traspaso de datos innecesario en los archivos que están a punto de caducar, el traspaso de archivos de los volúmenes SnapLock que caducan se

pospondrá hasta pasados unos días después de la fecha de BEGIN RECLAIM PERIOD date. Puesto que los datos están protegidos en el archivador SnapLock hasta la fecha de END RECLAIM PERIOD, no representa ningún riesgo posponer este traspaso de los datos. Esto permite que finalice el proceso de caducidad de IBM Spectrum Protect. Después de ese número de días, si todavía existen datos válidos en un volumen SnapLock que caduca, éstos se traspasarán a un nuevo volumen SnapLock, con lo que los datos siguen estando protegidos.

Puesto que los datos inicialmente estaban archivados, es posible que se hayan producido cambios en los parámetros de retención de los mismos (por ejemplo, en la clase de gestión o en los parámetros de agrupación de copia) o es posible que se haya aplicado una espera de supresión a esos datos. Sin embargo, los datos de ese volumen solo estarán protegidos por SnapLock hasta la fecha de END RECLAIM PERIOD. Los datos que no hayan caducado se traspasan a nuevos volúmenes SnapLock durante el periodo de reclamación de IBM Spectrum Protect. Si se producen errores al traspasar los datos a un nuevo volumen SnapLock, se emite un mensaje de aviso que indica que los datos pronto dejarán de estar protegidos. Si el error persiste, emita el mandato MOVE DATA para el volumen con problemas.

Atención: No inhabilite el proceso de reclamación de una agrupación de almacenamiento SnapLock. Una vez inhabilitado el proceso, el servidor de IBM Spectrum Protect no tiene forma de mostrar los mensajes de aviso de que los datos dejarán de estar protegidos. Esta situación también puede producirse si se inhabilitan la reclamación y migración para todo el servidor (por ejemplo, si se ha establecido NOMIGRRECL en el archivo de opciones del servidor). Asegúrese de que los datos estén protegidos al gestionar las agrupaciones de almacenamiento SnapLock.

## Configuración de la característica SnapLock para la retención basada en sucesos

---

Los datos almacenados en volúmenes SnapLock gestionados por IBM Spectrum Protect para retención de datos y la retención basada en sucesos pueden provocar una reclamación excesiva, lo que causará una disminución en el rendimiento del servidor.

Si los datos se gestionan mediante la retención basada en sucesos, IBM Spectrum Protect establece inicialmente el periodo de retención en el valor más grande de los valores RETVER y RETMIN para el grupo de copias archivadas. Cuando el volumen entra en el periodo de reclamación y los datos que permanecen en el volumen se trasladan, el periodo de retención del volumen de destino se establece en el periodo de retención restante de los datos, que normalmente es 0. El nuevo volumen entrará en el periodo de reclamación poco de recibir los datos, lo que provocará la reclamación de volúmenes que se acababan de crear.

Puede evitar esta situación utilizando la opción de servidor RETENTIONEXTENSION. Esta opción permite al servidor establecer o ampliar la fecha de retención de un volumen SnapLock. Puede especificar un valor en el rango de 30 - 9999 días. El valor predeterminado es 365 días.

Al seleccionar volúmenes de una agrupación de almacenamiento SnapLock para la reclamación, el servidor comprueba si el volumen está dentro del periodo de reclamación:

- Si el volumen no está dentro del periodo de retención, no se realiza ninguna acción. El volumen no se reclama y la fecha de retención no se modifica.
- Si el volumen está dentro del periodo de reclamación, el servidor comprueba si el porcentaje de espacio reclamable del volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento o del porcentaje de umbral pasado en el parámetro THRESHOLD de un mandato RECLAIM STGPOOL:
  - Si el espacio reclamable es mayor que el umbral, el servidor reclama el volumen y define la fecha de retención del volumen de destino en el valor mayor de los siguientes:
    - El periodo de retención restante de los datos más 30 días para el periodo de reclamación.
    - El valor RETENTIONEXTENSION más 30 días para el periodo de reclamación.
  - Si el espacio reclamable no es mayor que el umbral, el servidor restablece la fecha de retención del volumen según la cantidad especificada en la opción RETENTIONEXTENSION. El nuevo periodo de retención se calcula agregando el número de días especificado a la fecha actual.

En los ejemplos descritos a continuación, el volumen SnapLock, VolumeA, está en una agrupación de almacenamiento cuyo umbral de reclamación se establece en 60%. La opción de servidor RETENTIONEXTENSION se define en 365 días. El periodo de retención para VolumeA está en el periodo de reclamación. En las siguientes situaciones se muestra cómo queda afectada la retención:

- El espacio reclamable en VolumeA es inferior al 60%. La fecha de retención de VolumeA se amplía en 365 días.
- El espacio reclamable en VolumeA es superior al 60%, y el periodo de retención restante de los datos es superior a 365 días. VolumeA se reclama, y la fecha de retención del volumen de destino se define en el periodo de retención restante de los datos más 30 días para el periodo de reclamación.
- El espacio reclamable en VolumeA es superior al 60%, y el periodo de retención de los datos es inferior a 365 días. VolumeA se reclama y su fecha de retención se define en 365 días, el valor RETENTIONEXTENSION más 30 días para el periodo de reclamación.

## Protección de datos continua con la característica SnapLock

---

Si los datos se almacenan en un volumen con la característica SnapLock habilitada, y los datos se mueven o copian a un volumen que no sea SnapLock, los datos pierden la protección exclusiva por hardware que proporcionan los volúmenes NetApp WORM.

El servidor de IBM Spectrum Protect permite este tipo de movimiento. Sin embargo, si los datos se mueven de un volumen WORM FILE a otro tipo de medio, puede que los datos dejen de estar protegidos contra la supresión por error o intencionada. Si estos datos se encuentran en volúmenes WORM para cumplir los requisitos de retención y protección de datos para finalidades de condiciones de uso y se traspasan a otro medio, puede que los datos dejen de cumplir dichos requisitos. Debe configurar sus agrupaciones de almacenamiento de forma que este tipo de datos se mantenga en las agrupaciones de almacenamiento formadas por volúmenes WORM SnapLock durante todo el periodo de retención de datos.

## Configuración de los volúmenes SnapLock como volúmenes WORM FILE de IBM Spectrum Protect

---

Para cumplir los estrictos requisitos de los datos archivados, habilite la característica NetApp SnapLock.

### Acerca de esta tarea

---

Al definir o actualizar configuraciones que incluyen agrupaciones de almacenamiento SnapLock, asegúrese de que la opción RECLAMATIONTYPE=SNAPLOCK esté especificada para las agrupaciones de almacenamiento seleccionadas para los parámetros NEXTSTGPOOL, RECLAIMSTGPOOL y COPYSTGPOOLS.

Si configura las agrupaciones de almacenamiento de esta manera, ayuda a asegurar la protección de sus datos. Si define una agrupación de almacenamiento siguiente, de reclamación, de copia o de datos activos sin seleccionar la opción RECLAMATIONTYPE=SNAPLOCK, la agrupación de almacenamiento no está protegida. El mandato se ejecuta correctamente, pero se emite un mensaje de error.

### Procedimiento

---

Para configurar un volumen SnapLock para utilizar como un volumen IBM Spectrum Protect WORM FILE, complete los siguientes pasos:

1. Instale y configure SnapLock en el servidor de archivos NetApp. Asegúrese de configurar correctamente los períodos de retención mínimo, máximo y predeterminado. Para obtener instrucciones, consulte la documentación de NetApp.
2. Instale y configure el servidor de IBM Spectrum Protect.
3. Habilite la protección de retención de datos de archivos emitiendo mandato SET ARCHIVERETENTIONPROTECTION:

```
set archiveretentionprotection on
```

4. Configure la política mediante el mandato DEFINE COPYGROUP. Seleccione los valores RETVER y RETMIN en el grupo de copias archivadas que cumpla sus requisitos de protección de datos del almacenamiento WORM. Si no se especifican los valores RETVER ni RETMIN, se utilizan los valores de clases de gestión predeterminados.
5. Configure el almacenamiento mediante el mandato DEFINE DEVCLASS.
  - o Utilice la clase de dispositivo FILE.
  - o Especifique el parámetro DIRECTORY para que apunte al directorio o directorios de los volúmenes SnapLock.
6. Defina una agrupación de almacenamiento utilizando la clase de dispositivo que se define en el paso 5 emitiendo el mandato DEFINE STGPOOL y especifique el parámetro RECLAMATIONTYPE=SNAPLOCK.
7. Actualice el grupo de copias para que señale a la agrupación de almacenamiento emitiendo el mandato UPDATE COPYGROUP.
8. Utilice la API (interfaz de programación de aplicaciones) de IBM Spectrum Protect para archivar sus objetos en la agrupación de almacenamiento de SnapLock. Esta función no está disponible en los clientes de copia de seguridad/archivado de IBM Spectrum Protect estándar.

## Reparación y recuperación de datos en agrupaciones de almacenamiento de contenedores de directorios

---

Puede reparar extensiones de datos dañados en agrupaciones de almacenamiento de contenedores de directorios y recuperar datos perdidos después de un siniestro.

Las extensiones de datos forman parte de un archivo que se crea durante el proceso de eliminación de duplicados de datos. Las extensiones se comparan con otras extensiones de archivo para identificar los duplicados. Si su agrupación de almacenamiento de contenedores de directorio tiene archivos o directorios dañados, puede reparar las extensiones de datos con duplicados eliminados

desde el servidor de réplica de destino, el servidor de réplica de origen o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.

- Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino  
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen desde el servidor de réplica de destino.
- Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor  
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorios en el servidor de origen recuperando las extensiones de datos deduplicados de los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor del local o de fuera del local.
- Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor  
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.
- Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino  
Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de destino, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de origen.
- Reparación de agrupaciones de almacenamiento después de un siniestro  
Puede reparar las agrupaciones de almacenamiento de contenedores de directorio y recuperar los datos perdidos después de un siniestro.
- Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado  
Si se daña un volumen de cinta que almacena una copia de las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de copia de contenedor, puede sustituir el volumen.

**Conceptos relacionados:**

Estrategias para la protección ante siniestro

**Tareas relacionadas:**

Soluciones de protección de datos

Recuperación de pérdida de datos o de paradas del sistema

## Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino

---

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen desde el servidor de réplica de destino.

### Antes de empezar

---

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Asegúrese de que exista espacio suficiente en la agrupación de almacenamiento de contenedores de directorio para los datos recuperados. El parámetro PREVIEW=YES del mandato REPAIR STGPOOL especifica la cantidad de datos que se repararán. Si no hay espacio suficiente, utilice el mandato DEFINE STGPOOLDIRECTORY para proporcionar espacio.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados se reparan con las extensiones que se han protegido en el servidor de réplica de destino.

Restricción: Puede emitir el mandato REPAIR STGPOOL para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en otra agrupación de almacenamiento de un servidor de réplica de destino mediante el mandato PROTECT STGPOOL.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

## Procedimiento

---

1. Si sospecha que existen daños menores, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores en el nivel de directorio, de modo que pueda identificar las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio. Si identifica las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar. Para ahorrar tiempo y recursos, únicamente realice la auditoría de los contenedores que sospecha que están dañados. Si cree que su agrupación de almacenamiento de contenedores de directorio presenta un daño más grave, emita el mandato AUDIT CONTAINER en el nivel de la agrupación de almacenamiento.

Por ejemplo, para realizar la auditoría de un directorio, n:\pooldir, de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
```

Para realizar una auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Es posible que el proceso de auditoría tarde varias horas.

2. Para reparar una agrupación de almacenamiento de contenedores de directorio, emita el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER. Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

3. Identifique cualquier extensión dañada adicional con el mandato QUERY DAMAGED.
4. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:

- a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
- b. Si un directorio de agrupación de almacenamiento completo está dañado, cree un nuevo directorio de agrupación de almacenamiento de sustitución mediante el mandato DEFINE STGPOOLDIRECTORY.
- c. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

- d. Opcionalmente, emita el mandato DELETE STGPOOLDIRECTORY para suprimir el directorio de la agrupación de almacenamiento vacío que ha sustituido por un nuevo directorio en el paso 4.b.

## Qué hacer a continuación

---

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

### Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)  
DEFINE SCHEDULE (Definir una planificación para un mandato de administración)



QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)  
PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)  
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)  
DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)  
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

## Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor

---

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorios en el servidor de origen recuperando las extensiones de datos deduplicados de los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor del local o de fuera del local.

### Antes de empezar

---

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados se reparan con las extensiones que se han protegido en las agrupaciones de almacenamiento de copia de contenedor.

Restricción: Puede emitir el mandato REPAIR STGPOOL para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en las agrupaciones de almacenamiento de copia de contenedor mediante el mandato PROTECT STGPOOL.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

### Procedimiento

---

1. Si sospecha que existen daños menores, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores en el nivel de directorio, de modo que pueda identificar las incoherencias entre la base de datos y la agrupación de almacenamiento de contenedores de directorio. Si identifica las extensiones de datos dañados en la agrupación de almacenamiento de contenedores de directorio, puede determinar qué extensiones de datos se deben reparar. Para ahorrar tiempo y recursos, únicamente realice la auditoría de los contenedores que sospecha que están dañados. Si cree que su agrupación de almacenamiento de contenedores presenta un daño más grave, emita el mandato AUDIT CONTAINER en el nivel de la agrupación de almacenamiento. Por ejemplo, para realizar la auditoría de un directorio, n:\pooldir, de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1 stgpooldirectory=n:\pooldir
```

Para realizar una auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

Es posible que el proceso de auditoría tarde varias horas.

Durante la operación de reparación, el servidor le solicita los volúmenes que necesita. En el paso 3, traerá los volúmenes al local y los comprobará en la biblioteca. Los volúmenes necesarios se deben llevar al local y comprobar en la biblioteca.

2. Para obtener una vista previa de la operación de reparación y generar la lista de los volúmenes de cinta necesarios para la operación, emita el mandato REPAIR STGPOOL y especifique los parámetros SRCLOCATION=LOCAL y PREVIEW=YES.

Por ejemplo, para obtener la vista previa de la operación de reparación de una agrupación de almacenamiento con el nombre STGPOOL1 de las agrupaciones de almacenamiento de copia de contenedor, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local preview=yes
```

Es posible que el proceso de vista previa tarde algún tiempo en finalizar.

3. Si algunos de los volúmenes necesarios están fuera del local, realice los pasos siguientes:
  - a. Utilice la lista de la operación de vista previa para determinar qué volúmenes deben regresar al local.
  - b. Cuando los volúmenes estén en el local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE.
  - c. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.

Para obtener instrucciones detalladas sobre la función del gestor de recuperación ante siniestro (DRM), consulte Utilización del gestor de recuperación ante siniestro para entornos de cinta (V7.1.1).

4. En función de la información que obtenga durante la operación de vista previa, asegúrese de que la agrupación de almacenamiento tiene espacio suficiente para los datos recuperados. Si no hay espacio suficiente, utilice el mandato DEFINE STGPOOLDIRECTORY para proporcionar espacio.
5. Para reparar la agrupación de almacenamiento de contenedores de directorio, emita el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=LOCAL.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde una agrupación de almacenamiento de copia de contenedor, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

6. Identifique cualquier extensión dañada adicional con el mandato QUERY DAMAGED.
7. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde las agrupaciones de almacenamiento de copia de contenedor, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:
  - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
  - b. Si un directorio de agrupación de almacenamiento completo está dañado, cree un nuevo directorio de agrupación de almacenamiento de sustitución mediante el mandato DEFINE STGPOOLDIRECTORY.
  - c. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.  
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

- d. Opcionalmente, emita el mandato DELETE STGPOOLDIRECTORY para suprimir el directorio de la agrupación de almacenamiento vacío que ha sustituido por un nuevo directorio en el paso 7.b.
8. Si ha reparado un directorio de agrupación de almacenamiento completo, suprima el directorio original, que está vacío y se ha sustituido por un nuevo directorio. Suprima el directorio original emitiendo el mandato DELETE STGPOOLDIRECTORY.

## Qué hacer a continuación

---

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

### Referencia relacionada:

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)  
DEFINE SCHEDULE (Definir una planificación para un mandato de administración)  
QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)  
PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)  
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)  
DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)  
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

# Reparación de agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor

---

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de origen, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor.

## Antes de empezar

---

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

Asegúrese de que exista espacio suficiente en la agrupación de almacenamiento de contenedores de directorio para los datos recuperados. El parámetro `PREVIEW=YES` del mandato `REPAIR STGPOOL` especifica la cantidad de datos que se repararán. Si no hay espacio suficiente, utilice el mandato `DEFINE STGPOOLDIRECTORY` para proporcionar espacio.

## Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones que se han protegido en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor de un servidor de origen.

Restricción: Puede emitir el mandato `REPAIR STGPOOL` para una agrupación de almacenamiento especificada únicamente si ya ha copiado los datos en otra agrupación de almacenamiento de un servidor de réplica de destino, o en agrupaciones de almacenamiento de copia de contenedor, mediante el mandato `PROTECT STGPOOL`.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato `REPAIR STGPOOL` falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato `REPAIR STGPOOL` falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

## Procedimiento

---

1. Intente reparar la agrupación de almacenamiento desde el servidor de réplica realizando los pasos de la sección Reparación de agrupaciones de almacenamiento desde un servidor de réplica de destino.
2. Si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino, repare las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor realizando los pasos de la sección Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor.
3. Si ha reparado las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor, emita el mandato `PROTECT STGPOOL` y especifique el parámetro `TYPE=REPLSERVER` para las agrupaciones de almacenamiento del servidor de réplica de origen.

## Qué hacer a continuación

---

Si continúa detectando datos dañados después de un periodo de tiempo, emita el mandato `AUDIT CONTAINER` para la agrupación de almacenamiento de contenedores de directorio para determinar si existen daños más generalizados. Por ejemplo, para realizar la

auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

**Referencia relacionada:**

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)

REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)

DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

## Reparación de agrupaciones de almacenamiento en un servidor de réplica de destino

---

Si están dañados los archivos, directorios o agrupaciones de almacenamiento en un servidor de réplica de destino, puede reparar las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino recuperando las extensiones de datos con duplicados eliminados desde el servidor de réplica de origen.

### Antes de empezar

---

Evalúe su entorno de almacenamiento para determinar si las interrupciones, los problemas de red o las anomalías de hardware están dañando los datos o están provocando que los datos parezcan dañados. Si los problemas de su entorno están dañando los datos, identifique y resuelva los problemas.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños:

- Los daños menores debidos a que se han suprimido accidentalmente archivos o directorios, se han sobrescrito archivos, se han realizado cambios accidentales en los permisos de archivos o a que se han producido errores de disco por problemas de hardware.
- Daños moderados debidos a errores de disco o errores de montaje de disco. Este tipo de daños genera la pérdida de uno o varios directorios pero no la pérdida de toda la agrupación de almacenamiento.

Como parte de la operación del mandato PROTECT STGPOOL, se reparan las extensiones dañadas en la agrupación de almacenamiento de destino. Para que se puedan reparar, las extensiones ya deben estar marcadas como dañadas en el servidor de destino. Por ejemplo, un mandato AUDIT CONTAINER podría identificar daños en la agrupación de almacenamiento de destino antes de que se emita el mandato PROTECT STGPOOL.

### Procedimiento

---

1. Proteja las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio en un servidor de origen emitiendo el mandato PROTECT STGPOOL.

Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio con el nombre POOL1, emita el siguiente mandato:

```
protect stgpool pool1
```

Espere a que finalice el proceso de protección.

2. Para identificar las extensiones de datos dañadas que se encuentran en la agrupación de almacenamiento de contenedores de directorio del servidor de destino, emita el mandato AUDIT CONTAINER.

Por ejemplo, para realizar la auditoría de una agrupación de almacenamiento con el nombre STGPOOL1, emita el mandato siguiente:

```
audit container stgpool=stgpool1
```

3. Repare las extensiones dañadas en la agrupación de almacenamiento de destino emitiendo de nuevo el mandato PROTECT STGPOOL en el servidor de origen. Las extensiones dañadas en la agrupación de almacenamiento de destino se marcarán como dañadas y se repararán.
4. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.

**Referencia relacionada:**

AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

DEFINE SCHEDULE (Definir una planificación para un mandato de administración)  
QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)  
PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)  
REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)  
DEFINE STGPOOLDIRECTORY (Definir un directorio de agrupaciones de almacenamiento)  
DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

## Reparación de agrupaciones de almacenamiento después de un siniestro

---

Puede reparar las agrupaciones de almacenamiento de contenedores de directorio y recuperar los datos perdidos después de un siniestro.

En caso de siniestro, si su sitio primario ya no está disponible, puede reparar sus agrupaciones de almacenamiento de contenedores de directorio restaurándolas en un nuevo servidor de destino de su sitio de recuperación.

- Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro  
Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.
- Reparación de agrupaciones de almacenamiento desde un servidor de réplica después de un siniestro  
Si se produce un siniestro en un servidor de réplica, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.
- Reparación de las agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.  
Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

### Referencia relacionada:

Determinar si se deben utilizar agrupaciones de almacenamiento de copia de contenedor para la protección frente a siniestro

## Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro

---

Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de origen
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Está utilizando el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local desde un servidor de origen. Ha recuperado los volúmenes de cinta de fuera del local y los tiene en su sitio de recuperación.
- No ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en un servidor de réplica de destino.
- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dsmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de

dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

## Procedimiento

---

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.  
Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Si ha protegido la agrupación de almacenamiento de contenedores de directorio utilizando las agrupaciones de almacenamiento de copia de contenedor en el local y fuera del local, emita el mandato UPDATE STGPOOL para la copia del local de las agrupaciones de almacenamiento de copia de contenedor y especifique el parámetro ACCESS=UNAVAILABLE.
3. Cuando los volúmenes de la agrupación de almacenamiento de copia de contenedor de fuera del local regresen al local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE.
4. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.
5. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=LOCAL.  
Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde agrupaciones de almacenamiento de copia de contenedor de fuera del local, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=local
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

6. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
7. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

## Reparación de agrupaciones de almacenamiento desde un servidor de réplica después de un siniestro

---

Si se produce un siniestro en un servidor de réplica, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de réplica
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos desde un servidor de réplica de origen a un servidor de réplica de destino. El servidor de réplica de destino se ejecuta en su sitio de recuperación.
- No ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local.
- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dsmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de

dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

## Procedimiento

---

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica de destino, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

3. Si no ha utilizado scripts de configuración Blueprint para configurar el servidor de réplica de destino, es posible la estructura de archivos del servidor de réplica de destino no coincida con la información almacenada en la base de datos. Opcionalmente, elimine los directorios de la agrupación de almacenamiento que no existan en el servidor de réplica de destino, emitiendo el mandato DELETE STGPOOLDIRECTORY.
4. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
5. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad para permitir que se lleven a cabo las operaciones de copia de seguridad del cliente. Después de los dos ciclos de copia de seguridad, realice estos pasos:
  - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
  - b. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.  
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

6. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

### Referencia relacionada:

QUERY DAMAGED (Consultar los datos de la agrupación de almacenamiento dañada)

## Reparación de las agrupaciones de almacenamiento en un entorno con un servidor de réplica y volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.

---

Si se produce un siniestro en un servidor de origen, puede reparar las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio desde el servidor de réplica de destino o desde los volúmenes de cinta de la agrupación de almacenamiento de copia de contenedor que se encuentra fuera del local. La agrupación de almacenamiento de copia de contenedor se repara en un servidor de destino de una ubicación de recuperación.

### Acerca de esta tarea

---

Utilice el procedimiento para reparar los siguientes tipos de daños graves:

- Pérdida completa de todas las agrupaciones de almacenamiento de contenedores en el servidor de origen
- Pérdida completa del sitio primario

En este caso de ejemplo de recuperación ante siniestro se presupone lo siguiente:

- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos desde un servidor de réplica de origen a un servidor de réplica de destino. El servidor de réplica de destino se ejecuta en su sitio de recuperación.
- Ha utilizado el mandato PROTECT STGPOOL para realizar la copia de seguridad de los datos en las agrupaciones de almacenamiento de copia de contenedor fuera del local.
- Ha utilizado IBM Spectrum Protect Blueprints para configurar el servidor de origen de IBM Spectrum Protect y también ha utilizado scripts de configuración de Blueprint para restaurar el entorno configurando un nuevo servidor de destino en un sitio de recuperación. Los scripts han copiado versiones de copia de seguridad de la base de datos de IBM Spectrum Protect, el archivo de opciones del servidor (dsmserv.opt), el archivo de historial de volúmenes (volhist.out) y el archivo de configuración de dispositivos (devconfig.out) en sus ubicaciones originales en el servidor de recuperación. Después de ejecutar los scripts puede ver los directorios vacíos que se acaban de crear en el servidor de recuperación.

Cuando intenta reparar una agrupación de almacenamiento de contenedores de directorio desde un servidor de réplica de destino, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- El servidor de réplica de destino no está disponible.
- La agrupación de almacenamiento de destino está dañada.
- Se produce una parada de red.

Cuando repara una agrupación de almacenamiento de contenedores de directorio desde las agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla si se produce cualquiera de las condiciones siguientes:

- La agrupación de almacenamiento de copia de contenedor no está disponible.
- La agrupación de almacenamiento de copia de contenedor está dañada.
- La agrupación de almacenamiento de copia de contenedor no está disponible o está dañada.

## Procedimiento

---

1. Marque todas las extensiones de datos de la agrupación de almacenamiento de contenedores como dañadas emitiendo el mandato AUDIT CONTAINER para la agrupación de almacenamiento de contenedor, en el nivel de agrupación de almacenamiento, y especifique el parámetro ACTION=MARKDAMAGED.

Por ejemplo, para auditar una agrupación de almacenamiento con el nombre STGPOOL1 y marcarla como dañada, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=markdamaged
```

2. Si ha protegido la agrupación de almacenamiento de contenedores de directorio utilizando las agrupaciones de almacenamiento de copia de contenedor en el local y fuera del local, emita el mandato UPDATE STGPOOL para la copia del local de las agrupaciones de almacenamiento de copia de contenedor y especifique el parámetro ACCESS=UNAVAILABLE.
3. Cuando los volúmenes de la agrupación de almacenamiento de copia de contenedor de fuera del local regresen al local, compruébelos en la biblioteca emitiendo el mandato CHECKIN LIBVOLUME con el parámetro STATUS=PRIVATE. Si ahora traslada los volúmenes de cinta al local, estará preparado para reparar las extensiones dañadas de los volúmenes de cinta de copia de contenedor, si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino.
4. Actualice el estado de los volúmenes emitiendo el mandato UPDATE STGPOOL y especificando el parámetro ACCESS=READWRITE.
5. Repare la agrupación de almacenamiento emitiendo el mandato REPAIR STGPOOL y especifique el parámetro SRCLOCATION=REPLSERVER.

Por ejemplo, para reparar una agrupación de almacenamiento con el nombre STGPOOL1 desde un servidor de réplica de destino, emita el mandato siguiente:

```
repair stgpool stgpool1 srclocation=replserver
```

Cuando emite el mandato REPAIR STGPOOL, se suprimen las extensiones dañadas del volumen inmediatamente después de que hayan sido reparadas. Las extensiones dañadas no se retienen según el valor especificado con el parámetro REUSEDELAY.

6. Si no ha utilizado scripts de configuración Blueprint para configurar el servidor de réplica de destino, es posible la estructura de archivos del servidor de réplica de destino no coincida con la información almacenada en la base de datos. Opcionalmente, elimine los directorios de la agrupación de almacenamiento que no existan en el servidor de réplica de destino. Emita el mandato DELETE STGPOOLDIRECTORY para suprimir los directorios que no estén en el servidor de réplica de destino.
7. Confirme que no existen extensiones dañadas adicionales con el mandato QUERY DAMAGED.
8. Si no se pueden reparar las extensiones dañadas desde el servidor de réplica de destino, puede reparar las extensiones dañadas desde las agrupaciones de almacenamiento de copia de contenedor de fuera del local. Para obtener las instrucciones, consulte



Reparación de agrupaciones de almacenamiento desde volúmenes de agrupación de almacenamiento de copia de contenedor después de un siniestro.

9. Confirme que no existen extensiones dañadas adicionales volviendo a emitir el mandato QUERY DAMAGED.
10. Si se detectan daños y no se pueden reparar las extensiones con duplicados eliminados desde el servidor de réplica, todavía es posible repararlas. En algunos casos, el nodo del cliente vuelve a enviar los datos durante una operación de copia de seguridad y las extensiones dañadas se reparan. Espere a que se ejecuten dos ciclos de copia de seguridad. Después de los dos ciclos de copia de seguridad, realice estos pasos:
  - a. Para confirmar que se ha reparado el daño, vuelva a emitir el mandato QUERY DAMAGED.
  - b. Para eliminar objetos que hacen referencia a datos dañados, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED.  
Por ejemplo, para auditar una agrupación de almacenamiento de contenedores de directorio con el nombre STGPOOL1 y eliminar los objetos dañados, emita el mandato siguiente:

```
audit container stgpool=stgpool1 action=removedamaged
```

11. Repita este procedimiento para reparar todas las agrupaciones de almacenamiento.

## Sustitución de un volumen de cinta de agrupación de almacenamiento de copia de contenedor dañado

---

Si se daña un volumen de cinta que almacena una copia de las extensiones de datos con duplicados eliminados de una agrupación de almacenamiento de copia de contenedor, puede sustituir el volumen.

### Procedimiento

---

1. Suprima el volumen de cinta dañado emitiendo el mandato DELETE VOLUME y especificando el parámetro DISCARDDATA=YES. Por ejemplo, para suprimir un volumen con el nombre VOLUME1, emita el siguiente mandato:

```
delete volume volume1 discarddata=yes
```

2. Puede proteger las extensiones de datos de una agrupación de almacenamiento de contenedores de directorio copiando los datos en los volúmenes existentes de una agrupación de almacenamiento de copia de contenedor. Emita el mandato PROTECT STGPOOL desde el servidor de origen.  
Por ejemplo, para proteger una agrupación de almacenamiento de contenedores de directorio con el nombre POOL1, emita el siguiente mandato:

```
protect stgpool pool1 type=local
```

#### Referencia relacionada:

PROTECT STGPOOL (Protección de datos de agrupación de almacenamiento)  
DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

## Mandatos, opciones y programas de utilidad del servidor

---

Utilice mandatos para administrar y configurar el servidor, opciones para personalizar el servidor y los programas de utilidad para realizar tareas especiales cuando el servidor no se está ejecutando.

- Gestión del servidor desde la línea de mandatos  
IBM Spectrum Protect proporciona varias interfaces de línea de mandatos diferentes para gestionar servidores de IBM Spectrum Protect.
- Comandos de administración  
Los comandos de administración están disponibles para gestionar y configurar el servidor.
- Opciones de servidor  
Durante la instalación, IBM Spectrum Protect proporciona un archivo de opciones de servidor que contiene un conjunto de opciones predeterminadas para iniciar el servidor.
- Herramientas del servidor  
Utilice las herramientas del servidor para realizar tareas especiales en el servidor mientras éste no está en ejecución.
- Códigos de retorno de los scripts para IBM Spectrum Protect  
Puede escribir scripts de IBM Spectrum Protect que utilizan códigos de retorno para determinar cómo continúa el proceso de script. Los códigos de retorno pueden ser de una de estas tres gravedades: OK, WARNING, ERROR.
- Programas de utilidad de dispositivos  
Puede utilizar programas de utilidad de dispositivos para las tareas que están relacionadas con la configuración de dispositivos de almacenamiento para el servidor de IBM Spectrum Protect.

- Scripts del servidor y macros para la automatización  
Puede automatizar las tareas administrativas más comunes creando scripts del servidor de IBM Spectrum Protect o macros del cliente administrativo. Los scripts del servidor se almacenan en la base de datos del servidor y pueden planificarse para ejecutarse con un comando de planificación de administración. Las macros del cliente administrativo se almacenan como archivos en el cliente administrativo.

## Gestión del servidor desde la línea de mandatos

---

IBM Spectrum Protect proporciona varias interfaces de línea de mandatos diferentes para gestionar servidores de IBM Spectrum Protect.

### Acerca de esta tarea

---

Están disponibles las interfaces de línea de mandatos siguientes:

#### Cliente de línea de comandos de administración

El cliente de línea de comandos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal. Se instala como parte del proceso de instalación del servidor de IBM Spectrum Protect. Se puede acceder al cliente de administración remotamente.

En el cliente de administración, puede emitir cualquier mandato de servidor.

#### Consola del servidor

La consola del servidor es una ventana de línea de mandatos en el sistema en el que está instalado el servidor. Por consiguiente, para utilizar la consola del servidor, debe encontrarse en la ubicación física del sistema servidor.

En comparación con el cliente de administración, las capacidades de la consola del servidor son limitadas. Desde la consola del servidor, no puede emitir determinados mandatos y no puede direccionar mandatos a otros servidores. Además, no puede especificar que determinados mandatos se procesen antes de que puedan emitirse otros mandatos. No obstante, esta limitación puede ser útil si, por ejemplo, desea ejecutar dos mandatos en sucesión rápida.

#### Línea de mandatos de Centro de operaciones

En el Centro de operaciones, puede acceder a la línea de mandatos de IBM Spectrum Protect. Puede que desee utilizar esta línea de mandatos para emitir mandatos del servidor y completar determinadas tareas de IBM Spectrum Protect que no están soportadas en el Centro de operaciones.

Los scripts de servidor proporcionan la automatización de las tareas administrativas comunes. Una macro es un archivo que contiene uno o varios comandos de administración de IBM Spectrum Protect. Cuando se emite el mandato MACRO, el servidor procesa todos los mandatos del archivo de macro en orden, incluidos los mandatos que están contenidos en las macros anidadas.

- Emisión de comandos del cliente de administración  
El cliente de línea de comandos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal.
- Emisión de mandatos desde el Centro de operaciones  
En la interfaz de mandatos del Centro de operaciones, puede emitir mandatos para gestionar servidores de IBM Spectrum Protect que están configurados como servidores concentradores o de radio.
- Emisión de comandos desde la consola del servidor  
IBM Spectrum Protect proporciona un ID de usuario denominado SERVER\_CONSOLE que permite emitir comandos y administrar el servidor desde la consola del servidor después de instalar IBM Spectrum Protect. Durante la instalación, SERVER\_CONSOLE se registra automáticamente como un administrador y se le otorga autorización del sistema.
- Especificación de comandos de administración  
Los mandatos se componen de nombres de mandatos y suelen contener parámetros y variables. Los diagramas de sintaxis muestran las reglas que deben seguirse al especificar comandos.
- Control del proceso de comandos  
Puede ejecutar algunos comandos de IBM Spectrum Protect secuencialmente o simultáneamente con otros comandos. También puede direccionar los comandos de un servidor a otros servidores para su proceso.
- Realización de tareas simultáneamente en varios servidores  
El direccionamiento de comandos permite direccionar los comandos a uno o más servidores para que los procesen y, a continuación, recopilar la salida de estos servidores.
- Clases de privilegio  
La autorización que se otorga a un administrador mediante la clase de privilegio determina qué mandatos de administración puede emitir el administrador.

#### Conceptos relacionados:

Scripts de servidor

#### Referencia relacionada:

## Emisión de comandos del cliente de administración

---

El cliente de línea de comandos de administración es un programa que se ejecuta en un servidor de archivos, estación de trabajo o sistema principal.

### Acerca de esta tarea

---

Asegúrese de que su el servidor y el cliente de administración utilizan idiomas compatibles. Consulte el apartado LANGUAGE para conocer opciones de idioma y entorno regional. Si el cliente y el servidor utilizan idiomas diferentes, los mensajes que genere IBM Spectrum Protect podrían no ser comprensibles.

Consejo: Las series de texto que se envían desde el cliente al servidor no dependen del valor de idioma del servidor. El texto se muestra correctamente si el cliente administrativo se ejecuta en el mismo entorno local al enviar la serie y al recibir la serie.

Por ejemplo, suponga que actualiza un campo de contacto de nodo con un valor que contiene caracteres nacionales (`update node miNodo contact=información_contacto_NL`), y más adelante consulta el nodo (`query node miNodo format=detailed`). Si el cliente se ejecuta en el mismo entorno local cuando se actualiza y cuando se consulta, la *información\_contacto\_NL* se visualiza correctamente. Si actualiza el campo de contacto de nodo cuando el cliente se ejecuta en un entorno local y consulta el nodo cuando el cliente se está ejecutando en un entorno local diferente, es posible que la *información\_contacto\_NL* no se visualice correctamente.

- Inicio y detención del cliente de administración  
Utilice el comando DSMADMC para iniciar una sesión del cliente de administración.
- Supervisión de actividades del servidor desde el cliente de administración  
Para supervisar actividades de IBM Spectrum Protect, como la migración del servidor e inicios de sesión de cliente, ejecute el cliente de administración en modalidad de consola. No puede entrar ningún comando de administración en modalidad de consola.
- Supervisión de montajes de medios extraíbles del cliente de administración  
Para supervisar el montaje y desmontaje de medios extraíbles, ejecute el cliente de administración en modalidad de montaje. Cuando el cliente se ejecuta en modalidad de montaje, no puede especificar comandos de administración.
- Proceso de mandatos individuales desde el cliente de administración  
Utilice la modalidad de proceso por lotes para especificar un solo comando de administración. La sesión del cliente de administración finaliza automáticamente cuando se procesa el mandato.
- Proceso de una serie de comandos del cliente de administración  
Utilice la modalidad interactiva para procesar una serie de comandos de administración.
- Formateo de la salida de los comandos  
IBM Spectrum Protect formatea la salida procesada de los comandos según el ancho de la pantalla o de la ventana.
- Cómo guardar la salida del comando en una ubicación especificada  
El uso más común para redirigir la salida es guardar la salida de los comandos de consulta en un archivo o programa especificado. A continuación, puede examinar el contenido del archivo o, en algunos casos, imprimir dicho contenido.
- Opciones de cliente de administración  
En todas las modalidades del cliente de administración, se pueden utilizar las opciones para modificar las respuestas a la sesión del cliente de administración.

## Inicio y detención del cliente de administración

---

Utilice el comando DSMADMC para iniciar una sesión del cliente de administración.

### Acerca de esta tarea

---

El servidor de IBM Spectrum Protect debe encontrarse en ejecución para que un cliente de administración pueda conectarse.

### Procedimiento

---

- Para iniciar una sesión del cliente de administración en modalidad de línea de comandos, especifique este comando en la estación de trabajo.

```
dsmadmc -id=admin -password=admin -dataonly=yes
```

Si especifica el comando DSMADMC con las opciones -ID y -PASSWORD como se muestra, no se le solicitan un ID de usuario y una contraseña.

- Para detener una sesión de cliente de línea de comandos administrativos, escriba el mandato siguiente:

quit

- Para interrumpir un comando DSMADMC antes de que el servidor de IBM Spectrum Protect termine de procesarlo, utilice el comando UNIX `kill -9` en una línea de comandos disponible. No pulse `Control+C` porque, cuando finaliza la sesión, puede producir resultados inesperados.

## Supervisión de actividades del servidor desde el cliente de administración

Para supervisar actividades de IBM Spectrum Protect, como la migración del servidor e inicios de sesión de cliente, ejecute el cliente de administración en modalidad de consola. No puede entrar ningún comando de administración en modalidad de consola.

### Procedimiento

- Para iniciar una sesión de cliente de administración en modalidad de consola, especifique el siguiente comando:

```
dsmadmc -consolemode
```

Se le solicitará una contraseña si está activada la autenticación para el servidor. Si no desea que se le solicite el ID de usuario y la contraseña, entre el mandato DSMADMC con las opciones `-ID` y `-PASSWORD`.

- Para finalizar una sesión de cliente de administración en modalidad de consola, utilice una secuencia de interrupción de teclado.

Sistema operativo	Secuencia de interrupción
Clientes de UNIX y Linux	Control+C
Clientes de Windows	Control+C o Control+INTER

## Supervisión de montajes de medios extraíbles del cliente de administración

Para supervisar el montaje y desmontaje de medios extraíbles, ejecute el cliente de administración en modalidad de montaje. Cuando el cliente se ejecuta en modalidad de montaje, no puede especificar comandos de administración.

### Procedimiento

- Para iniciar una sesión de cliente de administración en modalidad de montaje, especifique el siguiente comando:

```
dsmadmc -mountmode
```

Se le solicitará una contraseña si está activada la autenticación para el servidor. Si no desea que se le solicite el ID de usuario y la contraseña, entre el mandato DSMADMC con las opciones `-ID` y `-PASSWORD`.

- Para finalizar una sesión de cliente de administración en modalidad de montaje, utilice una secuencia de interrupción de teclado.

Sistema operativo	Secuencia de interrupción
Clientes de UNIX y Linux	Control+C
Clientes de Windows	Control+C o Control+INTER

## Proceso de mandatos individuales desde el cliente de administración


Utilice la modalidad de proceso por lotes para especificar un solo comando de administración. La sesión del cliente de administración finaliza automáticamente cuando se procesa el mandato.

### Procedimiento

Para iniciar una sesión de cliente de administración en modalidad de proceso por lotes, use el siguiente mandato `dsmadmc mandato_servidor`:

Si no desea que se le solicite el identificador de usuario y la contraseña, puede entrar el mandato DSMADMC con las opciones `-ID` y `-PASSWORD`.

En modalidad por lotes, debe entrar el comando completo en una línea. Si un comando no cabe en una línea, entre el comando utilizando una macro o un script. Si especifica un parámetro con un texto utilizando la modalidad de proceso por lotes, delimite el texto entre comillas simples ( ' ') en la macro. No utilice comillas dobles para los comandos en la modalidad por lotes, pues puede que el sistema operativo no analice correctamente las comillas.

 Sistemas operativos Windows Puede eludir esta restricción de las comillas dobles en la modalidad por lotes para los clientes de Windows con el carácter de escape de barra inclinada invertida (\). Por ejemplo, en el parámetro OBJECTS del mandato DEFINE CLIENTACTION, puede especificar la serie con el carácter \ delante de las comillas dobles del comando.

```
dsmadmc -id=admin -password=admin define
clientaction test_node domain=test_dom
action=restore objects="'C:\Archivos de programa\test\*'"'
```

## Proceso de una serie de comandos del cliente de administración

---

Utilice la modalidad interactiva para procesar una serie de comandos de administración.

### Acerca de esta tarea

---

Para arrancar una sesión de cliente de administración en modalidad interactiva, debe haber disponible una sesión del servidor. Para garantizar la disponibilidad de las sesiones del servidor para sesiones de administración y de nodo cliente, la modalidad interactiva del cliente de administración se desconecta si se cumplen una o varias de las condiciones siguientes:

- El servidor se ha detenido utilizando el comando HALT.
- Los comandos no se han emitido desde la sesión de cliente de administración durante el plazo de tiempo especificado con la opción del servidor IDLETIMEOUT.
- La sesión del cliente de administración se ha cancelado con el comando CANCEL SESSION.

### Procedimiento

---

Para iniciar una sesión de cliente de administración en modalidad interactiva, utilice el siguiente mandato: `dsmadmc`.

Puede utilizar caracteres de continuación en la modalidad interactiva. Para obtener más información, consulte el apartado Utilización de caracteres de continuación para entrar mandatos largos.

Puede reiniciar automáticamente la sesión de cliente de administración si especifica otro comando cada vez que aparece el indicador `tsm: nombre_servidor >`.

No especifique un comando de servidor con el comando DSMADMC. Si lo hace, se iniciará el cliente de administración en modo por lotes, no en modo interactivo. Por ejemplo, no especifique:

```
dsmadmc comando_servidor
```

## Formateo de la salida de los comandos

---

IBM Spectrum Protect formatea la salida procesada de los comandos según el ancho de la pantalla o de la ventana.

### Procedimiento

---

- Si la anchura de la pantalla o ventana no es suficiente para visualizar la salida horizontalmente, IBM Spectrum Protect organiza y visualiza la información verticalmente.
- Puede formatear la salida de los mandatos QUERY utilizando las opciones del cliente de administración DISPLAYMODE y OUTFILE.

## Cómo guardar la salida del comando en una ubicación especificada

---

El uso más común para redirigir la salida es guardar la salida de los comandos de consulta en un archivo o programa especificado. A continuación, puede examinar el contenido del archivo o, en algunos casos, imprimir dicho contenido.

### Acerca de esta tarea

---

En algunos sistemas operativos, es posible redirigir la salida de un comando si se utilizan caracteres especiales como, por ejemplo, `>`, `>>` y `|`. Los caracteres de redirección dirigen la salida de un comando a un archivo o programa que se especifique en lugar de dirigirla a la pantalla. Puede guardar la salida de un comando entrando los caracteres de redirección al final del comando. Para redirigir la salida, deje un espacio en blanco entre el carácter de redirección y el nombre del archivo o programa. Consulte los ejemplos siguientes.

Al redirigir la salida, debe seguir los convenios de denominación del sistema operativo en el que esté ejecutando el cliente administrativo.

## Procedimiento

Los ejemplos de la tabla siguiente muestran cómo redirigir la salida del mandato.

Tarea	Procedimiento
Redirigir la salida del comando QUERY DOMAIN a un nuevo archivo en modalidad interactiva o de proceso por lotes	Utilice un único signo de mayor que (>) para redirigir la salida a un nuevo archivo o grabar sobre un archivo existente:  <code>dsmadmc -id=xxx -pa=xxx query domain acctg &gt; dominfo.acc</code>
Agregar la salida de un comando QUERY DOMAIN al final de un archivo existente en modalidad de proceso por lotes o interactiva	Utilice dos signos de mayor que (>>) para añadir la salida al final de un archivo existente:  <code>dsmadmc -id=xxx -pa=xxx query domain acctg &gt;&gt; dominfo.acc</code>
Redirigir toda la salida de una sesión de cliente de administración en modalidad de consola a un programa denominado filter.exe	Utilice la barra vertical ( ) para dirigir toda la salida de una sesión a un programa:  <code>dsmadmc -console -id=admin -password=xxx   filter.exe</code>  El programa se puede configurar para supervisar la salida de mensajes individuales a medida que se producen y realizar la acción adecuada como, por ejemplo, enviar correo a otro usuario.
En la modalidad de consola, redirigir toda la salida a un archivo	Especifique la opción -OUTFILE con el nombre de un archivo de destino. Por ejemplo, el comando siguiente redirige toda la salida al archivo save.out:  <code>dsmadmc -id=sullivan -password=secret -consolemode -outfile=save.out</code>

## Opciones de cliente de administración

En todas las modalidades del cliente de administración, se pueden utilizar las opciones para modificar las respuestas a la sesión del cliente de administración.

### Sintaxis

```
-----  
v                                     |  
>>-DSMADMC-----+-----+----->  
      '-opción_cliente_administración-'  
  
>--+-----+-----<<  
      '-comando_servidor-'
```

### Ejemplo de uso de opciones del cliente administrativo

Puede especificar el mandato DSMADMC con su ID de usuario y su contraseña si utiliza las opciones -ID y -PASSWORD para que no se le solicite esa información. Para que IBM Spectrum Protect redirija toda la salida a un archivo, especifique la opción -OUTFILE con un nombre de archivo destino. Por ejemplo, para emitir el comando QUERY NODE en modalidad de proceso por lotes con la salida redirigida al archivo SAVE.OUT, especifique:

```
dsmadmc -id=sullivan -password=secret -outfile=save.out query node
```

### Opciones

Las opciones de cliente de administración se pueden especificar con el comando DSMADMC y sólo son válidas desde una sesión de cliente de administración. Puede teclear una opción en letras mayúsculas, minúsculas o en cualquier combinación de mayúsculas/minúsculas. Las letras en mayúsculas indican la abreviatura más reducida que resulta aceptable. Si una opción aparece totalmente en letras mayúsculas, no se puede abreviar.

#### -ALWAYSPrompt

Especifica que se visualice un indicador de comandos si la entrada se lleva a cabo desde el teclado o si es redirigida (por ejemplo, desde un archivo). Si no se especifica esta opción y se redirige la entrada, el indicador de comandos no se graba.

Si la entrada se redirige, sólo se visualiza la salida del comando. Si se especifica esta opción, se visualizan el indicador de comandos y la salida de comando.

**-CHECKAliashalt**

Permite al cliente de administración reconocer un alias para el comando HALT tal como se ha establecido en la opción de servidor ALIASHALT. Consulte la publicación ALIASHALT para obtener más detalles.

**-COMMA delimited**

Especifica que cualquier salida tabular desde una consulta del servidor se ha de formatear como series separadas por comas, en lugar de en un formato legible. Esta opción está concebida para utilizarse principalmente al redirigir la salida de una consulta SQL (comando SELECT). El formato de valores separados mediante comas es un formato de datos estándar que la mayoría de los programas comunes pueden procesar, incluidos las hojas de cálculo, las bases de datos y los programas de generación de informes.

**-CONsolemode**

Especifica que IBM Spectrum Protect se ejecuta en modalidad de consola. La mayor parte de la salida de consola del servidor se repite en la pantalla. La excepción son artículos tales como respuestas a mandatos de consulta que se emiten desde la consola, salida de rastreo o cualquier mensaje del sistema que se visualiza en la consola.

**-DATAONLY=NO o YES**

Especifica si la información de versión del producto y las cabeceras de salida se muestran con la salida. El valor predeterminado es NO.

NO

Especifica que se muestre la información de versión del producto y las cabeceras de columna de salida.

YES

Suprime la información de versión del producto y las cabeceras de columna de salida.

**-DISPLAymode=LIST o TABLE**

Puede forzar la salida QUERY en formato tabular o lista independientemente del ancho de columna de la ventana de línea de mandatos.

Si está utilizando la opción -DISPLAYMODE y desea que la salida vaya a un archivo, no especifique la opción -OUTFILE. Para escribir en el archivo utilice la redirección.

**-ID=ID\_usuario**

Especifica el ID de usuario del administrador.

**-Itemcommit**

Especifica que IBM Spectrum Protect valida los comandos que hay en un script o en una macro a medida que se procesa cada comando.

**-MOUNTmode**

Especifica que IBM Spectrum Protect se ejecuta en modalidad de montaje. Todos los mensajes de montaje de medios extraíbles se repetirán su pantalla.

**-NEWLINEAFTERPrompt**

Especifica que un carácter de línea nueva debe escribirse después de que el indicador de mandatos y los mandatos que se han entrado desde el teclado se visualizan debajo de la petición. Si no se especifica esta opción, los mandatos especificados desde el teclado se visualizan en la parte derecha de la petición.

**-NOConfirm**

Especifica que no desea que IBM Spectrum Protect solicite confirmación antes de procesar mandatos que afectan a la disponibilidad del servidor o de los datos que gestiona el servidor.

**-OUTfile**

Especifica que la salida de una consulta del servidor se visualiza en una fila. Si la salida en una fila supera el ancho de columna que define el servidor, la salida se visualiza en varias líneas en dicha fila. Esta opción sólo está disponible en modalidad de proceso por lotes.

**-OUTfile=nombreadarchivo**

Especifica que la salida de un servidor se redirige a un archivo especificado. En la modalidad de proceso por lotes, la salida se redirige al archivo que especifique y el formato de la salida coincide con el formato de la salida de la pantalla.



En las sesiones de modalidad interactiva, de consola o de montaje, la salida se visualiza en la pantalla.



**-PAssword=contraseña**

Especifica la contraseña del administrador.

**-Quiet**

Especifica que IBM Spectrum Protect no visualiza mensajes de salida estándares en su pantalla. Sin embargo, cuando utilice esta opción, continuarán apareciendo determinados mensajes de error.

 **Sistemas operativos AIX**  **Sistemas operativos Linux-SERveraddress**

 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifica la stanza del servidor en el archivo dsm.sys. El cliente utiliza la stanza del servidor para determinar el servidor al que se conecta. La opción SERVERADDRESS está soportada por clientes administrativos que se ejecutan solo en sistemas operativos UNIX, Linux y Macintosh.

**-TAB delimited**

Especifica que cualquier salida tabular desde una consulta del servidor se ha de formatear como series separadas por tabulaciones en lugar de en un formato legible. Esta opción está concebida para utilizarse principalmente al redirigir la salida de

una consulta SQL (comando SELECT). El formato de valor separado por tabulaciones es un formato de datos estándar que pueden procesar muchos programas comunes, incluidos generadores de informes, de bases de datos y hojas de cálculo.

-TCPPort

Especifica una dirección de puerto TCP/IP para un servidor de IBM Spectrum Protect. La opción TCPPORT solo está soportada por clientes de administración que se ejecutan en sistemas operativos Windows y es válida en la línea de mandatos del cliente de administración de Windows.

-TCPServeraddress

Especifica una dirección de servidor TCP/IP para un servidor de IBM Spectrum Protect. La opción TCPSEVERADDRESS sólo está soportada por clientes de administración que se ejecutan en sistemas operativos Windows y es válida en la línea de mandatos del cliente de administración de Windows.

Además de las opciones que se listan aquí, también puede especificar cualquier opción que se encuentra en el archivo de opciones del cliente. Cada opción debe tener antepuesto un guión y estar delimitada con un espacio.


## Emisión de mandatos desde el Centro de operaciones

---

En la interfaz de mandatos del Centro de operaciones, puede emitir mandatos para gestionar servidores de IBM Spectrum Protect que están configurados como servidores concentradores o de radio.

### Procedimiento

---

Para abrir la interfaz de línea de mandatos, pase el ratón sobre el icono de globo  en la barra de menús del Centro de operaciones y pulse Creador de comandos.

## Emisión de comandos desde la consola del servidor

---

IBM Spectrum Protect proporciona un ID de usuario denominado SERVER\_CONSOLE que permite emitir comandos y administrar el servidor desde la consola del servidor después de instalar IBM Spectrum Protect. Durante la instalación, SERVER\_CONSOLE se registra automáticamente como un administrador y se le otorga autorización del sistema.

### Acerca de esta tarea

---

Si tiene privilegios del sistema, puede revocar u otorgar nuevos privilegios al ID de usuario SERVER\_CONSOLE. No puede realizar ninguna de las acciones siguientes:

- Inscribir o actualizar el identificador de usuario SERVER\_CONSOLE
- Bloquear o desbloquear el identificador de usuario SERVER\_CONSOLE
- Redenominar el identificador de usuario SERVER\_CONSOLE
- Suprimir el identificador de usuario SERVER\_CONSOLE
- Direccionar comandos del identificador de usuario SERVER\_CONSOLE

La consola del sistema no admite todos los comandos de IBM Spectrum Protect. No se puede especificar el parámetro WAIT desde la consola del servidor.

## Especificación de comandos de administración

---

Los mandatos se componen de nombres de mandatos y suelen contener parámetros y variables. Los diagramas de sintaxis muestran las reglas que deben seguirse al especificar comandos.

### Acerca de esta tarea

---

Para mostrar la ayuda de línea de comandos para los comandos de servidor que tienen nombres exclusivos, puede escribir `help nombre_comando`, donde `nombre_comando` es el nombre del comando de servidor para el que desea información. Por ejemplo, para mostrar ayuda para el comando REGISTER NODE, escriba `help nodo de registro`. La sintaxis del comando y las descripciones de parámetro se muestran en la salida.

Puede escribir también `help` seguido del número de tema del comando. Los números de tema se muestran en la ayuda de línea de comandos, por ejemplo:

```
3.0 Administrative commands
  3.46 REGISTER
    3.46.1 REGISTER ADMIN (Registrar un administrador)
    3.46.2 REGISTER LICENSE (Registrar una nueva licencia)
    3.46.3 REGISTER NODE (Registrar un nodo)
```



Para mostrar ayuda sobre el comando REGISTER NODE, escriba:

```
help 3.46.3
```

Utilice números de tema para mostrar la ayuda de línea de mandatos para los subcomandos. DEFINE DEVCLASS es un ejemplo de un mandato que tiene subcomandos. Por ejemplo, puede especificar el mandato DEFINE DEVCLASS para las clases de dispositivo 3590 y para las clases de dispositivo 3592:

```
3.0 Administrative commands
...
3.13.10 DEFINE DEVCLASS (Definir una clase de dispositivo)
  3.13.10.1 DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
  3.13.10.2 DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
  ...
```

Para mostrar ayuda para el mandato DEFINE DEVCLASS para las clases de dispositivo 3590, escriba:

```
help 3.13.10.1
```

- Lectura de los diagramas de sintaxis  
Para leer un diagrama de sintaxis que indica cómo especificar un mandato, siga la ruta de la línea. Léalo de izquierda a derecha y de arriba a abajo.
- Utilización de caracteres de continuación para entrar mandatos largos  
Los caracteres de continuación resultan útiles para procesar un mandato cuya longitud es mayor que la anchura de la pantalla o ventana. Puede utilizar caracteres de continuación en la modalidad interactiva del cliente de administración.
- Denominación de objetos de IBM Spectrum Protect  
IBM Spectrum Protect restringe el número y tipo de caracteres que puede utilizar para nombrar objetos.
- Utilización de caracteres comodín para especificar nombres de objetos  
En algunos comandos, como por ejemplo los comandos de consulta, puede utilizar caracteres comodín para crear una expresión que coincida con un patrón de modo que especifique más de un objeto. Utilizar caracteres comodín facilita la adaptación de un comando a sus necesidades.
- Especificación de descripciones en parámetros de palabra clave  
Si una descripción (una serie de texto) de un parámetro empieza por comillas simples o dobles o incluye blancos intercalado o signos igual, deberá especificar el valor entre comillas simples (') o dobles (").

## Lectura de los diagramas de sintaxis

---

Para leer un diagrama de sintaxis que indica cómo especificar un mandato, siga la ruta de la línea. Léalo de izquierda a derecha y de arriba a abajo.

- El símbolo >>--- indica el principio de un diagrama de sintaxis.
- El símbolo ---> al final de una línea indica que el diagrama de sintaxis continúa en la línea siguiente.
- El símbolo >--- al inicio de una línea indica que un diagrama de sintaxis es la continuación de la línea anterior.
- El símbolo --->< indica el fin de un diagrama de sintaxis.

## Nombres de comando

---

El nombre del mandato puede componerse de una sola palabra de acción como, por ejemplo, HALT, o de una palabra de acción y de un objeto para la acción como, por ejemplo, DEFINE DOMAIN. Puede especificar el mandato en cualquier columna de la línea de entrada.

Especifique el nombre de mandato completo o la abreviatura especificada en el diagrama de sintaxis del mandato. Las letras en mayúsculas indican la abreviatura más reducida que resulta aceptable. Si un mandato aparece totalmente en letras mayúsculas, no se puede abreviar. Puede especificar el mandato en letras mayúsculas, letras minúsculas o en cualquier combinación de mayúsculas y minúsculas. En este ejemplo, puede entrar CMDNA, CMDNAM o CMDNAME en cualquier combinación de mayúsculas/minúsculas.

```
>>-CMDName-----><
```

Nota: Los nombres de mandato del texto descriptivo siempre se especifican en mayúsculas.

## Parámetros necesarios

---

Cuando un parámetro está en la misma línea que el nombre del mandato, el parámetro es necesario. Cuando hay dos o más valores de parámetros en una pila y uno de ellos está en la línea, *debe* especificar un valor.

En este ejemplo, debe entrar PARMNAME=A, PARMNAME=B o PARMNAME=C. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>-PARMName-----+A-+-----<<
      +-B-+
      '-C-'
```

## Parámetros opcionales

Cuando un parámetro está debajo de la línea, dicho parámetro es opcional. En este ejemplo, puede especificar PARMNAME=A o no especificar nada. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>+-----+-----<<
    '-PARMName-----A-'
```

Cuando dos o más valores de parámetro están en una pila debajo de la línea, todos son opcionales. En este ejemplo, puede especificar PARMNAME=A, PARMNAME=B, PARMNAME=C o no especificar nada. No incluya ningún espacio en blanco inmediatamente antes o después del signo igual (=).

```
>>+-----+-----<<
    '-PARMName-----+A-+-'
      +-B-+
      '-C-'
```

## Valores predeterminados

Los valores predeterminados están sobre la línea. El sistema utiliza los valores predeterminados a menos que los modifique. Puede modificar temporalmente el valor predeterminado especificando una opción de la pila que se encuentra debajo de la línea.

En este ejemplo, PARMNAME=A es el valor predeterminado. También puede especificar PARMNAME=A, PARMNAME=B o PARMNAME=C. No incluya ningún espacio en blanco antes o después del signo igual (=).

```
.-PARMName-----A-----
>>+-----+-----<<
    '-PARMName-----+A-+-'
      +-B-+
      '-C-'
```

## Variables

Los elementos en minúsculas resaltados (de este modo) indican variables. En estos ejemplos, nombre\_var representa las variables:

```
>>-CMDName--nombre_var-----<<
```

```
>>+-----+-----<<
    '-PARMname-----nombre_var-'
```

## Caracteres especiales

Debe codificar estos símbolos tal y como aparecen en el diagrama de sintaxis.

- \* Asterisco
- :
- Dos puntos
- ,
- Coma
- =
- Signo de igual
- 
- Guión
- ( )

Paréntesis

Punto

## Repetición de valores

Una flecha de retorno hacia la izquierda significa que el elemento se puede repetir. Un carácter en la flecha significa que debe separar los elementos repetidos con dicho carácter.

```
.-,-----  
V          |  
>>---nombre_archivo-+-----><
```

## Elementos repetibles

Una pila de valores seguida de una flecha de retorno hacia la izquierda significa que puede seleccionar más de un valor o, si está permitido, repetir un mismo elemento. En este ejemplo, puede seleccionar más de un valor, delimitando cada nombre con una coma. No incluya ningún espacio en blanco antes o después del signo igual (=).

```
.-,-----  
V          |  
>>-PARMName-----+valor1-+-----><  
                    +-valor2-+  
                    '-valor3-'
```

## Notas a pie de página

Las notas a pie de página se incluyen entre paréntesis.

```
.-,-----  
V (1)      |  
>>-----nombre_archivo-+-----><
```

Notas:

1. Puede especificar hasta cinco nombres de archivo.

## Especificación de parámetros

El orden en que especifique los parámetros puede ser importante. En el siguiente ejemplo se muestra una parte del mandato que se utiliza para definir una agrupación de almacenamiento de copia:

```
>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->  
>--POOLtype-----COPY--+-----+----->  
                    '-DESCRIPTION-----descripción-'  
  
.REclaim-----100-----  
>--+-----+-----><  
    '-REclaim-----porcentaje-'
```

Los primeros dos parámetros de este comando (*nombre\_agrupación* y *nombre\_clase\_dispositivo*) son parámetros necesarios. *nombre\_agrupación* y *nombre\_clase\_dispositivo* también son posicionales. Es decir, deben especificarse en el orden que se muestra, inmediatamente después del nombre del mandato. El parámetro POOLTYPE es un parámetro de palabra clave necesario. DESCRIPTION y RECLAIM son parámetros de palabra clave opcionales. Los parámetros de palabra clave se identifican con un signo igual que especifica un valor determinado o una variable. Los parámetros de palabra clave deben seguir a los parámetros posicionales en un mandato.

Todas las entradas de mandato siguientes, en las que los parámetros de palabra clave se ordenan de forma distinta, son aceptables:

```
define stgpool mycopypool mydeviceclass pooltype=copy  
description=engineering  
reclaim=50
```

```
define stgpool mycopypool mydeviceclass description=engineering
pooltype=copy
reclaim=50
```

El ejemplo siguiente, en el que uno de los parámetros de posición aparece a continuación de un parámetro de palabra clave, no es aceptable:

```
define stgpool mycopypool pooltype=copy mydeviceclass
description=engineering
reclaim=50
```

## Fragmentos de sintaxis

---

Algunos diagramas, debido a su longitud, deben mostrar partes de la sintaxis en fragmentos. El nombre del fragmento aparece entre barras verticales en el diagrama.

El fragmento ampliado aparece en el diagrama después de una cabecera con el mismo nombre de fragmento. Una cabecera con el nombre de fragmento identifica el fragmento ampliado. Son necesarios mandatos que aparezcan directamente en la línea.

En este ejemplo, el fragmento se denomina "Fragmento".

```
>>-| Fragmento |-----><
Fragmento
.-A-.
|---+---+-----|
+-B-+
'-C-'
```

## Utilización de caracteres de continuación para entrar mandatos largos

---

Los caracteres de continuación resultan útiles para procesar un mandato cuya longitud es mayor que la anchura de la pantalla o ventana. Puede utilizar caracteres de continuación en la modalidad interactiva del cliente de administración.

### Acerca de esta tarea

---

Sin caracteres de continuación, puede especificar hasta 256 caracteres. Con los caracteres de continuación, este límite se amplía a 1500 caracteres.

Nota: En el mandato MACRO, los valores máximos se aplican después de que se hayan aplicado variables de sustitución. Con los caracteres de continuación, puede efectuar lo siguiente:

- Especificar un guión al final de la línea que desea continuar.  
Por ejemplo:

```
register admin pease mypasswd -
contact="david, ext1234"
```

- Continúe una lista de valores entrando un guión o una barra inclinada invertida, sin ningún espacio en blanco que le preceda, después de la última coma de la lista que entre en la primera línea. A continuación, entre los elementos restantes de la lista en la línea siguiente sin ningún espacio en blanco que le preceda. Por ejemplo:

```
stgpools=stg1, stg2, stg3, -
stg4, stg5, stg6
```

- Continúe una serie de valores que aparecen entre comillas entrando la primera parte de la serie que aparece entre comillas, seguida por un guión o barra inclinada invertida al final de la línea. A continuación, entre el resto de la serie en la línea siguiente, incluida en el mismo tipo de comillas.  
Por ejemplo:

```
contact="david pease, bldg. 100, room 2b, san jose,"-
"ext. 1234, alternate contact-norm pass, ext 2345"
```

IBM Spectrum Protect concatena las dos series sin espacios en blanco. Debe utilizar este método sólo para continuar una serie de valores entre comillas en más de una línea.

## Denominación de objetos de IBM Spectrum Protect

---

IBM Spectrum Protect restringe el número y tipo de caracteres que puede utilizar para nombrar objetos.

## Acerca de esta tarea

Puede utilizar los caracteres siguientes para definir nombres de objetos.

Carácter	Descripción
A-Z	Cualquier letra, A-Z
0-9	Cualquier número, 0-9
_	Subrayado
.	Punto
-	Guión
+	Más
&	Ampersand

La tabla siguiente muestra la longitud máxima de caracteres que se permite para asignar nombres a los objetos.

Tipo de nombre	Longitud máxima
Administradores, conjuntos de opciones de cliente, nodos cliente, contraseñas, grupos de servidores, nombres de servidores, nombres de espacios de archivos virtuales.	64
Identificadores de exportación reinicializable	64
Direcciones TCP/IP de alto y de bajo nivel (IPv4 o IPv6)	64
Clases de dispositivo, unidades, bibliotecas, clases de gestión, dominios de políticas, perfiles, scripts de planificación, juegos de copias de seguridad, agrupaciones de almacenamiento	30

Puede utilizar los caracteres siguientes para definir nombres de contraseñas:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Las contraseñas consideradas "LOCAL" son aquellas que se autentican con el servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas. Una vez actualizado un nodo o administrador para que utilice el parámetro SESSIONSECURITY=STRICT, la contraseña pasa a distinguir entre mayúsculas y minúsculas la siguiente vez que se cambia. Las contraseñas consideradas "LDAP" son aquellas que se autentican con un servidor de directorio LDAP y distinguen entre mayúsculas y minúsculas.

Cuando se utilizan mandatos DEFINE para definir volúmenes de base de datos, de anotaciones de recuperación y de agrupaciones de almacenamiento, el convenio de denominación del nombre del volumen depende del tipo de medio de acceso secuencial o medio de acceso aleatorio que esté utilizando. Consulte el VOLUME específico para obtener detalles.

## Utilización de caracteres comodín para especificar nombres de objetos

En algunos comandos, como por ejemplo los comandos de consulta, puede utilizar caracteres comodín para crear una expresión que coincida con un patrón de modo que especifique más de un objeto. Utilizar caracteres comodín facilita la adaptación de un comando a sus necesidades.

## Acerca de esta tarea

Los caracteres comodín que utilice dependen del sistema operativo desde el que emite los comandos. Por ejemplo, puede utilizar caracteres comodín, como un asterisco (\*) en lugar de cualquier carácter (0 o más), o puede utilizar un signo de interrogación (?) o un signo de porcentaje (%) para hacer coincidir con exactitud un carácter.

La Tabla 1 proporciona referencias a los caracteres comodín para algunos sistemas operativos. Utilice los caracteres comodín adecuados a su sistema.

Tabla 1. Caracteres comodín por sistema operativo

Sistema operativo	Coincide cualquiera	Coincide exactamente uno
AIX, Linux, Windows	*	?

Sistema operativo	Coincide cualquiera	Coincide exactamente uno
TSO	*	%

Por ejemplo, si desea consultar todas las clases de gestión cuyos nombres comiencen por DEV en todos los juegos de políticas de DOMAIN1, y su sistema utiliza un asterisco como el carácter para *cualquier coincidencia*, puede entrar:

```
query mgmtclass domain1 * dev*
```

Si su sistema utiliza el signo de interrogación como el carácter de *coincidencia exacta con un carácter* y desea consultar las clases de gestión en POLICYSET1 en DOMAIN1, puede escribir:

```
query mgmtclass domain1 policyset1 mc?
```

IBM Spectrum Protect visualizará la información sobre las clases de gestión que tengan los nombres MC.

La Tabla 2 muestra ejemplos adicionales sobre la utilización de caracteres comodín en lugar de cualquier carácter.

Tabla 2. Carácter de cualquier coincidencia

Patrón	Coincide con	No coincide con
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrrs	ars, aabrs, abrrs
ab*ef*rs	abefrs, abefghrs	abefr, abers

La Tabla 3 muestra ejemplos adicionales sobre el uso de caracteres comodín que coincidan exactamente con un carácter. El signo de interrogación (?) se puede sustituir por un signo de porcentaje (%) si la plataforma utiliza dicho carácter en lugar de (?).

Tabla 3. Carácter de coincidencia exacta

Patrón	Coincide con	No coincide con
ab?	abc	ab, abab, abzzzz
ab?rs	abfrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzzrs	abrs, abjrs, abkkrs

## Especificación de descripciones en parámetros de palabra clave

Si una descripción (una serie de texto) de un parámetro empieza por comillas simples o dobles o incluye blancos intercalado o signos igual, deberá especificar el valor entre comillas simples (') o dobles (").

### Acerca de esta tarea

Las comillas iniciales y finales tienen que ser del mismo tipo. Por ejemplo, si existe una comilla simple inicial, debe haber también una comilla simple final.

Por ejemplo, para registrar un nuevo nodo cliente denominado Louie, con una contraseña secret y con su cargo incluido como información de contacto, entre:

```
register node louie secret contact="manager of dept. 61f"
```

La tabla siguiente presenta los modos de especificar una descripción para el parámetro CONTACT. El valor puede contener comillas, espacios en blanco intercalados o signos de igual.

Para esta descripción	Especifique lo siguiente
manager	contact=manager
manager's	contact="manager's" o contact='manager's'
"manager"	contact=""manager"" o contact=""manager""
manager's report	contact="manager's report" o contact='manager's report'
manager's "report"	contact='manager's "report"'

Para esta descripción	Especifique lo siguiente
manager=dept. 61f	contact='manager=dept. 61f'
manager reports to dept. 61f	contact='manager reports to dept. 61f' o contact="manager reports to dept. 61f"

## Control del proceso de comandos

Puede ejecutar algunos comandos de IBM Spectrum Protect secuencialmente o simultáneamente con otros comandos. También puede direccionar los comandos de un servidor a otros servidores para su proceso.

### Acerca de esta tarea

- Proceso de comandos de servidor  
IBM Spectrum Protect procesa los comandos de administrador en primer plano o como proceso subordinado. Los comandos que se procesan en primer plano deben haber finalizado para poder emitir otro comando. Cuando los comandos se procesan en un proceso subordinado, puede emitir comandos adicionales en cualquier momento.
- Detener procesos en segundo plano  
Utilice el comando CANCEL PROCESS para cancelar los comandos que generan procesos subordinados.

## Proceso de comandos de servidor

IBM Spectrum Protect procesa los comandos de administrador en primer plano o como proceso subordinado. Los comandos que se procesan en primer plano deben haber finalizado para poder emitir otro comando. Cuando los comandos se procesan en un proceso subordinado, puede emitir comandos adicionales en cualquier momento.

La mayor parte de los comandos de IBM Spectrum Protect se procesan en primer plano. En el caso de algunos mandatos que normalmente se procesan en un proceso subordinado (por ejemplo, BACKUP DB), puede especificar el parámetro WAIT (WAIT=YES) para que el mandato se procese en primer plano. Es posible que desee procesar un comando en primer plano en lugar de hacerlo en segundo plano por alguno de estos motivos:

- Para determinar rápidamente si un comando se ha completado correctamente. Cuando se emite un comando que se procesa en primer plano, IBM Spectrum Protect envía un mensaje de confirmación que indica que el comando ha finalizado correctamente. Si procesa el comando en segundo plano, necesitará abrir informes de operaciones o consultar el registro de actividad para determinar si el comando ha finalizado correctamente.
- Para supervisar las actividades del servidor (por ejemplo, los mensajes) en el cliente administrativo mientras se está procesando un comando. Esto puede ser preferible a realizar búsquedas en un registro de actividades largo después de que el comando haya finalizado.
- Para poder iniciar otro proceso de inmediato después de que haya finalizado un comando. Por ejemplo, podría especificar WAIT=YES para un comando que no tarde mucho en procesarse, de manera que cuando finalice pueda iniciar el proceso de otro comando de inmediato.
- Para serializar los comandos de un script administrativo cuando sea importante que un comando finalice antes de que otro empiece.

Compruebe la descripción del comando individual para determinar si el comando tiene un parámetro WAIT.

Puede cancelar los comandos que se procesan en primer plano desde la consola del servidor o desde otra sesión de cliente de administración.

A cada proceso subordinado se le asigna un número de proceso. Utilice el comando QUERY PROCESS para obtener el estado y el número de proceso de un proceso subordinado.

Nota:

- Si va a definir una planificación con un comando que especifica WAIT=NO (valor predeterminado) y emite QUERY EVENT para determinar el estado de la operación planificada, las operaciones con errores notificarán un estado de evento COMPLETED con un código de retorno OK. Para que la salida de QUERY EVENT refleje el estado de error, el parámetro WAIT debe establecerse en YES. Esto ejecuta la operación planificada en primer plano y le informa del estado cuando finalice.
- No puede procesar comandos en primer plano desde la consola del servidor.

## Detener procesos en segundo plano

Utilice el comando CANCEL PROCESS para cancelar los comandos que generan procesos subordinados.

## Acerca de esta tarea

---

Utilice el comando QUERY PROCESS para obtener el estado y el número de proceso de un proceso subordinado. Si un proceso subordinado está activo cuando lo cancela, el servidor detiene el proceso. Cualquier cambio que no se haya validado se suprimirá por caducidad. Sin embargo, los cambios validados no se suprimirán por caducidad.

Cuando emite un comando QUERY desde el cliente de administración, se podrían generar varias pantallas de salida. Si esto ocurre no es necesaria una salida adicional, el administrador puede cancelar la pantalla de salida a la estación de trabajo cliente. Si lo hace, no finalizará el proceso del comando.

## Realización de tareas simultáneamente en varios servidores

---

El direccionamiento de comandos permite direccionar los comandos a uno o más servidores para que los procesen y, a continuación, recopilar la salida de estos servidores.

### Acerca de esta tarea

---

Para direccionar comandos a otros servidores, es necesario que tenga el mismo ID y contraseña de administrador así como la autorización de administración exigida en todos los servidores a los que se redirecciona el comando. No puede direccionar comandos a otros servidores desde la consola del servidor.

Una vez se ha terminado de procesar el comando en todos los servidores, se visualiza la salida completa para cada servidor. Por ejemplo, la salida de SERVER\_A se visualiza totalmente, seguida de la salida de SERVER\_B. La salida incluye mensajes de resumen para cada servidor e identifica el servidor que ha procesado la salida. Los códigos de retorno indican si los comandos se han procesado correctamente en los servidores. Estos códigos de retorno incluyen una de tres gravedades: 0, ERROR o WARNING.

Todo servidor que se identifica como el destino de un comando direccionado debe definirse primero mediante el comando DEFINE SERVER. El comando se direcciona automáticamente a todos los servidores especificados como miembros de un grupo de servidores o a los servidores individuales especificados con el comando.

Los ejemplos siguientes describen cómo direccionar el comando QUERY STGPOOL a un servidor, a varios servidores, a un grupo de servidores, a varios grupos de servidores, o a una combinación de servidores y grupos de servidores. Cada servidor o grupo de servidores de una lista debe estar separado con una coma, sin espacios.

## Direccionamiento de comandos a un único servidor

---

### Procedimiento

Para direccionar el comando QUERY STGPOOL al servidor denominado ASTRO, entre:

```
astro: query stgpool
```

Con dos puntos después del nombre de servidor se indica el fin de la información de direccionamiento. Esto se denomina el *prefijo del servidor*. Otra forma de indicar que la información de direccionamiento ha terminado es encerrar entre paréntesis el nombre del servidor, por ejemplo:

```
(astro) query stgpool
```

## Direccionamiento de comandos a varios servidores

---

### Acerca de esta tarea

#### Procedimiento

Para direccionar el comando QUERY STGPOOL a varios servidores denominados HD\_QTR, MIDAS, SATURN, entre:

```
hd_qtr,midas,saturn: query stgpool
```

Si el primer servidor no está definido en IBM Spectrum Protect, el comando se direccionará al siguiente servidor definido de la lista de servidores.

También puede especificar el comando de este modo:

```
(hd_qtr,midas,saturn) query stgpool
```

## Direccionamiento de comandos a un grupo de servidores

---



## Acerca de esta tarea

En este ejemplo, el grupo de servidores ADMIN tiene los servidores denominados SECURITY, PAYROLL y PERSONNEL definidos como miembros del grupo. El comando se direccionará a cada uno de estos servidores.

## Procedimiento

Para direccionar el comando QUERY STGPOOL al grupo de servidores llamado ADMIN, especifique:

```
admin: query stgpool
```

También puede especificar el comando de este modo:

```
(admin) query stgpool
```

---

## Direccionamiento de comandos a grupos de servidores

### Acerca de esta tarea

En este ejemplo, el grupo de servidores ADMIN2 tiene los servidores SERVER\_A, SERVER\_B y SERVER\_C definidos como miembros del grupo, y el grupo de servidores ADMIN3 tiene los servidores ASTRO, GUMBY y CRUSTY definidos como miembros del grupo. El comando se direccionará a los servidores SERVER\_A, SERVER\_B, SERVER\_C, ASTRO, GUMBY y CRUSTY.

## Procedimiento

Para direccionar el comando QUERY STGPOOL a dos grupos de servidores denominados ADMIN2 y ADMIN3, especifique:

```
admin2,admin3: query stgpool
```

También puede especificar el comando de este modo:

```
(admin2,admin3) query stgpool
```

---

## Direccionamiento de comandos a dos servidores y un grupo de servidores

### Acerca de esta tarea

En este ejemplo, el grupo de servidores DEV\_GROUP tiene los servidores SALES, MARKETING y STAFF definidos como miembros del grupo. El comando se direccionará a los servidores SALES, MARKETING, STAFF, MERCURY y JUPITER.

## Procedimiento

Para direccionar el comando QUERY STGPOOL al grupo de servidores denominado DEV\_GROUP y a los servidores denominados MERCURY y JUPITER, entre:

```
dev_group,mercury,jupiter: query stgpool
```

También puede especificar el comando de este modo:

```
(dev_group,mercury,jupiter) query stgpool
```

---

## Direccionamiento de comandos dentro de scripts

### Acerca de esta tarea

Si direcciona comandos dentro de los scripts, debe delimitar el servidor o el grupo de servidores con paréntesis y omitir los dos puntos. De lo contrario, el comando no se direccionará al emitir el comando RUN y sólo se ejecutará en el servidor donde se emite el comando RUN.

Por ejemplo, para direccionar el comando QUERY STGPOOL dentro de un script:

## Procedimiento

1. Se definirá el script denominado QU\_STG para direccionarlo al grupo de servidores DEV\_GROUP.

```
define script qu_stg "(dev_group) query stgpool"
```

2. Se ejecutará el script QU\_STG:

## Resultados

En este ejemplo, el grupo de servidores DEV\_GROUP tiene los servidores SALES, MARKETING y STAFF definidos como miembros del grupo. El comando QUERY STGPOOL se direccionará a estos servidores.

## Clases de privilegio

La autorización que se otorga a un administrador mediante la clase de privilegio determina qué mandatos de administración puede emitir el administrador.

Existen cuatro clases de privilegios de administrador en IBM Spectrum Protect:

- Sistema
- Política
- Almacenamiento
- Operador

Después de que un administrador se ha registrado mediante la utilización del comando REGISTER ADMIN, el administrador puede emitir un conjunto limitado de comandos, incluidos todos los comandos de consulta. Cuando se instala IBM Spectrum Protect, la consola del servidor se define como un administrador del sistema denominado SERVER\_CONSOLE y se le otorga privilegio de sistema.

- Comandos que requieren privilegio de sistema  
Un administrador con privilegio de sistema tiene el nivel de autorización más alto para el servidor. Con el privilegio de sistema un administrador puede emitir cualquier mandato de administración y posee autorización para gestionar todos los dominios de políticas y todas las agrupaciones de almacenamiento.
- Comandos que requieren privilegio de políticas  
Un administrador con privilegio de políticas puede emitir comandos relacionados con objetos de gestión de políticas, como dominios de políticas, juegos de políticas, clases de gestión, grupos de copia y planificaciones. El privilegio de políticas puede no tener restricciones o puede estar restringido a agrupaciones de dominios de política específicos.
- Comandos que requieren privilegio de almacenamiento  
Un administrador con privilegio de almacenamiento puede emitir comandos que asignen y controlen recursos de almacenamiento para el servidor. El privilegio de almacenamiento puede no tener restricciones o puede estar restringido a agrupaciones de almacenamiento específicas.
- Comandos que requieren privilegio de operador  
Un administrador con privilegio de operador puede emitir comandos que controlan la operación inmediata del servidor y la disponibilidad del medio de almacenamiento.
- Comandos que puede emitir cualquier administrador  
Existen algunos comandos que pueden ser utilizados por cualquier administrador, incluso si no se le ha otorgado ningún privilegio de administrador específico.

## Comandos que requieren privilegio de sistema

Un administrador con privilegio de sistema tiene el nivel de autorización más alto para el servidor. Con el privilegio de sistema un administrador puede emitir cualquier mandato de administración y posee autorización para gestionar todos los dominios de políticas y todas las agrupaciones de almacenamiento.

La Tabla 1 lista los comandos que pueden emitir los administradores que posean privilegio de sistema. En algunos casos, los administradores con niveles inferiores de autorización, como por ejemplo el privilegio de almacenamiento sin restricciones, también pueden emitir estos mandatos. Además, la opción de servidor REQSYSAUTHOUTFILE puede utilizarse para especificar que determinados mandatos requieren privilegios del sistema si provocan que el servidor grabe en un archivo externo. Para obtener más información sobre esta opción de servidor, revise REQSYSAUTHOUTFILE.

Tabla 1. Comandos de privilegio de sistema

Nombre de mandato	Nombre de mandato
-------------------	-------------------

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> <li>• AUDIT LDAPDIRECTORY</li> <li>• AUDIT LICENSES</li> <li>• ACCEPT DATE</li> <li>• BEGIN EVENTLOGGING</li> <li>• CANCEL EXPIRATION</li> <li>• CANCEL PROCESS</li> <li>• CANCEL REPLICATION</li> <li>• CANCEL REQUEST</li> <li>• CANCEL RESTORE</li> <li>• CLEAN DRIVE</li> <li>• COPY ACTIVATEDATA</li> <li>• COPY DOMAIN</li> <li>• COPY POLICYSET</li> <li>• COPY PROFILE</li> <li>• COPY SCHEDULE (Nota de revisión.)</li> <li>• COPY SCRIPT</li> <li>• COPY SERVERGROUP</li> <li>• DEFINE BACKUPSET</li> <li>• DEFINE CLIENTACTION</li> <li>• DEFINE CLIENTOPT</li> <li>• DEFINE CLOPTSET</li> <li>• DEFINE COLLOGGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DEFINE DEVCLASS</li> <li>• DEFINE DOMAIN</li> <li>• DEFINE DRIVE</li> <li>• DEFINE EVENTSERVER</li> <li>• DEFINE GRPMEMBER</li> <li>• DEFINE LIBRARY</li> <li>• DEFINE MACHINE</li> <li>• DEFINE MACHNODEASSOCIATION</li> <li>• DEFINE NODEGROUP</li> <li>• DEFINE NODEGROUPMEMBER</li> <li>• DEFINE PATH</li> <li>• DEFINE PROFASSOCIATION</li> <li>• DEFINE PROFILE</li> <li>• DEFINE RECMEDMACHASSOCIATION</li> <li>• DEFINE RECOVERYMEDIA</li> <li>• DEFINE SCHEDULE (Nota de revisión.)</li> <li>• DEFINE SCRIPT</li> <li>• DEFINE SERVER</li> <li>• DEFINE SERVERGROUP</li> </ul>	<ul style="list-style-type: none"> <li>• DEFINE SPACETRIGGER</li> <li>• DEFINE STGPOOL</li> <li>• DEFINE SUBSCRIPTION</li> <li>• DEFINE VIRTUALFSMAPPING</li> <li>• DEFINE VOLUME</li> <li>• DELETE BACKUPSET</li> <li>• DELETE CLIENTOPT</li> <li>• DELETE CLOPTSET</li> <li>• DEFINE COLLOGGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DELETE DOMAIN</li> <li>• DELETE DRIVE</li> <li>• DELETE EVENTSERVER</li> <li>• DELETE GRPMEMBER</li> <li>• DELETE LIBRARY</li> <li>• DELETE MACHINE</li> <li>• DELETE MACHNODEASSOCIATION</li> <li>• DELETE NODEGROUP</li> <li>• DELETE NODEGROUPMEMBER</li> <li>• DELETE PROFASSOCIATION</li> <li>• DELETE PROFILE</li> <li>• DELETE RECMEDMACHASSOCIATION</li> <li>• DELETE RECOVERYMEDIA</li> <li>• DELETE SCHEDULE (Nota de revisión.)</li> <li>• DELETE SCRIPT</li> <li>• DELETE SERVER</li> <li>• DELETE SERVERGROUP</li> <li>• DELETE SPACETRIGGER</li> <li>• DELETE STGPOOL</li> <li>• DELETE SUBSCRIBER</li> <li>• DELETE SUBSCRIPTION</li> <li>• DELETE VIRTUALFSMAPPING</li> <li>• DISABLE EVENTS</li> <li>• ENABLE EVENTS</li> <li>• END EVENTLOGGING</li> <li>• EXPIRE INVENTORY</li> <li>• EXPORT ADMIN</li> <li>• EXPORT NODE</li> <li>• EXPORT POLICY</li> <li>• EXPORT SERVER</li> <li>• GENERATE BACKUPSET</li> <li>• GRANT AUTHORITY</li> </ul>

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> <li>• GRANT PROXYNODE</li> <li>• IDENTIFY DUPLICATES</li> <li>• IMPORT NODE</li> <li>• IMPORT POLICY</li> <li>• IMPORT SERVER</li> <li>• INSERT MACHINE</li> <li>• LABEL LIBVOLUME</li> <li>• LOCK ADMIN</li> <li>• LOCK PROFILE</li> <li>• MIGRATE STGPOOL</li> <li>• MOVE DRMEDIA</li> <li>• MOVE MEDIA</li> <li>• MOVE GRPMEMBER</li> <li>• NOTIFY SUBSCRIBERS</li> <li>• PERFORM LIBACTION</li> <li>• PING SERVER</li> <li>• PREPARE</li> <li>• QUERY BACKUPSETCONTENTS</li> <li>• QUERY MEDIA</li> <li>• QUERY RPFCONTENT</li> <li>• QUERY TOC</li> <li>• RECLAIM STGPOOL</li> <li>• RECONCILE VOLUMES</li> <li>• REGISTER ADMIN</li> <li>• REGISTER LICENSE</li> <li>• REMOVE ADMIN</li> <li>• REMOVE REPLNODE</li> <li>• RENAME ADMIN</li> <li>• RENAME SCRIPT</li> <li>• RENAME SERVERGROUP</li> <li>• RENAME STGPOOL</li> <li>• REPLICATE NODE</li> <li>• RESET PASSEXP</li> <li>• RESTORE NODE</li> <li>• REVOKE AUTHORITY</li> <li>• REVOKE PROXYNODE</li> <li>• RUN</li> <li>• SET ACCOUNTING</li> <li>• SET ACTLOGRETENTION</li> <li>• SET ARCHIVERETENTIONPROTECTION</li> <li>• SET ARREPLRULEDEFAULT</li> <li>• SET BKREPLRULEDEFAULT</li> <li>• SET CLIENTACTDURATION</li> </ul>	<ul style="list-style-type: none"> <li>• SET CONFIGMANAGER</li> <li>• SET CONFIGREFRESH</li> <li>• SET CONTEXTMESSAGING</li> <li>• SET CROSSDEFINE</li> <li>• SET DBRECOVERY</li> <li>• SET DEFAULTAUTHENTICATION</li> <li>• SET DRMACTIVEDATASTGPOOL</li> <li>• SET DRMCHECKLABEL</li> <li>• SET DRMCMDFILENAME</li> <li>• SET DRMCOPYCONTAINERSTGPOOL</li> <li>• SET DRMCOPYSTGPOOL</li> <li>• SET DRMCOURIERNAME</li> <li>• SET DRMDBBACKUPEXPIREDAYS</li> <li>• SET DRMFILPROCESS</li> <li>• SET DRMINSTRPREFIX</li> <li>• SET DRMNOTMOUNTABLENAME</li> <li>• SET DRMPPLANPREFIX</li> <li>• SET DRMPPLANVPOSTFIX</li> <li>• SET DRMPRIMSTGPOOL</li> <li>• SET DRMRPFEXPIREDAYS</li> <li>• SET DRMVaultNAME</li> <li>• SET EVENTRETENTION</li> <li>• SET INVALIDPWLIMIT</li> <li>• SET LDAPPASSWORD</li> <li>• SET LDAPUSER</li> <li>• SET LICENSEAUDITPERIOD</li> <li>• SET MAXCMDRETRIES</li> <li>• SET MAXSCHEDSESSIONS</li> <li>• SET MINPWLENGTH</li> <li>• SET PASSEXP</li> <li>• SET QUERYSCHEDPERIOD</li> <li>• SET RANDOMIZE</li> <li>• SET REPLRETENTION</li> <li>• SET REPLSERVER</li> <li>• SET RETRYPERIOD</li> <li>• SET SCHEDMODES</li> <li>• SET SERVERHLADDRESS</li> <li>• SET SERVERLLADDRESS</li> <li>• SET SERVERNAME</li> <li>• SET SERVERPASSWORD</li> <li>• SET SPREPLRULEDEFAULT</li> <li>• SET SUBFILE</li> <li>• SET TOCLOADRETENTION</li> </ul>
<ul style="list-style-type: none"> <li>• SETOPT</li> <li>• UNLOCK ADMIN</li> <li>• UNLOCK PROFILE</li> <li>• UPDATE ADMIN</li> <li>• UPDATE BACKUPSET</li> <li>• UPDATE CLIENTOPT</li> <li>• UPDATE CLOPTSET</li> <li>• UPDATE COLLOGGROUP</li> <li>• UPDATE DEVCLASS</li> <li>• UPDATE DRIVE</li> <li>• UPDATE LIBRARY</li> <li>• UPDATE LIBVOLUME</li> <li>• UPDATE MACHINE</li> </ul>	<ul style="list-style-type: none"> <li>• UPDATE NODEGROUP</li> <li>• UPDATE PATH</li> <li>• UPDATE PROFILE</li> <li>• UPDATE RECOVERYMEDIA</li> <li>• UPDATE REPLRULE</li> <li>• UPDATE SCHEDULE (Nota de revisión.)</li> <li>• UPDATE SCRIPT</li> <li>• UPDATE SERVER</li> <li>• UPDATE SERVERGROUP</li> <li>• UPDATE SPACETRIGGER</li> <li>• UPDATE VIRTUALFSMAPPING</li> <li>• UPDATE VOLHISTORY</li> <li>• VALIDATE LANFREE</li> <li>• VALIDATE REPLICATION</li> </ul>
<p>Nota: Este mandato está limitado por la autoridad que se otorga como administrador. El privilegio de sistema sólo es necesario para las planificaciones de mandatos de administración. El privilegio de sistema o de políticas es necesario para las planificaciones de operaciones de cliente.</p>	

## Comandos que requieren privilegio de políticas

Un administrador con privilegio de políticas puede emitir comandos relacionados con objetos de gestión de políticas, como dominios de políticas, juegos de políticas, clases de gestión, grupos de copia y planificaciones. El privilegio de políticas puede no tener restricciones o puede estar restringido a agrupaciones de dominios de política específicos.

El privilegio de políticas sin restricciones le permite emitir todos los mandatos de administrador que requieran privilegio de políticas. Puede emitir comandos que afecten a todos los dominios de políticas existentes, al igual que a cualquier dominio de políticas que se defina más adelante. Un administrador con privilegio de políticas sin restricciones no puede definir, suprimir o copiar dominios de políticas.

El privilegio de políticas con restricciones le permite emitir mandatos de administrador que afectan a uno o más dominios de políticas para los que se le ha otorgado autorización. Por ejemplo, el mandato DELETE MGMTCLASS requiere que tenga privilegio de políticas para el dominio de políticas al que pertenece la clase de gestión.

La Tabla 1 lista los mandatos que puede emitir un administrador con privilegio de políticas.

Tabla 1. Comandos de privilegio de políticas

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> <li>• ACTIVATE POLICYSET</li> <li>• ASSIGN DEFMGMTCLASS</li> <li>• CLEAN DRIVE</li> <li>• BACKUP NODE</li> <li>• COPY MGMTCLASS</li> <li>• COPY POLICYSET</li> <li>• COPY SCHEDULE (Revise nota 2.)</li> <li>• DEFINE ASSOCIATION</li> <li>• DEFINE BACKUPSET</li> <li>• DEFINE COPYGROUP</li> <li>• DEFINE CLIENTACTION</li> <li>• DEFINE CLIENTOPT</li> <li>• DEFINE MGMTCLASS</li> <li>• DEFINE NODEGROUP</li> <li>• DEFINE NODEGROUPMEMBER</li> <li>• DEFINE POLICYSET</li> <li>• DEFINE SCHEDULE</li> <li>• DELETE ASSOCIATION</li> <li>• DELETE BACKUPSET</li> <li>• DELETE COPYGROUP</li> <li>• DELETE EVENT (Revise nota 1.)</li> <li>• DELETE FILESPACE</li> <li>• DELETE MGMTCLASS</li> <li>• DELETE NODEGROUP</li> <li>• DELETE NODEGROUPMEMBER</li> </ul>	<ul style="list-style-type: none"> <li>• DELETE POLICYSET</li> <li>• DELETE PATH</li> <li>• DELETE SCHEDULE (Revise nota 2.)</li> <li>• GENERATE BACKUPSET</li> <li>• LOCK NODE</li> <li>• QUERY BACKUPSETCONTENTS</li> <li>• REGISTER NODE</li> <li>• REMOVE NODE</li> <li>• RENAME FILESPACE</li> <li>• RENAME NODE</li> <li>• SET SUMMARYRETENTION</li> <li>• RESTORE NODE</li> <li>• QUERY TOC</li> <li>• UNLOCK NODE</li> <li>• UPDATE BACKUPSET</li> <li>• UPDATE COPYGROUP</li> <li>• UPDATE DOMAIN</li> <li>• UPDATE MGMTCLASS</li> <li>• UPDATE NODE</li> <li>• UPDATE NODEGROUP</li> <li>• UPDATE POLICYSET</li> <li>• UPDATE SCHEDULE (Revise nota 2.)</li> <li>• VALIDATE POLICYSET</li> </ul>
<p>Notas:</p> <ol style="list-style-type: none"> <li>1. Este comando puede estar limitado a un dominio de políticas. Un administrador con privilegio de políticas sin restricciones o privilegio de políticas limitado a un dominio de políticas especificado puede emitir este comando.</li> <li>2. Este mandato está limitado por la autoridad que se otorga como administrador. El privilegio de sistema sólo es necesario para las planificaciones de mandatos de administración. El privilegio de sistema o de políticas es necesario para las planificaciones de operaciones de cliente.</li> </ol>	

## Comandos que requieren privilegio de almacenamiento

Un administrador con privilegio de almacenamiento puede emitir comandos que asignen y controlen recursos de almacenamiento para el servidor. El privilegio de almacenamiento puede no tener restricciones o puede estar restringido a agrupaciones de almacenamiento específicas.

El privilegio de almacenamiento sin restricciones le permite emitir todos los comandos de administrador que requieran privilegio de almacenamiento. Puede emitir comandos que afecten a todas las agrupaciones de almacenamiento existentes, al igual que a cualquier agrupación de almacenamiento que se defina más adelante. También puede emitir comandos que afecten a la base de datos y a las

anotaciones de recuperación. Un administrador con privilegio de almacenamiento sin restricciones no puede definir ni suprimir agrupaciones de almacenamiento.

El privilegio de almacenamiento con restricciones le permite emitir comandos de administrador que afectan únicamente a una agrupación de almacenamiento para la que se le ha otorgado autorización. Por ejemplo, el comando DELETE VOLUME únicamente afecta a un volumen de agrupación de almacenamiento que se ha definido en una agrupación de almacenamiento específica.

La Tabla 1 lista los comandos que puede emitir un administrador con privilegio de almacenamiento.

Tabla 1. Comandos de privilegio de almacenamiento

Nombre de mandato	Nombre de mandato
<ul style="list-style-type: none"> <li>• AUDIT LIBRARY</li> <li>• AUDIT VOLUME (Nota de revisión.)</li> <li>• BACKUP DB</li> <li>• BACKUP DEVCONFIG</li> <li>• BACKUP STGPOOL</li> <li>• BACKUP VOLHISTORY</li> <li>• CHECKIN LIBVOLUME</li> <li>• CHECKOUT LIBVOLUME</li> <li>• COPY ACTIVATEDATA (Nota de revisión.)</li> <li>• DEFINE COLLOGGROUP</li> <li>• DEFINE COLLOCMEMBER</li> <li>• DEFINE DATAMOVER</li> <li>• DEFINE DEVCLASS</li> <li>• DEFINE DRIVE</li> <li>• DEFINE LIBRARY</li> <li>• DEFINE PATH</li> <li>• DEFINE VIRTUALFSMAPPING</li> <li>• DEFINE VOLUME (Nota de revisión.)</li> <li>• DEFINE SPACETRIGGER</li> <li>• DELETE COLLOGGROUP</li> <li>• DELETE COLLOCMEMBER</li> <li>• DELETE DATAMOVER</li> <li>• DELETE DEVCLASS</li> <li>• DELETE DRIVE</li> <li>• DELETE LIBRARY</li> <li>• DELETE PATH</li> </ul>	<ul style="list-style-type: none"> <li>• DELETE SPACETRIGGER</li> <li>• DELETE VIRTUALFSMAPPING</li> <li>• DELETE VOLHISTORY</li> <li>• DELETE VOLUME (Nota de revisión.)</li> <li>• GRANT PROXYNODE</li> <li>• LABEL LIBVOLUME</li> <li>• MIGRATE STGPOOL</li> <li>• MOVE DATA (Nota de revisión.)</li> <li>• MOVE MEDIA</li> <li>• QUERY TAPEALERTMSG</li> <li>• RECLAIM STGPOOL</li> <li>• RESTORE STGPOOL</li> <li>• RESTORE VOLUME</li> <li>• REVOKE PROXYNODE</li> <li>• SET TAPEALERTMSG</li> <li>• UPDATE COLLOGGROUP</li> <li>• UPDATE DATAMOVER</li> <li>• UPDATE DEVCLASS</li> <li>• UPDATE DRIVE</li> <li>• UPDATE LIBRARY</li> <li>• UPDATE PATH</li> <li>• UPDATE SPACETRIGGER</li> <li>• UPDATE STGPOOL (Nota de revisión.)</li> <li>• UPDATE VIRTUALFSMAPPING</li> </ul>
<p>Nota: Este mandato puede estar limitado a una agrupación de almacenamiento. Un administrador con privilegio de almacenamiento sin restricciones o privilegio de almacenamiento limitado a una agrupación de almacenamiento especificada puede emitir este mandato.</p>	

## Comandos que requieren privilegio de operador

Un administrador con privilegio de operador puede emitir comandos que controlan la operación inmediata del servidor y la disponibilidad del medio de almacenamiento.

La Tabla 1 lista los comandos que un administrador con privilegio de operador puede emitir.

Tabla 1. Comandos de privilegio de operador

Nombre de comando	Nombre de comando
<ul style="list-style-type: none"> <li>• CANCEL SESSION</li> <li>• DISABLE SESSIONS</li> <li>• DISMOUNT VOLUME</li> <li>• ENABLE SESSIONS</li> <li>• HALT</li> </ul>	<ul style="list-style-type: none"> <li>• MOVE DRMEDIA</li> <li>• MOVE MEDIA</li> <li>• QUERY MEDIA</li> <li>• REPLY</li> <li>• UPDATE VOLUME</li> <li>• VARY</li> </ul>

## Comandos que puede emitir cualquier administrador

Existen algunos comandos que pueden ser utilizados por cualquier administrador, incluso si no se le ha otorgado ningún privilegio de administrador específico.

La Tabla 1 lista los mandatos que cualquier administrador registrado puede emitir.

Tabla 1. Comandos emitidos por todos los administradores

Nombre de comando	Nombre de comando
<ul style="list-style-type: none"> <li>• COMMIT</li> <li>• HELP</li> <li>• ISSUE MESSAGE</li> <li>• MACRO</li> <li>• PARALLEL</li> <li>• QUERY ACTLOG</li> <li>• QUERY ADMIN</li> <li>• QUERY ASSOCIATION</li> <li>• QUERY AUDITOCUPANCY</li> <li>• QUERY BACKUPSET</li> <li>• QUERY CLOPTSET</li> <li>• QUERY COLLOGGROUP</li> <li>• QUERY CONTENT</li> <li>• QUERY COPYGROUP</li> <li>• QUERY DATAMOVER</li> <li>• QUERY DB</li> <li>• QUERY DBSPACE</li> <li>• QUERY DEVCLASS</li> <li>• QUERY DIRSPACE</li> <li>• QUERY DOMAIN</li> <li>• QUERY DRIVE</li> <li>• QUERY DRMEDIA</li> <li>• QUERY DRMSTATUS</li> <li>• QUERY ENABLED</li> <li>• QUERY EVENT</li> <li>• QUERY EVENTRULES</li> <li>• QUERY EVENTSERVER</li> <li>• QUERY FILESPACE</li> <li>• QUERY LIBRARY</li> <li>• QUERY LIBVOLUME</li> <li>• QUERY LICENSE</li> <li>• QUERY LOG</li> <li>• QUERY MACHINE</li> <li>• QUERY MGMTCLASS</li> <li>• QUERY MOUNT</li> <li>• QUERY NASBACKUP</li> </ul>	<ul style="list-style-type: none"> <li>• QUERY NODE</li> <li>• QUERY NODEDATA</li> <li>• QUERY NODEGROUP</li> <li>• QUERY OCCUPANCY</li> <li>• QUERY OPTION</li> <li>• QUERY PATH</li> <li>• QUERY POLICYSET</li> <li>• QUERY PROCESS</li> <li>• QUERY PROFILE</li> <li>• QUERY PROXYNODE</li> <li>• QUERY RECOVERYMEDIA</li> <li>• QUERY REPLICATION</li> <li>• QUERY REPLNODE</li> <li>• QUERY REPLRULE</li> <li>• QUERY REQUEST</li> <li>• QUERY RESTORE</li> <li>• QUERY RPFIL</li> <li>• QUERY SCHEDULE</li> <li>• QUERY SCRIPT</li> <li>• QUERY SERVER</li> <li>• QUERY SERVERGROUP</li> <li>• QUERY SESSION</li> <li>• QUERY SPACETRIGGER</li> <li>• QUERY STATUS</li> <li>• QUERY STGPOOL</li> <li>• QUERY SUBSCRIBER</li> <li>• QUERY SUBSCRIPTION</li> <li>• QUERY SYSTEM</li> <li>• QUERY VIRTUALFSMAPPING</li> <li>• QUERY VOLHISTORY</li> <li>• QUERY VOLUME</li> <li>• QUIT</li> <li>• ROLLBACK</li> <li>• SELECT</li> <li>• SERIAL</li> </ul>

## Comandos de administración

Los comandos de administración están disponibles para gestionar y configurar el servidor.

La información sobre cada comando incluye:

- Una descripción de las tareas que realiza un comando
  - La clase de privilegio del administrador que es necesaria para utilizar el comando
  - Un diagrama de sintaxis que identifica los parámetros necesarios y opcionales del comando
  - Las descripciones de cada uno de los parámetros del comando
  - Ejemplos de cómo utilizar el comando
  - Una lista de los comandos relacionados
- ACCEPT DATE (aceptar la fecha del sistema actual)  
Utilice este comando para que el servidor pueda iniciar un proceso normal, cuando el servidor no inicia un proceso normal a causa de una discrepancia entre la fecha del servidor y la fecha actual del sistema.
  - ACTIVATE POLICYSET (Activar un nuevo juego de políticas)  
Utilice este comando para copiar el contenido de un juego de políticas en el juego de políticas ACTIVE del dominio. El servidor utiliza las reglas del juego de políticas ACTIVE para gestionar las operaciones de cliente en el dominio. Puede definir varios

- juegos de políticas para un dominio de políticas, pero únicamente puede haber un juego de políticas activo. El juego de políticas ACTIVE actual se sustituye por el que especifique al emitir este comando. Sólo puede modificar el juego de políticas ACTIVE activando otro juego de políticas.
- **ASSIGN DEFMGMTCLASS** (asignar una clase de gestión predeterminada)  
Utilice este comando para especificar una clase de gestión como la clase de gestión predeterminada para un juego de políticas. Para poder activar el juego de políticas, debe asignar una clase de gestión predeterminada a un juego de políticas.
  - **AUDIT commands**  
Utilice los mandatos AUDIT para revisar o examinar si tanto la información de la base de datos como el volumen de agrupación de almacenamiento están en un estado correcto. El mandato AUDIT LDAPDIRECTORY elimina los nodos o ID de administrador de un servidor de directorio LDAP, que no autentican sus contraseñas con el servidor de directorio LDAP.
  - **Comandos BACKUP**  
Utilice los comandos BACKUP para crear copias de seguridad de información u objetos IBM Spectrum Protect.
  - **BEGIN EVENTLOGGING** (Iniciar anotación de eventos)  
Utilice este mandato para empezar a anotar eventos en uno o varios receptores. Un receptor para el que se ha iniciado la anotación de eventos es un *receptor activo*.
  - **Comandos CANCEL**  
Utilice el comando CANCEL para finalizar una tarea o un proceso antes de que se haya completado.
  - **CHECKIN LIBVOLUME** (Dar de alta un volumen de almacenamiento en una biblioteca)  
Utilice este comando para agregar un volumen de acceso secuencial o una cinta de limpieza al inventario del servidor para una biblioteca automatizada. El servidor utilizará un volumen que resida físicamente en una biblioteca automatizada hasta que dicho volumen se haya dado de alta.
  - **CHECKOUT LIBVOLUME** (Dar de baja un volumen de almacenamiento de una biblioteca)  
Utilice este mandato para suprimir del inventario del servidor un volumen de almacenamiento de acceso secuencial de una biblioteca automatizada. Este comando crea un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.
  - **CLEAN DRIVE** (Limpiar una unidad)  
Utilice este comando si desea que IBM Spectrum Protect cargue inmediatamente un cartucho limpiador en una unidad al margen de la frecuencia de limpieza.
  - **COMMIT** (controlar la validación de comandos en una macro)  
Utilice este comando para controlar cuándo se valida un comando en una macro y para actualizar la base de datos cuando los comandos terminan el proceso. Si se emite en la modalidad de consola del cliente de administración, este comando no genera ningún mensaje.
  - **CONVERT STGPOOL** (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)  
Utilice este mandato para convertir una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Puede utilizar agrupaciones de almacenamiento de contenedores para la deduplicación de datos del lado de cliente y en línea.
  - **Comandos COPY**  
Utilice los comandos COPY para crear una copia de los objetos o datos de IBM Spectrum Protect.
  - **DEACTIVATE DATA** (Desactivar datos para un nodo de cliente)  
Utilice este comando para especificar que los datos activos que se han copiado para un nodo de cliente de aplicaciones antes de una fecha especificada ya no son necesarios. El comando marca los datos como inactivos para que puedan suprimirse de acuerdo con las políticas de retención de datos.
  - **Comandos DECOMMISSION**  
Utilice los comandos DECOMMISSION para eliminar nodos cliente del entorno de producción. Los nodos de cliente pueden ser aplicaciones, sistemas y máquinas virtuales.
  - **Comandos DEFINE**  
Utilice los comandos DEFINE para crear objetos de IBM Spectrum Protect.
  - **Comandos DELETE**  
Utilice los mandatos DELETE para suprimir o eliminar un objeto de IBM Spectrum Protect.
  - **Comandos DISABLE**  
Utilice los comandos DISABLE para que el servidor no pueda realizar determinados tipos de operaciones.
  - **Comandos DISMOUNT**  
Utilice el comando DISMOUNT para desmontar un volumen mediante la dirección de dispositivo real o mediante el nombre de volumen.
  - **DISPLAY OBJNAME** (Mostrar un nombre de objeto completo)  
Utilice este comando para IBM Spectrum Protect que se visualice un nombre de objeto completo si el nombre que figura en un mensaje o en la salida de una consulta está abreviado por razones de limitación de longitud. Los nombres de objeto que son muy largos pueden ser difíciles de mostrar y usar en funciones normales del sistema operativo. El servidor IBM Spectrum Protect abreviará nombres largos y les asignará un ID de señal que puede utilizarse si el nombre de la ruta del objeto sobrepasa los 1024 bytes. El ID de señal se muestra en una cadena que incluye identificadores para el nodo, el espacio de archivos y el nombre del objeto. El formato es: [TSMOBJ:nID.fsID.objID]. Cuando se especifica con el comando DISPLAY OBJNAME, el ID de señal puede utilizarse para que se muestre el nombre completo del objeto.



- Comandos ENABLE  
Utilice el comando ENABLE para que el servidor pueda realizar algunos tipos de operaciones.
- ENCRYPT STGPOOL (Cifrar datos en una agrupación de almacenamiento)  
Utilice este mandato para cifrar datos en una agrupación de almacenamiento de contenedores de directorio o de contenedores de nube.
- END EVENTLOGGING (Detener eventos de anotaciones)  
Utilice este mandato para dejar de anotar los eventos en un receptor activo.
- EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)  
Utilice este comando para iniciar manualmente el proceso de caducidad de inventario. El proceso de caducidad de inventario elimina las copias de los archivos de archivado y de copia de seguridad de cliente del almacenamiento del servidor. La eliminación se basa en las especificaciones de política de los grupos de copia de archivado y de copia de seguridad y archivo de las clases de gestión a las que están vinculados los archivos.
- Comandos EXPORT  
Utilice el mandato EXPORT para copiar información de un servidor de IBM Spectrum Protect en un medio extraíble secuencial.
- EXTEND DBSPACE (Incrementar el espacio para la base de datos)  
Utilice este comando para aumentar el espacio para la base de datos añadiendo directorios para que los utilice la base de datos.
- Comandos GENERATE  
Utilice los comandos GENERATE para los conjuntos de copia de seguridad para un espacio de archivos o un nodo cliente seleccionado.
- Comandos GRANT  
Utilice el comando GRANT para otorgar el acceso o los privilegios apropiados.
- HALT (Concluir el servidor)  
Utilice este comando para concluir el servidor. El comando HALT fuerza una conclusión precipitada, que cancela todas las sesiones de nodo cliente y de administración, aunque no se hayan completado.
- HELP (Obtener ayuda sobre comandos y mensajes de error)  
Utilice este comando para visualizar los comandos de administración y los mensajes de error. Puede emitir el mandato desde un cliente de línea de mandatos de administración.
- IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)  
Utilice este comando para iniciar o detener procesos que identifiquen datos duplicados en una agrupación de almacenamiento. Puede especificar el número de proceso de identificación de duplicados y su duración.
- Comandos IMPORT  
Utilice los mandatos IMPORT para importar información desde los medios de exportación a un servidor de IBM Spectrum Protect.
- INSERT MACHINE (Insertar información de características o instrucciones de recuperación)  
Utilice este comando para agregar características de máquina cliente o instrucciones de recuperación a la información de la máquina existente en la base de datos.
- ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)  
Utilice este comando con el proceso de código de retorno en un script para emitir un mensaje desde un script del servidor para determinar dónde se encuentra el problema con un comando del script.
- LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)  
Utilice este comando para etiquetar volúmenes de cinta o, en una biblioteca automatizada, para etiquetar automáticamente los volúmenes a medida que se dan de alta. Con este comando, servidor utiliza la etiqueta larga que, con frecuencia, los volúmenes llevan previamente etiquetada.
- LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)  
Utilice este comando para cargar el conjunto predeterminado de desencadenantes de alertas en el servidor de IBM Spectrum Protect.
- Comandos LOCK  
Utilice el comando LOCK para impedir que los usuarios accedan al servidor.
- MACRO (Invocar una macro)  
Utilice este comando para invocar un archivo desde la línea de comandos de administración que contiene uno o varios comandos de administración de IBM Spectrum Protect que deben ejecutarse.
- MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)  
Utilice este comando para migrar archivos de una agrupación de almacenamiento a la agrupación de almacenamiento siguiente de la jerarquía de almacenamiento.
- Comandos MOVE  
Utilice los comandos MOVE para transferir datos de copia de seguridad o datos archivados entre agrupaciones de almacenamiento o bien para trasladar medios de recuperación ante siniestro al local o fuera del local.
- NOTIFY SUBSCRIBERS (Notificar a servidores gestionados que actualicen los perfiles)  
Utilice este comando en un gestor de configuración para notificar a uno o varios servidores gestionados que soliciten que su información de configuración se renueve inmediatamente.
- PERFORM LIBACTION (Definir o suprimir todas las unidades y rutas de una biblioteca)  
Utilice este comando para definir o suprimir todas las unidades y sus rutas para una única biblioteca en un paso.
- PING SERVER (Comprobar la conexión entre servidores)  
Utilice este mandato para comprobar la conexión entre el servidor local y un servidor remoto.

- **PREPARE (crear un archivo de plan de recuperación)**  
Utilice este mandato para crear un archivo de plan de recuperación, que contiene la información necesaria para recuperar un servidor de IBM Spectrum Protect. El archivo del plan de recuperación se puede almacenar en un sistema de archivos que sea accesible para el servidor de origen o en un servidor de destino.
- **PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)**  
Utilice este mandato para proteger los datos de una agrupación de almacenamiento de contenedores de directorio almacenando una copia de los datos en otra agrupación de almacenamiento en un servidor de destino de duplicación o en el mismo servidor protegiendo los datos en cinta. Cuando protege la agrupación de almacenamiento de contenedores de directorio, puede intentar posteriormente reparar los daños en la agrupación de almacenamiento mediante el mandato REPAIR STGPOOL.
- **Comandos QUERY**  
Utilice los comandos QUERY para solicitar o visualizar información sobre los objetos de IBM Spectrum Protect.
- **QUIT (finalizar la modalidad interactiva del cliente de administración)**  
Utilice este comando para finalizar una sesión de cliente de administración en modalidad interactiva.
- **RECLAIM STGPOOL (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)**  
Utilice este mandato para reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial. La reclamación no traslada las versiones inactivas de los datos de copia de seguridad de los volúmenes en las agrupaciones de datos activos.
- **RECONCILE VOLUMES (Reconciliar diferencias en definiciones de volúmenes virtuales)**  
Emita este mandato desde el servidor de origen para reconciliar las diferencias que hay entre las definiciones de volúmenes virtuales del servidor de origen y las copias archivadas del servidor de destino. IBM Spectrum Protect localiza todos los volúmenes de la clase de dispositivo especificada del servidor de origen y todas las copias archivadas correspondientes del servidor de destino. El inventario del servidor de destino también se compara con la definición local de los volúmenes virtuales para ver si existen incoherencias.
- **Comandos REGISTER**  
Utilice los mandatos REGISTER para definir o agregar objetos para IBM Spectrum Protect.
- **Comandos REMOVE**  
Utilice los mandatos REMOVE para eliminar un objeto de IBM Spectrum Protect.
- **Comandos RENAME**  
Utilice los comandos RENAME para cambiar el nombre de un objeto existente.
- **REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)**  
Utilice este mandato para reparar extensiones con duplicados eliminados en una agrupación de almacenamiento de contenedores de directorio. Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones de las que se ha hecho copia de seguridad en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.
- **REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)**  
Utilice este comando para replicar los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, o a grupos definidos de nodos de clientes.
- **REPLY (Permitir una petición para continuar el proceso)**  
Utilice este comando y un número de identificación para informar al servidor de que ha finalizado una operación solicitada. No todas las peticiones de servidor requieren una respuesta. Este comando sólo es necesario si el mensaje de petición indica específicamente que se necesita una respuesta.
- **RESET PASSEXP (restablecer caducidad de contraseña)**  
Utilice el mandato RESET PASSEXP para restablecer el período de caducidad de las contraseñas en el período de caducidad común para las contraseñas de administrador y de nodo de cliente. El mandato RESET PASSEXP no se aplica a las contraseñas que se almacenan en un servidor de directorios LDAP.
- **RESTART EXPORT (Reiniciar una operación de exportación suspendida)**  
Utilice este comando para reiniciar una operación de exportación suspendida.
- **Comandos RESTORE**  
Utilice los comandos RESTORE para restaurar las agrupaciones de almacenamiento o volúmenes IBM Spectrum Protect.
- **Comandos REVOKE**  
Utilice los comandos REVOKE para revocar el acceso o los privilegios.
- **ROLLBACK (Retrotraer cambios no validados en una macro)**  
Utilice este mandato en una macro para deshacer todos los cambios de proceso que han realizado los mandatos que el servidor ha ejecutado pero que todavía no se han validado en la base de datos. Un cambio validado es permanente y no se puede retrotraer. El mandato ROLLBACK es útil para probar las macros.
- **RUN (ejecutar un script de IBM Spectrum Protect)**  
Utilice este mandato para ejecutar un script de IBM Spectrum Protect. Para emitir este comando en otro servidor, el script que se ejecuta debe estar definido en ese servidor.
- **SELECT (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)**  
Utilice el mandato SELECT para crear y dar formato a una consulta personalizada de la base de datos de IBM Spectrum Protect .
- **Comandos SET**  
Utilice los comandos SET para especificar valores que afectan a varias operaciones de IBM Spectrum Protect.
- **SETOPT (Establecer una opción de servidor para actualización dinámica)**  
Puede utilizar el mandato SETOPT para actualizar la mayoría de las opciones de servidor dinámicamente sin detener y reiniciar el

servidor. Para la opción DBDIAGLOGSIZE, debe detener e iniciar el servidor. Un mandato SETOPT que esté en una macro o en un script no se puede retrotraer.

- SHRED DATA (destruir datos)

Utilice este comando para iniciar manualmente el proceso de destrucción de los datos confidenciales suprimidos. La destrucción manual de datos es posible únicamente si la destrucción automática está inhabilitada.

- SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)

Utilice este comando para suspender una operación de exportación de servidor a servidor que tiene un valor de FILEDATA que no es NONE. La operación de exportación que desea suspender debe haber pasado la fase de inicialización para poder considerarse seleccionable para la suspensión. El estado de la operación de exportación se guarda. La operación puede reiniciarse mediante la emisión del comando RESTART EXPORT.

- Mandatos UNLOCK

Utilice los comandos UNLOCK para restablecer el acceso después de que se haya bloqueado un objeto.

- Comandos UPDATE

Utilice el comando UPDATE para modificar uno o más atributos de un objeto IBM Spectrum Protect existente.

- Comandos VALIDATE

Utilice el comando VALIDATE para verificar que un objeto esté completo o sea válido para IBM Spectrum Protect.

- VARY (Activar o desactivar un volumen de acceso aleatorio)

Utilice este comando para activar o desactivar un volumen de agrupación de almacenamiento de acceso aleatorio en el servidor.

## ACCEPT DATE (aceptar la fecha del sistema actual)

---

Utilice este comando para que el servidor pueda iniciar un proceso normal, cuando el servidor no inicia un proceso normal a causa de una discrepancia entre la fecha del servidor y la fecha actual del sistema.

Cuando el servidor no comienza el proceso normal debido a una discrepancia entre la fecha del servidor y la fecha actual, este comando obliga al servidor a aceptar la fecha y hora actuales como válidas. Si la hora del sistema es válida y el servidor no se ha ejecutado durante cierto tiempo, este comando debería ejecutarse para permitir el comienzo del proceso normal del servidor.

Atención: Si la fecha del sistema no es válida o el servidor se creó o se ejecutó previamente con una fecha del sistema no válida y se emite este comando, cualquier proceso del servidor o comando que utilice fechas puede tener resultados imprevistos. Por ejemplo, la caducidad de los archivos puede verse afectada. Cuando el servidor se inicia con la fecha correcta, los archivos con copias de seguridad con fecha en el futuro no serán consideradas para caducidad hasta que se alcance la fecha futura. Los archivos con copias de seguridad con fechas que han pasado caducarán antes. Cuando el proceso del servidor detecta una fecha futura, se emitirá un mensaje de error.

Si el servidor detecta una fecha u hora no válidas, las sesiones del servidor se inhabilitarán (como si se hubiera emitido el comando DISABLE SESSIONS). No se pueden continuar procesando las operaciones de caducidad, migración, reclamación y supresión de información histórica de volúmenes.

Utilice el comando ENABLE SESSIONS ALL después de haber emitido el comando ACCEPT DATE para volver a habilitar las sesiones que han de iniciarse.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-ACcept Date-----<<
```

## Parámetros

---

Ninguno.

## Ejemplo: aceptar la fecha del sistema actual

---

Permitir que el servidor acepte la fecha actual como la fecha válida.

```
accept date
```

## Comandos relacionados

---

Tabla 1. Comando relacionado con ACCEPT DATE

Comando	Descripción
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.

## ACTIVATE POLICYSET (Activar un nuevo juego de políticas)

Utilice este comando para copiar el contenido de un juego de políticas en el juego de políticas ACTIVE del dominio. El servidor utiliza las reglas del juego de políticas ACTIVE para gestionar las operaciones de cliente en el dominio. Puede definir varios juegos de políticas para un dominio de políticas, pero únicamente puede haber un juego de políticas activo. El juego de políticas ACTIVE actual se sustituye por el que especifique al emitir este comando. Sólo puede modificar el juego de políticas ACTIVE activando otro juego de políticas.

Antes de activar un juego de políticas, compruebe que el juego de políticas está completo y es válido con el comando VALIDATE POLICYSET.

El comando ACTIVATE POLICYSET no se ejecutará correctamente si se da alguna de las condiciones que se indican a continuación:

- Un grupo de copia especifica una agrupación de almacenamiento de copia como destino.
- Una clase de gestión especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.
- El juego de políticas no tiene ninguna clase de gestión predeterminada.
- Se ha especificado un parámetro TOCDESTINATION y la agrupación de almacenamiento es una agrupación de copia o bien tiene un formato de datos distinto de NATIVE o NONBLOCK.

El juego de políticas ACTIVE y el último juego de políticas activado no son necesariamente idénticos. Puede modificar el juego de políticas original que ha activado sin que afecte al juego de políticas ACTIVE.

Si el servidor tiene la protección de retención de datos activada, deben darse las condiciones siguientes:

- Todas las clases de gestión del juego de políticas que se va a activar deben contener un grupo de copia archivada.
- Si existe una clase de gestión en el juego de políticas activo, debe existir una clase de gestión con el mismo nombre en el juego de políticas que se va a activar.
- Si existe un grupo de copia archivada en el juego de políticas activo, el grupo de copia correspondiente en el juego de políticas que se va a activar debe tener un valor de RETVER que sea por lo menos tan alto como los valores correspondientes en el grupo de copia activo.

Atención: La protección de retención sólo se aplica a los objetos de archivado.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

### Sintaxis

```
>>-ACTivate Policyset--nombre_dominio--nombre_juego_políticas--><
```

### Parámetros

nombre\_dominio (Necesario)  
Especifica el dominio de políticas para el que desea activar un juego de políticas.

nombre\_juego\_políticas (Necesario)  
Especifica el juego de políticas que se va a activar.

### Ejemplo: activar un juego de políticas en un dominio de políticas específico

Activar el juego de políticas VACATION en el dominio de políticas EMPLOYEE\_RECORDS.

```
activate policyset employee_records vacation
```

### Comandos relacionados

Tabla 1. Comandos relacionados con ACTIVATE POLICYSET

Comando	Descripción
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## ASSIGN DEFMGMTCLASS (asignar una clase de gestión predeterminada)

Utilice este comando para especificar una clase de gestión como la clase de gestión predeterminada para un juego de políticas. Para poder activar el juego de políticas, debe asignar una clase de gestión predeterminada a un juego de políticas.

Para garantizar que los clientes siempre podrán realizar la copia de seguridad y las copias archivadas, seleccione una clase de gestión predeterminada que contenga un grupo de copia archivada y un grupo de copia de seguridad.

El servidor utiliza la clase de gestión predeterminada para gestionar los archivos de cliente si no hay ninguna clase de gestión asignada o adecuada. Por ejemplo, el servidor utiliza la clase de gestión predeterminada si el usuario no especifica una clase de gestión en la lista de inclusión/exclusión.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

### Sintaxis

```
>>-ASSign DEFMGmtclass--nom_dominio--nom_juego_políticas--nom_clase-><
```

### Parámetros

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas para el que desea asignar una clase de gestión predeterminada. No puede asignar una clase de gestión predeterminada al juego de políticas ACTIVE.

nom\_clase (Necesario)

Especifica la clase de gestión que será la clase de gestión predeterminada para el juego de políticas.

### Ejemplo: asignar una clase de gestión predeterminada

Asignar DEFAULT1 como la clase de gestión predeterminada para el juego de políticas SUMMER del dominio de políticas PROG1.

```
assign defmgmtclass prog1 summer default1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con ASSIGN DEFMGMTCLASS



Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.

Comando	Descripción
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## AUDIT commands

Utilice los mandatos AUDIT para revisar o examinar si tanto la información de la base de datos como el volumen de agrupación de almacenamiento están en un estado correcto. El mandato AUDIT LDAPDIRECTORY elimina los nodos o ID de administrador de un servidor de directorio LDAP, que no autentican sus contraseñas con el servidor de directorio LDAP.

- AUDIT CONTAINER
  - AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)
  - AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)
- AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)
- AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)
- AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)
- AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)
- AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Mandatos AUDIT CONTAINER

Utilice el mandato AUDIT CONTAINER para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes.

- AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)  
Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.
- AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)  
Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de directorio.

## AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de nubes)

Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de nubes. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.

Puede utilizar este mandato para realizar las siguientes acciones para un contenedor de una agrupación de almacenamiento de contenedores de nubes:

- Explorar el contenido de un contenedor para validar la integridad de las extensiones de datos
- Eliminar datos de un contenedor marcado como *dañado*, como por ejemplo cuando un archivo tiene referencias en la base de datos del servidor, pero contiene datos faltantes o corrompidos en la nube.
- Marcar un contenedor completo como *dañado*



Consejo: Si especifica el parámetro ACTION=SCANALL en una agrupación de almacenamiento IBM® Cloud Object Storage que utiliza una cámara de seguridad con la indexación de nombres inhabilitada, la operación de auditoría explora toda la cámara de seguridad para identificar extensiones huérfanas en cada contenedor. En esta situación, especifique WAIT=YES si desea que la operación de auditoría espere a que finalice la exploración de extensiones huérfanas antes de que notifique la auditoría como completada. Esta exploración de extensiones huérfanas sólo se produce si no se especifica un nombre de contenedor. Si especifica un contenedor que se encuentra en una cámara de seguridad con la indexación de nombres inhabilitada, la operación de auditoría no explora extensiones huérfanas.

#### REMOVEDamaged

Especifica que el servidor elimina cualquier referencia a extensiones dañadas de la base de datos de servidor. Las extensiones dañadas también se eliminan de la agrupación de almacenamiento del contenedor de la nube, si se han encontrado. El servidor también elimina las extensiones huérfanas de la agrupación de almacenamiento de contenedor en la nube y elimina las referencias a estas extensiones huérfanas de la base de datos, según especifica el parámetro FORCEORPHANDBDEL.

#### MARKDamaged

Especifica que el servidor marca explícitamente todas las extensiones de datos en el contenedor como dañadas.

#### SCANDamaged

Especifica que el servidor sólo comprueba las extensiones dañadas existentes en el contenedor.

Importante: si no existe ninguna conexión con la nube, los parámetros ACTION=SCANALL y ACTION=SCANDAMAGED no se ejecutan. Sin embargo, el parámetro ACTION=MARKDAMAGED se ejecuta según lo esperado sin conexión de nube, y el parámetro ACTION=REMOVEDAMAGED marca los datos dañados como huérfanos. En cuanto se restablece la conexión con la nube, el servidor suprime las extensiones huérfanas.

Condición de restablecimiento de estado: Si la auditoría no detecta un error con una extensión de datos marcada como dañada, el estado de la extensión de datos se restablece. A continuación, la extensión de datos puede utilizarse. Esta condición proporciona un medio de restablecer el estado de las extensiones de datos dañadas si los errores se deben a un problema corregible. Las opciones SCANALL y SCANDAMAGED son las únicas opciones que restablecen una extensión dañada si se descubre que no está dañadas.

#### FORCEOrphanbdel

Especifica que el servidor fuerza la supresión de extensiones huérfanas de la base de datos del servidor, aunque no se hayan suprimido de la agrupación de almacenamiento del contenedor de la nube. Este parámetro es opcional. Si especifica este parámetro, también debe especificar el parámetro ACTION=REMOVEDAMAGED. Las opciones siguientes están disponibles:

#### Yes

Especifica que el servidor suprime cualquier extensión huérfana de la base de datos del servidor, aunque no se hayan suprimido de la agrupación de almacenamiento del contenedor de la nube.

#### No

Especifica que el servidor conserva las extensiones huérfanas en la base de datos del servidor, si no se pueden suprimir de la agrupación de almacenamiento del contenedor de la nube. Este es el valor predeterminado.

#### MAXProcess

Especifica el número de procesos paralelos que se utilizarán para comprobar un contenedor en una agrupación de almacenamiento de contenedores de nubes. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

Restricción: El servidor omite este parámetro cuando se utiliza MAXPROCESS con el parámetro ACTION=REMOVEDAMAGED.

#### Wait

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

#### No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras el comando se está procesando. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

#### Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se muestran en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.

#### BEGINDate

Especifica el valor del rango de fechas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no una fecha inicial, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha antes de que se realizara la primera auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:



Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para auditar todos los contenedores que se auditaron la semana pasada, especifique BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

#### BEGINTime

Especifica el valor del rango de horas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado es 00:00:00. Si no especificó un rango de fechas, el valor predeterminado es la fecha de hoy. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	10:30:08
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00. Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-04:00 o -04:00. Si emite este mandato a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect audita contenedores cuya última hora de auditoría sea las 5:30 o posterior en la fecha inicial.

#### ENDDate

Especifica el valor del rango de fechas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no un valor, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha después de que se realizara la última auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para incluir contenedores auditados hasta ayer, puede especificar ENDDATE=TODAY-1 o ENDDATE= -1.

Valor	Descripción	Ejemplo
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Para incluir contenedores auditados el décimo día del mes actual.

#### ENDTime

Especifica el valor del rango de horas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado son las 23:59:59. Este parámetro es opcional.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	10:30:08
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00.  Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o anterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30.  Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, se auditan los contenedores cuya última hora de auditoría sea las 5:30 o anterior en la fecha final especificada.

## Ejemplo: auditar un contenedor específico en una agrupación de almacenamiento de contenedor de nubes

Audite el contenedor 42-00000my000example000container000 de la agrupación de almacenamiento de contenedor de nubes.

```
audit container 42-00000my000example000container000 action=scanall
```




## Ejemplo: auditar una agrupación de almacenamiento de contenedores de nubes en un marco de tiempo específico

Auditar una agrupación de almacenamiento de contenedores de nubes llamada POOL3 e incluir solamente los contenedores de ayer entre las 9:30 y las 12:30.

```
audit container stgpool=pool3 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabla 1. Comandos relacionados con AUDIT CONTAINER

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY CONTAINER	Visualiza información sobre un contenedor.
QUERY DAMAGED	Muestra información sobre los archivos dañados.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

# AUDIT CONTAINER (Verificar la coherencia de la información de base de datos de un contenedor de directorios)

Utilice este mandato para buscar incoherencias entre la información de base de datos y un contenedor en una agrupación de almacenamiento de contenedores de directorio.

Puede utilizar este mandato para realizar las siguientes acciones para un contenedor de una agrupación de almacenamiento de contenedores de directorio:

- Explorar el contenido de un contenedor para validar la integridad de las extensiones de datos
- Eliminar los datos dañados de un contenedor
- Marcar un contenedor completo como dañado

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-AUDit CONTainer--+nombre_contenedor-----+-->
      +-STGpool---nombre_agrupación-----+
      '-STGpool---nombre_agrupación--STGPOOLDirectory---nombre_directorio-'

.-Action---SCANAll-----.
>--+-----+-----+----->
  '-Action---+SCANAll---+-'
        +-REMOVEDamaged-+
        +-MARKDamaged---+
        '-SCANDamaged---'

.-MAXProcess---4-----.-Wait---No-----.
>--+-----+-----+----->
  '-MAXProcess---número-' '-Wait---+No--+-'
                        '-Yes-'

.-BEGINDate---antes_primera_auditoria-.
>--+-----+-----+----->
  '-BEGINDate---fecha_inicio-----'

.-BEGINTime---00:00:00----.
>--+-----+-----+----->
  '-BEGINTime---hora_inicio-'

.-ENDDate---después_última_auditoria-.
>--+-----+-----+----->
  '-ENDDate---fecha_final-----'

.-ENDTime---23:59:59-----.
>--+-----+-----+-----><
  '-ENDTime---hora_finalización-'
```

## Parámetros

### nombre\_contenedor

Especifica el nombre del contenedor que desea auditar. Si no especifica este parámetro, debe especificar una agrupación de almacenamiento de contenedores de directorio.

### STGpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que desea auditar. Este parámetro es opcional. Si sólo especifica este parámetro, se auditan todos los contenedores definidos para la agrupación de almacenamiento. Si no especifica este parámetro, debe especificar un contenedor.

### STGPOOLDirectory

Especifica el nombre del directorio de agrupación de almacenamiento de contenedores que desea auditar. Este parámetro es opcional. Si especifica este parámetro, se auditan todos los contenedores definidos en el directorio de agrupación de almacenamiento de contenedores. Para especificar este parámetro, también debe especificar una agrupación de almacenamiento.

### Acción

Especifica la acción que realizará el servidor cuando se realiza la auditoría de un contenedor de una agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

**SCANALL**

Especifica que el servidor identifica los registros de base de datos que hacen referencia a las extensiones de datos con incoherencias. Este es el valor predeterminado. El servidor marca la extensión de datos como dañada en la base de datos. Consejo: Si ha utilizado el mandato PROTECT STGPOOL en una agrupación de almacenamiento de contenedores de directorio en el servidor de destino, puede reparar la extensión de datos dañada utilizando el mandato REPAIR STGPOOL.

**REMOVEDamaged**

Especifica que el servidor elimina los archivos de la base de datos que hagan referencia a la extensión de datos dañada.

**MARKDdamaged**

Especifica que el servidor marca explícitamente todas las extensiones de datos en el contenedor como dañadas.

**SCANDamaged**

Especifica que el servidor sólo comprueba las extensiones dañadas existentes en el contenedor.

Condición de restablecimiento de estado: Si la auditoría no detecta un error con una extensión de datos marcada como dañada, el estado de la extensión de datos se restablece. A continuación, la extensión de datos puede utilizarse. Esta condición proporciona un medio de restablecer el estado de las extensiones de datos dañadas si los errores se deben a un problema corregible. Las opciones SCANALL y SCANDAMAGED son las únicas opciones que restablecen una extensión dañada si se descubre que no está dañadas.

**MAXProcess**

Especifica el número de procesos paralelos que se utilizarán para comprobar un contenedor en una agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

**Wait**

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

**No**

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras el comando se está procesando. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

**Yes**

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se muestran en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.

**BEGINDate**

Especifica el valor del rango de fechas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no una fecha inicial, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha antes de que se realizara la primera auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para auditar todos los contenedores que se auditaron la semana pasada, especifique BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM

Valor	Descripción	Ejemplo
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Para incluir contenedores auditados el décimo día del mes actual.

#### BEGINTime

Especifica el valor del rango de horas en el que la auditoría debe iniciarse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se establece de 00:00:00 a 23:59:59. El valor predeterminado es 00:00:00. Si no especificó un rango de fechas, el valor predeterminado es la fecha de hoy. Este parámetro es opcional.

Puede especificar la fecha de inicio de la auditoría de una de las maneras siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	10:30:08
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00.  Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-04:00 o -04:00.  Si emite este mandato a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect audita contenedores cuya última hora de auditoría sea las 5:30 o posterior en la fecha inicial.

#### ENDDate

Especifica el valor del rango de fechas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de fechas especificado. Si especifica una hora pero no un valor, se utiliza la fecha actual. Si no especifica una fecha inicial y una fecha final, se auditan todos los contenedores. El valor predeterminado es la fecha después de que se realizara la última auditoría del contenedor. Este parámetro es opcional.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/2016
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1.  Para incluir contenedores auditados hasta ayer, puede especificar ENDDATE=TODAY-1 o ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Para incluir contenedores auditados un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Para incluir contenedores auditados el décimo día del mes actual.

#### ENDTime

Especifica el valor del rango de horas en el que la auditoría debe detenerse. Se auditan los contenedores que se auditaron por última vez dentro del rango de horas especificado. Si no especifica una hora inicial y una hora final, el rango de tiempo se

establece de 00:00:00 a 23:59:59. El valor predeterminado son las 23:59:59. Este parámetro es opcional. Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	10:30:08
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00.  Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, se auditan los contenedores cuya última hora de auditoría sea las 12:00 o anterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30.  Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, se auditan los contenedores cuya última hora de auditoría sea las 5:30 o anterior en la fecha final especificada.

### Ejemplo: auditar un contenedor de agrupación de almacenamiento determinado

Audite el contenedor de agrupación de almacenamiento 0000000000000721.dcf.

```
audit container n:\ddcont2\07\0000000000000721.dcf action=scanall
```

### Ejemplo: Eliminar los datos dañados de una agrupación de almacenamiento de contenedores de directorio

Auditar una agrupación de almacenamiento de contenedores de directorio llamada NEWDEDUP y eliminar los archivos dañados.

```
audit container stgpool=newdedup action=removedamaged
```

### Ejemplo: Marcar como dañados todos los datos de una agrupación de almacenamiento de contenedores de directorio

Auditar una agrupación de almacenamiento de contenedores de directorio llamada NEWDEDUP y marcar todos los archivos como dañados.

```
audit container stgpool=newdedup maxprocess=2 action=markdamaged
```

### Ejemplo: auditar una agrupación de almacenamiento de contenedores de directorios en un marco de tiempo específico

Auditar una agrupación de almacenamiento de contenedores de directorios llamada POOL2 e incluir solamente los contenedores anteriores a ayer entre las 9:30 y las 12:30.

```
audit container stgpool=pool2 begindate=today-1  
begintime=09:30:00 endtime=12:30:00
```

Tabla 1. Comandos relacionados con AUDIT CONTAINER

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
MOVE CONTAINER	Mueve el contenido de un contenedor de agrupación de almacenamiento a otro contenedor.
QUERY DAMAGED	Muestra información sobre los archivos dañados.

## AUDIT LDAPDIRECTORY (Auditar un servidor de directorios LDAP)

Utilice este mandato para auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de LDAP (Lightweight Directory Access Protocol). El servidor LDAP y el espacio de nombres se especifican mediante una o varias opciones LDAPURL.

Restricción: Utilice este mandato únicamente si ha configurado la autenticación de contraseña, como se describe en la sección Autenticación de los usuarios mediante un servidor LDAP. La información que se proporciona acerca del mandato AUDIT LDAPDIRECTORY únicamente se aplica a los entornos en los que la autenticación de contraseña se ha configurado como se describe en la sección Autenticación de los usuarios mediante un servidor LDAP.

Los nodos y los ID de usuario administrador que no autentican sus contraseñas con el servidor de directorios LDAP se suprimen con el mandato AUDIT LDAPDIRECTORY FIX=YES . Los nodos e ID de usuario administrador que ya no existen en la base de datos de IBM Spectrum Protect también se eliminan.

Antes de emitir este mandato, asegúrese de que se especifica la opción LDAPURL en el archivo dsmserv.opt . Consulte la opción LDAPURL para obtener más información. Si especificó más de una opción LDAPURL en el archivo dsmserv.opt , cada opción está validada en el orden en el que se colocaron. Si la opción LDAPURL no está especificada, el mandato falla.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegios de sistema.

## Sintaxis

---

```

      .-Fix-----No-----.
>>-AUDIT LDAPdirectory--+-----+----->
      '-Fix-----+No--+'
              '-Yes-'

      .-Wait-----No-----.
>--+-----+-----<
      '-Wait-----+No--+'
              '-Yes-'
```

## Parámetros

---

### Fix

Este parámetro opcional especifica cómo el servidor de IBM Spectrum Protect resuelve las incoherencias entre la base de datos y el directorio externo. El valor predeterminado es NO. Puede especificar los siguientes valores:

#### No

El servidor informa de todas las incoherencias, pero no cambia el directorio externo.

#### Yes

El servidor resuelve las inconsistencias que puede y sugiere más acciones, si es necesario.

Importante: Si hay entradas LDAP que se comparten con otros servidores de IBM Spectrum Protect, la selección YES puede hacer que esos servidores dejen de estar sincronizados.

### Wait

Este parámetro opcional especifica si se ha de esperar a que el servidor de IBM Spectrum Protect complete el proceso de este comando de forma subordinada. El valor predeterminado es NO. Puede especificar los siguientes valores:

#### No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

#### Yes

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: Auditar un directorio LDAP y reparar las incoherencias

---

Realice una auditoría del directorio LDAP que ha especificado en la opción LDAPURL. El servidor IBM Spectrum Protect resuelve algunas inconsistencias.

```
audit ldapdirectory fix=yes
```

```
ANR2749W El administrador ADMIN1 estaba ubicado en el servidor de directorios LDAP pero no
```

en la base de datos.  
 ANR2749W El administrador ADMIN2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.  
 ANR2749W El nodo NODE1 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.  
 ANR2749W El nodo NODE2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.  
 ANR2748W El nodo NODE1 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.  
 ANR2748W El nodo NODE2 estaba ubicado en el servidor de directorios LDAP pero no en la base de datos.  
 ANR2745I Se ha completado el mandato AUDIT LDAPDIRECTORY: solo hay 4 entradas del administrador de nodo en el servidor de directorio LDAP (no en el servidor de IBM Spectrum Protect), solo hay 0 entradas de administrador en el servidor de IBM Spectrum Protect (no en el servidor de directorio LDAP), solo hay 2 entradas de nodo en el servidor de directorio LDAP (no en el servidor de IBM Spectrum), solo hay 0 entradas de nodo en el servidor de IBM Spectrum Protect, (no en el servidor de directorio LDAP), 6 entradas se han suprimido del servidor LDAP en total.

## Comandos relacionados

Tabla 1. Mandatos relacionados con AUDIT LDAPDIRECTORY

Comando	Descripción
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.

## AUDIT LIBRARY (Inventarios de volúmenes de auditoría en una biblioteca automatizada)

Utilice este comando para auditar y sincronizar inventarios de volúmenes en una biblioteca automatizada.

Cuando se emite el comando AUDIT LIBRARY en un cliente de biblioteca, el cliente sincroniza su inventario con el inventario del gestor de bibliotecas. Si el cliente de biblioteca detecta incongruencias, las corrige por medio de un cambio en la propiedad del volumen en el gestor de biblioteca.

Cuando se emite el comando AUDIT LIBRARY en un servidor en el que la biblioteca es SCSI, 349X o ACSLS (LIBTYPE=SCSI, LIBTYPE=349X o LIBTYPE=ACSL), el servidor sincroniza su inventario con el inventario del dispositivo de bibliotecas. Si el servidor detecta incoherencias, elimina los volúmenes ausentes de su inventario.

- En las bibliotecas SCSI, el servidor actualiza también las ubicaciones de los volúmenes de su inventario que han sido trasladados desde la última auditoría.
- En las bibliotecas 349X, el servidor garantiza también que los volúmenes reutilizables se encuentran en la categoría reutilizable y los volúmenes privados en la categoría privada.

Cuando se emite el comando AUDIT LIBRARY en un servidor que es un gestor de bibliotecas de la biblioteca (SHARED=YES), el servidor actualiza la propiedad de sus volúmenes si detecta incoherencias.

Con independencia del servidor o del tipo de biblioteca, la emisión del comando AUDIT LIBRARY no agrega automáticamente nuevos volúmenes a una biblioteca. Para agregar nuevos volúmenes, debe utilizar el comando CHECKIN LIBVOLUME.

Atención: Las siguientes precauciones son aplicables sólo a las bibliotecas SCSI, 349X y ACSLS (LIBTYPE=SCSI, LIBTYPE=349X y LIBTYPE=ACSL):

- La ejecución del comando AUDIT LIBRARY impide que tenga lugar cualquier otra actividad de biblioteca hasta que se ha completado la auditoría. Por ejemplo, el servidor no procesará, restaurará ni recuperará peticiones que impliquen a la biblioteca



cuando esté ejecutándose el mandato AUDIT LIBRARY.

- Si está realizándose cualquier otra actividad en la biblioteca, no emita el comando AUDIT LIBRARY. La emisión del comando AUDIT LIBRARY cuando una biblioteca está activa puede producir resultados imprevisibles (por ejemplo, una condición de bloqueo) si un proceso que está accediendo actualmente a la biblioteca intenta adquirir un nuevo montaje de cinta.

Este comando crea un proceso subordinado que puede cancelar con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-AUDIT LIBRARY--nombre_biblioteca----->
.-CHECKLabel----Yes-----
>--+-----+-----+-----+-----+----->
'-CHECKLabel----+Yes----+'
                '-Barcode-'

.-REFRESHstate----No-----
>--+-----+-----+-----+-----+-----><
'-REFRESHstate----+No----+'
                '-Yes-'
```

## Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de auditar.

CHECKLabel

Especifica cómo se comprueba la etiqueta del volumen de almacenamiento durante el proceso de auditoría. Este parámetro sólo se aplica a las bibliotecas SCSI. Este parámetro se pasa por alto en otros tipos de bibliotecas. El valor predeterminado es YES.

Los valores posibles son:

Yes

Especifica que el servidor comprueba cada etiqueta de volumen para verificar la identidad del volumen.

Barcode

Especifica que el servidor utiliza el lector de códigos de barra para leer la etiqueta de almacenamiento. Al utilizar códigos de barras, el tiempo de proceso de la auditoría disminuye. Este parámetro sólo se aplica a las bibliotecas SCSI.

Atención: Si el escáner no puede leer una etiqueta de código de barras determinada, o si falta una etiqueta de código de barras, el servidor carga esa cinta en una unidad para leer la etiqueta.

REFRESHstate

Especifica si la información del servidor sobre una biblioteca, que normalmente se obtiene durante la inicialización, se renueva para que se reflejen los cambios en la configuración. Si se establece el parámetro REFRESHSTATE en Yes, esta acción se realiza sin necesidad de reiniciar el servidor o redefinir la biblioteca. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor no actualiza el estado de la biblioteca al auditar esta.

Yes

Especifica que el servidor no actualiza el estado de la biblioteca cuando se emite el mandato AUDIT LIBRARY.

## Ejemplo: auditar una biblioteca automatizada

Auditar la biblioteca automatizada EZLIFE.

```
audit library ezlif
```

## Comandos relacionados

Tabla 1. Comandos relacionados con AUDIT LIBRARY

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.

Comando	Descripción
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE LIBRARY	Suprime una biblioteca.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

## AUDIT LIBVOLUME (Verificar información de base de datos para un volumen de cinta)

Utilice este mandato para determinar si un volumen de cinta está intacto y para auditar datos en cualquier volumen de cinta.

Puede emitir el mandato AUDIT LIBVOLUME desde cualquier volumen de cinta que está incorporado en una biblioteca. El mandato se ejecuta en segundo plano de forma predeterminada. Puede emitir el mandato desde los tipos de bibliotecas siguientes que tienen unidades IBM® TS1140, IBM LTO 5 o una unidad de cintas de generación posterior:

- biblioteca de cintas SCSI
- Biblioteca virtual de cintas (VTL)

La tabla siguiente describe las unidades de cinta que pueden verificar volúmenes de cinta con tipos de soporte para unidades de cinta de IBM TS1140 y IBM LTO 5 y una generación posterior de LTO:

Tabla 1. Unidades de cinta y tipos de soporte

Unidad	Tipo de medio
TS1140	JB, JX, JA, JW, JJ, JR, JC, JY y JK
IBM LTO 5	LTO 3, LTO 4 y LTO 5
IBM LTO 6	LTO 4, LTO 5 y LTO 6
IBM LTO 7	LTO 5, LTO 6 y LTO 7

La tabla siguiente describe el nivel mínimo de controlador de dispositivo que se requiere para ejecutar el mandato:

Tabla 2. Nivel mínimo de controlador de dispositivo de IBM

Nombre de controlador	Nivel de controlador de dispositivo
Controlador Atape en AIX	12.3.5.00
controlador lin_tape en Linux	1.6.7.00
Controlador de cintas de IBM en Windows	6.2.2.00

Restricción: No puede emitir el mandato CANCEL PROCESS mientras el mandato AUDIT LIBVOLUME está en curso.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones para la biblioteca en la que se ha definido el volumen de cinta.

### Sintaxis

```
>>-AUDit LIBVolume--nombre_biblioteca--nombre_volumen----->
      .-Wait----No-----
>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
      '-Wait----+No--+-'
           '-Yes-'
```

## Parámetros

---

nombre\_biblioteca (necesario)

Especifica el nombre del volumen de biblioteca donde está ubicado el volumen de cinta que desea auditar.

nombre\_volumen (necesario)

Especifica el nombre del volumen de cinta físico que desea auditar.

Wait (Opcional)

Especifica si la operación de auditoría o verificación se ha completado en primer plano o en segundo plano. Este parámetro es opcional. Las opciones siguientes están disponibles:

No

Especifica que la operación se ha completado en segundo plano. El valor NO es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse.

## Ejemplo: Auditar un volumen de cinta

---

Audite la biblioteca EZLIFE que tiene un volumen de cinta que se denomina KM0347L5.

```
audit libvolume ezlife KM0347L5
```

## AUDIT LICENSES (Auditoría de utilización de almacenamiento del servidor)

---

Utilice este comando para hacer la auditoría del almacenamiento del servidor que utilizan los nodos cliente y la de las licencias del servidor. La auditoría determina si la configuración actual es conforme a los plazos de licencia.

Una auditoría crea un proceso subordinado que puede cancelar con el comando CANCEL PROCESS. Si detiene el servidor y vuelve a iniciarlo, se ejecutará automáticamente una auditoría, tal como especifica el comando SET LICENSEAUDITPERIOD. Para ver los resultados de la auditoría, utilice el comando QUERY LICENSE.

Atención: La auditoría del almacenamiento del servidor puede emplear una gran cantidad de tiempo de CPU. Puede utilizar la opción del servidor AUDITSTORAGE para especificar que no se haga la auditoría del almacenamiento.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-AUDit LICenses-----><
```

## Parámetros

---

Ninguno.

## Ejemplo: auditar licencias de servidor

---

Emitir el comando AUDIT LICENSES.

```
audit licenses
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con AUDIT LICENSES

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY AUDITOCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.

Comando	Descripción
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.

## AUDIT VOLUME (verificar la información de base de datos de un volumen de agrupación de almacenamiento específico)

Utilice este comando para comprobar si hay incoherencias entre la información de la base de datos y un volumen de agrupación de almacenamiento. La información de proceso que se genera durante la realización de una auditoría se envía a las anotaciones de actividades y a la consola del servidor.

Restricción: No puede utilizar este mandato para volúmenes que están asignados a agrupaciones de almacenamiento de copias de contenedor.

Sólo es posible auditar volúmenes que pertenecen a agrupaciones de almacenamiento con DATAFORMAT=NATIVE y DATAFORMAT=NONBLOCK.

No se puede hacer la auditoría de un volumen si éste se está suprimiendo de una agrupación de almacenamiento primaria o de copia.

Mientras hay un proceso de auditoría activo, los clientes no pueden restaurar datos del volumen especificado ni almacenar nuevos datos en ese volumen.

Si el servidor detecta un archivo con errores, el manejo de dicho archivo dependerá del tipo de agrupación de almacenamiento al que pertenezca el volumen, de si se ha especificado la opción FIX en este comando y de si el archivo se ha almacenado también en un volumen asignado a otras agrupaciones.

Si IBM Spectrum Protect no detecta errores para un archivo que estaba marcado como dañado, el estado del archivo se restablece para que pueda utilizarse.

El servidor no suprime las copias archivadas que están retenidas para supresión. Si la protección de retención de copias archivadas está activada, el servidor no suprimirá las copias archivadas cuyo período de retención no haya caducado.

Para visualizar información acerca del contenido de un volumen de agrupación de almacenamiento, utilice el comando QUERY CONTENT.

Para auditar varios volúmenes, puede utilizar los parámetros FROMDATE y TODATE. Utilice el parámetro STGPOOL para auditar todos los volúmenes en una agrupación de almacenamiento. Cuando utilice los parámetros FROMDATE, TODATE o ambos, el servidor limita la auditoría sólo a los volúmenes de medios secuenciales que cumplen los criterios de fecha e incluye todos los volúmenes de disco activados del almacenamiento. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Si ejecuta un servidor con la protección de retención de archivado activada y tiene datos almacenados en agrupaciones de almacenamiento que se han definido con el parámetro RECLAMATIONTYPE=SNAPLOCK, la última fecha de acceso del archivador NetApp SnapLock para un volumen debe ser igual a la fecha de finalización del período de reclamación que ha de visualizarse al emitir un mandato QUERY VOLUME F=D en ese volumen. Durante el proceso de AUDIT VOLUME, se comparan esas fechas. Si no coinciden y el mandato AUDIT VOLUME se está ejecutando con el parámetro FIX=NO, se emitirá un mensaje indicándole que el mandato se debe ejecutar con el parámetro FIX=YES para resolver la incoherencia. Si no coinciden y el mandato AUDIT VOLUME se está ejecutando con el parámetro FIX=YES, se solucionarán las incoherencias.

Atención: Utilice el parámetro FIX=YES sólo si la unidad de cintas y la infraestructura de red de área de almacenamiento (SAN) son estables. Asegúrese de que los cabezales de cinta estén limpios y que los controladores de dispositivos estén estables y sean fiables. De lo contrario, corre el riesgo de suprimir datos sin errores cuando utilice este parámetro. El servidor no puede determinar si una cinta está dañada físicamente o si una infraestructura de cinta no es estable.

Este mandato crea un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento en la que está definido el volumen.

## Sintaxis

```

                                .-Fix-----No-----.
>>-AUDit Volume--+-nombre_volumen-+-----+----->
                    '-| A |-----' '-Fix-----+No--+-'
                                '-Yes-'

.-SKIPPartial-----No-----. .-Quiet-----No-----.
>+-----+-----+-----+-----<
'-SKIPPartial-----+No--+-' '-Quiet-----+No--+-'
                    '-Yes-'           '-Yes-'

A (como mínimo debe especificarse uno de estos parámetros)

|+-----+-----+-----+----->
| (1)                                     |
'|-----STGPool-----nombreagrupación-|

(1)                                     (1)
.------FROMDate-----TODAY-. .-TODate-----TODay-----.
>+-----+-----+-----+-----|
'|-----FROMDate-----date-----' '-TODate-----date-----'

```

### Notas:

1. No es posible especificar un nombre de volumen si especifica un nombre de agrupación de almacenamiento, FROMDATE o TODATE.

## Parámetros

### nombre\_volumen

Especifica el nombre del volumen de agrupación de almacenamiento que desea auditar. Este parámetro es necesario si no especifica una agrupación de almacenamiento. No es posible especificar un nombre de volumen con los parámetros FROMDATE y TODATE.

### Fix

Especifica cómo el servidor resuelve las incoherencias entre el inventario de la base de datos y el volumen de agrupación de almacenamiento especificado. Este parámetro es opcional. El valor predeterminado es NO.

Las acciones que realiza el servidor dependen también de si el volumen está asignado a una agrupación de almacenamiento primaria o de copia.

#### **Agrupación de almacenamiento primaria:**

Nota: Si el comando AUDIT VOLUME no detecta ningún error en un archivo que anteriormente se había marcado como dañado, IBM Spectrum Protect restablecerá el estado del archivo para que éste pueda utilizarse. Esto proporciona un medio de restaurar el estado de los archivos dañados si se determina que los errores son a causa de un problema de hardware corregible, como por ejemplo un cabezal de cinta que esté sucio.

#### Fix=No

IBM Spectrum Protect notifica, pero sin suprimirlos, los registros de la base de datos que hacen referencia a archivos con incoherencias:

- IBM Spectrum Protect marca el archivo como dañado en la base de datos. Si una copia de seguridad se almacena en una agrupación de almacenamiento de copia, el archivo puede restaurarse con el comando RESTORE VOLUME o RESTORE STGPOOL.
- Si el archivo es una copia en caché, las referencias al archivo que haya en este volumen se pueden suprimir emitiendo el comando AUDIT VOLUME y especificando FIX=YES. Si el archivo físico no es una copia en caché y existe un duplicado almacenado en una agrupación de almacenamiento de copia, éste puede restaurarse con el comando RESTORE VOLUME o RESTORE STGPOOL.

#### Fix=Yes

El servidor arregla todas las incoherencias a medida que se detectan:

- Si el archivo es una copia en caché, el servidor suprime los registros de base de datos que hagan referencia al archivo en caché. El archivo primario se almacena en otro volumen.

- Si el archivo físico no es una copia en caché, y el archivo se almacena también en una o más agrupaciones de almacenamiento de copia, se informará acerca del error y el archivo físico se marcará como dañado en la base de datos. Puede restaurar el archivo físico con el comando RESTORE VOLUME o RESTORE STGPOOL.
- Si el archivo físico no es una copia en caché, y el archivo físico no está almacenado en una agrupación de almacenamiento de copia, se suprimen de la base de datos todos los archivos lógicos en los que se han detectado incoherencias.
- Si la protección de retención de archivado se ha activado con el comando SET ARCHIVERETENTIONPROTECTION, podrá suprimirse una copia en caché de los datos, si es necesario. Los datos de las agrupaciones de almacenamiento primarias y de copia sólo se pueden marcar como dañados y no se pueden suprimir nunca.

No utilice el comando AUDIT VOLUME con FIX=YES si está ejecutándose un proceso de restauración (RESTORE STGPOOL o RESTORE VOLUME). El comando AUDIT VOLUME podría dar lugar a que la restauración no se completara.

**Agrupación de almacenamiento de copia:**

Fix=No

El servidor notifica el error y marca la copia del archivo físico como dañada en la base de datos.

Fix=Yes

El servidor suprime todas las referencias al archivo físico y a los registros de la base de datos que señalen a un archivo físico que no exista.

SKIPPartial

Especifica si IBM Spectrum Protect debe pasar por alto los archivos parciales, que son archivos que ocupan varios volúmenes de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Cuando se realiza una operación de auditoría en un volumen de medio de acceso secuencial, este parámetro impide montajes de medios de acceso secuencial adicionales que pueden ser necesarios para realizar una auditoría de cualquier archivo parcial. Los valores posibles son:

No

IBM Spectrum Protect audita los archivos que ocupan varios volúmenes.

A menos que especifique SKIPPARTIAL=YES, IBM Spectrum Protect intenta procesar cada archivo almacenado en el volumen, incluidos los archivos que abarcan otros volúmenes, y fuera de los mismos. Para auditar los archivos que ocupan varios volúmenes, deben cumplirse las condiciones siguientes:

- En los volúmenes de acceso secuencial, los volúmenes de acceso secuencial adicionales deben tener una modalidad de acceso de lectura/grabación o sólo lectura.
- En los volúmenes de acceso aleatorio, los volúmenes adicionales deben estar en activo.

Yes

IBM Spectrum Protect sólo audita los archivos que están almacenados en el volumen que se va a auditar. Se desconoce el estado de los archivos parciales.

Quiet

Especifica si IBM Spectrum Protect envía mensajes informativos detallados a las anotaciones de actividad y a la consola del servidor acerca de archivos irrecuperables del volumen. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que IBM Spectrum Protect envía mensajes informativos detallados y un resumen. Cada mensaje contiene el nodo, el espacio de archivos y nombre de cliente del archivo.

Yes

Especifica que IBM Spectrum Protect sólo envía un informe resumido.

FROMDate

Especifica la fecha inicial del rango para auditar volúmenes. El valor predeterminado es la fecha actual. Se auditan todos los volúmenes de medios secuenciales que cumplen los criterios de rango horario grabados con posterioridad a esta fecha. El servidor incluye todos los volúmenes de disco activados en el almacenamiento. El servidor inicia un proceso de auditoría para cada volumen y ejecuta el proceso en serie. No se puede utilizar este parámetro si se ha especificado un volumen. Este parámetro es opcional. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	10/15/2001  Si se especifica una fecha, se evaluarán todos los volúmenes candidatos que se grabaron en dicha fecha (que se inicia a las 12:00:01 am).

Valor	Descripción	Ejemplo
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para visualizar información empezando por los volúmenes grabados hace una semana, puede especificar FROMDATE=TODAY-7 o FROMDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### TODate

Especifica la fecha final del rango de volúmenes que se va a auditar. Se auditan todos los volúmenes de medios secuenciales que cumplen los criterios de rango horario grabados con anterioridad a esta fecha. El servidor incluye todos los volúmenes de disco activados en el almacenamiento. Si no especifica un valor, el servidor toma la fecha actual como valor predeterminado. No se puede utilizar este parámetro si se ha especificado un volumen. Este parámetro es opcional. Para limitar el número de volúmenes que pueden incluir volúmenes de disco, utilice los parámetros FROMDATE, TODATE y STGPOOL.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	10/15/2001 Si se especifica una fecha, se evaluarán todos los volúmenes candidatos que se grabaron en dicha fecha (que finaliza a las 11:59:59 pm).
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1. Para visualizar la información creada hasta ayer, puede especificar TODATE=TODAY-1, o simplemente, TODATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### STGPool

Este parámetro especifica que el servidor sólo audita los volúmenes de la agrupación de almacenamiento especificada. Este parámetro es opcional. No se puede utilizar este parámetro si se ha especificado un volumen.

### Ejemplo: verificar la información de base de datos de un volumen de agrupación de almacenamiento específico

Compruebe que la información de base de datos del volumen de agrupación de almacenamiento PROG2 sea coherente con los datos almacenados en el volumen. IBM Spectrum Protect arregla todas las incoherencias.

```
audit volume prog2 fix=yes
```

## Ejemplo: verificar la información de base de datos de todos los volúmenes en los que se ha grabado durante un rango de fechas específico

Verifique que la información de base de datos de todos los volúmenes en los que se ha grabado entre el 20/3/2002 y el 22/3/2002 sea coherente con los datos almacenados en el volumen.

```
audit volume fromdate=03/20/2002 todate=03/22/2002
```

## Ejemplo: verificar la información de base de datos de todos los volúmenes de una agrupación de almacenamiento específica

Verifique que la información de base de datos para todos los volúmenes de la agrupación de almacenamiento STPOOL3 sea coherente con los datos almacenados hoy en el volumen.

```
audit volume stgpool=STPOOL3
```

## Ejemplo: verificar la información de base de datos de todos los volúmenes de una agrupación de almacenamiento específica en la que se ha grabado durante los dos últimos días

Verifique que la información de base de datos para todos los volúmenes de la agrupación de almacenamiento STPOOL3 sea coherente con los datos almacenados en el volumen durante los últimos dos días.

```
audit volume stgpool=STPOOL3 fromdate=-1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con AUDIT VOLUME

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
SET ARCHIVERETENTIONPROTECTION	Especifica si la protección de retención de datos está activada.

## Comandos BACKUP

Utilice los comandos BACKUP para crear copias de seguridad de información u objetos IBM Spectrum Protect.

- BACKUP DB (copia de seguridad de la base de datos)
- BACKUP DEVCONFIG (Crear copias de seguridad de la información de configuración de dispositivos)
- BACKUP NODE (Copia de seguridad de un nodo NAS)
- BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)
- BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)

## BACKUP DB (copia de seguridad de la base de datos)

Utilice este mandato para realizar una copia de seguridad de una base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.

Atención: Para restaurar una base de datos, el servidor debe utilizar la información del archivo de historial de volumen y el archivo de configuración de dispositivo. Debe realizar copias del archivo de historial de volumen y el archivo de configuración de dispositivo, y guardarlas. Estos archivos no pueden volverse a crear.

Para determinar cuánto espacio de almacenamiento adicional necesita una copia de seguridad, emita el mandato QUERY DB.



Restricciones: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 6.3 y se está utilizando un servidor versión 7.1.

Una vez que la copia de seguridad de base de datos se ha completado, el servidor de IBM Spectrum Protect realiza una copia de seguridad de la información, en función de las opciones que se han especificado en el archivo de opciones del servidor. Se realiza una copia de seguridad de la siguiente información:

- Se realiza una copia de seguridad de la información de historial de volúmenes secuenciales en todos los archivos que la opción VOLUMEHISTORY especifica
- Se realiza una copia de seguridad de la información sobre la configuración de dispositivos en todos los archivos que la opción DEVCONFIG especifica
- La clave de cifrado maestra de servidor

Si no hay espacio suficiente en el volumen o espacio de archivos del directorio de registros activos definido, puede establecer la opción de DB2 *overflowlogpath* para utilizar un directorio que tenga el espacio disponible necesario. Por ejemplo, utilice el mandato siguiente para utilizar el directorio `/home/tsminst2/overflow_dir`:

```
db2 update db cfg for TSMDB1 using overflowlogpath /home/tsminst2/overflow_dir
```

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-BACKUP DB--DEVclass-----nombre_clase_dispositivo----->
. -Type-----Full-----
>+-----+----->
'-Type-----+Incremental+-'
      +-Full-----+
      '-DBSnapshot--'

>+-----+----->
|                                     |
|                                     |
|          V                          |
| -VOLumentnames-----+---nombre_volumen+-----+
|          '-FILE:--nombre_archivo-'

. -NUMStreams-----1----- . -Scratch-----Yes-----
>+-----+-----+-----+----->
'-NUMStreams-----número-' '-Scratch-----+Yes+-'
                                     '-No--'

. -Wait-----No----- . -DEDUPDEvice-----No-----
>+-----+-----+-----+----->
'-Wait-----+No--+-' '-DEDUPDEvice-----+No--+-'
      '-Yes-'                                     '-Yes-'

. -COMPRESS-----No----- . -PROTECTKeys-----Yes-----
>+-----+-----+-----+----->
|                                     |
|                                     |
|          (1) | '-PROTECTKeys-----+No--+-'
| -COMPRESS-----+No--+-----+
|          '-Yes-'                                     '-Yes-'

>+-----+-----+-----+-----><
'-PASSword-----nombre_contraseña-'
```

Notas:

1. El valor predeterminado para el parámetro COMPRESS es condicional. Si especifica el parámetro COMPRESS en el mandato BACKUP DB, modifica cualquier valor de parámetro COMPRESS establecido en el mandato SET DBRECOVERY. De lo contrario, el valor establecido en el mandato SET DBRECOVERY es el valor predeterminado.

## Parámetros

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial que se ha de utilizar para la copia de seguridad. Si emite el mandato BACKUP DB y la clase de dispositivo no es la especificada en el mandato SET DBRECOVERY, aparecerá un mensaje de

aviso. Sin embargo, la operación de copia de seguridad continuará y no se verá afectada por ello.

Si el mandato SET DBRECOVERY no se ha emitido para definir una clase de dispositivo, el mandato BACKUP DB falla.

Restricción:

- No puede utilizar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA.
- Una operación de restauración de la base de datos falla si el origen de la restauración es una biblioteca FILE. Se crea una biblioteca FILE si la clase de dispositivo FILE especifica SHARED=YES.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la copia de seguridad, IBM Spectrum Protect cancela las operaciones con prioridad más baja como, por ejemplo, operaciones de reclamación, para que haya una unidad disponible para la copia de seguridad.

Type

Especifica el tipo de copia de seguridad que se ha de ejecutar. Este parámetro es opcional. El valor predeterminado es FULL. Son posibles los siguientes valores:

Full

Especifica que desea ejecutar una copia de seguridad completa de la base de datos de IBM Spectrum Protect.

Incremental

Especifica que desea ejecutar una copia de seguridad incremental de la base de datos de IBM Spectrum Protect. Una imagen de copia de seguridad incremental (o acumulativa) contiene una copia de todos los datos de la base de datos que se han cambiado desde la última operación satisfactoria de copia de seguridad completa.

DBSnapshot

Especifica que desea ejecutar una copia de seguridad completa de la base de datos de ADSM en un momento específico. Se copia todo el contenido de la base de datos y se crea una nueva copia de seguridad completa de la base de datos ADSM en un momento específico sin interrumpir la serie de copia de seguridad completa e incremental existente de la base de datos.

VOLumentnames

Especifica los volúmenes que se utilizan para hacer la copia de seguridad de la base de datos. Este parámetro es opcional. Sin embargo, si especifica SCRATCH=NO, debe especificar una lista de volúmenes.

nombre\_volumen

Especifica los volúmenes que se utilizan para hacer la copia de seguridad de la base de datos. Puede especificar varios volúmenes separando los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre del archivo que contiene la lista de volúmenes que se utiliza para la copia de seguridad de base de datos. El nombre de cada volumen debe estar en una línea aparte. Las líneas en blanco y las líneas de comentarios, que empiezan con un asterisco, no se tienen en cuenta.

Por ejemplo, para utilizar volúmenes DB0001, DB0002 y DB0003, cree un archivo que contenga estas líneas:

```
DB0001
DB0002
DB0003
```

Asigne un nombre apropiado al archivo. Por ejemplo:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA

A continuación, puede especificar los volúmenes para el mandato, del modo siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux

```
VOLUMENAMES=FILE:TAPEVOL
```

 Sistemas operativos Windows

```
VOLUMENAMES=FILE:TAPEVOL.DATA
```

NUMStreams

Especifica el número de corrientes de movimiento de datos paralelas que se utilizan cuando se realiza la copia de seguridad de la base de datos. El valor mínimo es 1 y el máximo es 32. Aumentar el valor provoca un aumento correspondiente en el número de sesiones de copia de seguridad de base de datos que se van a utilizar y en el número de unidades que se van a utilizar por clase de dispositivo. Si especifica un valor NUMSTREAMS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. De lo contrario, se utiliza el valor establecido en el mandato SET DBRECOVERY. El valor NUMSTREAMS se utiliza para todos los tipos de copias de seguridad de base de datos.

Si se especifica un valor mayor que el número de unidades disponibles para la clase de dispositivo, se utiliza el número de unidades disponibles. Las unidades disponibles son las definidas en la clase de dispositivo por el parámetro MOUNTLIMIT o por el número de unidades en línea para la clase de dispositivo especificada. La sesión se visualiza en la salida de QUERY SESSION. Si aumenta el número de corrientes, se utilizan más volúmenes de la clase de dispositivo correspondiente a esta operación. El uso de más volúmenes puede mejorar la velocidad de las copias de seguridad de base de datos, pero a expensas de que haya más volúmenes que no se utilizan completamente.

#### Scratch

Especifica si pueden utilizarse volúmenes reutilizables para la copia de seguridad. Este parámetro es opcional. El valor predeterminado es YES. Son posibles los siguientes valores:

##### Yes

Especifica que pueden utilizarse volúmenes reutilizables.

Si especifica SCRATCH=YES y el parámetro VOLUMENAMES, IBM Spectrum Protect sólo utiliza volúmenes reutilizables si no hay espacio disponible en los volúmenes especificados.

Si no incluye una lista de los volúmenes utilizando el parámetro VOLUMENAMES, debe especificar SCRATCH=YES o utilizar el valor predeterminado.

##### No

Especifica que no pueden utilizarse los volúmenes reutilizables.

Si especifica volúmenes con el parámetro VOLUMENAMES y SCRATCH=NO, la copia de seguridad no se hará si no hay suficiente espacio disponible para almacenar los datos de copia de seguridad en los volúmenes especificados.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. El valor predeterminado es NO. Son posibles los siguientes valores:

##### No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si se cancela un proceso en segundo plano BACKUP DB, puede que ya se haya realizado la copia de seguridad de parte de la base de datos antes de haberse ejecutado la cancelación.

##### Yes

Especifica que el servidor procesa este mandato en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el mandato finaliza. Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### DEDUPDEvice

Especifica que el dispositivo de almacenamiento de destino da soporte a la eliminación de datos duplicados. Cuando se establece en YES, el formato de las imágenes de copia de seguridad está optimizado para los dispositivos de deduplicación de datos, lo que hace que las operaciones de copia de seguridad resulten más eficaces. Son posibles los valores siguientes:

##### No

Especifica que el dispositivo de almacenamiento de destino no da soporte a la eliminación de datos duplicados. NO es el valor predeterminado.

Asegúrese de que este parámetro se establece en NO para los siguientes dispositivos:

- Bibliotecas SCSI
- Todos los dispositivos definidos con una clase de dispositivo FILE
- Bibliotecas de cintas virtuales (VTL) que no soportan la función de eliminación de duplicados de datos

##### Yes

Especifica que un dispositivo de destino admite la eliminación de duplicados de datos y que desea optimizar las copias de seguridad para esta función. Puede establecer este parámetro en YES si está utilizando bibliotecas de cintas virtuales (VTL) que admiten la eliminación de duplicados de datos.

#### COMPRESS

Especifica si se comprimen los volúmenes que se crean mediante el mandato BACKUP DB. El valor COMPRESS se utiliza para todos los tipos de copias de seguridad de base de datos. Este parámetro es opcional. El valor predeterminado es conditional. Si

especifica el parámetro COMPRESS en el mandato BACKUP DB, altera temporalmente cualquier valor establecido en el mandato SET DBRECOVERY. De lo contrario, el valor establecido en el mandato SET DBRECOVERY es el valor predeterminado. Puede especificar uno de los siguientes valores:

No

Especifica que los volúmenes que se crean mediante el mandato BACKUP DB no se comprimen.

Yes

Especifica que los volúmenes que se crean mediante el mandato BACKUP DB se comprimen.

Restricciones:

- Tenga cuidado al especificar el parámetro COMPRESS. La utilización de compresión durante las copias de seguridad de la base de datos puede reducir el tamaño de los archivos de copia de seguridad. Sin embargo, la compresión puede aumentar el tiempo necesario para completar el proceso de copia de seguridad de base de datos.
- No realice copias de seguridad de datos comprimidos en una cinta. Si el entorno del sistema almacena copias de seguridad de base de datos en la cinta, establezca el parámetro COMPRESS en No en los mandatos SET DBRECOVERY y BACKUP DB.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows PROTECTKeys

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor que se utiliza para cifrar los datos de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es el valor que se especifica para el parámetro PROTECTKEYS en el mandato SET DBRECOVERY. Puede especificar uno de los siguientes valores:

No

Especifica que las copias de seguridad de base de datos no incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=NO, debe hacer copia de seguridad de la clave de cifrado maestra manualmente para el servidor y hacer que la clave está disponible cuando implementa la recuperación tras desastre.

Yes

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Atención: Si especifica PROTECTKEYS=YES, también debe especificar el parámetro PASSWORD.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows PASSWORD

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. El valor predeterminado es el valor que se especifica para el parámetro PASSWORD en el mandato SET DBRECOVERY.

Importante: Asegúrese de que recuerda esta contraseña. Si especifica una contraseña para las copias de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos.

## Ejemplo: Ejecutar una copia de seguridad incremental utilizando un volumen reutilizable

Ejecutar una copia de seguridad incremental de la base de datos, utilizando un volumen reutilizable. Utilice una clase de dispositivo FILE para la copia de seguridad.

```
backup db devclass=file type=incremental
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows

## Ejemplo: Cifrar datos de agrupación de almacenamiento en copias de seguridad de base de datos

Cifrar los datos de agrupación de almacenamiento especificando que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Emita el mandato siguiente:

```
backup db protectkeys=yes password=password_name
```

## Comandos relacionados

Tabla 1. Comandos relacionados con BACKUP DB

Comando	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.



| v | |  
 '-Filenames-----nombre\_archivo---+-'

## Parámetros

### FileNames

Especifica los archivos donde debe almacenarse la información de configuración de dispositivos. Puede especificar varios archivos separándolos con comas y sin espacios intercalados. Este parámetro es opcional.

Si no especifica un nombre de archivo, IBM Spectrum Protect almacena la información en todos los archivos especificados con la opción DEVCONFIG del archivo de opciones del servidor.

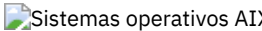
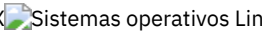
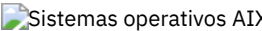
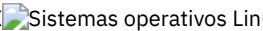
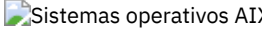
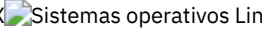
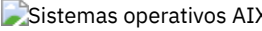
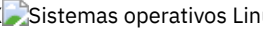
## Ejemplo: realizar la copia de seguridad de la información de configuración de un dispositivo en un archivo

Realizar la copia de seguridad de la información de configuración de un dispositivo en un archivo denominado DEVICE.

```
backup devconfig filenames=device
```

## Comandos relacionados

Tabla 1. Comandos relacionados con BACKUP DEVCONFIG

Comando	Descripción
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DEVCLASS	Define una clase de dispositivo.
  DEFINE DEVCLASS (servidor de medios de z/OS)	  Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
  UPDATE DEVCLASS (servidor de medios de z/OS)	  Cambia los atributos de una clase de dispositivo para el almacenamiento gestionado por un servidor de medios de z/OS.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE PATH	Cambia los atributos asociados con una ruta.
UPDATE SERVER	Actualiza la información sobre un servidor.

## BACKUP NODE (Copia de seguridad de un nodo NAS)

Utilice este comando para iniciar una operación de copia de seguridad de un nodo de almacenamiento conectado a red (NAS).

Las copias de seguridad que se crean para nodos NAS con este comando BACKUP NODE cuentan con funciones equivalentes a las de las copias de seguridad que se crean mediante el comando BACKUP NAS en un cliente de IBM Spectrum Protect. Puede restaurar estas copias de seguridad con el comando RESTORE NODE del servidor o con el comando RESTORE NAS del cliente.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas para el dominio al que está asignado el nodo o autorización de propietario de cliente en el nodo.

## Sintaxis

```
>>-Backup Node--nombre_nodo----->
>+-----+-----+----->
| .,-----|
| v-----| |
|'-----nombre_sistema_archivos-----'|
>+-----+-----+----->
| .-TOC-----Preferred-----|
|'-MGmtclass-----clase_gest-' |'-TOC-----+No-----+-'
|                                     +-Preferred+
|                                     '-Yes-----'|
>+-----+-----+----->
| .-Wait-----No-----| .-MODE-----DIFFerential-----|
|'-Wait-----+No--+-' |'-MODE-----+FULL-----+-'
|   '-Yes-'           |'-DIFFerential-'|
>+-----+-----+----->
| .-TYPE-----BACKUPImage-----|
|'-TYPE-----+BACKUPImage+-'
|   '-SNAPMirror--'|
<<
```

## Parámetros

### nombre\_nodo (Obligatorio)

Especifica el nodo para el que se realizará la copia de seguridad. No es posible utilizar caracteres comodín ni una lista de nombres.

### nombre\_sistema\_archivos

Especifica el nombre de uno o varios sistemas de archivos de los que se hará copia de seguridad. También puede especificar nombres de espacios de archivos virtuales definidos para el nodo NAS. El nombre de sistema de archivos que especifique no puede contener caracteres comodín. Puede especificar más de un sistema de archivos separando los nombres con comas y sin espacios intercalados.

Si no especifica un sistema de archivos, se hará copia de seguridad de todos los sistemas de archivos. Se realiza una copia de seguridad de todos los espacios de archivos virtuales definidos para el nodo NAS como parte de la imagen del sistema de archivos, no por separado.

Si en el dispositivo NAS existe un sistema de archivos con el mismo nombre que el espacio de archivos virtual especificado, IBM Spectrum Protect cambiará automáticamente el nombre del espacio de archivos existente en la base de datos del servidor y realizará una copia de seguridad del sistema de archivos NAS que coincide con el nombre especificado. Si el espacio de archivos virtual tiene datos de copia de seguridad, también se cambiará el nombre de la definición asociada a él.

Consejo: Consulte el parámetro del nombre del espacio de archivos virtual en el comando DEFINE VIRTUALFSMAPPING para obtener más información acerca de las consideraciones que se aplican a la asignación de nombres.

Para determinar los sistemas de archivos que deben procesarse, el servidor no utilizará sentencias DOMAIN.NAS, INCLUDE.FS.NAS o EXCLUDE.FS.NAS en ningún archivo de opciones de cliente o conjunto de opciones de cliente. Si hace copia de seguridad de varios sistemas de archivos, cada sistema de archivos se copiará como un proceso de servidor separado.

### MGmtclass

Especifica el nombre de la clase de gestión con la que se vinculan estos datos de copia de seguridad. Si no se especifica una clase de gestión, los datos de copia de seguridad se vinculan a la clase de gestión predeterminada del dominio de políticas al que está asignado el nodo. Para determinar la clase de gestión, el servidor *no* utilizará sentencias INCLUDE.FS.NAS en ningún archivo de opciones de cliente o conjunto de opciones de cliente. Puede que la clase de gestión de destino haga referencia a una agrupación nativa de IBM Spectrum Protect, en cuyo caso, los datos NDMP (Network Data Management Protocol) se enviarán a la

jerarquía nativa de IBM Spectrum Protect. Después de que ello haya tenido lugar, los datos permanecerán en la jerarquía de IBM Spectrum Protect. Los datos que fluyen a las agrupaciones nativas de IBM Spectrum Protect lo hacen por medio de la LAN, y los datos que fluyen a las agrupaciones NAS pueden conectarse directamente o bien por medio de una SAN.

Cuando especifica una clase de gestión con el mandato BACKUP NODE, todas las versiones de los datos de copia de seguridad que pertenecen al nodo NAS se vuelven a vincular a la nueva clase de gestión.

## TOC

Especifica si debe guardarse una tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Cuando determine si desea guardar una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se ha guardado una tabla de contenido, podrá utilizar el comando QUERY TOC para determinar el contenido de una copia de seguridad del sistema de archivos junto con el comando RESTORE NODE para restaurar archivos individuales o árboles de directorios. También podrá utilizar el cliente de copia de seguridad/archivado de web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y elegir los archivos y directorios que han de restaurarse. La creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Para la creación de una tabla de contenido se necesitan de forma adicional procesos, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.
- Una tabla de contenido para un sistema de archivos NAS no puede tener una ruta de directorio con más de 1024 caracteres.
- Si no se ha guardado una tabla de contenido para una copia de seguridad del sistema de archivos, todavía podrá restaurar archivos individuales o árboles de directorios utilizando el comando RESTORE NODE siempre que conozca el nombre cualificado al completo de cada archivo o directorio que ha de restaurarse y la imagen en la que se ha realizado la copia de seguridad de ese objeto.

Este parámetro es opcional. El valor predeterminado es Preferred. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para las copias de seguridad del sistema de archivos.

Preferred

Especifica que debe guardarse la información de la tabla de contenido para las copias de seguridad del sistema de archivos. Sin embargo, la ejecución de una copia de seguridad no resultará anómala sólo porque se produzca un error durante la creación de la tabla de contenido. Éste es el valor predeterminado.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada copia de seguridad del sistema de archivos. La ejecución de una copia de seguridad resultará anómala si se produce un error durante la creación de la tabla de contenido.

Atención: Si se especifica MODE=DIFFERENTIAL y se ha solicitado una tabla de contenido (TOC=PREFERRED o TOC=YES), pero la última imagen completa no tiene ninguna, se realizará una copia de seguridad completa y se creará una tabla de contenido para esa copia de seguridad completa.

## Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este comando en un proceso subordinado. Utilice el comando QUERY PROCESS para supervisar el proceso subordinado de este comando.

Yes

Especifica que el servidor procesa este comando en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza. Si hace copia de seguridad de varios sistemas de archivos, todos los procesos de copia de seguridad deben completarse antes de que finalice el comando.

Atención: No se puede especificar WAIT=YES desde la consola del servidor.

## MODE

Especifica si las copias de seguridad del sistema de archivos serán completas o diferenciales. El valor predeterminado es DIFFERENTIAL.

FULL

Especifica que debe hacerse copia de seguridad de todo el sistema de archivos.

DIFFerential

Especifica que sólo debe hacerse copia de seguridad de los archivos que se han modificado desde la copia de seguridad completa más reciente. Si opta por efectuar una copia de seguridad diferencial y no se encuentra una copia de seguridad



completa, se realizará una copia de seguridad completa. No puede especificar TYPE=SNAPMIRROR cuando el parámetro MODE está definido como DIFFERENTIAL.

## TYPE

Especifica el método de copia de seguridad utilizado para realizar la operación de copia de seguridad NDMP. El valor predeterminado para este parámetro es BACKUPIIMAGE y debe utilizarse para realizar una copia de seguridad diferencial o básica estándar de NDMP. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser específicos para un servidor de archivos determinado. Los valores posibles son:

### BACKUPIImage

Especifica que debe hacerse una copia de seguridad del sistema de archivos utilizando una operación de vuelco NDMP. Este es el método predeterminado para realizar una copia de seguridad NDMP. La operación de tipo BACKUPIIMAGE admite copias de seguridad diferenciales y completas, procesos de restauración de nivel de archivo y copias de seguridad de nivel de directorio.

### SNAPMirror

Especifica que el sistema de archivos debe copiarse en una agrupación de almacenamiento de IBM Spectrum Protect utilizando la función NetApp SnapMirror to Tape. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos. Por lo general, una copia de seguridad SnapMirror se realiza en bastante menos tiempo que una copia de seguridad NDMP convencional y completa del sistema de archivos. Sin embargo, existen limitaciones y restricciones sobre el uso de las imágenes SnapMirror. La función SnapMirror to Tape está indicada para utilizarse como una opción de recuperación ante siniestro para copiar sistemas de archivos NetApp muy voluminosos en un almacenamiento secundario.

En la mayoría de los sistemas de archivos NetApp, utilice el método de copia de seguridad diferencial o completa NDMP estándar. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más información.

Cuando defina el parámetro TYPE como SNAPMirror, se aplican las siguientes restricciones:

Restricciones:

- No puede especificar TOC=YES o TOC=PREFERRED.
- El nombre\_sistema\_archivos no puede ser un nombre de espacio de archivos virtual.
- La instantánea que se crea automáticamente mediante el servidor de archivos durante la operación de copia de SnapMirror se suprimirá al final de la operación.
- Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM® N-Series.

## Ejemplo: realizar una copia de seguridad completa

Realizar una copia de seguridad completa en el sistema de archivos /vol/vol10 del nodo NAS denominado NAS1.

```
backup node nas1 /vol/vol10 mode=full
```

## Ejemplo: realizar una copia de seguridad de un directorio y crear una tabla de contenido

Realizar una copia de seguridad del directorio /vol/vol2/mikes en el nodo NAS1 y crear una tabla de contenido para la imagen. Para los dos ejemplos siguientes, se da por supuesto que la información de Tabla 1 contiene las definiciones de espacio de archivos virtual que existen en el servidor para el nodo NAS1.

```
backup node nas1 /mikesdir
```

Tabla 1. Definiciones de espacio de archivos virtual

Nombre de espacio de archivos virtual	Sistema de archivos	Ruta
/mikesdir	/vol/vol2	/mikes
/DataDirVol2	/vol/vol2	/project1/data
/TestDirVol1	/vol/vol1	/project1/test

## Ejemplo: realizar una copia de seguridad de dos directorios

Realizar la copia de seguridad de los directorios /vol/vol2/project1/data y /vol/vol1/project1/test del nodo NAS1. Consulte la información de Tabla 1 para obtener las definiciones de espacio de archivos virtual que existen en el servidor para el nodo NAS1.

```
realizar una copia de seguridad del nodo nas1 /DataDirVol2,  
/testdirvol1 mode=full toc=yes
```

Tabla 2. Comandos relacionados con BACKUP NODE

Comando	Descripción
BACKUP NAS (mandato de cliente)	Crea una copia de seguridad de datos de un nodo NAS.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
QUERY TOC	Visualiza detalles sobre la tabla de contenido para una imagen de copia de seguridad especificada.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
RESTORE NAS (mandato de cliente)	Restaura una copia de seguridad de datos de un nodo NAS.
RESTORE NODE	Restaura un nodo de almacenamiento conectado a red (NAS).
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

**Conceptos relacionados:**

Copia de seguridad y restauración utilizando la característica NetApp SnapMirror to Tape

## BACKUP STGPOOL (Realizar copia de seguridad de los datos de la agrupación de almacenamiento primaria en la agrupación de almacenamiento de copia)

Utilice este comando para hacer copia de seguridad de los archivos de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.

Puede realizar copia de seguridad de datos desde una agrupación de almacenamiento primaria que se haya definido con el formato NATIVE, NONBLOCK, o cualquiera de los formatos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento de copia para la que va a realizarse la copia de seguridad de los datos debe tener el mismo formato de datos que la agrupación de almacenamiento primaria. IBM Spectrum Protect admite el traspaso de datos de fondo para las imágenes NDMP.

Si un archivo ya existe en la agrupación de almacenamiento de copia, no se realizará la copia de seguridad del archivo a menos que la copia del archivo que se encuentra en la agrupación de almacenamiento de copia se haya marcado como dañada. Sin embargo, no se creará una nueva copia si el archivo de la agrupación de almacenamiento primaria también se ha marcado como dañado. En una agrupación de almacenamiento de acceso aleatorio, no se hace copia de seguridad de las copias en caché de los archivos migrados ni de los archivos primarios dañados.

Consejo: La emisión de este mandato para una agrupación de almacenamiento primaria configurada para la eliminación de duplicados de datos elimina los datos duplicados, si la agrupación de almacenamiento de copia también está configurada para eliminación de duplicados de datos.

Si se inicia la migración de una agrupación de almacenamiento mientras se hace copia de seguridad de la agrupación de almacenamiento, es posible que se migren algunos archivos antes de que se haya hecho copia de seguridad de los mismos. Se recomienda que realice una copia de seguridad de las agrupaciones de almacenamiento que estén en la parte superior de la jerarquía de migración antes de realizar la copia de seguridad de las agrupaciones de almacenamiento que se encuentren en la parte inferior.

Restricciones:

- No ejecute los mandatos MOVE DRMEDIA y BACKUP STGPOOL simultáneamente. Asegúrese de que los procesos de copia de seguridad de agrupación de almacenamiento se han completado antes de emitir el mandato MOVE DRMEDIA.
- No puede realizar la copia de seguridad de los datos desde o hasta agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento de copia en la que se han de generar las copias de seguridad.

## Sintaxis

```
>>-BAckup STGpool--nom_agrupación_primaria--nom_agrupación_copia-->

  .-MAXPRocess---1-----
>-+-----+----->
  '-MAXPRocess---número-'

  .-Preview ---No-----
>-+-----+----->
  '-Preview---+No-----+
           +-Yes-----+
           |           (1) |
           '-VOLumesonly-----'

  .-SHREDTONshred---No-----    .-Wait---No-----
>-+-----+-----><
  '-SHREDTONshred---+No---+    '-Wait---+No---+
           '-Yes-'           '-Yes-'
```

### Notas:

1. Sólo es válida para agrupaciones de almacenamiento que están asociadas a una clase de dispositivo de acceso secuencial.

## Parámetros

### agrupación\_primaria (Obligatorio)

Especifica la agrupación de almacenamiento primaria.

### agrupación\_copia (Obligatorio)

Especifica la agrupación de almacenamiento de copia.

### MAXPRocess

Especifica el número máximo de procesos paralelos a utilizar para realizar copias de seguridad de archivos. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al utilizar varios procesos paralelos, se puede mejorar el rendimiento de la copia de seguridad. Se espera que el tiempo necesario para completar la copia de seguridad de agrupación de almacenamiento disminuya al utilizar varios procesos. Sin embargo, cuando se ejecutan varios procesos, en algunos casos uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso de copia de seguridad distinto.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo secuencial no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la copia de seguridad.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia y, si el tipo de dispositivo no es FILE, también necesita una unidad. Si está haciendo copia de seguridad de una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje extra para los volúmenes de agrupación de almacenamiento primaria y, si el tipo de dispositivo no es FILE, una unidad extra. Por ejemplo, suponga que especifica un máximo de tres procesos para hacer copia de seguridad de una agrupación de almacenamiento primaria secuencial en una agrupación de almacenamiento de copia de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo seis puntos de montaje y seis unidades.

Para previsualizar una copia de seguridad, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

### Preview

Especifica si se desea previsualizar la copia de seguridad sin ejecutarla. La previsualización muestra el número de archivos y bytes cuya copia de seguridad se hará y una lista de los volúmenes de agrupación de almacenamiento primaria que deberá montar. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que se hace la copia de seguridad.

Yes

Especifica que se desea previsualizar la copia de seguridad sin llevarla a cabo realmente.

VOLumesonly

Especifica que se desea previsualizar la copia de seguridad sólo como una lista de los volúmenes que deben montarse. Esta opción necesita el tiempo de proceso mínimo. La opción VOLUMESONLY sólo es válida para agrupaciones de almacenamiento asociadas a una clase de dispositivo de acceso secuencial. La opción VOLUMESONLY puede utilizarse para obtener una lista de volúmenes que necesita el proceso de copia de seguridad de la agrupación de almacenamiento. Por ejemplo:

```
backup stgpool primary_pool copystg preview=volumesonly
```

La lista de volúmenes se registra en el registro de actividad del servidor con el mensaje ANR1228I. Realice una consulta del registro de actividad del servidor para obtener la lista de volúmenes necesarios. Por ejemplo:

```
query actlog msg=1228
```

#### SHREDTONOshred

Especifica si se hará una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que fuerza la destrucción. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor no permitirá que se realice una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que fuerza la destrucción. Si la agrupación de almacenamiento primaria fuerza la destrucción, la operación falla.

Yes

Especifica que el servidor sí permitirá que se realice una copia de seguridad de los datos en una agrupación de almacenamiento de copia desde una agrupación de almacenamiento primaria que implementa la destrucción. Los datos de la agrupación de almacenamiento de copia no se destruyen cuando se eliminan.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el comando. Los mensajes creados a partir del proceso en segundo plano se visualizan en el registro de actividad o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, es posible que se haya hecho copia de seguridad de algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa esta operación en primer plano. Debe esperar a que la operación finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración al terminarse la operación.

Nota: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: realizar una copia de seguridad de la agrupación de almacenamiento primaria

Hacer copia de seguridad de la agrupación de almacenamiento primaria denominada PRIMARY\_POOL en la agrupación de almacenamiento de copia denominada COPYSTG.

```
backup stgpool primary_pool copystg
```

## Comandos relacionados

Tabla 1. Comandos relacionados con BACKUP STGPOOL

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.

Comando	Descripción
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.

## BACKUP VOLHISTORY (Guardar información histórica de volúmenes secuenciales)



Utilice este comando para hacer copia de seguridad de la información histórica de volúmenes secuenciales en uno o varios archivos.


Consejo: Debe utilizar la información histórica de volúmenes al volver a cargar la base de datos y auditar los volúmenes de agrupación de almacenamiento afectados. Si no puede iniciar el servidor, puede utilizar el archivo histórico de volúmenes para consultar la información sobre esos volúmenes en la base de datos.

El archivo histórico de volúmenes contiene información sobre los tipos de volúmenes siguientes:

- Volúmenes de anotaciones de archivado
- Volúmenes de copia de seguridad de base de datos
- Volúmenes de exportación
- Volúmenes de juegos de copias de seguridad
- Volúmenes de instantánea de base de datos
- Volúmenes de archivos del plan de recuperación de la base de datos
- Volúmenes de archivos del plan de recuperación
- Volúmenes de instantánea del archivo del plan de recuperación
- Los volúmenes de agrupación de almacenamiento de acceso secuencial siguientes:
  - Volúmenes agregados a las agrupaciones de almacenamiento
  - Volúmenes reutilizados mediante operaciones de reclamación o MOVE DATA
  - Volúmenes suprimidos con el comando DELETE VOLUME o durante la reclamación de volúmenes reutilizables

Atención: Para restaurar una base de datos, el servidor debe utilizar la información del archivo de historial de volumen y el archivo de configuración de dispositivo. Debe realizar copias del archivo de historial de volumen y el archivo de configuración de dispositivo, y guardarlas. Estos archivos no pueden volverse a crear.

 **Sistemas operativos AIX**  **Sistemas operativos Linux** Debe utilizar la opción de servidor VOLUMEHISTORY para especificar uno o más archivos históricos de volúmenes. IBM Spectrum Protect actualiza los archivos históricos de volúmenes siempre que se cambia la información histórica de volúmenes secuenciales del servidor.

 **Sistemas operativos Windows** En la instalación, el archivo de opciones del servidor contiene una opción VOLUMEHISTORY que especifica un archivo histórico de volúmenes predeterminado denominado volhist.out. IBM Spectrum Protect actualiza los archivos históricos de volúmenes siempre que se cambia la información histórica de volúmenes secuenciales del servidor.

Para garantizar que las actualizaciones se llevan cabo antes de detener el servidor, siga estos pasos:

- No esperar unos minutos antes de que se detenga el servidor si se ha emitido el mandato BACKUP VOLHISTORY.
- Especificar varias opciones VOLUMEHISTORY en el archivo de opciones del servidor.
- Comprobar que se ha actualizado el archivo histórico de volúmenes.

### Clase de privilegio

Todos los administradores pueden emitir este comando, excepto si incluye el parámetro FILENAMES. Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES, el administrador debe tener privilegio de sistema. Si el parámetro FILENAMES está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de políticas, de almacenamiento o de sistema.

### Sintaxis

```
>>-Backup VOLHistory----->
```

```
>-----<
|                                     |
|          v                          |
|'-FileNames-----nombre_archivo---+'
```

## Parámetros

### FileNames

Especifica el nombre del archivo en el que se ha de almacenar una copia de seguridad de la información histórica de volúmenes. Puede separar varios nombres de archivo con comas y sin espacios intercalados. Este parámetro es opcional.

Si no especifica un nombre de archivo, IBM Spectrum Protect almacena la información en todos los archivos especificados con la opción VOLUMEHISTORY del archivo de opciones del servidor.

## Ejemplo: realizar la copia de seguridad de la información del histórico de volúmenes en un archivo

Hacer copia de seguridad de la información histórica de volúmenes en un archivo denominado VOLHIST.

```
backup volhistory filenames=volhist
```

## Comandos relacionados

Tabla 1. Comandos relacionados con BACKUP VOLHISTORY

Comando	Descripción
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

## BEGIN EVENTLOGGING (Iniciar anotación de eventos)

Utilice este mandato para empezar a anotar eventos en uno o varios receptores. Un receptor para el que se ha iniciado la anotación de eventos es un *receptor activo*.

Al iniciarse el servidor, la anotación de eventos empieza automáticamente para la consola y las anotaciones de actividades, y para todos los receptores que se inician automáticamente basándose en el archivo de opciones del servidor. Puede utilizar este comando para empezar a anotar los eventos en los receptores para los que *no* se inician automáticamente la anotación de eventos. También puede utilizar este comando después de haber desactivado la anotación de eventos en uno o varios receptores.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-BEGin EVentlogging-----<
|                                     |
|          v                          |
|'-+--CONSOLE-----+--+'
|   +--ACTLOG-----+
|   +--EVENTSERVER----+
|   +--FILE-----+
|   +--FILETEXT-----+
|   |                   |
|   |                   | (1) |
|   +--NTEVENTLOG-----+
|   |                   |
|   |                   | (2) |
|   +--SYSLOG-----+
|   +--TIVOLI-----+
```

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

## Parámetros

Especifique uno o varios receptores. Puede especificar varios receptores separándolos con comas sin espacios intercalados. Si especifica ALL, se inicia la anotación para todos los receptores configurados. El valor predeterminado es ALL.

ALL

Especifica todos los receptores que están configurados para la anotación de eventos.

CONSOLE

Especifica la consola del servidor como receptor.

ACTLOG

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor.

EVENTSERVER


Especifica el servidor de eventos como receptor.


FILE


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

## Ejemplo: iniciar las anotaciones de eventos

Empezar a anotar eventos en las anotaciones de actividades de IBM Spectrum Protect.

```
begin eventlogging actlog
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con BEGIN EVENTLOGGING

Comando	Descripción
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## Comandos CANCEL

Utilice el comando CANCEL para finalizar una tarea o un proceso antes de que se haya completado.

- CANCEL EXPIRATION (Cancelar un proceso de caducidad)

- CANCEL EXPORT (Suprimir una operación de exportación suspendida)
- CANCEL PROCESS (Cancelar un proceso de administración)
- CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)
- CANCEL REQUEST (Cancelar una o más peticiones de montaje)
- CANCEL RESTORE (Cancelar una sesión de restauración reinicializable)
- CANCEL SESSION (Cancelar una o más sesiones cliente)

## CANCEL EXPIRATION (Cancelar un proceso de caducidad)

Utilice este comando para cancelar un número de proceso que se ejecuta como resultado de una operación de caducidad de inventario.

Utilice el comando CANCEL EXPIRATION si no se conoce el número de proceso de caducidad; de lo contrario, utilice CANCEL PROCESS y especifique el número del proceso de caducidad. Ambos comandos invocan el mismo código para finalizar el proceso de caducidad.

Puede utilizar el comando CANCEL EXPIRATION para automatizar la cancelación de un proceso de caducidad. Por ejemplo, si inicia la caducidad del inventario a medianoche y, debido a la carga de trabajo de mantenimiento en el servidor, el proceso debe finalizar a las 03:00, puede planificar un comando CANCEL EXPIRATION para que se ejecute a las 03:00 sin saber el número de proceso.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-CANcel EXPIration-----><
```

### Ejemplo: cancelar un proceso de caducidad de inventario

Cancelar el proceso que ha generado una operación de caducidad de inventario.

```
cancel expiration
```

### Comandos relacionados

Tabla 1. Comando relacionado con CANCEL EXPIRATION

Comando	Descripción
QUERY PROCESS	Muestra información sobre procesos subordinados.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.

## CANCEL EXPORT (Suprimir una operación de exportación suspendida)

Utilice este comando para suprimir una operación de exportación suspendida de servidor a servidor. Después de haber emitido el comando CANCEL EXPORT, no podrá reiniciar la operación de exportación. Emita el comando CANCEL PROCESS para suprimir una operación de exportación que actualmente está en ejecución.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-CANcel EXPort .-*-----+-----><
                '---identificador_exportación---'
```

### Parámetros

identificador\_exportación



Identificador exclusivo de la operación de exportación suspendida que desea suprimir. También puede especificar caracteres comodín en el identificador. Emita el comando QUERY EXPORT para que se visualice una lista de las operaciones de exportación actualmente suspendidas.

## Ejemplo: suprimir una operación de exportación suspendida específica

Cancelar la operación de exportación suspendida de servidor a servidor denominada EXPORTALLACCTNODES.

```
cancel export exportallacctnodes
```

## Ejemplo: suprimir todas las operaciones de exportación de servidor a servidor suspendidas

Cancelar todos los procesos de exportación suspendidos de servidor a servidor.

```
cancel export *
```

## Comandos relacionados




Tabla 1. Comandos relacionados con CANCEL EXPORT

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

## CANCEL PROCESS (Cancelar un proceso de administración)

Utilice este comando para cancelar un proceso subordinado que haya iniciado un comando de administración o un proceso como, por ejemplo, la migración de una agrupación de almacenamiento.

Los comandos siguientes generan procesos subordinados:

- AUDIT CONTAINER
- AUDIT LIBRARY
- AUDIT LICENSES
- AUDIT VOLUME
- BACKUP DB
- BACKUP NODE
- BACKUP STGPOOL
- CHECKIN LIBVOLUME
- CHECKOUT LIBVOLUME
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows
- CONVERT STGPOOL
- DELETE FILESPACE
- DELETE VOLUME
- EXPIRE INVENTORY
- EXPORT ADMIN
- EXPORT NODE
- EXPORT POLICY
- EXPORT SERVER
- GENERATE BACKUPSET
- IMPORT ADMIN
- IMPORT NODE
- IMPORT POLICY
- IMPORT SERVER
- MIGRATE STGPOOL
- MOVE DATA

- MOVE DRMEDIA
- MOVE MEDIA
- PREPARE
- PROTECT STGPOOL
- RECLAIM STGPOOL
- REPLICATE NODE
- RESTORE NODE
- RESTORE STGPOOL
- RESTORE VOLUME
- VARY

Las siguientes operaciones internas del servidor generan procesos subordinados:

- Caducidad de inventario
- Migración
- Reclamación

Para cancelar un proceso, debe disponer del número de proceso, que puede obtenerse mediante la emisión del comando QUERY PROCESS.

En algunos procesos, por ejemplo la reclamación, se generan peticiones de montaje para poder finalizar el proceso. Si un proceso tiene una petición de montaje pendiente, puede que el proceso no responda a un mandato CANCEL PROCESS hasta que se haya respondido a la petición de montaje o se haya cancelado utilizando mandato REPLY o el mandato CANCEL REQUEST o bien como resultado de un tiempo de espera excedido.

Emita el mandato QUERY REQUEST para obtener una lista de las peticiones abiertas o para consultar el registro de actividad y determinar si un proceso en particular tiene pendiente una petición de montaje. Una petición de montaje indica que hace falta un volumen para el proceso actual, pero el volumen no está disponible en la biblioteca. Puede que no esté disponible el volumen si el administrador emite el mandato MOVE MEDIA o el mandato CHECKOUT LIBVOLUME o si elimina manualmente el volumen de la biblioteca.

Después de haberse emitido un comando CANCEL PROCESS para una operación de exportación, el proceso no puede reiniciarse. Para detener una operación de exportación de servidor a servidor pero permitir que se pueda reiniciar posteriormente, emita el mandato SUSPEND EXPORT.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-CANcel PRocess--número_proceso-----><
```

## Parámetros

*número\_proceso* (Obligatorio)  
Especifica el número del proceso subordinado que desea cancelar.

## Ejemplo: cancelar un proceso en segundo plano utilizando su número de proceso





Cancelar el proceso subordinado número 3.

```
cancel process 3
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CANCEL PROCESS

Comando	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL REQUEST	Cancela las peticiones pendientes de montaje de volúmenes.

Comando	Descripción
 CONVERT STGPOOL	 Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
 PROTECT STGPOOL	 Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
REPLY	Permite que una petición siga procesándose.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

## CANCEL REPLICATION (Cancelar los procesos de réplica de nodos)

Utilice este comando para cancelar todos los procesos de réplica de nodos.

Emita este comando en el servidor que actúe como origen para los datos replicados.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-CANcel REPLication-----><
```

### Parámetros

Ninguno.

### Ejemplo: cancelar los procesos de réplica de nodos

Cancele todos los procesos de réplica de nodo.

```
cancel replication
```

### Comandos relacionados

Tabla 1. Comandos relacionados con CANCEL REPLICATION

Comando	Descripción
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.

## CANCEL REQUEST (Cancelar una o más peticiones de montaje)

Utilice este comando para cancelar una o varias peticiones de montaje de medios pendientes. Para cancelar una petición de montaje, necesita saber el número de petición asignado a la misma. Este número está incluido en el mensaje de petición de montaje y también puede mostrarse con el comando QUERY REQUEST.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

## Sintaxis

```
>>-CANcel REQuest---+--número_petición+---+-----+-----><
      '-All-----'    '-PERManent-'
```

## Parámetros

número\_petición

Especifica el número de la petición de montaje que se ha de cancelar.

ALL

Especifica que se cancelan todas las peticiones de montaje pendientes.

PERManent

Especifica que desea que el servidor marque los volúmenes para los que está cancelando una petición de montaje como no disponibles. Este parámetro es opcional.

## Ejemplo: cancelar una petición de montaje

Cancelar la petición número 2.

```
cancel request 2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CANCEL REQUEST

Comando	Descripción
QUERY REQUEST	Muestra información acerca de todas las peticiones de montaje pendientes.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

## CANCEL RESTORE (Cancelar una sesión de restauración reiniciable)

Utilice este comando para cancelar una sesión de restauración reiniciable. Puede cancelar las sesiones de restauración que tengan el estado activo o reiniciable. Todas las peticiones de montaje pendientes relacionadas con esta sesión se cancelarán automáticamente.

Para que se visualicen las sesiones reiniciables, utilice el comando QUERY RESTORE.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de operador.

## Sintaxis

```
>>-CANcel--REStore---+--número_sesión+-----><
      '-All-----'
```

## Parámetros

número\_sesión

Especifica el número de la sesión de restauración reiniciable. Una sesión activa es un número positivo y una sesión reiniciable es un número negativo.

ALL

Especifica que se han de cancelar todas las sesiones de restauración reiniciables.

## Ejemplo: cancelar operaciones de restauración

Cancelar todas las operaciones de restauración.

```
cancel restore all
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CANCEL RESTORE

Comando	Descripción
QUERY RESTORE	Muestra información acerca de las sesiones de restauración reiniciables.

## CANCEL SESSION (Cancelar una o más sesiones cliente)

Utilice este mandato para cancelar sesiones existentes de nodo cliente o de administración, y para forzar la desactivación de una sesión de administración o de nodo cliente en el servidor. Todas las peticiones de montaje pendientes relacionadas con esta sesión se cancelarán automáticamente. El nodo cliente debe iniciar una nueva sesión para reanudar las actividades.

Si cancela una sesión que se encuentra en estado desocupado en espera (IdleW) la sesión de cliente volverá a conectarse automáticamente con el servidor cuando éste vuelva a iniciar el envío de datos.

Si este comando interrumpe un proceso como, por ejemplo, de copia de seguridad o archivado, el resultado de los procesos activos en el momento de la interrupción se retrotraen y no se validan en la base de datos.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de operador.

## Sintaxis

```
>>-CANcel SEssion--+-número_sesión+-----><
                    '-ALL-----'
```

## Parámetros

número\_sesión

Especifica el número de sesiones administrativas, de servidor o de nodo cliente que desea cancelar.

ALL

Especifica que se cancelan todas las sesiones de nodo cliente. No puede utilizar este parámetro para cancelar las sesiones de cliente o servidor administrativas.

## Ejemplo: cancelar una sesión de nodo cliente específica

Cancelar la sesión de nodo cliente con NODEP (sesión 3).

```
cancel session 3
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CANCEL SESSION

Comando	Descripción
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.

## CHECKIN LIBVOLUME (Dar de alta un volumen de almacenamiento en una biblioteca)




Utilice este comando para agregar un volumen de acceso secuencial o una cinta de limpieza al inventario del servidor para una biblioteca automatizada. El servidor utilizará un volumen que resida físicamente en una biblioteca automatizada hasta que dicho volumen se haya dado de alta.

Importante:

1. El proceso del comando CHECKIN LIBVOLUME no esperará a que exista una unidad disponible, aunque la unidad sólo se encuentre en estado IDLE. Si es necesario, puede hacer que una unidad de biblioteca esté disponible emitiendo el comando DISMOUNT VOLUME para desmontar el volumen. Después de que exista una unidad de biblioteca disponible, vuelva a emitir el comando CHECKIN LIBVOLUME.
2. No debe definir las unidades, dar de alta medios o etiquetar los volúmenes en una biblioteca externa. El servidor proporciona una interfaz que los sistemas de gestión de medios externos utilizan para intercambiar información con el servidor.
3. Al dar de alta cintas WORM distintas de 3592, debe emplear CHECKLABEL=YES o se dan de alta como cintas de lectura/grabación normales.

Este comando crea un proceso subordinado que puede cancelar con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis correspondiente a las bibliotecas SCSI

```
>>-CHECKIn LIBVolume--nombre_biblioteca----->
                                     .-SEARCH-----No-.
>----+--nombre_volumen--+-----+----->
      +-SEARCH-----Yes--+-----+-----+
      |                   '-| A |-'         |
      '-SEARCH-----Bulk--+-----+-----'
                                     '-| A |-'

                                     .-OWNeR-----"-----
>--STaTus-----+--PRiVate+--+-----+----->
      +-SCRatch+   '-OWNeR-----nombre_servidor-'
      '-CLEaner-'

      .-CHECKLabel-----Yes----- .-SWAP-----No-----
>+-----+-----+-----+----->
      '-CHECKLabel-----+--Yes-----+   '-SWAP-----+--No--+-'
      +-No-----+                         '-Yes-'
      '-Barcode-'

      .-WAITime-----60-----
>+-----+-----+-----+-----<
      '-WAITime-----valor-'   '-CLEanings-----número---'

A (SEARCH=Yes, SEARCH=Bulk)

|---+--VOLRange-----+--nombre_volumen1,nombre_volumen2---+-----|
|                   .-,-----+-----|
|                   V                   |
|'-VOLList-----+--nombre_volumen+-----+-----|
|                   '-FILE:--nombre_archivo-'
```

## Sintaxis correspondiente a las bibliotecas 349X

```
>>-CHECKIn LIBVolume--nombre_biblioteca----->
                                     .-SEARCH-----No-.
>----+--nombre_volumen--+-----+----->
      '-SEARCH-----Yes--+-----+-----'
```

```

      '-| A |-'
      .-OWNeR---""-----
>--STATus---+PRIVate+----->
      '-SCRatch-' '-OWNeR---nombre_servidor-'

      .-CHECKLabel---Yes-----
>+----->
      '-CHECKLabel---+Yes+-' '-DEVType---+3590+-'
      '-No--' '-3592-'

      .-SWAP---No----- .-WAITTime---60-----
>+-----<
      '-SWAP---+No+-' '-WAITTime---valor-'
      '-Yes-'

A (SEARCH=Yes)

|++VOLRange---nombre_volumen1,nombre_volumen2---|
|          .-,-----|
|          V          |
'-VOLList---+---nombre_volumen+-----|
      '-FILE:--nombre_archivo-'

```

## Sintaxis correspondiente a las bibliotecas ACSLS

```

>>CHECKIn LIBVolume--nombre_biblioteca----->
      .-SEARCH---No-.
>---+nombre_volumen---+----->
      '-SEARCH---Yes---+'
      '-| A |-'

      .-OWNeR---""-----
>--STATus---+PRIVate+----->
      '-SCRatch-' '-OWNeR---nombre_servidor-'

      .-CHECKLabel---Yes----- .-SWAP---No-----
>+----->
      '-CHECKLabel---+Yes+-' '-SWAP---+No+-'
      '-No--' '-Yes-'

      .-WAITTime---60-----
>+-----<
      '-WAITTime---valor-'

A (SEARCH=Yes)

|++VOLRange---nombre_volumen1,nombre_volumen2---|
|          .-,-----|
|          V          |
'-VOLList---+---nombre_volumen+-----|
      '-FILE:--nombre_archivo-'

```

## Parámetros

**nombre\_biblioteca** (Necesario)

Especifica el nombre de la biblioteca.

**nombre\_volumen**

Especifica el nombre de volumen del volumen de almacenamiento que se está dando de alta. Este parámetro es obligatorio si SEARCH es NO. No especifique este parámetro si SEARCH es igual a YES o BULK. Si está dando de alta un volumen en una biblioteca SCSI con varios puertos de entrada/salida, se da de alta el volumen que tenga la ranura de número más bajo.

**STATus** (obligatorio)

Especifica el estado del volumen. Los valores posibles son:

**PRIVate**

Especifica que el volumen es un volumen privado que sólo se monta si se solicita por el nombre.

**SCRatch**

Especifica que el volumen es un nuevo volumen reutilizable. Este volumen puede montarse para satisfacer las peticiones de montaje de volumen reutilizable durante las operaciones de almacenamiento de datos o de exportación.

Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

#### CLEaner

Especifica que el volumen es un cartucho limpiador y no un cartucho de datos. El parámetro CLEANINGS es necesario con los cartuchos limpiadores y debe establecerse en el número de usos del limpiador.

CHECKLABEL=YES no es válido para dar de alta un cartucho limpiador. Utilice STATUS=CLEANER para dar de alta un cartucho limpiador aparte del cartucho de datos.

#### OWNer

Especifica qué cliente de biblioteca es el propietario de un volumen privado en una biblioteca que se comparta en una SAN. El volumen para el que se especifique la propiedad debe ser privado. No se puede especificar una propiedad para un volumen reutilizable. Además, no se puede especificar un propietario cuando utiliza SEARCH=YES o SEARCH=BULK.

Cuando emite el comando CHECKIN LIBVOLUME, el servidor valida el propietario. Si no especifica este parámetro, el servidor utilizará el predeterminado y delegará la propiedad del volumen al cliente de biblioteca propietario, según lo registrado en el archivo histórico de volúmenes del gestor de biblioteca. Si el volumen no es propiedad de ningún cliente de biblioteca, el servidor delegará la propiedad al gestor de biblioteca.

#### SEARCH

Especifica si el servidor busca en la biblioteca para localizar volúmenes que no se han dado de alta antes. Este parámetro es opcional. El valor predeterminado es NO.

Los valores posibles son:

##### No

Especifica que sólo se ha de dar de alta en la biblioteca el volumen indicado.

**En bibliotecas SCSI:** el servidor emite una solicitud para que se inserte el volumen en una ranura de cartucho en la biblioteca o, si está disponible, en un puerto de entrada. La ranura del cartucho o el puerto de entrada se identifican mediante su dirección de elemento. **En bibliotecas 349X:** el volumen puede encontrarse ya en la biblioteca o puede colocarlo en la estación de E/S cuando se le solicite.

##### Yes

Especifica que el servidor busca en la biblioteca los volúmenes que deben darse de alta. Se pueden utilizar los páramtros VOLRANGE o VOLLIST para limitar la búsqueda. Al utilizar este parámetro, tenga en cuenta las siguientes restricciones:

- Si la biblioteca es compartida entre aplicaciones, el servidor podría examinar un volumen requerido por otra aplicación. Para las bibliotecas 349X, el servidor solicita al gestor de bibliotecas que determine todos los volúmenes que están asignados a la categoría SCRATCH o PRIVATE, y a la categoría INSERT.
- Para las bibliotecas SCSI, no especifique a la vez SEARCH=YES y CHECKLABEL=NO en el mismo comando.

##### Bulk

Especifica que el servidor busca en los puertos de Entrada/Salida de la biblioteca los volúmenes que se puedan dar de alta automáticamente. Esta opción sólo se aplica a las bibliotecas SCSI.

Importante:

1. No especifique CHECKLABEL=NO y SEARCH=BULK a la vez.
2. Puede utilizar el parámetro VOLRANGE o VOLLIST para limitar la búsqueda.

#### VOLRange

Especifica un rango de nombres de volúmenes, separados con comas. Puede utilizar este parámetro para limitar la búsqueda de volúmenes que deben comprobarse al especificar SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca dentro del rango especificado, el mandato finalizará sin errores.

Especifique solamente los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Los 21 se dan de alta en: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Los 3 volúmenes se dan de alta en: bar11a, bar12a, bar13a.
volrange=123400,123410	Los 11 volúmenes se dan de alta en: 123400, 123401, ...123409, 123410.

#### VOLList



Especifica una lista de volúmenes. Puede utilizar este parámetro para limitar la búsqueda de volúmenes que deben comprobarse al especificar SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca que se encuentren en la lista, el comando finaliza sin errores.

Los valores posibles son:

nombre\_volumen

Especifica uno o más nombres de valores separados por comas y sin espacios intercalados. Por ejemplo:  
VOLLIST=TAPE01,TAPE02.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el comando. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar los volúmenes TAPE01, TAPE02 y TAPE03, debe crear un archivo, TAPEVOL, que contenga las siguientes líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Puede especificar los volúmenes para el comando según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Atención: El nombre de archivo es sensible a las mayúsculas/minúsculas.

CHECKLabel

Especifica si el servidor debe leer etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo. Este parámetro es opcional. El valor predeterminado es YES.

Los valores posibles son:

Yes

Especifica que durante la operación de dar de alta se intenta leer la etiqueta de medio.

Atención:

1. Para las bibliotecas SCSI, no especifique a la vez SEARCH=YES y CHECKLABEL=NO en el mismo comando.
2. Para los medios WORM distintos de 3592, debe especificar YES.

No

Especifica que durante la operación de dar de alta no se lee la etiqueta del medio. Sin embargo, si se suprime la comprobación de etiqueta pueden producirse errores en el futuro (por ejemplo, una etiqueta equivocada o un volumen etiquetado de forma incorrecta pueden ocasionar errores). En el caso de las bibliotecas 349X y ACSLS, especifique NO para evitar tener que cargar cartuchos en una unidad para leer la etiqueta del medio. Estas bibliotecas siempre devuelven la información de etiqueta externa en cartuchos y IBM Spectrum Protect utiliza esa información.

Barcode

Especifica que el servidor lee la etiqueta de código de barras si la biblioteca tiene un lector de códigos de barras y los volúmenes tienen etiquetas externas de código de barras. Puede disminuir el tiempo del proceso de dar de alta si utiliza el código de barras. Este parámetro sólo se aplica a las bibliotecas SCSI.

Si el lector de códigos de barras no puede leer una determinada etiqueta de código de barras, el servidor monta la cinta y lee la etiqueta interna.

DEVType

Especifica el tipo de dispositivo del volumen que se está dando de alta. Este parámetro es necesario si ninguna de las unidades de esta biblioteca tiene rutas definidas.

3590

Especifica que el tipo de dispositivo del volumen que se está dando de alta es 3590.

3592

Especifica que el tipo de dispositivo del volumen que se está dando de alta es 3592.

SWAP

Especifica si el servidor intercambia volúmenes, si no hay disponible una ranura de biblioteca vacía. El volumen seleccionado (el volumen de intercambio destino) para la operación de intercambio se expulsa de la biblioteca y se sustituye por el volumen que se está dando de alta. El servidor identifica un volumen de intercambio destino comprobando si hay un volumen reutilizable disponible. Si no hay ninguno, el servidor identifica el volumen montado con menor frecuencia.

Este parámetro es opcional. El valor predeterminado es NO. Este parámetro sólo tiene aplicación si se ha especificado un nombre de volumen en el mandato. Los valores posibles son:

No

Especifica que el servidor sólo da de alta el volumen si hay disponible una ranura vacía.

Yes

Especifica que si no hay disponible una ranura vacía, el servidor intercambia cartuchos para dar de alta el volumen.

#### WAITTime

Especifica el número de minutos que el servidor esperará su respuesta o responderá a una petición. Especifique un valor dentro del rango de 0 a 9999. Si desea que el servidor le pregunte, especifique un tiempo de espera mayor que cero. El valor predeterminado es de 60 minutos. Por ejemplo, supongamos que el servidor le solicita que inserte una cinta en el puerto de entrada/salida de una biblioteca. Si ha especificado un tiempo de espera de 60 minutos, el servidor emitirá una petición y esperará 60 minutos a que responda a la petición. Imaginemos, sin embargo, que especifica 0 como tiempo de espera. Si ya ha insertado una cinta, un tiempo de espera cero dará lugar a que la operación continúe sin que se formule ninguna pregunta. Si *no* ha insertado una cinta, un tiempo de espera igual a cero hará que la operación dé error.

#### CLEanings

Especifique el valor recomendado para el cartucho limpiador individual (normalmente indicado en el cartucho). El parámetro Cleanings sólo se aplica a bibliotecas SCSI. Este parámetro es necesario si STATUS=CLEANER.

Si en la biblioteca se da de alta a varios limpiadores, sólo se utilizará uno hasta que el valor CLEANINGS de éste disminuya hasta cero. A continuación, se seleccionará otro limpiador, y podrá darse de baja y descartar el primer limpiador.

### Ejemplo: dar de alta a un volumen en una biblioteca SCSI

Dar de alta a un volumen denominado WPDV00 en la biblioteca SCSI denominada AUTO.

```
checkin libvolume auto wpdv00 status=scratch
```

### Ejemplo: utilizar un lector de códigos de barra para explorar una biblioteca en busca de un cartucho limpiador

Explorar una biblioteca SCSI denominada AUTOLIB1 y, empleando un lector de códigos de barra, buscar el cartucho limpiador CLNV. Utilice SEARCH=YES, pero limite la búsqueda mediante el parámetro VOLLIST.

```
checkin libvolume autolib1 search=yes vollist=cleanv status=cleaner  
cleanings=10 checklabel=barcode
```

### Ejemplo: explorar una biblioteca para establecer los volúmenes no utilizados de un rango específico en estado de reutilización

Explorar una biblioteca 349X denominada ABC, y limitar la búsqueda al rango de volúmenes no utilizados BAR110 a BAR130, y establecer éstos en estado de reutilización.

```
checkin libvolume abc search=yes volrange=bar110,bar130  
status=scratch
```

### Ejemplo: explorar una biblioteca para establecer un volumen específico en estado de reutilización

Utilizar el lector de códigos de barra para explorar una biblioteca SCSI denominada MYLIB para buscar VOL1 y establecer éste en estado de reutilización.

```
checkin libvolume mylib search=yes vollist=vol1 status=scratch  
checklabel=barcode
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CHECKIN LIBVOLUME

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.

Comando	Descripción
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.




## CHECKOUT LIBVOLUME (Dar de baja un volumen de almacenamiento de una biblioteca)

Utilice este mandato para suprimir del inventario del servidor un volumen de almacenamiento de acceso secuencial de una biblioteca automatizada. Este comando crea un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

Restricciones:

1. El proceso de dar de baja no espera a que una unidad esté disponible, incluso si la unidad se encuentra en estado IDLE. Si es necesario, puede hacer que la unidad de biblioteca esté disponible desmontando el volumen con el comando DISMOUNT VOLUME. Después de que exista una unidad disponible, podrá volver a emitir el comando CHECKOUT LIBVOLUME.
2. Antes de dar de baja volúmenes de una biblioteca 349X, asegúrese de que el recurso de entrada y salida de cartuchos 349x disponga de suficientes ranuras vacías para dar de baja los volúmenes. El gestor de bibliotecas 3494 no informa a una aplicación de que el recurso de entrada y salida de cartuchos está lleno. Acepta peticiones de expulsión de un cartucho y espera hasta que se vacía el recurso de entrada y salida de cartuchos antes de volver al servidor. Puede parecer que IBM Spectrum Protect esté colgado, pero no lo está. Compruebe la biblioteca y borre las peticiones de intervención.
3. Antes de dar de baja volúmenes de una biblioteca ACSLS, asegúrese de que la prioridad CAP de ACSLS es mayor que cero. Si la prioridad CAP es cero, deberá especificar un valor para el parámetro CAP en el comando CHECKOUT LIBVOLUME.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis correspondiente a las bibliotecas SCSI

```
>>-CHECKOut LIBVolume--nombre_biblioteca----->
      .-REMove-----Bulk-----.
```

```

>-----+nombre_volumen+-----+-----+----->
  '-| A |-----'      '-REMove--==++-Yes--+'
                                +-No---+
                                '-Bulk-'

.-CHECKLabel---+Yes----- . -FORCE---+No-----
>-----+-----+-----+-----><
  '-CHECKLabel---+Yes--+'  '-FORCE---+No--+'
                        '-No--'      '-Yes-'

```

A

```

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|          .,-----|
|          V          |
'-VOLList---+-----nombre_volumen+-----+'
          '-FILE:--nombre_archivo-'

```

## Sintaxis correspondiente a las bibliotecas 349X

---

```

>>-CHECKOut LIBVolume--nombre_biblioteca----->
                                .-REMove---+Bulk-----
>-----+nombre_volumen+-----+-----+-----><
  '-| A |-----'      '-REMove--==++-Yes--+'
                                +-No---+
                                '-Bulk-'

```

A

```

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|          .,-----|
|          V          |
'-VOLList---+-----nombre_volumen+-----+'
          '-FILE:--nombre_archivo-'

```

## Sintaxis correspondiente a las bibliotecas ACSLS

---

```

>>-CHECKOut LIBVolume--nombre_biblioteca----->
                                .-REMove---+Yes-----
>-----+nombre_volumen+-----+-----+----->
  '-| A |-----'      '-REMove--==++-Yes--+'
                                +-No---+
                                '-Bulk-'

>-----+-----+-----+-----><
  '-CAP---+-----x,y,z---'

```

A

```

|---+VOLRange---+-----nombre_volumen1,nombre_volumen2---+-----|
|          .,-----|
|          V          |
'-VOLList---+-----nombre_volumen+-----+'
          '-FILE:--nombre_archivo-'

```

## Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca.

nombre\_volumen

Especifica el nombre del volumen.

VOLRange

Especifica dos nombres de volúmenes separados por una coma. Este parámetro es un rango de volúmenes que deben darse de baja. Si no hay volúmenes en la biblioteca dentro del rango especificado, el comando finalizará sin errores.

Especifique solamente los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Se dan de baja los 21 volúmenes: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Se dan de baja 3 los volúmenes: bar11a, bar12a, bar13a.
volrange=123400,123410	Se dan de baja los 11 volúmenes: 123400, 123401, ...123409, 123410.

#### VOLLIST

Especifica una lista de los volúmenes que han de darse de baja. Si no hay volúmenes en la biblioteca que se encuentren en la lista, el comando finaliza sin errores.

Los valores posibles son:

nombre\_volumen

Especifica los nombres de uno o varios volúmenes que se utilizan para el comando. Ejemplo: VOLLIST=TAPE01,TAPE02.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el comando. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar los volúmenes TAPE01, TAPE02 y TAPE03, debe crear un archivo, TAPEVOL, que contenga las siguientes líneas:

```
TAPE01
TAPE02
TAPE03
```

Puede especificar los volúmenes para el comando según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Atención: El nombre de archivo es sensible a las mayúsculas/minúsculas.

#### REMOVe

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles, en función del tipo de biblioteca, son YES, BULK y NO. La respuesta del servidor a cada una de estas opciones y los valores predeterminados se describen en las siguientes secciones.

**Bibliotecas 349X:** El valor predeterminado es BULK. La tabla siguiente muestra cómo responde el servidor en las bibliotecas 349X.

Tabla 1. Cómo responde el servidor a bibliotecas 349X

REMOVE=YES	REMOVE=BULK	REMOVE=NO
El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.	El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.	El gestor de biblioteca 3494 no expulsa el volumen.  El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

**Bibliotecas SCSI:** El valor predeterminado es BULK. La tabla siguiente muestra cómo responde el servidor en las bibliotecas SCSI.

Tabla 2. Cómo responde el servidor a bibliotecas SCSI

Si una biblioteca . . .	Y REMOVE=YES, ...	Y REMOVE=BULK, ...	Y REMOVE=NO, ...
No tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un comando REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un comando REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un comando REPLY.

Si una biblioteca . . .	Y REMOVE=YES, ...	Y REMOVE=BULK, ...	Y REMOVE=NO, ...
Posee puertos de entrada/salida y un puerto de entrada/salida <i>está disponible</i>	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un comando REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un comando REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un comando REPLY.
Posee puertos de entrada/salida, pero <i>no hay puertos disponibles</i> .	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un comando REPLY.	El servidor espera que un puerto de entrada/salida se haga disponible.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un comando REPLY.

**Bibliotecas ACSLS:** El valor predeterminado es YES. Si el parámetro se establece en YES, y el CAP tiene un valor de prioridad de selección automática de 0, se debe especificar un ID de CAP. La tabla siguiente muestra cómo responde el servidor en las bibliotecas ACSLS.

Tabla 3. Cómo responde el servidor a bibliotecas ACSLS

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho a la estación de E/S que convenga y elimina la entrada de volumen del inventario de bibliotecas del servidor.	El servidor no expulsa el cartucho. El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

CHECKLabel

Especifica si el servidor lee las etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo.

Atención: Este parámetro no sirve para las bibliotecas 349X o ACSLS de IBM®.

Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que el servidor intenta leer la etiqueta del medio para verificar que se está dando de baja el volumen correcto.

No

Especifica que durante la operación de dar de baja no se lee la etiqueta del medio. De este modo se mejora el rendimiento ya que no se produce el proceso de lectura.

FORCE

Especifica si el servidor da de baja un volumen si se produce un error de entrada/salida (E/S) al leer la etiqueta.

Atención: Este parámetro no sirve para las bibliotecas 349X o ACSLS de IBM.

Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

El servidor no da de baja un volumen de almacenamiento si se produce un error de E/S al leer la etiqueta.

Yes

El servidor da de baja el volumen de almacenamiento aunque haya un error de E/S.

CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

x

El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.

y

El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.

z

El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

## Ejemplo: dar de baja un volumen y comprobar la etiqueta

Dar de baja el volumen denominado EXB004 de la biblioteca denominada FOREST. Lea la etiqueta para verificar el nombre del volumen, pero no extraiga el volumen de la biblioteca.

```
checkout libvolume forest exb004 checklabel=yes remove=no
```

## Comandos relacionados

Tabla 4. Comandos relacionados con CHECKOUT LIBVOLUME

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

## CLEAN DRIVE (Limpiar una unidad)

Utilice este comando si desea que IBM Spectrum Protect cargue inmediatamente un cartucho limpiador en una unidad al margen de la frecuencia de limpieza.

Existen consideraciones especiales si tiene previsto utilizar este comando con una biblioteca SCSI que proporciona limpieza automática mediante el hardware del dispositivo.

Restricción: No se puede ejecutar el comando CLEAN DRIVE para una unidad cuyo único origen de ruta sea un servidor de archivos NAS.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-CLEAN DRIVE--nombre_biblioteca--nombre_unidad-----<<
```

## Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca a la que se asigna la unidad.

nombre\_unidad (Obligatorio)

Especifica el nombre de la unidad.

## Ejemplo: limpiar una unidad de cintas

Ya ha definido una biblioteca denominada AUTOLIB mediante el comando DEFINE LIBRARY y ya ha dado de alta un cartucho limpiador en la biblioteca mediante el comando CHECKIN LIBVOL. Informe al servidor de que la unidad TAPEDRIVE3 de esta biblioteca debe limpiarse.

```
clean drive autolib tapedrive3
```

## Comandos relacionados

Tabla 1. Comandos relacionados con CLEAN DRIVE

Comando	Descripción
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DRIVE	Suprime una unidad de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
UPDATE DRIVE	Cambia los atributos de una unidad.

## COMMIT (controlar la validación de comandos en una macro)

Utilice este comando para controlar cuándo se valida un comando en una macro y para actualizar la base de datos cuando los comandos terminan el proceso. Si se emite en la modalidad de consola del cliente de administración, este comando no genera ningún mensaje.

Si se produce un error durante el proceso de los comandos de una macro, el servidor finaliza el proceso de la macro y retrotrae todos los cambios (desde la última ejecución de COMMIT). Una vez validado un comando, no se puede suprimir por caducidad.

Si desea controlar el proceso del comando, asegúrese de que la sesión de cliente de administración no está ejecutándose con la opción ITEMCOMMIT. La opción ITEMCOMMIT valida los comandos de un script o de una macro a medida que se procesa *cada* comando.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-COMMIT-----><
```

## Parámetros

Ninguno.

## Ejemplo: controlar la validación de los comandos de una macro

En la modalidad interactiva del cliente de administración, registrar y otorgar autorización a los nuevos administradores utilizando una macro denominada REG.ADM. Los cambios se validarán después de que cada administrador se haya registrado y posea autorización.

Contenido de la macro:

```
/* REG.ADM-register admin políticas & otorgar autorización*/  
REGister Admin sara hobby  
GRant AUTHority sara CLasses=Policy  
COMMIT /* Validar cambios */  
REGister Admin ken plane  
GRant AUTHority ken CLasses=Policy  
COMMIT /* Validar cambios */
```






## Comandos relacionados

Tabla 1. Comandos relacionados con COMMIT

Comando	Descripción
MACRO	Ejecuta un archivo de macro especificado.
ROLLBACK	Descarga cualquier cambio no confirmado en la base de datos desde que se ejecutó el último COMMIT.

### Conceptos relacionados:

Macros de cliente administrativo

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## CONVERT STGPOOL (Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores)

Utilice este mandato para convertir una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Puede utilizar agrupaciones de almacenamiento de contenedores para la deduplicación de datos del lado de cliente y en línea.

Restricciones: Se aplican las siguientes restricciones a la conversión de la agrupación de almacenamiento:

- Sólo puede convertir una agrupación de almacenamiento una vez.
- No puede actualizar la agrupación de almacenamiento durante el proceso de la conversión. Los procesos de migración y movimiento de datos no están disponibles.
- Debe actualizar todas las políticas para garantizar que el destino especifique una agrupación de almacenamiento que no esté convertida ni en proceso de conversión.

Durante el proceso de la conversión, todos los datos de la agrupación de almacenamiento de origen se trasladan a la agrupación de almacenamiento de destino. Cuando finaliza el proceso, la agrupación de almacenamiento de origen deja de estar disponible. Cuando una agrupación de almacenamiento no está disponible, no puede grabar ningún dato en ella. La agrupación de almacenamiento de origen se puede elegir para supresión pero no se suprime automáticamente. Puede restaurar los datos a partir de la agrupación de almacenamiento de origen, si fuera necesario.

Atención: Durante la conversión de la agrupación de almacenamiento, los datos se suprimen de las agrupaciones de almacenamiento de copia y las agrupaciones de almacenamiento de datos activos. Esta acción se realiza incluso aunque haya especificado el número de días que deben transcurrir después de suprimir todos los archivos de un volumen, antes de que se pueda volver a grabar el volumen o devolver a la agrupación reutilizable.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

## Sintaxis

```
>>-CONvert STGpool--source_stgpool--target_stgpool----->  
  .-MAXPProcess---8-----  
>>+-----+-----+-----+-----+-----<<  
  '-MAXPProcess-----número--' '-Duration---minutos-'
```

## Parámetros

agrupación\_almacenamiento\_origen (Obligatorio)

Especifique una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) para el proceso de archivado y copia de seguridad. Este parámetro es obligatorio.

agrup\_alm\_destino (Necesario)

Especifique el nombre de la agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube en la que se va a convertir la agrupación de almacenamiento. Este parámetro es obligatorio la primera vez que emite este mandato.

Consejo: Si reinicia la conversión de la agrupación de almacenamiento y la agrupación de almacenamiento de destino es diferente del valor que ha especificado la primera vez que ha emitido el mandato CONVERT STGPOOL, el mandato fallará.

#### MAXProcess

Especifica el número máximo de procesos paralelos que se pueden utilizar para convertir datos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un número dentro del rango de 1 a 99. El valor predeterminado es 8.

Consejo: Los cambios en el valor predeterminado se guardan automáticamente. Si reinicia la conversión de la agrupación de almacenamiento y el valor de parámetro es diferente al valor especificado la primera vez que se emitió el mandato CONVERT STGPOOL, se utilizará el valor especificado más recientemente.

#### DURation

Especifica el número máximo de minutos que debería tardar una conversión antes de que se cancele. Cuando el número de minutos especificado transcurren, el servidor cancela todos los procesos de conversión para la agrupación de almacenamiento. Puede especificar un número dentro del rango de 1 a 9999. Este parámetro es opcional. Si no especifica este parámetro, la conversión se ejecuta hasta que se completa.

Consejo: La conversión de agrupación de almacenamiento para agrupaciones de almacenamiento grandes puede durar días. Utilice este parámetro para limitar la cantidad de tiempo de la conversión de agrupación de almacenamiento diaria. Como práctica recomendada, planifique la conversión durante al menos 2 horas para la agrupación de almacenamiento que utilice una clase de dispositivo FILE y al menos 4 horas para VTL.

## Ejemplo: Convertir una agrupación de almacenamiento y especificar un número máximo de procesos

Convierta una agrupación de almacenamiento denominada DEDUPPOOL1, mueva los datos a una agrupación de almacenamiento de contenedores denominada DIRPOOL1 y especifique un máximo de 25 procesos.

```
convert stgpool deduppool1 dirpool1 maxprocess=25
```

Tabla 1. Mandatos relacionados con CONVERT STGPOOL

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.
QUERY CONVERSION	Consultar estado de conversión de una agrupación de almacenamiento.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.

## Comandos COPY

Utilice los comandos COPY para crear una copia de los objetos o datos de IBM Spectrum Protect.

- COPY ACTIVE DATA (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)
- COPY CLOPTSET (Copiar un conjunto de opciones de cliente)
- COPY DOMAIN (Copiar un dominio de políticas)
- COPY MGMTCLASS (Copiar una clase de gestión)
- COPY POLICYSET (Copiar un juego de políticas)
- COPY PROFILE (Copiar un perfil)
- COPY SCHEDULE (Copiar una planificación de cliente o de comando de administración)
- COPY SCRIPT (copiar un script de IBM Spectrum Protect)
- COPY SERVERGROUP (Copiar un grupo de servidores)

## COPY ACTIVE DATA (Copiar datos de copia de seguridad activos desde una agrupación de almacenamiento primaria hasta una agrupación de datos activos)

Utilice este comando para copiar versiones activas de datos de copias de seguridad de una agrupación de almacenamiento primaria en una agrupación de datos activos. La principal ventaja que ofrecen las agrupaciones de datos activos son las restauraciones rápidas del cliente. Copie los datos activos regularmente para garantizar la protección de los datos ante la posibilidad de que se produzca un siniestro.

Si un archivo ya existe en la agrupación de datos activos, el archivo no se copiará a menos que la copia del archivo en la agrupación de datos activos esté marcada como dañada. Sin embargo, no se creará una nueva copia si el archivo de la agrupación de almacenamiento primaria también está marcado como dañado. En una agrupación de almacenamiento de acceso aleatorio, no se copian ni las copias en caché de los archivos migrados ni los archivos primarios dañados.

Si la migración de una agrupación de almacenamiento se inicia mientras están copiándose datos activos, puede que algunos archivos se migren antes de haberse copiado. Por este motivo, antes de copiar los datos activos de las agrupaciones de almacenamiento que ocupan una posición baja en la jerarquía de la migración, primero debe copiar los datos activos de las agrupaciones de almacenamiento que ocupan una posición más alta en la jerarquía de la migración. Antes de iniciar un proceso de copia, asegúrese de que ha completado el anterior.

Recuerde:

- Sólo puede copiar datos activos de las agrupaciones de almacenamiento que tienen un formato de datos NATIVE o NONBLOCK.
- La emisión de este comando para una agrupación de almacenamiento primaria configurada para eliminación de duplicados elimina los datos duplicados, si la agrupación de datos activos también está configurada para eliminación de duplicados.

## Clase de privilegio

Para emitir este comando, debe disponer de privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido para la agrupación de datos activos desde la que están copiándose versiones activas de datos de copia de seguridad.

## Sintaxis

```
>>-COPY ACTIVEdata--nom_agrupación_primaria--nom_agrupación_datos_act-->
. -MAXProcess-----1----- .
>-----+-----+----->
' -MAXProcess-----número--- '

. -Preview ----No----- .   . -Wait-----No----- .
>-----+-----+-----+-----+----->
' -Preview-----+No-----+ '   ' -Wait-----+No--+ '
      +-Yes-----+           ' -Yes- '
      |                (1) |
      '-VOLumesonly-----'

. -SHREDTONoshred-----No----- .
>-----+-----+-----><
' -SHREDTONoshred-----+No--+ '
      ' -Yes- '

```

Notas:

1. El parámetro VOLUMESONLY sólo se aplica a las agrupaciones de almacenamiento de acceso secuencial.

## Parámetros

nombre\_agrupación\_primaria (Obligatorio)

Especifica la agrupación de almacenamiento primaria.

nombre\_agrupación\_datos\_activos (Obligatorio)

Especifica la agrupación de datos activos.

MAXProcess

Especifica el número máximo de procesos paralelos que han de utilizarse para copiar archivos. Este parámetro es opcional. Especifique un valor entre 1 y 999. El valor predeterminado es 1.

Mediante la utilización de varios procesos paralelos puede mejorarse el rendimiento del mandato COPY ACTIVE DATA. Se espera que el tiempo necesario para copiar datos activos disminuirá al utilizar varios procesos. Sin embargo, cuando se ejecutan varios procesos, en algunos casos, puede que uno o varios de los procesos deban esperar para poder utilizar un volumen ya esté utilizando un proceso COPY ACTIVE DATA distinto.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, el servidor utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y de unidades disponibles depende de otras actividades de servidor y del sistema y también de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la copia de datos activos.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de datos activos y, si el tipo de dispositivo no es FILE, también necesita una unidad. Si está copiando datos activos de una agrupación de almacenamiento de acceso secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si el tipo de dispositivo no es FILE, una unidad adicional. Por ejemplo, suponga que especifica un máximo de 3 procesos para copiar una agrupación de almacenamiento primaria secuencial en una agrupación de datos activos de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de seis, y debe haber disponibles como mínimo seis puntos de montaje y seis unidades.

Para utilizar el parámetro PREVIEW, sólo se utiliza un único proceso, y no se necesitan puntos de montaje ni unidades.

#### Preview

Especifica si se desea previsualizar los datos activos sin copiarlos. En la previsualización se muestran el número de archivos y de bytes que han de copiarse y una lista de los volúmenes de agrupación de almacenamiento primaria que debe montar. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se copiarán los datos activos.

Yes

Especifica que se desea previsualizar el proceso pero sin copiar ningún dato.

VOLumesonly

Especifica que se desea previsualizar el proceso sólo como una lista de los volúmenes que deben montarse. Esta opción necesita el tiempo de proceso mínimo.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el comando. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, puede que algunos archivos ya se hayan copiado antes de aplicarse la cancelación.

Yes

Especifica que el servidor realiza esta operación en primer plano. Debe esperar a que la operación finalice para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración al terminarse la operación.

No se puede especificar WAIT=YES desde la consola del servidor.

#### SHREDTONOshred

Especifica si los datos deben copiarse desde una agrupación de almacenamiento primaria que aplique la destrucción a una agrupación de datos activos que no aplique la destrucción. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no permite que se copien los datos de una agrupación de almacenamiento primaria que implementa la destrucción de datos en una agrupación de datos activos que no implementa la destrucción de datos. Si la agrupación de almacenamiento primaria implementa la destrucción de datos y la agrupación de datos activos no, la operación fallará.

Yes

Especifica que el servidor permite que se copien los datos de una agrupación de almacenamiento primaria que implementa la destrucción de datos en una agrupación de datos activos que no implementa la destrucción de datos. Los datos de la agrupación de datos activos no se destruirán cuando se eliminen.

## Ejemplo: copiar datos de la agrupación de almacenamiento primaria en la agrupación de datos activos

Copiar los datos activos de una agrupación de almacenamiento primaria denominada PRIMARY\_POOL en una agrupación de datos activos denominada ACTIVEPOOL. Emita el comando:

```
copy activedata primary_pool activepool
```

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY ACTIVE DATA

Comando	Descripción
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## COPY CLOPTSET (Copiar un conjunto de opciones de cliente)

Utilice este comando para copiar un conjunto de opciones de cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

### Sintaxis

```
>>-COPY CLOptset--nom_conjunto_opcion_actual--nuevo_nom_conjunto_opc-><
```

### Parámetros

nombre\_conjunto\_opciones\_actual (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente que se ha de copiar.  
nombre\_conjunto\_opciones\_nuevo (Obligatorio)  
Especifica el nombre del nuevo conjunto de opciones del cliente. La longitud máxima del nombre es de 64 caracteres.

## Ejemplo: copiar un conjunto de opciones de cliente

Copiar un conjunto de opciones de cliente denominado ENG en un nuevo conjunto de opciones denominado ENG2.

```
copy cloptset eng eng2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY CLOPTSET

Comando	Descripción
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

## COPY DOMAIN (Copiar un dominio de políticas)

Utilice este comando para crear una copia de un dominio de políticas.

El servidor copia la información siguiente en el nuevo dominio:

- La descripción del dominio de políticas
- Los conjuntos de políticas del dominio de políticas (inclusive el conjunto de políticas ACTIVE, si se ha activado un conjunto de políticas)
- Las clases de gestión de cada juego de políticas (incluida la clase de gestión predeterminada, si se ha asignado)
- Los grupos de copia de cada clase de gestión

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-COpy D0main--nombre_dominio_actual--nombre_nuevo_dominio----><
```

## Parámetros

nombre\_dominio\_actual (Obligatorio)  
Especifica el dominio de políticas que se copia.  
nombre\_nuevo\_dominio (Obligatorio)  
Especifica el nombre del nuevo dominio de políticas. La longitud máxima de este nombre es de 30 caracteres.

## Ejemplo: copiar un dominio de políticas en un nuevo dominio de políticas

Copiar el dominio de política STANDARD a un nuevo dominio de política, ENGPOLDOM, entrando el mandato siguiente:

```
copy domain standard engpoldom
```

ENGPOLDOM ahora contiene el juego de políticas, la clase de gestión, el grupo de copia de seguridad y el grupo de copia archivada estándar.

Tabla 1. Comandos relacionados con COPY DOMAIN

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## COPY MGMTCLASS (Copiar una clase de gestión)

Utilice este comando para crear una copia de una clase de gestión en el mismo juego de políticas.

El servidor copia la información siguiente en la nueva clase de gestión:

- La descripción de la clase de gestión
- Los grupos de copia definidos en la clase de gestión
- Todos los atributos de gestión de archivos para los clientes IBM Spectrum Protect for Space Management

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la nueva clase de gestión.

### Sintaxis

```
>>-COPy MGMTclass--nombre_dominio--nombre_juego_políticas----->
>--nombre_clase_actual--nombre_nueva_clase-----<<
```

## Parámetros

- nombre\_dominio (Necesario)  
Especifica el dominio de políticas al que pertenece la clase de gestión.
- nombre\_juego\_políticas (Necesario)  
Especifica el juego de políticas al que pertenece la clase de gestión.
- nombre\_clase\_actual (Obligatorio)  
Especifica la clase de gestión que se copia.
- nombre\_clase\_nueva (Obligatorio)  
Especifica el nombre de la nueva clase de gestión. La longitud máxima de este nombre es de 30 caracteres.

## Ejemplo: copiar una clase de gestión en una nueva clase de gestión

Copiar la clase de gestión ACTIVEFILES en una nueva clase de gestión denominada FILEHISTORY. La clase de gestión está en el juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS.

```
copy mgmtclass employee_records vacation  
activefiles filehistory
```

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY MGMTCLASS

Comando	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

## COPY POLICYSET (Copiar un juego de políticas)

Utilice este mandato para copiar un juego de políticas (inclusive el juego de políticas ACTIVE) en el mismo dominio de políticas.

El servidor copia la información siguiente en el nuevo juego de políticas:

- La descripción del juego de políticas
- Las clases de gestión de cada juego de políticas (incluida la clase de gestión predeterminada, si se ha asignado)
- Los grupos de copia de cada clase de gestión

Las políticas del nuevo conjunto de políticas no entran en vigor a menos que establezca el nuevo conjunto como conjunto de políticas ACTIVE.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece el nuevo juego de políticas.

## Sintaxis

```
>>-COPY Policyset--nom_dominio--nom_juego_actual--nuevo_nom_juego-><
```

## Parámetros

- nombre\_dominio (Necesario)



Especifica el dominio de políticas al que pertenece el juego de políticas.  
 nombre\_conjunto\_actual (Obligatorio)  
 Especifica el juego de políticas que se va a copiar.  
 nombre\_conjunto\_nuevo (Obligatorio)  
 Especifica el nombre del nuevo juego de políticas. La longitud máxima de este nombre es de 30 caracteres.

## Ejemplo: copiar un juego de políticas en un nuevo juego de políticas

Copiar el juego de políticas VACATION en el nuevo juego de políticas HOLIDAY en el dominio de políticas EMPLOYEE\_RECORDS.  
`copy policyset employee_records vacation holiday`

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## COPY PROFILE (Copiar un perfil)

Utilice este comando en un gestor de configuración para copiar un perfil y todos los nombres de objetos asociados en un nuevo perfil.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-COpy PROFIle--nombre_perfil_actual--nombre_perfil_nuevo-----><
```

### Parámetros

nombre\_perfil\_actual (Obligatorio)  
 Especifica el perfil que se copia.  
 nombre\_perfil\_nuevo (Obligatorio)  
 Especifica el nombre del nuevo perfil. La longitud máxima del nombre de perfil es de 30 caracteres.

## Ejemplo: realizar una copia de un perfil

Copiar un perfil denominado VAL en otro perfil denominado VAL2.

```
copy profile val val2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY PROFILE

Comando	Descripción
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.

Comando	Descripción
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## COPY SCHEDULE (Copiar una planificación de cliente o de comando de administración)

Utilice este comando para crear una copia de una planificación.

El comando COPY SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones del cliente o a los comandos de administración. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con COPY SCHEDULE

Comando	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY SCHEDULE	Muestra información sobre planificaciones.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)  
Utilice el comando COPY SCHEDULE para crear una copia de una planificación para las operaciones de cliente. Puede copiar una planificación en un dominio de políticas o de un dominio de políticas a otro dominio de políticas. Utilice el comando DEFINE ASSOCIATION para asociar la nueva planificación a los nodos cliente.
- COPY SCHEDULE (Crear una copia de una planificación para las operaciones de administración)  
Utilice el comando COPY SCHEDULE para crear una copia de una planificación de comandos de administración.

## COPY SCHEDULE (Crear una copia de una planificación para las operaciones de cliente)

Utilice el comando COPY SCHEDULE para crear una copia de una planificación para las operaciones de cliente. Puede copiar una planificación en un dominio de políticas o de un dominio de políticas a otro dominio de políticas. Utilice el comando DEFINE ASSOCIATION para asociar la nueva planificación a los nodos cliente.



```
>--Type-----Administrative--+-----+-----><
      '-REPlace-----+No---+'
      '-Yes-'
```

## Parámetros

nombre\_planificación\_actual (Obligatorio)

Especifica el nombre de la planificación que desea copiar.

nombre\_planificación\_nueva (Obligatorio)

Especifica el nombre de la nueva planificación. Puede especificar hasta 30 caracteres para el nombre.

Si el nombre de la planificación ya está definido, debe especificar REPLACE=YES o el comando no se ejecutará.

Type=Administrative

Especifica que se copiará una planificación de comando de administración.

REPlace

Especifica si se sustituye una planificación de comando de administración. El valor predeterminado es NO. Los valores son:

No

Especifica que no se sustituye una planificación de comando de administración.

Yes

Especifica que se sustituye una planificación de comando de administración.

## Ejemplo: copiar una planificación de comandos de administración en otra planificación

Copiar la planificación de comando de administración, DATA\_BACKUP, y denominar la planificación DATA\_ENG. Si ya existe una planificación con este nombre, se sustituirá.

```
copy schedule data_backup data_eng
type=administrative replace=yes
```

## COPY SCRIPT (copiar un script de IBM Spectrum Protect)

Utilice este comando para copiar un script de IBM Spectrum Protect existente en un nuevo script con un nombre distinto.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de operador, políticas, almacenamiento o sistema.

## Sintaxis

```
>>-COPy SCRIPT--nombre_script_actual--nombre_nuevo_script-----><
```

## Parámetros

nombre\_script\_actual (Obligatorio)

Especifica el nombre del script que desea copiar.

nombre\_script\_nuevo (Obligatorio)

Especifica el nombre del nuevo script. Puede especificar hasta 30 caracteres para el nombre.

## Ejemplo: realizar una copia de un script

Copiar el script TESTDEV en un nuevo script y denominarlo ENGDEV.

```
copy script testdev engdev
```

## Comandos relacionados

Tabla 1. Comandos relacionados con COPY SCRIPT

Comando	Descripción
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.

Comando	Descripción
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

## COPY SERVERGROUP (Copiar un grupo de servidores)

Utilice este mandato para crear una copia de un grupo de servidores.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-COPY SERVERGroup--nombre_grupo_actual--nombre_nuevo_grupo---<<
```

### Parámetros

nombre\_grupo\_actual (Obligatorio)

Especifica el grupo de servidores que se copia.

nombre\_grupo\_nuevo (Obligatorio)

Especifica el nombre del nuevo grupo de servidores. La longitud máxima de este nombre es de 64 caracteres.

### Ejemplo: realizar una copia de un grupo de servidores

Copiar el grupo de servidores GRP\_PAYROLL en el nuevo grupo HQ\_PAYROLL.

```
copy servergroup grp_payroll hq_payroll
```

### Comandos relacionados

Tabla 1. Comandos relacionados con COPY SERVERGROUP

Comando	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVER	Suprime la definición de un servidor.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVER	Actualiza la información sobre un servidor.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## DEACTIVATE DATA (Desactivar datos para un nodo de cliente)

Utilice este comando para especificar que los datos activos que se han copiado para un nodo de cliente de aplicaciones antes de una fecha especificada ya no son necesarios. El comando marca los datos como inactivos para que puedan suprimirse de acuerdo con las políticas de retención de datos.

Restricción: El mandato DEACTIVATE DATA sólo es aplicable a los clientes de aplicaciones que protegen bases de datos de Oracle.

Cuando emite el comando DEACTIVATE DATA, todos los datos de copia de seguridad activos que se almacenaron antes de la fecha especificada quedan inactivos. Los datos ya no podrán recuperarse y se suprimen cuando caducan.

El comando DEACTIVATE DATA afecta únicamente a los archivos que se han copiado en el servidor antes de la fecha y la hora especificadas. Los archivos que se han copiado después de la fecha especificada continúan estando accesibles y el cliente todavía puede acceder al servidor.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

```
>>-DEACTivate DAta--nombre_nodo--TODate-----fecha----->
      .-TOTime-----23:59:59-.  .-Wait-----No-----.
>--+-----+-----+-----+-----<
      '-TOTime-----hora-----'  '-Wait-----No---+'
                                     '-Yes-'
```

## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre de un nodo de cliente de aplicaciones cuyos datos se van a desactivar.

TODate (Obligatorio)

Especifica la fecha a utilizar para seleccionar los archivos de copia de seguridad que se van a desactivar. IBM Spectrum Protect desactiva únicamente los archivos cuya fecha sea la misma o anterior a la fecha que especifique. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	23/01/2014
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-30 o -30. Para desactivar los archivos con 30 días de antigüedad o más, puede especificar TODAY-30 o -30.
EOLM	Fin del último mes. El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Desactivar los archivos que estaban activos un día antes del último día del mes anterior.
BOTM	Principio de este mes. El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Desactivar los archivos que estaban activos el día 10 del mes actual.

TOTime

Especifica que desea desactivar los archivos que se han creado en el servidor antes de esta hora en la fecha especificada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Especifique la hora utilizando uno de los siguientes valores:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:30:22
NOW	La hora actual en la fecha especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada	NOW+03:00 o +03:00.  Si emite el comando DEACTIVATE DATA a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect desactiva los archivos que se colocaron en el servidor a las 12:00 o antes en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada	NOW-03:30 o -03:30.  Si emite el comando DEACTIVATE DATA a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect desactiva los archivos que se colocaron en el servidor a las 5:30 o antes en la fecha especificada.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Especifique los siguiente valores:

#### No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

#### Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: desactivar los datos para un nodo de cliente de protección de datos

El nodo de cliente BANDIT es un cliente de aplicaciones de IBM Spectrum Protect para bases de datos: Data Protection for Oracle. Todos los datos de copia de seguridad están activos, por lo que todos los datos de copia de seguridad se retienen. El siguiente comando desactiva los datos que se copiaron antes del 3 de enero de 2014, por lo que pueden suprimirse cuando caduquen.

```
deactivate data bandit todate=01/23/2014
```

Para desactivar los datos periódicamente para que puedan suprimirse cuando caduquen, ejecute el siguiente comando desde una planificación de cliente.

```
deactivate data bandit todate=today
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEACTIVATE DATA

Comando	Descripción
DECOMMISSION NODE	Pone fuera de servicio una aplicación o un sistema.
DECOMMISSION VM	Pone fuera de servicio una máquina virtual.

## Comandos DECOMMISSION

Utilice los comandos DECOMMISSION para eliminar nodos cliente del entorno de producción. Los nodos de cliente pueden ser aplicaciones, sistemas y máquinas virtuales.

- DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)
- DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

## DECOMMISSION NODE (Poner fuera de servicio un sistema o una aplicación)

Utilice este comando para eliminar del entorno de producción un nodo de cliente de una aplicación o un sistema. Cualquier copia de seguridad de los datos almacenados para el nodo de cliente caducará según la configuración de políticas a menos que suprima explícitamente los datos.

Atención: Esta acción no se puede invertir y provoca la supresión de los datos. Aunque este comando no suprime la definición de nodo de cliente hasta que caduquen sus datos, no puede volver a poner en servicio el nodo cliente. Después de emitir este comando, el nodo de cliente no puede acceder al servidor y no se realiza ninguna copia de seguridad de sus datos. El nodo de cliente está bloqueado y sólo puede desbloquearse para restaurar archivos. Los espacios de archivos que pertenecen al nodo de cliente, y el propio nodo de cliente, se terminan por eliminar.

Utilizando este comando, puede poner fuera de servicio los siguientes tipos de nodos de cliente:

### Nodos de cliente de aplicaciones

Los nodos de cliente de aplicaciones incluyen los servidores de correo electrónico, las bases de datos y otras aplicaciones. Por ejemplo, cualquiera de las siguientes aplicaciones puede ser un nodo de cliente de aplicaciones:

- IBM Spectrum Protect Snapshot
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect for Virtual Environments

### Nodos de cliente del sistema

Los nodos de cliente del sistema incluyen las estaciones de trabajo, los servidores de archivos NAS (almacenamiento conectado a la red) y los clientes API.

Cuando un nodo de cliente ya no es necesario en el entorno de producción, puede emitir este comando para iniciar una operación controlada y gradual para ponerlo fuera de servicio. El comando realiza las siguientes acciones:

- Suprime todas las asociaciones de planificación del nodo de cliente. Las planificaciones ya no se ejecutan en el nodo de cliente. Esta acción es equivalente a emitir el comando DELETE ASSOCIATION para cada planificación con la que esté asociado el nodo de cliente.
- Impide que el cliente acceda al servidor. Esta acción es equivalente a emitir el comando LOCK NODE.

Cuando finaliza el comando, ya no se realiza ninguna copia de seguridad de los datos del nodo de cliente en el servidor. Los datos que se han copiado antes de poner fuera de servicio el nodo de cliente no se suprimen inmediatamente del servidor. No obstante, todas las versiones de archivos de copia de seguridad, incluida la copia de seguridad más reciente, ahora son copias inactivas. Los archivos del cliente se conservan en el servidor de acuerdo con las políticas de gestión de almacenamiento.

Una vez que han caducado todos los periodos de retención de datos y se han eliminado del almacenamiento del servidor todas las copias de archivos de archivado y copia de seguridad del cliente, IBM Spectrum Protect suprime los espacios de archivos que pertenecen al nodo fuera de servicio. Esta acción es equivalente a emitir el comando DELETE FILESPACE.

Una vez suprimidos los espacios de archivos del nodo fuera de servicio, la definición de nodo se suprime del servidor. Esta acción es equivalente a emitir el comando REMOVE NODE.

Después de poner fuera de servicio un nodo cliente, pero antes de eliminarlo del servidor, puede utilizar el comando QUERY NODE para comprobar que el nodo de cliente está fuera de servicio.

Restricción: No puede poner fuera de servicio un nodo de cliente que esté configurado para la réplica. Puede determinar el estado de réplica de un nodo de cliente utilizando el comando QUERY NODE. Si un nodo de cliente está configurado para la réplica, puede eliminar el nodo de cliente de la réplica utilizando el comando REMOVE REPLNODE.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio del sistema.

## Sintaxis

```
>>-DECommission Node--nombre_nodo--+-Wait-----No-----+-----><
                                     '-Wait-----+No--+-'
                                     '-Yes-'
```



## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo de cliente que se va a poner fuera de servicio.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: poner fuera de servicio un nodo de cliente

Ponga fuera de servicio el nodo de cliente CODY.

```
decommission node cody
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DECOMMISSION NODE

Comando	Descripción
DECOMMISSION VM	Pone fuera de servicio una máquina virtual.
DEACTIVATE DATA	Desactiva los datos de un nodo de cliente.

## DECOMMISSION VM (Poner fuera de servicio una máquina virtual)

Utilice este comando para eliminar una máquina virtual individual en un nodo de centro de datos. El espacio de archivos que representa la máquina virtual sólo se suprime del servidor después de que caduquen sus datos de copia de seguridad.

Atención: Este comando no puede invertirse y provoca la supresión de los datos. Aunque este comando no suprime el espacio de archivos de máquina virtual hasta que caduquen sus datos, no puede volver a poner en servicio la máquina virtual.

Cuando una máquina virtual ya no es necesaria en el entorno de producción, puede emitir este comando para iniciar una eliminación por fases del espacio de archivos de máquina virtual del servidor. El comando DECOMMISSION VM marca todos los datos que se han copiado para la máquina virtual como inactivos, para que puedan suprimirse según las políticas de retención de datos. Después de que caduquen todos los datos que se han copiado para la máquina virtual, se suprime el espacio de archivos que representa la máquina virtual. El comando DECOMMISSION VM sólo afecta a la máquina virtual que identifique. El nodo de centro de datos y las otras máquinas virtuales que están alojadas en el nodo de centro de datos no se verán afectados.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

```
>>-DECommission VM--nombre_nodo--nombre_vm----->
                                     .-Wait----No-----
>--+-----+-----+-----+-----<<
  '-NAMEType-----FSID---'  '-Wait-----+--Yes-+-'
                               '-No--'
```

## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo de centro de datos que aloja la máquina virtual que se va a poner fuera de servicio.

nombre\_vm (Obligatorio)

Identifica el espacio de archivos que representa la máquina virtual que se va a poner fuera de servicio. Cada máquina virtual que está alojada en un nodo de centro de datos se representa como un espacio de archivos.

Si el nombre incluye uno o más espacios, debe escribir el nombre entre comillas dobles cuando se emita el mandato.

De forma predeterminado, el servidor interpreta el nombre del espacio de archivos que especifica utilizando la página de códigos del servidor y también intenta convertir el nombre de espacio de archivo de la página de códigos del servidor a la página de códigos UTF-8. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

Si el nombre de la máquina virtual es un nombre distinto al inglés, este parámetro debe especificar el ID del espacio de archivos (FSID). Si especifica el parámetro NAMETYPE, puede indicar al servidor que interprete el nombre de espacio de archivos por su ID de espacio de archivos (FSID) en su lugar.

NAMETYPE

Especifique cómo desea que el servidor interprete el nombre de espacio de archivos especificado para identificar la máquina virtual. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede especificar el siguiente valor:

FSID

El servidor interpreta el nombre de espacio de archivos por su identificador de espacio de archivos (FSID).

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Sí

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplos: Dejar fuera de servicio una máquina virtual

Ponga fuera de servicio la máquina virtual CODY.

```
decommission vm dept06node cody
```

Dejar fuera de servicio la máquina virtual

```
decommission vm dept06node "cody 2"
```

Ponga fuera de servicio una máquina virtual especificando su ID de espacio de archivos.

```
decommission vm dept06node 7 nametype=fsid
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DECOMMISSION VM

Comando	Descripción
DECOMMISSION NODE	Pone fuera de servicio una aplicación o un sistema.
DEACTIVATE DATA	Desactiva los datos de un nodo de cliente.

## Comandos DEFINE

Utilice los comandos DEFINE para crear objetos de IBM Spectrum Protect.

- DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)
- DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)

- DEFINE BACKUPSET (Definir un juego de copias de seguridad)
- DEFINE CLIENTACTION (Definir una acción de cliente única)
- DEFINE CLIENTOPT (Definir una opción en un conjunto de opciones)
- DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)
- DEFINE COLLOGROUP (Definir un grupo de proximidad)
- DEFINE COLLOCMEMBER (Definir un miembro de grupo de proximidad)
- DEFINE COPYGROUP (Definir un grupo de copia)
- DEFINE DATAMOVER (Definir un transportador de datos)
- DEFINE DEVCLASS (Definir una clase de dispositivo)
- DEFINE DOMAIN (Definir un nuevo dominio de políticas)
- DEFINE DRIVE (Definir una unidad en una biblioteca)
- DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)
- DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)
- DEFINE LIBRARY (Definir una biblioteca)
- DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)
- DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)
- DEFINE MGMTCLASS (Definir una clase de gestión)
- DEFINE NODEGROUP (Definir un grupo de nodos)
- DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)
- DEFINE PATH (Definir una ruta)
- DEFINE POLICYSET (Definir un juego de políticas)
- DEFINE PROFASSOCIATION (Definir una asociación de perfil)
- DEFINE PROFILE (Definir un perfil)
- DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)
- DEFINE RECOVERYMEDIA (Definir medio de recuperación)
- DEFINE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)
- DEFINE SCRIPT (definir un script de IBM Spectrum Protect)
- DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)
- DEFINE SERVERGROUP (Definir un grupo de nodo)
- DEFINE SPACETRIGGER (Definir desencadenante de espacio)
- DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)
- DEFINE STGPOOL (Definir una agrupación de almacenamiento)
- DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)
- DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)
- DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)
- DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)

## DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)

Utilice este mandato para desencadenar una alerta siempre que un servidor emita un determinado mensaje de error. Puede definir un número de mensaje para que sea un desencadenante de alerta, asignarlo a una categoría o especificar administradores a los que se pueda notificar de la alerta por correo electrónico.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

      .-n-----
      v           |
>>-Define ALERTTrigger----+--número_mensaje+----->

      .-CAteGory----Server-----
>--+-----+----->
      '-CAteGory----+Application+-'
          +-INventory---+
          +-CLient-----+
          +-DEvice-----+
          +-SErver-----+
          +-STorage-----+
          +-SYstem-----+
          '-VMclient----'

>--+-----+-----<

```

```

|           .-,------ . |
|           v             | |
|'-Admin--==-----nombre_admin-+-'|

```

## Parámetros

### número\_mensaje (Obligatorio)

Especifica el número de mensaje que desea asociar con el desencadenante de la alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres.

### CATegory

Especifica el tipo de categoría de la alerta, que está determinado por los tipos de mensajes. El valor predeterminado es SERVER. Nota: Si se cambia la categoría de un desencadenante de alerta, no se cambia la categoría de las alertas existentes en el servidor. Las nuevas alertas se clasifican dentro de la nueva categoría. Especifique uno de los siguientes valores:

#### APplication

La alerta se clasifica como una categoría de aplicación. Por ejemplo, puede especificar esta categoría para los mensajes asociados con los clientes de aplicación (TDP).

#### INventory

La alerta se clasifica como categoría de inventario. Por ejemplo, puede especificar esta categoría para mensajes que están asociados con la base de datos, el archivo de registro activo o el archivo de registro de archivado.

#### CLient

La alerta se clasifica como una categoría de cliente. Por ejemplo, puede especificar esta categoría para los mensajes asociados con actividades de cliente generales.

#### DEvice

La alerta se clasifica como una categoría de dispositivo. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados a las clases de dispositivos, bibliotecas, unidades o vías de acceso.

#### SErver

La alerta se clasifica como una categoría de servidor general. Por ejemplo, puede especificar esta categoría para los mensajes asociados a las actividades del servidor generales o a sucesos.

#### STorage

La alerta se clasifica como una categoría de almacenamiento. Por ejemplo, puede especificar esta categoría para los mensajes asociados con las agrupaciones de almacenamiento.

#### SYstems

La alerta se clasifica como una categoría de clientes del sistema. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con los clientes de archivado y copia de seguridad del sistema o archivado y copia de seguridad de gestión de almacenamiento jerárquico (HSM).

#### VMclient

La alerta se clasifica bajo la categoría VMclient. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con clientes de máquina virtual.

### ADmin

Este parámetro opcional especifica el nombre del administrador que recibe el correo electrónico de notificación de esta alerta. El desencadenante de alerta se ha definido satisfactoriamente aunque no se ha especificado ningún nombre de administrador.

## Asignar dos números de mensaje a una alerta

Emita el siguiente mandato para especificar que desea que dos números de mensaje desencadenen una alerta:

```
define alertrigger ANR1067E,ANR1073E
```

## Asignar un número de mensaje a una alerta y enviarlo por correo electrónico a dos administradores

Emita el mandato siguiente para especificar los números de mensaje que desea que desencadenen una alerta y hacer que se envíen por correo electrónico a dos administradores:

```
define alertrigger ANR1067E,ANR1073E Admin=BILL,DJADMIN
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DEFINE ALERTTRIGGER

Comando	Descripción
---------	-------------

Comando	Descripción
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

## DEFINE ASSOCIATION (Asociar nodos de cliente a una planificación)

Utilice este mandato para asociar uno o varios clientes a una planificación. Debe asignar un nodo de cliente al dominio de políticas al que pertenezca la planificación. Los nodos cliente procesan las operaciones según las planificaciones asociadas a los nodos.

Nota:

1. IBM Spectrum Protect no puede ejecutar varias planificaciones al mismo tiempo para el mismo nodo de cliente.
2. En una macro, es posible que el servidor se detenga si algunos comandos (por ejemplo, REGISTER NODE y DEFINE ASSOCIATION) no se han validado inmediatamente después de haberlos emitido. Puede especificar que todos los mandatos de una macro vayan seguidos de COMMIT. Sin embargo, una solución más sencilla consiste en incluir la opción ITEMCOMMIT en el mandato DSMADMC.

### Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio de políticas al que pertenece la planificación

### Sintaxis

```
>>-DEFine ASSOCIation--nombre_dominio--nombre_planificación----->
      .-,-----
      v          |
>---nombre_nodo+-----><
```

### Parámetros

nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre\_planificación (Obligatorio)

Especifica el nombre de la planificación que desea asociar con uno o más clientes.

nombre\_nodo (Obligatorio)

Especifica el nombre de un nodo de cliente o una lista de nodos cliente que se ha de asociar a la planificación especificada. Debe separar los elementos de la lista con comas. No deje espacios en blanco entre los elementos y las comas. Puede utilizar un carácter comodín para especificar un nombre. El comando no asociará un cliente de la lista con la planificación si:

- El cliente ya está asociado con la planificación especificada.
- El cliente no está asignado al dominio de políticas al que pertenece la planificación.
- El cliente es un nombre de nodo NAS. Todos los nodos NAS se pasarán por alto.

### Ejemplo: asociar nodos cliente a una planificación

Asociar los nodos cliente SMITH o JOHN a la planificación WEEKLY\_BACKUP. Los clientes asociados están asignados al dominio de políticas EMPLOYEE\_RECORDS.

```
define association employee_records
weekly_backup smith*,john*
```

## Ejemplo: asociar nodos cliente a una planificación

Asociar los nodos cliente JOE, TOM y LARRY a la planificación WINTER. Los clientes asociados están asignados al dominio de políticas EMPLOYEE\_RECORDS; sin embargo, el cliente JOE ya está asociado con la planificación WINTER.

```
define association employee_records
winter joe,tom,larry
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE ASSOCIATION

Comando	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.
DELETE ASSOCIATION	Suprime la asociación entre los clientes y una planificación.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.

## DEFINE BACKUPSET (Definir un juego de copias de seguridad)

Utilice este mandato para definir un conjunto de copias de seguridad de cliente que anteriormente se había generado en un servidor y ponerlo a disposición del servidor que está ejecutando este mandato. El nodo cliente tiene la opción de restaurar el conjunto de copias de seguridad desde el servidor que ejecuta este mandato en lugar de hacerlo en el que se generó el conjunto de copias de seguridad.

Cualquier conjunto de copias de seguridad que se haya generado en un servidor puede definirse para otro servidor cuando los servidores comparten un tipo de dispositivo común. El nivel del servidor para el que se está definiendo el conjunto de copias de seguridad debe ser igual o más alto que el nivel del servidor que ha generado el conjunto de copias de seguridad.

También puede utilizar el comando DEFINE BACKUPSET para volver a definir un juego de copias de seguridad que se había suprimido en un servidor.

## Clase de privilegio

Si la opción del servidor REQSYSAUTHOUTFILE se establece en YES (el valor predeterminado), el administrador deberá disponer de privilegio de sistema. Si la opción del servidor REQSYSAUTHOUTFILE se establece en NO, el administrador deberá disponer de privilegio de sistema o de privilegio de políticas para el dominio al que se ha asignado el nodo cliente.

## Sintaxis

```

      .-,-,-----
      v'                               |
>>-DEFine BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'
>--prefijo_nombre_juego_copias_seguridad----->
>--DEVclass-----nombre_clase_dispositivo----->
      .-,-,-----
      v'                               |
>--VOLumes-----nombres_volúmenes----->
      .-RETention-----365-----
>+-----+-----
  '-RETention-----+días-----+'
      '-NOLimit-'

```

```

>-----+-----+-----+-----+-----+----->
'-DESCRiption-----descripci3n-'
.
.WHEREDATAType-----ALL-----
>-----+-----+-----+-----+-----+----->
|
|          V          |
|-----+-----+-----+-----+-----+-----|
'-WHEREDATAType-----+FILE--+--+-'
          '-IMAGE-'
>-----+-----+-----+-----+-----+----->
'-TOC-----+PREFERRED--+-'
          +-YES-----+
          '-NO-----'
>-----+-----+-----+-----+-----+-----<
'-TOCMGmtclass-----nombre_clase-'

```

## Parámetros

**nombre\_nodo** o **nombre\_grupo\_nodos** (Necesario)

Especifica el nombre de los nodos cliente o grupos de nodos cuyos datos se incluyen en los volúmenes de juegos de copias de seguridad especificados. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Si los volúmenes de conjuntos de copias de seguridad contienen conjuntos de copias de seguridad de varios nodos, se define cada conjunto de copias de seguridad cuyo nombre de nodo coincide con uno de los nombres de nodo especificados. Si los volúmenes contienen un conjunto de copias de seguridad para un nodo que actualmente no está registrado, el mandato DEFINE BACKUPSET no define el conjunto de copias de seguridad para dicho nodo.

**prefijo\_nombre\_juego\_copias\_seguridad** (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a definir en este servidor. La longitud máxima del nombre es de 30 caracteres.

Cuando se selecciona un nombre, IBM Spectrum Protect agrega un sufijo para crear el nombre de juego de copias de seguridad. Por ejemplo, si especifica el nombre del juego de copias de seguridad *mybackupset*, IBM Spectrum Protect agrega un número exclusivo como, por ejemplo, 3099, al nombre. El nombre de juego de copias de seguridad se identifica como *mybackupset.3099*. Si más adelante desea ver información acerca de este juego de copias de seguridad, puede especificar un carácter comodín en el nombre, como por ejemplo, *mybackupset\** o puede especificar el nombre completo como *mybackupset.3099*.

Si los volúmenes de conjuntos de copias de seguridad contienen conjuntos de copias de seguridad para varios nodos, los conjuntos de copias de seguridad se definen para cada nodo utilizando el mismo prefijo y sufijo del nombre del conjunto de copias de seguridad.

**DEVclass** (Necesario)

Especifica el nombre de la clase de dispositivo de los volúmenes para los que se lee el juego de copias de seguridad.

Nota: El tipo de dispositivo que está asociado con la clase de dispositivo que especifique debe coincidir con la clase de dispositivo con la que el conjunto de copias de seguridad se generó originalmente.

**VOLumes** (Obligatorio)

Especifica los nombres de los volúmenes que se utilizan para almacenar el conjunto de copias de seguridad. Puede especificar varios volúmenes separando los nombres con comas y sin espacios intercalados. Los volúmenes que especifique deben estar disponibles en el servidor que está definiendo el conjunto de copias de seguridad.

Nota: Los volúmenes que especifique deben estar en el orden en el que se crearon o el mandato DEFINE BACKUPSET no se ejecutará correctamente.

El servidor no verifica si cada volumen especificado para un conjunto de copias de seguridad de varios volúmenes contiene parte del conjunto de copias de seguridad. El primer volumen siempre se comprueba y en algunos casos también se comprueban otros volúmenes adicionales. Si estos volúmenes son correctos, se define el conjunto de copias de seguridad y todos los volúmenes que figuran en la lista del mandato quedan protegidos frente a la sobregrabación. Si un volumen que contiene parte del conjunto de copias de seguridad no figura en la lista del mandato, el volumen no queda protegido y puede sobregrabarse potencialmente durante las operaciones normales del servidor.

Nota: El servidor intenta, de manera predeterminada, crear una tabla de contenido cuando se define un conjunto de copias de seguridad. Si se especifica un volumen incorrecto, o si los volúmenes no figuran en la lista en el orden correcto, la creación de la tabla de contenido falla. Si se produce este error, compruebe la lista de volúmenes del mandato y opte por utilizar el mandato QUERY BACKUPSETCONTENTS para verificar el contenido del conjunto de copias de seguridad.

**RETention**

Especifica el número de días que se retiene en el servidor el juego de copias de seguridad. Puede especificar un entero de 0 a 30000. El valor predeterminado es 365 días. Los valores son:

días

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor.

NOLimit

Especifica que el conjunto de copias de seguridad debe retenerse indefinidamente en el servidor.

Si especifica NOLIMIT, IBM Spectrum Protect retiene los volúmenes que contienen el conjunto de copias de seguridad sin límite de tiempo, a menos que un usuario o un administrador suprima los volúmenes del almacenamiento del servidor.

DESCRiption

Especifica la descripción que se asociará al juego de copias de seguridad que pertenece al nodo cliente. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

WHEREDATAType

Especifica que se van a definir los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben definir. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben definir. ALL es el valor predeterminado.

FILE

Especifica que se va a definir un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad.

IMAGE

Especifica que se va a definir un juego de copias de seguridad de imagen. Los conjuntos de copias de seguridad de imagen contienen imágenes que ha creado el mandato BACKUP IMAGE del cliente de archivado y copia de seguridad.

TOC

Especifica si debe crearse una tabla de contenido (TOC) para el conjunto de copias de seguridad de nivel de archivo cuando éste se defina. Cuando defina conjuntos de copias de seguridad de datos de aplicación y de imagen se ignorará el parámetro TOC porque siempre se crea una tabla de contenido para estos conjuntos de copias de seguridad.

Cuando determine si desea crear una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se crea una tabla de contenido, podrá utilizar el cliente de archivado de copia de seguridad web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y elegir los archivos y directorios que han de restaurarse. Para crear una tabla de contenido debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión que ha especificado el parámetro TOCMGMTCLASS. Para crear una tabla de contenido, se necesitan de forma adicional procesos, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación del conjunto de copias de seguridad.
- Si no se guarda una tabla de contenido para un conjunto de copias de seguridad, todavía puede restaurar archivos individuales o árboles de directorios mediante el mandato RESTORE BACKUPSET del cliente de archivado y copia de seguridad, siempre que conozca el nombre completo de cada archivo o directorio que se desea restaurar.

Este parámetro es opcional. El valor predeterminado es Preferred. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para los juegos de copias de seguridad de nivel de archivo.

Preferred

Especifica que debe guardarse la información de la tabla de contenido para conjuntos de copias de seguridad de nivel de archivo. Sin embargo, un juego de copias de seguridad no fallará sólo porque se produzca un error durante la creación de la tabla de contenido.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada juego de copias de seguridad de nivel de archivo. Un juego de copias de seguridad fallará si se produce un error durante la creación de la tabla de contenido.

TOCMGmtclass

Especifica el nombre de la clase de gestión a la que la tabla de contenido debe estar vinculada. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado el nodo. En este caso, la creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

## **Ejemplo: definir un juego de copias de seguridad**

---



Defina el conjunto de copias de seguridad PERS\_DATA que pertenece al nodo cliente JANE en el servidor que está ejecutando este mandato. Retener el juego de copias de seguridad en el servidor durante 50 días. Especifique que los volúmenes VOL001 y VOL002 contienen los datos del juego de copias de seguridad. Los volúmenes los ha de leer un dispositivo asignado a la clase de dispositivo AGADM. Incluya una descripción.

```
define backupset jane pers_data devclass=agadm
volumes=vol1,vol2 retention=50
description="sector 7 base image"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE BACKUPSET

Comando	Descripción
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## DEFINE CLIENTACTION (Definir una acción de cliente única)

Utilice este comando para planificar uno o varios clientes para que procesen un comando de una acción única.

El servidor define automáticamente una planificación y asocia el nodo cliente a la planificación. El servidor asigna la prioridad de planificación 1, establece PERUNITS en ONETIME y determina el número de días que se debe mantener activa la planificación. El número de días se basa en el valor que se ha establecido con el comando SET CLIENTACTDURATION.

La rapidez con que el cliente procesa este comando depende de si la modalidad de planificación del cliente está definida en "por petición de servidor" o "por sondeo de cliente". El planificador del cliente debe estar iniciado en la estación de trabajo cliente para que el servidor pueda procesar la planificación.

Recuerde: El inicio del planificador de IBM Spectrum Protect depende del proceso de las otras hebras del servidor y de otros procesos del sistema principal del servidor de IBM Spectrum Protect. El plazo de tiempo necesario para iniciar el planificador también depende del tráfico de la red y del tiempo que se necesita para abrir un socket, para establecer la conexión con el cliente de IBM Spectrum Protect y para recibir una respuesta del cliente. En general, cuanto más numerosos sean los requisitos de proceso y de conectividad del cliente y del servidor de IBM Spectrum Protect, más tiempo tardará en iniciarse el planificador.

## Clase de privilegio

Para emitir este comando debe tener privilegio de sistema y privilegio de política o bien sin restricciones, o bien restringido al dominio de políticas al que pertenece la planificación.

## Sintaxis

```

      .-,-,-----
      v          |
>>-DEFine CLIENTAction-----nombre_nodo+----->

```



## RETRieve

Indica que la planificación recupera los archivos especificados con el parámetro OBJECTS.

Recuerde: Un segundo archivo especificado actúa como el destino de recuperación. Si necesita recuperar varios grupos de archivos, cree una planificación distinta para cada grupo de archivos.

## IMAGEBACKup

Especifica que la planificación hace copia de seguridad de los volúmenes lógicos especificados con el parámetro OBJECTS.

## IMAGERESore

Especifica que la planificación restaura los volúmenes lógicos especificados con el parámetro OBJECTS.

## Comando

Indica que la planificación procesa un comando de un sistema operativo de cliente o un script, especificado con el parámetro OBJECTS.

## Macro

Especifica que un cliente procesa una macro cuyo nombre de archivo se especifica con el parámetro OBJECTS.

## SUBACTion

Puede especificar uno de los siguientes valores:

""

Cuando una serie vacía (dos dobles comillas) se especifica con ACTION=BACKUP, la copia de seguridad es incremental.

## FASTBBack

Especifica que una operación de cliente FastBack identificada por el parámetro ACTION se va a planificar para procesar. El parámetro ACTION debe ser ARCHIVE o BACKUP.

## SYSTEMState

Especifica que se ha programado una copia de seguridad del estado del sistema.

## VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

## VM


Especifica que se ha programado una copia de seguridad VMware del cliente.

## OPTions

Especifica las opciones que se especifican en el comando planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el comando planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de comandos. Todas las opciones que se describen como válidas solamente en la línea de comandos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el comando planificado:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el comando DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el comando planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Para especificar `domain all-local -c: -d;`, escriba:
  - `options='-domain="all-local -c: -d:"'`

## Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

## Objects

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando ACTION=INCREMENTAL. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un comando o una macro, el objeto será el nombre del comando o macro que debe ejecutarse.

Si especifica ACTION=INCREMENTAL sin especificar ningún valor para este parámetro, el comando planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

## Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de
destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número
excesivo de argumentos de línea de
comandos
```

Si especifica ACTION=ARCHIVE, INCREMENTAL o SELECTIVE para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.

Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofos. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofos. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar C:\ARCHIVO 2, D:\ARCHIVOS GIF y E:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="C:\ARCHIVO 2" "D:\ARCHIVOS GIF" "E:\ARCHIVO DE PRUEBA"
- Para especificar D:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="'D:\ARCHIVO DE PRUEBA'"
- Para especificar D:\PRUEBA,ARCHIVO:
  - OBJECTS="'D:\PRUEBA,ARCHIVO'"

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar /home/archivo 2, /home/archivos gif y /home/archivo de prueba, escriba:
  - OBJECTS="/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba"
- Para especificar /home/archivo de prueba, escriba:
  - OBJECTS="'/home/archivo de prueba'"

## Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

Wait



nombre\_conjunto\_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones.

nombre\_opción (Obligatorio)

Especifica la opción de cliente que se agrega al conjunto de opciones.

Consulte el apartado Opciones de cliente que puede establecer el servidor para obtener una lista de las opciones válidas.

Nota: Para definir valores de inclusión/exclusión, especifique la opción de inclusión o exclusión con *nombre\_opción*, y utilice *valor\_opción* para especificar las sentencias de inclusión o exclusión válidas, como lo haría en el archivo de opciones. Por ejemplo:

```
define clientopt nombre_conjunto_opciones inclexcl  
    "include c:\proj\text\devel.*"
```

valor\_opción (Obligatorio)

Especifica el valor de la opción. Si la opción contiene más de un valor, éstos deben delimitarse por comillas.

Nota:

1. Las opciones QUIET y VERBOSE no tienen un valor de opción en el archivo de opciones del cliente. Para especificar estos valores en un conjunto de opciones de cliente del servidor, especifique el valor YES o NO.
2. Para añadir una opción INCLUDE o EXCLUDE para un nombre de archivo que contiene uno o más espacios, escriba la especificación de archivo entre comillas simples y la opción completa entre comillas dobles. Consulte el apartado Ejemplo: añadir una opción a un conjunto de opciones de cliente para obtener más información.
3. El valor de *valor\_opción* está limitado a 1.024 caracteres.

Force

Especifica si el servidor fuerza al cliente a utilizar el valor de conjunto de opciones. El valor no se tiene en cuenta con las opciones aditivas como, por ejemplo, INCLEXCL y DOMAIN. El valor predeterminado es NO. Este parámetro es opcional. Los valores son:

Yes

Especifica que el servidor impone forzosamente al cliente la utilización del valor. (El cliente no puede alterar temporalmente el valor.)

No

Especifica que el servidor no impone forzosamente al cliente la utilización del valor. (El cliente sí puede alterar temporalmente el valor.)

SEQnumber

Especifica un número de secuencia cuando se especifica un nombre de opción más de una vez. Este parámetro es opcional.

## Ejemplo: añadir una opción a un conjunto de opciones de cliente

---

Agregar una opción de cliente (MAXCMDRETRIES 5) a un conjunto de opciones de cliente denominado ENG.

```
define clientopt eng maxcmdretries 5
```

## Ejemplo: añadir una opción para excluir un archivo de la copia de seguridad

---

Añadir una opción de cliente al conjunto de opciones ENGBACKUP para excluir el archivo c:\admin\file.txt de los servicios de copia de seguridad.

```
define clientopt engbackup inclexcl "exclude c:\admin\file.txt"
```

## Ejemplo: añadir una opción para excluir un directorio de la copia de seguridad

---

Agregar una opción de cliente al conjunto de opciones WINSPEC para excluir un directorio temporal de Internet de los servicios de copia de seguridad. Cuando utilice la opción EXCLUDE o INCLUDE con nombres de archivo que contienen espacios, escriba la especificación de archivo entre comillas simples y la opción completa entre comillas dobles.

```
define clientopt winspec inclexcl "exclude.dir '*:\..\Temporary  
Internet Files'"
```

## Ejemplo: añadir una opción a los archivos de enlace en los directorios especificados

---

Añadir opciones de cliente al conjunto de opciones WINSPEC para enlazar todos los archivos de los directorios C:\Data y C:\Archivos de programa\My Apps con una clase de gestión denominada PRODCLASS.

```
define clientopt winspec inclexcl "include C:\Data\...\* prodclass"
define clientopt winspec inclexcl "include 'C:\Archivos de
programa\My Apps\...\*' prodclass"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE CLIENTOPT

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## DEFINE CLOPTSET (Definir un nombre de conjunto de opciones de cliente)

Utilice este comando para definir un nombre para un conjunto de opciones que puede asignar a los clientes para las operaciones de archivado, copia de seguridad, restauración y recuperación.

Para añadir opciones al nuevo conjunto, ejecute el comando DEFINE CLIENTOPT.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

### Sintaxis

```
>>-DEFine CLOptset--nombre_conjunto_opciones----->
>--+-----+-----><
  '-DESCRiption----descripción-'
```

### Parámetros

nombre\_conjunto\_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente. La longitud máxima del nombre es de 64 caracteres.

DESCRiption

Especifica una descripción del conjunto de opciones de cliente. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar encerrada entre comillas si contiene espacios en blanco. Este parámetro es opcional.

### Ejemplo: definir un conjunto de opciones de cliente

Para definir un conjunto de opciones de cliente denominado ENG, emita el comando siguiente:

```
define cloptset eng
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE CLOPTSET

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.

Comando	Descripción
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

## DEFINE COLLOGROUP (Definir un grupo de proximidad)

Utilice este mandato para definir un grupo de proximidad. Un *grupo de proximidad* es un grupo de nodos o espacios de archivos en un nodo cuyos datos se colocan en un número mínimo de volúmenes de acceso secuencial. Sus datos se asignan sólo si la definición de la agrupación de almacenamiento está establecida como proximidad por grupo (COLLOCATE=GROUP).

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine COLLOGGroup--nombre_grupo----->
>--+-----+----->
  '-DESCription----descripción-'<
```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad que desea crear. La longitud máxima del nombre es de 30 caracteres.

DESCription

Especifica una descripción del grupo de proximidad. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

### Definir un grupo de proximidad

Para definir un grupo de proximidad de espacio de archivos o nodo denominado GROUP1, emita el mandato siguiente:

```
define colloggroup group1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE COLLOGROUP

Comando	Descripción
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.



Comando	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## DEFINE COLLOCMEMBER (Definir un miembro de grupo de proximidad)

Emita este mandato para agregar un nodo de cliente a un grupo de proximidad o para agregar un espacio de archivos de un nodo a un grupo de proximidad. Un grupo de proximidad es un grupo de nodos o espacios de archivos en un nodo cuyos datos se colocan en un número mínimo de volúmenes de acceso secuencial.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de almacenamiento sin restricciones.

### Sintaxis

Agregar un nodo a un grupo de proximidad

```

      .-,-,-----,
      v          |
>>-DEFine COLLOCMember--nombre_grupo----nombre_nodo+-----><

```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad al que desea agregar un nodo de cliente.

nombre\_nodo

Especifica el nombre del nodo de cliente que desea agregar al grupo de proximidad. Puede especificar uno o más nombres.

Separe varios nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres.

Agregar un espacio de archivos de un nodo a un grupo de proximidad

```

>>-DEFine COLLOCMember--nombre_grupo--nombre_nodo----->

```

```

      .-,-,-----,
      v          |
>>-FIlespace-----nombre_espacio_archivos+----->
      .-NAMEType----SERVER-----
>+-----+----->
  '-NAMEType----+-SERVER---+'
      +-UNICODE-+
      '-FSID----'

      .-CODEType----BOTH-----,
>+-----+-----><
  '-CODEType----+-BOTH-----+'
      +-UNICODE----+
      '-NONUNICODE-'

```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad al que desea agregar un espacio de archivos.

nombre\_nodo

Especifica el nodo de cliente donde se encuentra el espacio de archivos.

Filespace

Especifica el *nombre\_espacio\_archivos* en el nodo de cliente que desea agregar al grupo de proximidad. Puede especificar uno o más nombres de espacio de archivos que se encuentren en un nodo de cliente específico. Si especifica varios nombres de espacio de archivos, separe los nombres con comas sin espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres de espacio de archivos. Por ejemplo:

```
define collocmember manufacturing linux237 filespace=*_linux_fs
```

Este mandato coloca todos los espacios de archivos en el nodo linux237 con un nombre que acaba con *\_linux\_fs* en el grupo de proximidad manufacturing.

Consulte la lista siguiente para obtener sugerencias sobre cómo trabajar con grupos de proximidad:

- Al agregar miembros a un nuevo grupo de proximidad, el tipo del primer miembro del grupo de proximidad determina el tipo del grupo de proximidad. El grupo puede ser un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.  
Restricción: Una vez que se ha establecido el tipo del grupo de proximidad, este no se puede cambiar.
- No puede mezclar tipos de miembro de grupo de proximidad al agregar miembros a un grupo de proximidad (un grupo de nodos o un grupo de espacios de archivos).
- Para un grupo de proximidad de espacio de archivos, puede agregar espacios de archivos al grupo. Los espacios de archivos deben utilizar el mismo valor que el parámetro *nombre\_nodo* que se ha especificado al establecer el grupo de proximidad.
- Se puede incluir un nodo de cliente en varios grupos de espacios de archivos. Sin embargo, si un nodo es miembro de un grupo de proximidad de nodo, no puede ser miembro de un grupo de proximidad de espacio de archivos.
- Un espacio de archivos puede ser miembro de solo un grupo de espacios de archivos.

NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Especifique este parámetro cuando el servidor se comunique con clientes que tengan soporte de Unicode. Un cliente de copia de seguridad/archivado con soporte de Unicode solamente está disponible para los sistemas Windows, Macintosh OS 9, Macintosh OS X y NetWare. El nombre de espacio de archivos no puede ser un carácter comodín cuando se especifica NAMETYPE para un grupo de asignación de espacio de archivos. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión del nombre depende de los caracteres que contienen realmente los nombres y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos por sus ID de espacio de archivos (FSID).

CODEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro cuando utilice un carácter comodín para el nombre de espacio de archivos. Por ejemplo:

```
define collocmember production Win_3419 filespace=* codetype=unicode
```

Este mandato de ejemplo agrega todos los espacios de archivos del nodo Win\_3419 al grupo de proximidad de producción. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Puede especificar uno de los siguientes valores:

BOTH

Incluir los espacios de archivos independientemente del tipo de página de códigos.

UNICODE

Incluir los espacios de archivos que solo están en Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en Unicode.

## Definir dos miembros de grupo de proximidad

Definir dos miembros, NODE1 y NODE2, para un grupo de proximidad, GROUP1.

```
define collocmember group1 node1,node2
```

## Definir un miembro de grupo de espacios de archivos CNTR90524, en el nodo clifton al grupo de proximidad TSM\_alpha\_1

```
define collocmember TSM_alpha_1 clifton filespace=CNTR90524
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE COLLOCMEMBER

Comando	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## DEFINE COPYGROUP (Definir un grupo de copia)

Utilice este mandato para definir un nuevo grupo de copia de seguridad o de copia archivada en una clase de gestión, un juego de políticas y un dominio de políticas específicos. El servidor utiliza los grupos de copia de seguridad y de copia archivada para controlar cómo hacen copias de seguridad y copias archivadas los clientes, y para gestionar las copias de seguridad y las copias archivadas.

Para que los clientes puedan utilizar el nuevo grupo de copia, debe activar el juego de políticas que contiene el nuevo grupo de copia.

Puede definir un grupo de copia archivada y un grupo de copia de seguridad para cada clase de gestión. Para asegurarse de que los nodos cliente pueden hacer copias de seguridad, incluya un grupo de copia de seguridad en la clase de gestión predeterminada de un juego de políticas.

Atención: El comando DEFINE COPYGROUP no se ejecutará correctamente si especifica como destino una agrupación de almacenamiento de copia.

El comando DEFINE COPYGROUP tiene dos formatos, uno para definir un grupo de copia de seguridad y otro para definir un grupo de copia archivada. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con DEFINE COPYGROUP

Comando	Descripción
---------	-------------





restantes se determina mediante el tiempo de retención especificado en los parámetros RETEXTRA y RETONLY. Los valores posibles son:

número

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad de los archivos que se han suprimido del sistema de archivos del cliente después de hacerse la copia de seguridad.

RETEExtra

Especifica el número de días que se ha de retener una versión de copia de seguridad una vez que esa versión se convierte en inactiva. Una versión de un archivo se convierte en inactiva cuando el cliente almacena otra copia de seguridad más reciente o cuando el cliente suprime el archivo de la estación de trabajo y luego ejecuta una copia de seguridad incremental completa. El servidor suprime las versiones inactivas basándose en el tiempo de retención aunque el número de versiones inactivas no sobrepase el número que permiten los parámetros VEREXISTS o VERDELETED. Este parámetro es opcional. El valor predeterminado es 30 días. Los valores posibles son:

días

Especifica el número de días que se retienen las versiones de copia de seguridad inactivas. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que las versiones de copia de seguridad inactivas se retienen de forma indefinida.

Si especifica NOLIMIT, el servidor suprimirá las versiones de copia de seguridad inactivas basándose en el parámetro VEREXISTS (si el archivo todavía existe en el sistema de archivos del cliente) o en el parámetro VERDELETED (si el archivo ya no existe en el sistema de archivos del cliente).

RETOOnly

Especifica el número de días que se retiene la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente. Este parámetro es opcional. El valor predeterminado es 60. Los valores posibles son:

días

Especifica el número de días que se retiene la última versión inactiva restante de un archivo. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que se desea conservar la última versión inactiva restante de un archivo de forma indefinida.

Si especifica NOLIMIT, el servidor retiene la última versión de copia de seguridad restante para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor.

MODE

Especifica si IBM Spectrum Protect sólo hace copia de seguridad de un archivo si éste se ha modificado desde la última copia de seguridad o si la hace siempre que un cliente solicita una copia de seguridad. Este parámetro es opcional. El valor predeterminado es MODIFIED. Los valores posibles son:

MODified

Especifica que IBM Spectrum Protect sólo hace copia de seguridad del archivo si éste se ha modificado desde la última copia de seguridad. IBM Spectrum Protect considera que un archivo se ha modificado si se cumple algunas de las siguientes condiciones:

- La fecha de última modificación es diferente
- El tamaño del archivo es diferente
- El propietario del archivo es diferente
- Los permisos de los archivos son diferentes

ABSolute

Especifica que IBM Spectrum Protect hace copia de seguridad del archivo independientemente de que se haya modificado.

El valor de MODE sólo se utiliza en la copia de seguridad incremental completa. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial.

SERialization

Especifica cómo debe procesar IBM Spectrum Protect los archivos o directorios cuando éstos se modifican durante el proceso de copia de seguridad. Este parámetro es opcional. El valor predeterminado es SHRSTATIC. Los valores posibles son:

SHRStatic

Especifica que IBM Spectrum Protect sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. IBM Spectrum Protect intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo o directorio se modifica durante cada intento de copia de seguridad, IBM Spectrum Protect no hace la copia de seguridad.

#### STatic

Especifica que IBM Spectrum Protect sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. IBM Spectrum Protect intenta efectuar la copia de seguridad una sola vez.

Las plataformas que no dan soporte a la opción STATIC toman de forma predeterminada el valor SHRSTATIC.

#### SHRDynamic

Especifica que si se modifica un archivo o directorio durante un intento de copia de seguridad, IBM Spectrum Protect hace copia de seguridad del archivo o directorio durante el último intento aunque el archivo o directorio se esté modificando. IBM Spectrum Protect intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

#### DYnamic

Especifica que IBM Spectrum Protect realiza la copia de seguridad de un archivo o directorio en el primer intento, independientemente de que el archivo o directorio esté modificándose durante el proceso de copia de seguridad. Atención: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar la copia de seguridad de un archivo o directorio mientras están produciéndose modificaciones. Como consecuencia, la versión de copia de seguridad puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se restaura un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una versión de copia de seguridad solo si el archivo o directorio no se está modificando.

#### TOCDestination

Especifica la agrupación de almacenamiento primaria en la que inicialmente se almacenará una tabla de contenido (TOC) para cualquier operación de copia de seguridad NDMP (protocolo de gestión de datos de red) u operación de juego de copias de seguridad para la que se genere una TOC. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino. La agrupación de almacenamiento que se especifique para el destino debe tener el formato de datos NATIVE o NONBLOCK. Para evitar que se produzcan retardos de montaje, se recomienda que la agrupación de almacenamiento tenga una clase de dispositivo DISK o DEVTYPE=FILE. La generación de la TOC es opcional en las operaciones de copia de seguridad NDMP, pero no está admitida en otras operaciones de copia de seguridad de imagen.

Si se solicita la creación de la TOC para una operación de copia de seguridad que utilice NDMP y la imagen está vinculada a una clase de gestión cuyo grupo de copia de seguridad no especifica un destino de TOC, el resultado de la operación dependerá del parámetro TOC de la operación de copia de seguridad.

- Si TOC=PREFERRED (el valor predeterminado), la copia de seguridad continuará sin crearse una TOC.
- Si TOC=YES, la copia de seguridad en su totalidad resultará anómala porque no puede crearse ninguna TOC.

## Ejemplo: crear un grupo de copias de seguridad

---

Crear un grupo de copia de seguridad denominado STANDARD para la clase de gestión ACTIVEFILES del juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS. El destino de copia de seguridad se establecerá en BACKUPPOOL. El intervalo mínimo entre copias de seguridad se establecerá en tres días, independientemente de si se han modificado los archivos. Se retendrán hasta cinco versiones de copia de seguridad mientras el archivo exista en el sistema de archivos del cliente.

```
define copygroup employee_records
vacation activefiles standard type=backup
destination=backuppool frequency=3
verexists=5 mode=absolute
```

## DEFINE COPYGROUP (Definir un grupo de copias archivadas)

---

Utilice este comando para definir un nuevo grupo de copia archivada en una clase de gestión, un juego de políticas y un dominio de políticas específicos.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

```
>>-DEFine COpYgroup--domain_name--policy_set_name--class_name-->
.-STANDARD-.
>--Type-----Archive----->
'-STANDARD-'

.-FREQuency----Cmd-.
>--DESTination---nombre_agrupación----->
'-FREQuency----Cmd-'

.-RETVer-----365-----.-RETInit----CREATION--.
>----->
'-RETVer-----+días---+' '-RETInit----Event---'
'-NOLimit-'

.-RETMin-----365-----.-MODE----ABSolute-.
>----->
'-RETMin-----días---' '-MODE----ABSolute-'

.-SERialization----SHRStatic-----.
>-----<
'-SERialization----+SHRStatic---+'
'+Static-----+'
'+SHRDYnamic-+'
'-DYnamic----'
```

## Parámetros

nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas para el que está definiendo el grupo de copia.

nombre\_juego\_políticas (Necesario)

Especifica el nombre del juego de políticas para el que está definiendo el grupo de copia.

No puede definir un grupo de copia para una clase de gestión que pertenezca al juego de políticas ACTIVE.

nom\_clase (Necesario)

Especifica el nombre de la clase de gestión para la que está definiendo el grupo de copia.

STANDARD

Especifica el nombre del grupo de copia, que debe ser STANDARD. Este parámetro es opcional. El valor predeterminado es STANDARD.

Type=Archive (Necesario)

Especifica que desea definir un grupo de copia archivada.

DESTination (Obligatorio)

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente la copia archivada. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency=Cmd

Especifica la frecuencia de copia, que debe ser CMD. Este parámetro es opcional. El valor predeterminado es CMD.

RETVer

Especifica el número de días que se ha de mantener una copia archivada. Este parámetro es opcional. El valor predeterminado es 365. Los valores posibles son:

días

Especifica la cantidad de tiempo que se mantiene la copia de un archivo. Puede especificar un entero entre 0 y 30.000. La opción del servidor RETENTIONEXTENSION puede afectar a la retención del volumen si las siguientes condiciones son verdaderas:

- Especifique cero para el número de días
- La agrupación de almacenamiento de destino para el grupo de copia de archivo es una agrupación de almacenamiento SnapLock (RECLAMATIONTYPE=SNAPLOCK)

Si se cumplen las dos condiciones y la retención de volúmenes está definida por el valor de la opción del servidor RETENTIONEXTENSION. El valor de la opción del servidor RETENTIONEXTENSION también se aplica si los datos se han copiado o movido a la agrupación de almacenamiento SnapLock por un proceso del servidor como la migración, o mediante los mandatos MOVE DATA o MOVE NODEDATA.

NOLimit

Especifica que desea conservar una copia archivada de forma indefinida.



Si especifica NOLIMIT, el servidor retiene las copias archivadas para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor. Si especifica NOLIMIT, no puede especificar también EVENT en el parámetro RETINIT.

El valor del parámetro RETVER puede afectar a la clase de gestión a la que el servidor vincula un directorio de copia archivada. Si el cliente no utiliza la opción ARCHMC, el servidor vincula los directorios de copia archivada con la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor vincula los directorios de copia archivada con la clase de gestión que presente el período de retención más reducido.

El parámetro RETVER del grupo de copia archivada de la clase de gestión a la que un objeto está vinculado determina el criterio de retención de cada objeto. Consulte el comando SET ARCHIVERETENTIONPROTECTION para obtener una descripción de la protección de datos.

Si la agrupación de almacenamiento primaria especificada en el parámetro DESTINATION pertenece a una clase de dispositivo Centera y la protección de datos está activada, el valor de RETVER se envía a Centera para la gestión de la retención. Consulte el comando SET ARCHIVERETENTIONPROTECTION para obtener una descripción de la protección de datos.

#### RETInit

Especifica cuándo comienza el tiempo de retención especificado en el atributo RETVER. Este parámetro es opcional. Si define el valor RETINIT durante la creación del grupo de copias, no podrá modificarlo más adelante. El valor predeterminado es CREATION. Los valores posibles son:

##### CREATion

Especifica que el tiempo de retención especificado en el atributo RETVER comienza en el momento en que una copia archivada se almacena en el servidor de IBM Spectrum Protect.

##### EVent

Especifica que el tiempo de retención especificado en el parámetro RETVER comienza en el momento en que una aplicación de cliente notifica al servidor de que se ha producido un evento de inicio de retención para la copia archivada. Si especifica RETINIT=EVENT, no puede especificar también RETVER=NOLIMIT.

Consejo: Puede especificar una espera de supresión en un objeto que se ha almacenado con RETINIT=EVENT y para el cual el evento no se ha producido. Si el evento se produce mientras el objeto está en espera de supresión, se inicia el período de retención, pero el objeto no se suprimirá mientras siga en espera de supresión.

#### RETMIn

Especifica el número mínimo de días que se conserva una copia archivada después de que se archiva. Este parámetro es opcional. El valor predeterminado es 365. Si especifica RETINIT=CREATION, este parámetro se pasa por alto.

#### MODE=ABSolute

Especifica que siempre se archiva un archivo cuando el cliente lo solicita. El valor de MODE debe ser ABSOLUTE. Este parámetro es opcional. El valor predeterminado es ABSOLUTE.

#### SERialization

Especifica cómo procesará IBM Spectrum Protect los archivos que se han modificado durante la operación de archivado. Este parámetro es opcional. El valor predeterminado es SHRSTATIC. Los valores posibles son:

##### SHRStatic

Especifica que IBM Spectrum Protect sólo hace copia archivada de un archivo si éste no se está modificando. IBM Spectrum Protect intenta efectuar una operación de archivado hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo se modifica durante el intento de archivado, IBM Spectrum Protect no archivará el archivo.

##### Static

Especifica que IBM Spectrum Protect sólo hace copia archivada de un archivo si éste no se está modificando. IBM Spectrum Protect intenta efectuar la operación de archivado una sola vez.

Las plataformas que no dan soporte a la opción STATIC toman de forma predeterminada el valor SHRSTATIC.

##### SHRDynamic

Especifica que si se modifica el archivo durante un intento de archivar, IBM Spectrum Protect archivará el archivo en el último intento aunque se esté modificando. IBM Spectrum Protect intenta la opción de archivado del archivo hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

##### Dynamic

Especifica que IBM Spectrum Protect realiza la copia archivada de un archivo en el primer intento, independientemente de si el archivo está modificándose durante el proceso de archivado.

Atención: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar una operación de archivado de un archivo mientras están produciéndose modificaciones. Como consecuencia, la copia archivada puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se recupera un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina

SERIALIZATION en el valor SHRSTATIC o STATIC para que IBM Spectrum Protect cree una copia de archivado sólo si no se está modificando el archivo.

## Ejemplo: definir un grupo de copias archivadas para la retención basada en eventos

Crear un grupo de copia archivada denominado STANDARD para la clase de gestión EVENTMC del juego de políticas SUMMER del dominio de políticas PROG1. Establecer el destino de la copia archivada en ARCHIVEPOOL, donde la copia archivada permanecerá hasta que el servidor reciba una notificación de que se ha producido un evento para iniciar el tiempo de retención, tras lo cual la copia archivada se conservará durante 30 días. La copia archivada se conservará durante un mínimo de 90 días tras su almacenamiento en el servidor, independientemente de cuándo se notifique al servidor de que se ha producido un evento para iniciar el tiempo de retención.

```
define copygroup prog1 summer eventmc standard type=archive
destination=archivepool retinit=event retver=30 retmin=90
```

## DEFINE DATAMOVER (Definir un transportador de datos)

Utilice este comando para definir un transportador de datos. Un transportador de datos es un dispositivo designado que acepta una solicitud de IBM Spectrum Protect para transferir datos. Un transportador de datos se puede utilizar para realizar operaciones de copia en el exterior.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DATAMover--nombre_transportador_datos----->
. -Type---NAS-----
>--+-----+----->
|              (1) (2) |
' -Type---+-NASCLUSTER-+-----'
      '-NASVSERVER-'

      .-LLAddress---1000-----
>--HLAddress---dirección--+----->
      '-LLAddress---puerto_tcp-'

>--USERid---ID_usuario--PASsword---contraseña----->
. -ONLine---Yes-----
>--+-----+-----DATAFormat---+NETAPPDump--+-----<
' -ONLine---+Yes-+-'      '+-CELERRADump-+'
      '-No--'              '-NDMPDump----'
```

Notas:

1. Puede especificar TYPE=NASCLUSTER y TYPE=NASVSERVER solo en un sistema operativo AIX, Linux o Windows.
2. Puede especificar TYPE=NASCLUSTER y TYPE=NASVSERVER sólo si DATAFORMAT=NETAPPDUMP.

### Parámetros

nombre\_transportador\_datos (Obligatorio)

Especifica el nombre del transportador de datos. Este nombre debe ser el mismo que el nombre de nodo con el que se ha registrado anteriormente mediante el mandato REGISTER NODE TYPE=NAS. Los datos de los que se hace copia de seguridad en este transportador de datos NAS se asignarán a este nombre de nodo en la base de datos del servidor. La longitud máxima permitida de este nombre es 64 caracteres.

Type

Especifica el tipo de transportador de datos. Este parámetro es opcional. El valor predeterminado es NAS.

NAS

Especifica que el transportador de datos es un servidor de archivos NAS.

NASCLUSTER

Especifica que el transportador de datos es un servidor de archivos NAS en clúster.

Restricción: Puede especificar el valor NASCLUSTER sólo si DATAFORMAT=NETAPPDUMP.

NASVSERVER

Especifica que el transportador de datos es un dispositivo de almacenamiento virtual dentro de un clúster.  
Restricción: Puede especificar el valor NASVSERVER sólo si DATAFORMAT=NETAPPDUMP.

**HLAddress (Obligatorio)**

Especifica la dirección IP numérica o el nombre de dominio que se utiliza para acceder al servidor de archivos NAS.

Consejo: Para determinar la dirección IP numérica, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener la dirección.

**LLAddress**

Especifica el número de puerto TCP para acceder al dispositivo NAS para sesiones con el protocolo NDMP (Network Data Management Protocol). Este parámetro es opcional. El valor predeterminado es 10000.

**USERid (Obligatorio)**

Especifica el ID de un usuario autorizado para iniciar una sesión con el servidor de archivos NAS. Por ejemplo, especifique el ID de usuario que se ha configurado en el servidor de archivos NetApp para las conexiones NDMP.

Consejo: Para determinar el ID de usuario, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener el ID de usuario.

**PASsword (Obligatorio)**

Especifica la contraseña del ID de usuario para iniciar una sesión en el servidor de archivos NAS.

Consejo: Para determinar la contraseña, acceda al servidor de archivos NAS. A continuación, siga las instrucciones de la documentación del servidor de archivos para obtener la contraseña.

**ONLine**

Especifica si el transportador de datos está disponible para utilizarlo. Este parámetro es opcional. El valor predeterminado es YES.

Yes

Es el valor predeterminado. Especifica que el transportador de datos está disponible para utilizarlo.

No

Especifica que el transportador de datos no está disponible para utilizarlo. Mientras se realicen las operaciones de mantenimiento de hardware, puede utilizar el mandato UPDATE DATAMOVER para desactivar el transportador de datos.

si se controla una biblioteca mediante una ruta desde un transportador de datos NAS a la biblioteca y el transportador de datos NAS está desactivado, el servidor no puede acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras el transportador de datos NAS está desactivado, no se inicializará la biblioteca.

**DATAFormat (Obligatorio)**

El formato de datos utilizado por este transportador de datos.

NETAPPDump

Se debe utilizar para los servidores de archivos NAS NetApp y para la serie N de IBM® System Storage.

CELERRADump

Se debe utilizar para los servidores de archivos NAS EMC Celerra.

NDMPDump

Se debe utilizar para los servidores de archivos NAS distintos de los servidores de archivos NetApp o EMC.

## Ejemplo: definir un transportador de datos mediante un nombre de dominio

---

Definir un transportador de datos para el nodo denominado NAS1. El nombre de dominio del transportador de datos es NETAPP2.EXAMPLE.COM en el puerto 10000.

```
define datamover nas1 type=nas hladdress=netapp2.example.com lladdress=10000
userid=root password=admin dataformat=netappdump
```

## Ejemplo: definir un transportador de datos mediante una dirección IP

---

Defina un transportador de datos para el nodo denominado NAS2. La dirección IP numérica para el transportador de datos es 203.0.113.0 en el puerto 10000. El servidor de archivos NAS no es un servidor de archivos NetApp ni EMC.

```
define datamover nas2 type=nas hladdress=203.0.113.0 lladdress=10000
userid=root password=admin dataformat=ndmpdump
```

## Ejemplo: definir un transportador de datos para un servidor de archivos en clúster mediante una dirección IP

---

Defina un transportador de datos para el servidor de archivos en clúster denominado NAS3. El servidor de archivos NAS es un dispositivo NetApp. La dirección IP numérica para el transportador de datos es 198.51.100.0 en el puerto 10000.



```
define datamover nas3 type=nascluster hladdress=198.51.100.0
lladdress=10000 userid=root password=admin dataformat=netappdump
```

Tabla 1. Comandos relacionados con DEFINE DATAMOVER

Comando	Descripción
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DATAMOVER	Suprimir un transportador de datos.
QUERY DATAMOVER	Visualiza definiciones de transportador de datos.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

## DEFINE DEVCLASS (Definir una clase de dispositivo)

Utilice este comando para definir una clase de dispositivo para un tipo de dispositivo de almacenamiento. El servidor exige que se defina una clase de dispositivo para poder utilizar un dispositivo.



Para ver la lista más actualizada de dispositivos soportados y los formatos válidos de las clases de dispositivo, consulte el sitio web Dispositivos soportados de IBM Spectrum Protect:  Sistemas operativos AIX  Sistemas operativos Windows

- Dispositivos compatibles con AIX y Windows

 Sistemas operativos Linux

- Dispositivos compatibles con Linux

Nota: La clase de dispositivo DISK la define IBM Spectrum Protect y no puede modificarse con el comando DEFINE DEVCLASS.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS).

Las siguientes clases de dispositivo de IBM Spectrum Protect se ordenan por tipo de dispositivo.



- DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
- DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
- DEFINE DEVCLASS (Definir una clase de dispositivo 4MM)
- DEFINE DEVCLASS (Definir una clase de dispositivo 8MM)
- DEFINE DEVCLASS (Definir una clase de dispositivo CENTERA)
- DEFINE DEVCLASS (Definir una clase de dispositivo DLT)
- DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE)
- DEFINE DEVCLASS (Definir una clase de dispositivo FILE)
-  Sistemas operativos AIX  Sistemas operativos Windows DEFINE DEVCLASS (Definir una clase de dispositivo GENERICTAPE)
- DEFINE DEVCLASS (Definir una clase de dispositivo LTO)
- DEFINE DEVCLASS (Definir una clase de dispositivo NAS)
- DEFINE DEVCLASS (Definir una clase de dispositivo REMOVABLEFILE)
- DEFINE DEVCLASS (Definir una clase de dispositivo SERVER)
- DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE)

Tabla 1. Comandos relacionados con DEFINE DEVCLASS

Comando	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.



Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3590B	10 GB	Formato sin comprimir (básico)
3590C	Consulte la nota 20 GB	Formato comprimido
3590E-B	10 GB	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Consulte la nota 20 GB	Formato comprimido, similar al formato 3590C
3590H-B	30 GB (cartucho J, longitud estándar) 60 GB (cartucho K, longitud ampliada)	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Consulte la nota 60 GB (cartucho J, longitud estándar) 120 GB (cartucho K, longitud ampliada)	Formato comprimido, similar al formato 3590C

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

Tabla 2. Selecciones de formato de grabación de dispositivos 3590

Dispositivo	Formato					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	Lectura/	Lectura/	–	–	–	–
Ultra SCSI	Grabación	Grabación	–	–	–	–
3590E	Lectura/	Lectura/	Lectura/	Lectura/	–	–
3590H	Grabación	Grabación	Grabación	Grabación	Lectura/	Lectura/
	Lectura	Lectura	Lectura	Lectura	Grabación	Grabación
	Lectura	Lectura				

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número



Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## DEFINE DEVCLASS (Definir una clase de dispositivo 3592)

Utilice la clase de dispositivo 3592 cuando utilice dispositivos de cinta 3592.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS).

### Clase de privilegio





## LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

El valor predeterminado es NO.

Son posibles los siguientes valores:

### READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

### WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

### No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades IBM® 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.

Consulte la nota técnica 1634851, Información adicional sobre la opción LBProtect de IBM Spectrum Protect, para ver una explicación sobre cuándo utilizar el parámetro LBProtect.

## WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

### Yes

Especifica que las unidades utilizan medios WORM.

### No

Especifica que las unidades no utilizan medios WORM.

### Recuerde:

1. Para utilizar el soporte WORM 3592 en bibliotecas 3584, debe especificar el parámetro WORM. El servidor distingue entre volúmenes reutilizables WORM y distintos de WORM. Sin embargo, para utilizar el soporte WORM 3592 en bibliotecas 349X, también deberá establecer WORMSCRATCHCATEGORY en el mandato DEFINE LIBRARY. Para obtener detalles, consulte el apartado DEFINE LIBRARY (Definir una biblioteca).
2. Cuando WORM=Yes, el único valor válido para el parámetro SCALECAPACITY es 100.
3. Consulte a sus proveedores para saber si su hardware tiene el nivel de soporte apropiado.

## SCALECAPacity

Especifica el porcentaje de la capacidad del medio que puede utilizarse para almacenar datos. Este parámetro es opcional. El valor predeterminado es 100. Los valores posibles son 20, 90 y 100.

Si el porcentaje de la capacidad de escala se establece en 100, se proporciona la capacidad máxima de almacenamiento. Si se establece en 20 se obtiene el tiempo de acceso más rápido.

Nota: El valor de la capacidad de escala sólo entra en vigor cuando se graban datos por primera vez en un volumen. Cualquier actualización de la clase de dispositivo de capacidad de escala no afecta a los volúmenes que ya tienen datos grabados hasta que el volumen se vuelve a poner en estado reutilizable.

## FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3592:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para 3592

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3592	300 GB	Formato sin comprimir (básico)
3592C	Consulte la nota 900 GB	Formato comprimido
3592-2	500 GB 700 GB	Cintas JA con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico)
3592-2C	1,5 TB 2,1 TB	Cintas JA con formato comprimido Cintas JB con formato comprimido
3592-3	640 GB 1 TB	Cintas JA con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico)
3592-3C	1,9 TB 3 TB	Cintas JA con formato comprimido Cintas JB con formato comprimido
3592-4	400 GB 1,5 TB 3,1 TB	Cintas JB con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico) Cintas JC con formato sin comprimir (básico)
3592-4C	1,2 TB 4,4 TB 9,4 TB	Cintas JK con formato comprimido Cintas JB con formato comprimido Cintas JC con formato comprimido
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser distinta del valor que aparece en la lista.		

Importante: Para un rendimiento óptimo, evite combinar distintas generaciones de unidades en una única biblioteca SCSI. Si debe combinar distintas generaciones de unidades en una biblioteca SCSI, utilice una de las configuraciones especiales que se describen en el tema sobre la combinación de generaciones de medios 3592.

También se necesitan configuraciones especiales para combinar distintas generaciones de unidades 3592 en bibliotecas 349x y ACSLS.

## ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

## PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

## MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

## MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

## MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir).

### ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifrarán otros tipos de volúmenes, por ejemplo, juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos). Si especifica ON y activa el método de cifrado del sistema o de la biblioteca, no se permitirá el cifrado de unidades y las operaciones de copia de seguridad fallarán.

### ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa el método de cifrado del sistema o de la biblioteca.

### EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad.

Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado.

En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

### OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado del sistema o de la biblioteca, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

## DEFINE DEVCLASS (Definir una clase de dispositivo 4MM)

Utilice la clase de dispositivo 4MM cuando utilice dispositivos de cinta de 4 mm.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----4MM----->
.-FORMAT-----DRIVE-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-FORMAT-----+--DRIVE--+' '-ESTCAPacity----tamaño-'
      +-DDS1--+
      +-DDS1C+
      +-DDS2--+
      +-DDS2C+
      +-DDS3--+
      +-DDS3C+
      +-DDS4--+
      +-DDS4C+
      +-DDS5--+
      +-DDS5C+
      +-DDS6--+
      '-DDS6C-'

.-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-PREFIX----+--ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTWait----60-----.-MOUNTRetention----60-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTWait----minutos-' '-MOUNTRetention----minutos-'

.-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+----->
'-MOUNTLimit----+--DRIVES--+'
      +-número+

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 4 mm que esta clase de dispositivo ha utilizado. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=4MM (Necesario)

Especifica que se asigna el tipo de dispositivo 4MM a la clase de dispositivo. La especificación 4MM indica que a esta clase de dispositivo se asignan dispositivos de cinta de 4 mm.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 4 mm:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para las cintas de 4 mm

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DDS1	2.6 GB (60 metros) 4.0 GB (90 metros)	Formato sin comprimir, sólo aplicable a cintas de 60 y 90 metros
DDS1C	Consulte la nota 1,3 GB (60 metros) 2,0 GB (90 metros)	Formato comprimido, sólo aplicable a cintas de 60 y 90 metros
DDS2	4 GB	Formato sin comprimir, sólo se aplica a cintas de 120 metros
DDS2C	Consulte la nota 8 GB	Formato comprimido, sólo se aplica a cintas de 120 metros
DDS3	12 GB	Formato sin comprimir, sólo se aplica a cintas de 125 metros
DDS3C	Consulte la nota 24 GB	Formato comprimido, sólo se aplica a cintas de 125 metros
DDS4	20 GB	Formato sin comprimir, sólo se aplica a cintas de 150 metros
DDS4C	Consulte la nota 40 GB	Formato comprimido, sólo se aplica a cintas de 150 metros
DDS5	36 GB	Formato sin comprimir cuando se utilizan medios DAT 72
DDS5C	Consulte la nota 72 GB	Formato comprimido cuando se utilizan medios DAT 72
DDS6	80 GB	Formato sin comprimir, cuando se utilizan medios DAT 160
DDS6C	Consulte la nota 160 GB	Formato comprimido, cuando se utilizan medios DAT 160

Formato	Capacidad estimada	Descripción
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 4 mm, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del nombre de archivo en el que el servidor graba las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor

del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## DEFINE DEVCLASS (Definir una clase de dispositivo 8MM)

Utilice la clase de dispositivo 8MM cuando utilice dispositivos de cinta de 8 mm.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----8MM----->
  .-WORM----No----- .-FORMAT----DRIVE-----
>+-----+-----+-----+-----+-----+----->
  '-WORM----+No--+-' '-FORMAT----+DRIVE+-'
      '-Yes-'                +-8200--+
                              +-8200C--+
                              +-8500--+
                              +-8500C--+
                              +-8900--+
                              +-AIT----+
                              +-AITC--+
                              +-M2----+
                              +-M2C--+
                              +-SAIT--+
                              +-SAITC+
                              +-VXA2--+
                              +-VXA2C+
                              +-VXA3--+
                              '-VXA3C-'

>+-----+-----+-----+-----+-----+----->
  '-ESTCAPacity----tamaño-'

  .-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+----->
  '-PREFIX----+ADSM-----+-'
      '-prefijo_volumen_cinta-'

  .-MOUNTRetention----60----- .-MOUNTWait----60-----
>+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'

  .-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+----->
  '-MOUNTLimit----+DRIVES+-'
      +-número+
      '-0-----'
```

### Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 8 mm que esta clase de dispositivo ha utilizado. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=8MM (Necesario)

Especifica que se asigna el tipo de dispositivo 8MM a la clase de dispositivo. La especificación 8MM indica que a esta clase de dispositivo se asignan dispositivos de cinta de 8 mm.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Nota: Si selecciona Yes, las únicas opciones disponibles para el parámetro FORMAT son:

- DRIVE
- AIT
- AITC

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 8 mm:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para cintas de 8 mm

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
8200	2,3 GB	Formato sin comprimir (estándar) con cartuchos de cintas de 112 metros
8200C	Consulte la nota 3,5 GB 4,6 GB	Formato comprimido con cartuchos de cintas de 112 metros estándar



<b>Formato</b>		<b>Descripción</b>
<b>Tipo de medio</b>	<b>Capacidad estimada</b>	
8500	Consulte la nota	Unidades (Lectura Grabación)
15 m	600 MB	Eliant 820 (RW)
15 m	600 MB	Exabyte 8500/8500C (RW)
15 m	600 MB	Exabyte 8505 (RW)
54 m	2,35 GB	Eliant 820 (RW)
54 m	2,35 GB	Exabyte 8500/8500C (RW)
54 m	2,35 GB	Exabyte 8505 (RW)
112 m	5 GB o 10 GB	Eliant 820 (RW)
112 m	5 GB o 10 GB	Exabyte 8500/8500C (RW)
112 m	5 GB o 10 GB	Exabyte 8505 (RW)
160 m XL	7 GB	Eliant 820 (RW)
8500C	Consulte la nota	Unidades (Lectura Grabación)
15 m	1,2 GB	Eliant 820 (RW)
15 m	1,2 GB	Exabyte 8500/8500C (RW)
15 m	1,2 GB	Exabyte 8505 (RW)
54 m	4,7 GB	Eliant 820 (RW)
54 m	4,7 GB	Exabyte 8500/8500C (RW)
54 m	4,7 GB	Exabyte 8505 (RW)
112 m	5 GB o 10 GB	Eliant 820 (RW)
112 m	5 GB o 10 GB	Exabyte 8500/8500C (RW)
112 m	5 GB o 10 GB	Exabyte 8505 (RW)
160 m XL	7 GB	Eliant 820 (RW)
8900	Consulte la nota	Unidad (Lectura Grabación)
15 m	–	Mammoth 8900 (R)
54 m	–	Mammoth 8900 (R)
112 m	–	Mammoth 8900 (R)
160 m XL	–	Mammoth 8900 (R)
22 m	2,5 GB	Mammoth 8900 (RW)
125 m	–	Mammoth 8900 (RW con actualización)
170 m	40 GB	Mammoth 8900 (RW)
AIT	Consulte la nota	Unidad
SDX1–25C	25 GB	Unidades
SDX1–35C	35 GB	AIT, AIT2 y AIT3
SDX2–36C	36 GB	Unidades
SDX2–50C	50 GB	AIT, AIT2 y AIT3
SDX3–100C	100 GB	Unidades AIT2 y AIT3
SDX3X-150C	150 GB	Unidades AIT2 y AIT3
SDX4–200C	200 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	400 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5
AITC	Consulte la nota	Unidad
SDX1–25C	50 GB	Unidades
SDX1–35C	91 GB	AIT, AIT2 y AIT3
SDX2–36C	72 GB	Unidades
SDX2–50C	130 GB	AIT, AIT2 y AIT3
SDX3–100C	260 GB	Unidades AIT2 y AIT3
SDX3X-150C	390 GB	Unidades AIT2 y AIT3
SDX4–200C	520 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	1040 GB	Unidades AIT3-Ex, AIT4 y AIT5
		Unidades AIT4 y AIT5
		Unidad AIT5

<b>Formato</b> <b>Tipo de medio</b>	<b>Capacidad estimada</b>	<b>Descripción</b>
M2 75 m 150 m 225 m	Consulte la nota 20 GB 40 GB 60 GB	Unidad (Lectura Grabación) Mammoth II (RW) Mammoth II (RW) Mammoth II (RW)
M2C 75 m 150 m 225 m	Consulte la nota 50 GB 100 GB 150 GB	Unidad (Lectura Grabación) Mammoth II (RW) Mammoth II (RW) Mammoth II (RW)
SAIT	Consulte la nota 500 GB	Unidad (Lectura Grabación) Sony SAIT1-500(RW)
SAITC	Consulte la nota 1300 GB (1,3 TB)	Unidad (Lectura Grabación) Sony SAIT1-500(RW)
VXA2 V6 (62 m) V10 (124 m) V17 (170 m)	Consulte la nota 20 GB 40 GB 60 GB	Unidad (Lectura Grabación) VXA-2
VXA2C V6 (62 m) V10 (124 m) V17 (170 m)	Consulte la nota 40 GB 80 GB 120 GB	Unidad (Lectura Grabación) VXA-2
VXA3 X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 40 GB 86 GB 160 GB	Unidad (Lectura Grabación) VXA-3
VXA3C X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota 80 GB 172 GB 320 GB	Unidad (Lectura Grabación) VXA-3
<p>Nota: Las capacidades reales pueden variar en función de los cartuchos y las unidades que se utilicen.</p> <ul style="list-style-type: none"> <li>• Para el formato M2C, la proporción de compresión normal es de 2,5:1.</li> <li>• Para los formatos AITC y SAITC, la proporción de compresión normal es de 2.6:1.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 8 mm, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el

nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## Ejemplo: definir una clase de dispositivo de 8 mm

Definir una clase de dispositivo que se denomina 8MMTAPE para un dispositivo 8 mm en una biblioteca denominada AUTO. El formato es DRIVE, el límite de montaje es 2, la retención de montaje es 10, el prefijo del volumen de cinta se denomina ADMSVOL y la capacidad estimada es 6 GB.

```
define devclass 8mmtape devtype=8mm library=auto
format=drive mountlimit=2 mountretention=10
prefix=adsmvol estcapacity=6G
```

## DEFINE DEVCLASS (Definir una clase de dispositivo CENTERA)

Utilice la clase de dispositivo CENTERA cuando utilice dispositivos de almacenamiento EMC Centera. El tipo de dispositivo CENTERA utiliza los archivos como volúmenes para almacenar los datos de forma secuencial. Es similar a la clase de dispositivo FILE.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>-DEVType----CENTERA----->
      .-,-----
      (1)  V      |
>-HLAddress-----dirección_ip+-?archivo_PEA----->
      .-MINCAPacity----100M---.  .-MOUNTLimit----1-----
>-+-----+-----+-----<
  '-MINCAPacity----tamaño-'  '-MOUNTLimit----número-'
```

#### Notas:

1. Para cada clase de dispositivo Centera, debe especificar una o varias direcciones IP. Sin embargo, la ruta y el nombre del archivo PEA (autorización de entrada de la agrupación) son opcionales, y una especificación del archivo PEA puede seguir a las direcciones IP. Utilice el carácter "?" para separar la ruta y el nombre de archivo PEA de las direcciones IP.

### Parámetros

#### nombre\_clase\_dispositivo (Necesario)


Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

#### DEVType=CENTERA (Necesario)


Especifica que se asigna el tipo de dispositivo Centera a esta clase de dispositivo. Todos los volúmenes pertenecientes a una agrupación de almacenamiento que está definida con esta clase de dispositivo son volúmenes lógicos que son un tipo de medio de acceso secuencial.

#### HLAddress


Especifica una o varias direcciones IP para el dispositivo de almacenamiento Centera y, opcionalmente, el nombre y la ruta de un archivo PEA (autorización de entrada de agrupación). Especifique las direcciones IP en formato decimal con punto (por ejemplo, 9.10.111.222). Un dispositivo Centera puede tener varias direcciones IP. Si se especifican varias direcciones IP, la operación de almacenamiento o recuperación intenta establecer una conexión utilizando cada dirección IP especificada hasta encontrar una dirección válida.

 Sistemas operativos AIX La ruta y el nombre del archivo PEA son sensibles a las mayúsculas y minúsculas.

Si añade el nombre y la ruta de un archivo PEA, asegúrese de que el archivo se almacena en un directorio del sistema que ejecuta el servidor. Separe el nombre y la ruta del archivo PEA de la dirección IP utilizando "?" como por ejemplo:

 Sistemas operativos Windows

```
HLADDRESS=9.10.111.222,9.10.111.223?c:\controlFiles\TSM.PEA
```

 Sistemas operativos AIX

```
HLADDRESS=9.10.111.222,9.10.111.223?/user/ControlFiles/TSM.PEA
```

Especifique sólo una ruta y nombre de archivo PEA para cada definición de clase de dispositivo. Si especifica dos clases de dispositivo Centera distintas que hagan referencia al mismo dispositivo de almacenamiento Centera y si las definiciones de clase

de dispositivo contienen distintas rutas y nombres de archivo PEA, el servidor utiliza el archivo PEA especificado en el parámetro HLADDRESS de la clase de dispositivo que se haya utilizado en primer lugar para abrir el dispositivo de almacenamiento Centera. Consejos:

1. El servidor no incluye un archivo PEA durante la instalación. Si no crea ningún archivo PEA, el servidor utilizará el perfil predeterminado de Centera, que permite a las aplicaciones leer, escribir, suprimir, depurar y consultar datos de un dispositivo de almacenamiento Centera. Para conseguir un control más estricto, cree un archivo PEA utilizando la interfaz de línea de mandatos proporcionada por EMC Centera. Para obtener detalles sobre la autenticación y autorización de Centera, consulte la publicación *Programmer's Guide* de EMC Centera.
2. También puede especificar la ruta y el nombre del archivo PEA en una variable de entorno utilizando la sintaxis CENTERA\_PEA\_LOCATION=rutaarchivo\_nombearchivo. La ruta y el nombre del archivo PEA especificados en esta variable de entorno se aplicarán a todos los clústeres de Centera. Si utiliza esta variable, no es necesario que especifique la ruta y el nombre del archivo PEA utilizando el parámetro HLADDRESS.

#### MINCAPacity

Especifica el tamaño mínimo para los volúmenes Centera que se asignan a una agrupación de almacenamiento de esta clase de dispositivo. Este valor representa la cantidad mínima de datos que se almacenan en un volumen Centera antes de que el servidor lo marque como lleno. Los volúmenes Centera seguirán aceptando datos hasta que se haya almacenado la cantidad mínima de datos. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor predeterminado es 100 MB (MINCAPACITY=100M). El valor mínimo permitido es 1 MB (MINCAPACITY=1M). El valor máximo permitido es 128 GB (MINCAPACITY=128G).

#### MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. El valor predeterminado es 1. Este parámetro es opcional. Puede especificar un número a partir de 0 o mayor; no obstante, la suma de todos los valores de límite de montaje para todas las clases de dispositivo asignadas al mismo dispositivo Centera no debe superar el número máximo de sesiones que permite Centera.

## DEFINE DEVCLASS (Definir una clase de dispositivo DLT)

Utilice la clase de dispositivo DLT cuando utilice dispositivos de cinta DLT.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary----nombre_biblioteca--DEVType---DLT----->
. -WORM----No----- . -FORMAT----DRIVE----- .
>+-----+-----+-----+----->
' -WORM----+No--+ ' ' -FORMAT----+DRIVE-----+ '
          '-Yes-'          +-DLT1-----+
                          +-DLT1C-----+
                          +-DLT10-----+
                          +-DLT10C-----+
                          +-DLT15-----+
                          +-DLT15C-----+
                          +-DLT20-----+
                          +-DLT20C-----+
                          +-DLT35-----+
                          +-DLT35C-----+
                          +-DLT40-----+
                          +-DLT40C-----+
                          +-DLT2-----+
                          +-DLT2C-----+
                          +-DLT4-----+
                          +-DLT4C-----+
                          +-SDLT-----+
                          +-SDLTC-----+
                          +-SDLT320--+
                          +-SDLT320C--+
                          +-SDLT600--+
```

```

+-SDLT600C-+
+-DLTS4-----+
'-DLTS4C---'

>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-ESTCAPacity---- tamaño-'

.-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-PREFIX----ADSM-----+
'-prefijo_volumen_cinta-'

.-MOUNTRetention---60-----.-MOUNTWait---60-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

.-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTLimit----DRIVES+-+
'+ número+
'-0-----'

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta DLT utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=DLT (Necesario)

Especifica que se asigna el tipo de dispositivo DLT a la clase de dispositivo. DLT indica que se asignan dispositivos de cinta DLT a esta clase de dispositivo.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Nota: El soporte para los medios WORM de DLT sólo está disponible para las unidades SDLT-600, Quantum DLT-V4 y Quantum DLT-S4 en las bibliotecas manuales, SCSI y ACSLS.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos DLT:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para DLT

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DLT1	40 GB	Formato sin comprimir sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT1C	Consulte la nota 1. 80 GB	Formato comprimido sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000

<b>Formato</b>	<b>Capacidad estimada</b>	<b>Descripción</b>
DLT10	10 GB	Formato sin comprimir sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT10C	Consulte la nota 1. 20 GB	Formato comprimido sólo con cartuchos CompacTape III Válido con unidades DLT4000, DLT7000 y DLT8000
DLT15	15 GB	Formato sin comprimir sólo con cartuchos CompacTape IIIxt Válido con unidades DLT4000, DLT7000 y DLT8000
DLT15C	Consulte la nota 1. 30 GB	Formato comprimido sólo con cartuchos CompacTape IIIxt Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20	20 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20C	Consulte la nota 1. 40 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT35	35 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT35C	Consulte la nota 1. 70 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT40	40 GB	Formato sin comprimir sólo con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT40C	Consulte la nota 1. 80 GB	Formato comprimido con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT2	80 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLTtape VS1
DLT2C	Consulte la nota 1. 160 GB	Formato comprimido, cuando se utilizan medios Quantum DLTtape VS1
DLT4	160 GB	Formato sin comprimir, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
DLT4C	Consulte la nota 1. 320 GB	Formato comprimido, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
SDLT Consulte la nota 2.	100 GB	Formato sin comprimir con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLTC Consulte la nota 2.	Consulte la nota 1. 200 GB	Formato comprimido con cartuchos Super DLT Tape 1 Válido con una unidad Super DLT
SDLT320 Consulte la nota 2.	160 GB	Formato sin comprimir, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT320C Consulte la nota 2.	Consulte la nota 1. 320 GB	Formato comprimido, cuando se utilizan medios Quantum SDLT I Válido con una unidad Super DLT
SDLT600	300 GB	Formato sin comprimir, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT
SDLT600C	Consulte la nota 1. 600 GB	Formato comprimido, cuando se utilizan medios SuperDLTtape-II Válido con una unidad Super DLT

Formato	Capacidad estimada	Descripción
DLTS4	800 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4
DLTS4C	Consulte la nota 1. 1,6 TB	Formato comprimido, cuando se utilizan medios Quantum DLT S4. Válido con una unidad DLT-S4
<p>Nota:</p> <ol style="list-style-type: none"> <li>1. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>2. IBM Spectrum Protect no admite una biblioteca que contenga unidades SDLT BRC (Backward Read Compatible) y SDLT NBRC (Non-Backward Read Compatible).</li> </ol>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información sobre capacidades estimadas, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:  
AB.CD2.E
- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este





```

.-PREFIX-----ADSM-----
>-----+-----+-----+-----+-----+----->
'-PREFIX-----+ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention-----60-----.  .-MOUNTWait-----60-----.
>-----+-----+-----+-----+-----+----->
'-MOUNTRetention-----minutos-'  '-MOUNTWait-----minutos-'

.-MOUNTLimit-----DRIVES-----
>-----+-----+-----+-----+-----+----->
'-MOUNTLimit-----+DRIVES-+'
      +-número-+
      '-0-----'

(1) (2)
.-DRIVEEncryption-----ALLOW-----
>-----+-----+-----+-----+-----+-----><
'-DRIVEEncryption-----+ON-----+'
      +-ALLOW-----+
      +-EXTernal-+
      '-OFF-----'

```

Notas:

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. Puede utilizar el cifrado de unidad solo en unidades Oracle StorageTek T10000B con un valor de formato de DRIVE, T10000B o T10000B-C, para unidades Oracle StorageTek T10000C con un valor de formato de DRIVE, T10000C o T10000C-C y para unidades Oracle StorageTek T10000D con un valor de formato de DRIVE, T10000D y T10000D-C.

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas ECARTRIDGE que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=ECARTRidge (Necesario)

Especifica que se asigna el tipo de dispositivo ECARTRIDGE a la clase de dispositivo. ECARTRIDGE indica que se asigna un tipo específico de dispositivo de cartucho de cinta (StorageTek) a esta clase de dispositivo.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

El valor predeterminado es NO.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de

calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades Oracle StorageTek T10000C y Oracle StorageTek T10000D.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Restricción: Si selecciona Sí, las únicas opciones que están disponibles para el parámetro FORMAT son:

- DRIVE
- T9840C
- T9840C-C
- T9840D
- T9840D-C
- T10000A
- T10000A-C
- T10000B
- T10000B-C
- T10000C
- T10000C-C
- T10000D
- T10000D-C

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

Importante: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos ECARTRIDGE:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840

Formato	Capacidad estimada	Descripción
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Notas:</p> <ul style="list-style-type: none"> <li>Algunos formatos utilizan la función de compresión por hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir).

Restricciones:

1. Solo puede utilizar el cifrado de unidad en las siguientes unidades:
  - Las unidades Sun StorageTek T10000B con un valor de formato DRIVE, T10000B o T10000B-C
  - Las unidades Sun StorageTek T10000C con un valor de formato DRIVE, T10000C o T10000C-C
  - Unidades Oracle StorageTek T10000D con un valor de formato DRIVE, T10000D o T10000D-C
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios de una sola grabación, varias lecturas (WORM). No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
3. Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

#### ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

#### ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

#### EXTERNAL



Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.


#### OFF



Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

## DEFINE DEVCLASS (Definir una clase de dispositivo FILE)

Utilice la clase de dispositivo FILE si utiliza archivos en el almacenamiento de disco magnético como volúmenes que almacenan datos secuencialmente (como en una cinta).

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo FILE no admite las bibliotecas EXTERNAL ni Remote Storage Manager.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS).

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
                                     .-MOUNTLimit----20-----
>--DEVType----FILE--+-----+----->
                                     '-MOUNTLimit----número-'

                                     .-MAXCAPacity----10G----.
>+-----+-----+----->
                                     '-MAXCAPacity----tamaño-'

                                     .-DIRectory---nombre_directorio_actual-.
>+-----+-----+----->
|                                     .-|-----|
|                                     v  |-----|
|                                     '-DIRectory---nombre_directorio-+-----'

                                     .-SHARed----No-----
>+-----+-----+-----<
|                                     '-SHARed----+No--+-'
|                                     '-Yes-'
```

### Parámetros

#### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.


#### DEVType=FILE (Necesario)

Especifica que se asigna el tipo de dispositivo FILE a la clase de dispositivo. FILE indica que se asigna un archivo a esta clase de dispositivo. Cuando el servidor necesita acceder a un volumen que pertenece a esta clase de dispositivo, abre un archivo y lee o graba datos del archivo.

Un archivo es un formato de medio de acceso secuencial.

#### MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. Este parámetro es opcional. El valor predeterminado es 20. Puede especificar un número de 0 a 4096.

 Sistemas operativos Windows Si la clase de dispositivo se comparte con un agente de almacenamiento (mediante la especificación del parámetro SHARED=YES), se definirán o se suprimirán unidades en función del valor de límite de montaje.



Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

#### MAXCAPacity

Especifica el tamaño máximo de los archivos de almacenamiento de datos definidos en una agrupación de almacenamiento de esta clase de dispositivo.

El valor del parámetro MAXCAPACITY también se utiliza como unidad de asignación cuando el desencadenante de espacio de la agrupación de almacenamiento crea volúmenes. El valor predeterminado son 10 GB (MAXCAPACITY=10G). El valor especificado debe ser menor o igual que el tamaño máximo admitido de un archivo en el sistema de archivos destino.



Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). Si está definiendo una clase de dispositivo FILE para los volúmenes de copia de seguridad de base de datos, especifique un valor para MAXCAPACITY que sea adecuado para el tamaño de la base de datos y que minimice el número de volúmenes de base de datos.


 Sistemas operativos AIX  Sistemas operativos Linux No defina un valor para MAXCAPACITY superior a 640M cuando este archivo se destine al soporte de CD REMOVABLEFILE. Un valor menor que un espacio utilizable del CD (650 MB) permite una coincidencia unívoca entre los archivos de la clase de dispositivo FILE y las copias que se encuentran en el CD.

#### DIRectory

Especifica las ubicaciones del directorio de los archivos utilizados en esta clase de dispositivo. Escriba comillas al principio y al final de la lista de directorios y utilice comas para separar los nombres de directorio individuales. Se permiten los caracteres especiales (por ejemplo, espacios en blanco) en los nombres de directorio. Por ejemplo, la lista de directorios "abc def,xyz" contiene dos directorios: abc def y xyz.



Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Linux El valor predeterminado es el directorio de trabajo actual del servidor que se utiliza en el momento en el que se emite el comando.



 Sistemas operativos Windows El valor predeterminado es el directorio de trabajo actual del servidor que se utiliza en el momento en el que se emite el comando. La información del registro de Windows se utiliza para determinar el directorio predeterminado.


Al especificar un nombre o nombres de directorio, identifica la ubicación donde el servidor coloca los archivos que representan los volúmenes de almacenamiento para esta clase de dispositivo.

Para el soporte de NetApp SnapLock (agrupaciones de almacenamiento con RECLAMATIONTYPE=SNAPLOCK, que van a utilizar esta clase de dispositivo), el directorio o directorios especificados con el parámetro DIRECTORY deben apuntar al directorio o directorios de los volúmenes NetApp SnapLock.

 Sistemas operativos AIX  Sistemas operativos Linux Al procesar el mandato, el servidor amplía el nombre o nombres de directorio especificados a forma completa, a partir del directorio raíz.

Si el servidor necesita asignar un volumen reutilizable, crea un nuevo archivo en uno de estos directorios. (El servidor puede elegir cualquiera de los directorios para crear nuevos volúmenes reutilizables.) Para los volúmenes reutilizables que se utilizan para almacenar datos del cliente, el archivo que crea el servidor tiene la extensión de nombre de archivo .bfs. Para los volúmenes reutilizables que se utilizan para almacenar datos de exportación, se utiliza la extensión .exp.

 Sistemas operativos AIX  Sistemas operativos Linux Por ejemplo, si define una clase de dispositivo con un directorio de tsmstor y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine /tsmstor/00566497.exp.

 Sistemas operativos Windows Por ejemplo, si define una clase de dispositivo con un directorio de c:\server y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine c:\server\00566497.exp.

Importante: Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Si el agente de almacenamiento no puede acceder al volumen FILE, puede hacer que las operaciones se reintenten en una ruta de sólo LAN o que fallen. Para obtener más información, consulte la descripción del parámetro DIRECTORY en el apartado DEFINE PATH (Definir una ruta).

Consejo: Si especifica varios directorios para una clase de dispositivo, asegúrese de que los directorios están asociados con sistemas de archivos separados. Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio agregando valores que representan el espacio que queda en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar inhabilitado. Si un desencadenante se inhabilita porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a habilitar el desencadenante con el siguiente comando: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

#### SHAREd

Especifica si esta clase de dispositivo FILE se compartirá entre el servidor y uno o más agentes de almacenamiento. Para prepararse para el compartimiento, se definirá de manera automática una biblioteca junto con un número de unidades correspondiente al valor del parámetro MOUNTLIMIT. Los nombres de unidad son el nombre de la biblioteca más un número comprendido entre 1 y el número de límite de montaje. Por ejemplo, si el nombre de la biblioteca es FILE y el límite de montaje está establecido en 4, las unidades se denominan FILE11, FILE12, FILE13 y FILE14.

Para obtener información acerca de los requisitos previos que deben aplicarse cuando el servidor y el agente de almacenamiento comparten el almacenamiento, consulte el sitio IBM® Support Portal for IBM Spectrum Protect.

## Ejemplo: definir una clase de dispositivo FILE con varios directorios

---

Definir una clase de dispositivo que especifica varios directorios.

#### Sistemas operativos AIX

```
define devclass multidir devtype=file
  directory=/usr/xyz,/usr/abc,/usr/uvw
```

#### Sistemas operativos Linux

```
define devclass multidir devtype=file
  directory=/opt/xyz,/opt/abc,/opt/uvw
```

#### Sistemas operativos Windows

```
define devclass multidir devtype=file
  directory=e:\xyz,f:\abc,g:\uvw
```

## Ejemplo: definir una clase de dispositivo FILE con capacidad de 50 MB

---

Definir una clase de dispositivo denominada PLAINFILES con un tipo de dispositivo FILE y con una capacidad máxima de 50 MB.

```
define devclass plainfiles devtype=file
  maxcapacity=50m
```

#### Sistemas operativos AIX Sistemas operativos Windows

## DEFINE DEVCLASS (Definir una clase de dispositivo GENERICTAPE)

---

Utilice la clase de dispositivo GENERICTAPE para las unidades de cinta admitidas por los controladores de dispositivo del sistema operativo.

Cuando se utiliza este tipo de dispositivo, el servidor no reconoce ningún tipo de dispositivo ni el formato de grabación de cartuchos. Dado que el servidor no reconoce el tipo de dispositivo, si se produce un error de E/S, la información de error será menos detallada en comparación con la información de error que se generaría para un tipo de dispositivo específico (por ejemplo, 8MM). Cuando defina dispositivos en el servidor, no combine varios tipos de dispositivos en el mismo tipo de dispositivo.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---



```

>>--DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary----nombre_biblioteca--DEVType----GENERICtape----->
. -MOUNTRetention----60-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-ESTCAPacity----tamaño-' '-MOUNTRetention----minutos-'
. -MOUNTWait----60----- . -MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<
'-MOUNTWait----minutos-' '-MOUNTLimit----DRIVES--'
+número+
'-0-----'

```

## Parámetros

### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

### LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

### DEVType=GENERICtape (Obligatorio)

Especifica que se asigna el tipo de dispositivo GENERICTAPE a la clase de dispositivo. GENERICTAPE indica que los volúmenes de esta clase de dispositivo se utilizan en las unidades de cintas que admite el controlador de dispositivo de cintas del sistema operativo.

El servidor reconoce que el medio se puede eliminar y que se pueden insertar más medios, sujetos a límites establecidos con el parámetro MOUNTLIMIT para la clase de dispositivo y el parámetro MAXSCRATCH para la agrupación de almacenamiento.

Los volúmenes de una clase de dispositivo con un tipo de dispositivo GENERICTAPE son volúmenes de acceso secuencial.

### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Especifique una capacidad adecuada a la unidad de cintas determinada que esté utilizándose.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este



```

.-MOUNTRetention----60----- .-MOUNTWait----60-----
>-----+-----+-----+----->
' -MOUNTRetention----minutos- ' -MOUNTWait----minutos- '

.-MOUNTLimit----DRIVES-----
>-----+-----+-----+----->
' -MOUNTLimit----+DRIVES--+
                +-número-+
                '-0-----'

                                (1) (2)
.-DRIVEEncryption----ALLOW-----
>-----+-----+-----+-----<
' -DRIVEEncryption----+ON-----+
                +-ALLOW----+
                +-EXTERNAL--+
                '-OFF-----'

```

**Notas:**

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas LTO que utiliza esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=LTO (Necesario)

Especifica que se asigna el tipo de dispositivo de cinta lineal abierta (LTO).

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

El valor predeterminado es NO.

Son posibles los siguientes valores:

**READWrite**

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

**WRITEOnly**

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

**No**

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: Se admite la protección de bloque lógico únicamente en IBM® LTO5 y unidades LTO6 soportadas.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. El campo puede contener uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Nota:

1. para utilizar medios WORM en una biblioteca, todas las unidades de la biblioteca deben admitir medios WORM.
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.)

#### FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

Cuando migre todas las unidades de dispositivos Ultrium a dispositivos Ultrium 2:

- Suprima todas las definiciones de unidades Ultrium existentes y las rutas asociadas a ellas.
- Defina las nuevas unidades y rutas Ultrium 2.

Si piensa en mezclar distintas generaciones de unidades y medios LTO, tenga en cuenta las siguientes restricciones.

Tabla 1. Posibilidades de lectura/grabación para diferentes generaciones de unidades LTO

Unidades	Soporte de primera generación	Soporte de segunda generación	Soporte de tercera generación	Soporte de cuarta generación	Soporte de quinta generación	Soporte de sexta generación
Primera generación	Lectura y grabación	n/d	n/d	n/d	n/d	n/d
Segunda generación	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d	n/d
Tercera generación <sup>1</sup>	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d
Cuarta generación <sup>2</sup>	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d
Quinta generación <sup>3</sup>	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d
Sexta generación <sup>4</sup>	n/d	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación

<sup>1</sup> En una biblioteca con una unidad de tercera generación, es necesario dar de baja todos los volúmenes reutilizables de primera generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de primera generación a sólo lectura.

<sup>2</sup> En una biblioteca con una unidad de cuarta generación, es necesario dar de baja todos los volúmenes reutilizables de segunda generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de segunda generación a sólo lectura.

<sup>3</sup> En una biblioteca con una unidad de quinta generación, todos los volúmenes reutilizables de tercera generación se tienen que dar de baja y todos los volúmenes de agrupación de almacenamiento de tercera generación se tienen que actualizar a sólo lectura.

<sup>4</sup> En una biblioteca con una unidad de sexta generación, es necesario dar de baja todos los volúmenes reutilizables de cuarta generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de cuarta generación a sólo lectura.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos LTO:

Tabla 2. Formato de grabación y capacidad estimada predeterminada para LTO

Formato	Capacidad estimada	Descripción
---------	--------------------	-------------

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
ULTRIUM	100 GB	Formato sin comprimir, utilizando cartuchos Ultrium
ULTRIUMC	Consulte la nota 200 GB	Formato comprimido, utilizando cartuchos Ultrium
ULTRIUM2	200 GB	Formato sin comprimir (estándar) con cartuchos Ultrium 2
ULTRIUM2C	Consulte la nota 400 GB	Formato comprimido con cartuchos Ultrium 2
ULTRIUM3	400 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 3
ULTRIUM3C	Consulte la nota 800 GB	Formato comprimido, con cartuchos Ultrium 3
ULTRIUM4	800 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 4
ULTRIUM4C	Consulte la nota 1,6 TB	Formato comprimido con cartuchos Ultrium 4
ULTRIUM5	1,5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 5
ULTRIUM5C	Consulte la nota 3.0 TB	Formato comprimido con cartuchos Ultrium 5
ULTRIUM6	2.5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 6
ULTRIUM6C	Consulte la nota 6.25 TB	Formato comprimido con cartuchos Ultrium 6
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información sobre capacidades estimadas, consulte Tabla 2.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El valor predeterminado es ALLOW (permitir). El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

Restricción: Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

#### ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

Nota: No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.)

#### ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

#### EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

#### OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.



## Ejemplo: definir una clase de dispositivo LTO


Definir una clase de dispositivo que se denomina LTOTAPE para una unidad LTO en una biblioteca denominada LTOLIB. El formato es ULTRIUM, el límite de montaje es 12, la retención de montaje es 5, el prefijo del volumen de cinta se denomina SMVOL y la capacidad estimada es 100 GB.

```
define devclass ltotape devtype=lto library=ltolib
format=ultrium mountlimit=12 mountretention=5
prefix=smvol estcapacity=100G
```

## DEFINE DEVCLASS (Definir una clase de dispositivo NAS)

Utilice la clase de dispositivo NAS cuando realice operaciones con el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad de servidores de archivos de almacenamiento conectado a red (NAS). La clase de dispositivo es para las unidades a las que da soporte el servidor de archivos NAS para copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo NAS no admite las bibliotecas EXTERNAL ni Remote Storage Manager.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo--DEVType----NAS-->
>--LIBRARY----nombre_biblioteca--MOUNTRetention----0----->
    .-MOUNTWait----60----- .-MOUNTLimit----DRIVES-----
>+-----+-----+-----+-----+-----+-----+----->
    '-MOUNTWait----minutos-' '-MOUNTLimit----+DRIVES+-'
                                   +-número+
                                   '-0-----'

>--ESTCAPacity----tamaño----->
    .-PREFIX----ADSM-----
>+-----+-----+-----+-----+-----+-----+----->
    '-PREFIX----+ADSM-----+'
        '-prefijo_volumen_cinta-'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

DEVType=NAS (Necesario)

Especifica que se asigna a la clase de dispositivo el tipo de dispositivo de almacenamiento conectado a red (NAS). El tipo de dispositivo NAS es para unidades conectadas a un servidor de archivos NAS y que este utiliza para hacer copia de seguridad de sistemas de archivos NAS.

#### LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta SCSI utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

#### MOUNTRetention=0 (Necesario)

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Cero (0) es el único valor admitido para clases de dispositivo con DEVType=NAS.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### ESTCAPacity (Obligatorio)

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.



## Ejemplo: definir una clase de dispositivo NAS

Definir una clase de dispositivo denominada NASTAPE para una unidad NAS en una biblioteca denominada NASLIB. El límite de montaje es DRIVES, la retención de montaje es 0, el prefijo del volumen de cinta se denomina SMVOL y la capacidad estimada es 200 GB.

```
define devclass nastape devtype=nas library=naslib
mountretention=0 mountlimit=drives
prefix=smvol estcapacity=200G
```

## DEFINE DEVCLASS (Definir una clase de dispositivo REMOVABLEFILE)

Utilice la clase de dispositivo REMOVABLEFILE para los dispositivos de medios extraíbles que están conectados como sistemas de archivos locales y extraíbles.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary----nombre_biblioteca--DEVType---REMOVABLEfile---->
  .-MAXCAPacity----espacio_restante-.
>--+-----+-----+----->
  '-MAXCAPacity----tamaño-----'
  .-MOUNTRetention----60----- .-MOUNTWait----60-----
>--+-----+-----+----->
  '-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'
  .-MOUNTLimit----DRIVES-----
>--+-----+-----+-----<
  '-MOUNTLimit----+DRIVES+-'
                    +-número+
                    '-0-----'
```

### Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)



Especifica el nombre del objeto de biblioteca definido que contiene las unidades de medios extraíbles que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=REMOVABLEfile (Necesario)

Especifica que se asigna el tipo de dispositivo REMOVABLEFILE a la clase de dispositivo. REMOVABLEFILE indica que los volúmenes de esta clase de dispositivo son archivos en medios locales extraíbles.

Los volúmenes de una clase de dispositivo con un tipo de dispositivo REMOVABLEFILE son volúmenes de acceso secuencial.



Utilice las herramientas del fabricante del dispositivo para dar formato (si es necesario) al medio y etiquetarlo. La etiqueta del medio debe cumplir las siguientes restricciones:

- La etiqueta no puede tener más de 11 caracteres.
- La etiqueta del volumen y el nombre del archivo que figura en el volumen deben coincidir con exactitud.
-  Sistemas operativos AIX  Sistemas operativos Windows El valor del parámetro MAXCAPACITY debe ser menor que la capacidad del medio.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes definidos en una agrupación de almacenamiento clasificada por esta clase de dispositivo. Este parámetro es opcional.

El parámetro MAXCAPACITY debe establecerse en un valor inferior a la capacidad del medio. Para los medios de CD, la capacidad máxima no debe exceder de 650 MB.

 Sistemas operativos AIX  Sistemas operativos Windows Dado que el servidor abre únicamente un archivo por medio físico extraíble, especifique una capacidad que permita que un archivo pueda utilizar totalmente la capacidad de su medio.

espacio\_restante

La capacidad máxima predeterminada es el espacio que queda en el medio después de utilizarlo por primera vez.

tamaño

Debe especificar este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes).

Por ejemplo, MAXCAPACITY=5M especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 MB. El valor más pequeño permitido es 1 MB (es decir, MAXCAPACITY=1M).

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## DEFINE DEVCLASS (Definir una clase de dispositivo SERVER)

Utilice la clase de dispositivo SERVER para utilizar los volúmenes de almacenamiento o los archivos archivados en otro servidor de IBM Spectrum Protect.

Si la protección de retención de datos se activa con el mandato SET ARCHIVERETENTIONPROTECTION, no podrá definir una clase de dispositivo de servidor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
--DEVType----SERVER--SERVERName----nombre_servidor----->
.-MAXCAPacity----500M---. .-MOUNTLimit----1-----.
>+-----+-----+-----+-----+-----+----->
'-MAXCAPacity----tamaño-' '-MOUNTLimit----número-'
.-MOUNTRetention----60-----.
>+-----+-----+-----+-----+-----+----->
'-MOUNTRetention----minutos-'
.-PREFIX----ADSM----- .
>+-----+-----+-----+-----+-----+----->
'-PREFIX----ADSM-----+-'
'-prefijo_volumen-'
.-RETRYPeriod----10----- .
>+-----+-----+-----+-----+-----+----->
'-RETRYPeriod----valor_reintento_(minutos)-'
.-RETRYInterval----30----- .
>+-----+-----+-----+-----+-----+-----><
'-RETRYInterval----retry_value_(seconds)-'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

DEVType=SERVER (Necesario)

Especifica una conexión remota que permite utilizar volúmenes virtuales.

SERVERName (Necesario)

Especifica el nombre del servidor. El parámetro SERVERNAME debe coincidir con un servidor definido.

MAXCAPacity

Especifica el tamaño máximo de los objetos creados en el servidor de destino; el valor predeterminado para este valor es 500M. Este parámetro es opcional.

500M

Especifica que la capacidad máxima es 500M (500 MB).

tamaño

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor mínimo permitido es 1 MB (MAXCAPACITY=1M).

MOUNTLimit

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino. Los intentos de acceder a más sesiones de las que indica el límite de montaje harán que el emisor de la solicitud tenga que esperar. Este parámetro es opcional. El valor predeterminado es 1. Puede especificar un número de 1 a 4096.

Los siguientes son los valores posibles:

1

Especifica que sólo se permite una sesión entre el servidor de origen y el servidor de destino.

número

Especifica el número de sesiones simultáneas entre el servidor de origen y el servidor de destino.

MOUNTRetention

Especifica el número de minutos que debe retenerse una conexión desocupada con el servidor de destino antes de que la conexión se cierre. Este parámetro es opcional. El valor predeterminado es 60. Puede especificar un número de 0 a 9999.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento

óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

#### RETRYPeriod

Especifica el período de reintento en minutos. El período de reintento es el intervalo de tiempo durante el cual el servidor debe intentar conectarse con un servidor destino, en caso de que se sospeche que existe un problema de comunicaciones. Este parámetro es opcional. Puede especificar un número de 0 a 9999. El valor predeterminado son 10 minutos.

#### RETRYInterval

Especifica el intervalo de reintentos en segundos. El intervalo de reintentos es la frecuencia con la que se realizan los intentos dentro de un período de tiempo específico. Este parámetro es opcional. Puede especificar un número de 1 a 9999. El valor predeterminado son 30 segundos.

## DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE)

Utilice el tipo de dispositivo VOLSAFE para trabajar con medios y unidades de la marca StorageTek VolSafe. Esta tecnología utiliza medios que no se pueden sobregabar. Por consiguiente, no emplee estos medios para copias de seguridad a corto plazo de archivos de cliente, la base de datos de servidor o cintas de exportación.

Restricciones:

1. No se admiten las bibliotecas con conexión NAS.
2. Los medios VolSafe y los medios de lectura/grabación deben estar en agrupaciones de almacenamiento independientes.
3. Incorpore cartuchos CHECKLABEL=YES en el mandato CHECKIN LIBVOLUME.
4. Etiquete cartuchos con OVERWRITE=NO en el mandato LABEL LIBVOLUME. Si los cartuchos VolSafe se etiquetan más de una vez, no se podrán grabar datos adicionales en ellos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----nombre_biblioteca--DEVType----VOLSAFE----->
      .-FORMAT----DRIVE-----.
>--WORM----Yes--+-----+----->
      '-FORMAT----+DRIVE----+'
          +-9840-----+
          +-9840-C----+
          +-T9840C----+
          +-T9840C-C--+
          +-T9840D----+
          +-T9840D-C--+
          +-T10000A---+
          +-T10000A-C-+
          +-T10000B---+
          +-T10000B-C-+
```

```

+-T10000C---+
+-T10000C-C-+
+-T10000D---+
'-T10000D-C-'

.MOUNTRetention-----60-----
>-----+-----+-----+-----+----->
'-ESTCAPacity-----tamaño-' '-MOUNTRetention-----minutos-'

.-PREFIX-----ADSM-----
>-----+-----+-----+-----+----->
'-PREFIX-----+ADSM-----+-'
'-prefijo_volumen-'

.-MOUNTWait-----60-----. .-MOUNTLimit-----DRIVES-----
>-----+-----+-----+-----+-----><
'-MOUNTWait-----minutos-' '-MOUNTLimit-----+DRIVES+-'
'-0-----'
+número+
'-0-----'

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas VolSafe que puede utilizar esta clase de dispositivo. Si alguna unidad de una biblioteca está activada para VOLSafe, todas las unidades de la biblioteca deben activarse para VOLSafe. Consulte la documentación de hardware para activar VolSafe en las unidades 9840 y T10000.

Para obtener información sobre cómo definir un objeto de biblioteca, consulte DEFINE LIBRARY (Definir una biblioteca).

DEVType=VOLSAFE (Necesario)

Especifica que se asigna el tipo de dispositivo VOLSAFE a la clase de dispositivo. La etiqueta de este tipo de cartucho puede sobregrabarse una vez, que es lo que hace IBM Spectrum Protect cuando graba el primer bloque de datos. Por consiguiente, es importante limitar el uso del mandato LABEL LIBVOLUME a una vez por volumen mediante el parámetro OVERWRITE=NO.

WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es obligatorio. El valor debe ser Sí.

Yes

Especifica que las unidades utilizan medios WORM.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Importante: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos VolSafe:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para medios Volsafe

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
9840	20 GB	Formato sin comprimir (estándar), cuando se utiliza un cartucho de 20 GB de 270 metros (885 pies) de cinta
9840-C	Consulte la nota 80 GB	Formato comprimido ampliado LZ-1 (4:1), cuando se utiliza un cartucho de 80 GB con 270 metros (885 pies) de cinta

Formato	Capacidad estimada	Descripción
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. El valor predeterminado es de 60 minutos. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es DRIVES. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

 Sistemas operativos AIX  Sistemas operativos Linux

## DEFINE DEVCLASS - servidor de medios de z/OS (Definir una clase de dispositivo para el servidor de medios de z/OS)

Utilice el comando DEFINE DEVCLASS para definir una clase de dispositivo para un tipo de dispositivo de almacenamiento. El servidor exige que se defina una clase de dispositivo para poder utilizar un dispositivo. Hay disponible un conjunto limitado de tipos de clase de dispositivo para los dispositivos a los que se accede mediante un servidor de medios de z/OS.

- DEFINE DEVCLASS (Definir una clase de dispositivo 3590 para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)
- DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS)

Tabla 1. Comandos relacionados con DEFINE DEVCLASS

Comando	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.





## LIBRARY (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

## DEVtype=3590 (Necesario)

Especifica que se asigna el tipo de dispositivo 3590 a la clase de dispositivo. 3590 indica que se asignan dispositivos de cartuchos de cinta IBM 3590 a esta clase de dispositivo.

Restricción: El servidor de medios de z/OS admite bloques de datos de 256 KB cuando la grabación se realiza en unidades de cinta 3590. Verifique que el hardware soporta esta posibilidad.

## FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3590

Formato	Descripción
3590B	Formato sin comprimir (básico)
3590C	Formato comprimido
3590E-B	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Formato comprimido, similar al formato 3590C
3590H-B	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Formato comprimido, similar al formato 3590C

Nota: Si el formato utiliza la función de compresión por hardware de la unidad de cintas, la capacidad real puede disminuir, dependiendo de la eficacia de la compresión.

## ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional. La capacidad estimada predeterminada para las cintas 3590 es de 9 GB.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

## PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

## MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este

parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

#### COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

#### Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

#### No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

#### RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

#### PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que dé soporte a la cinta 3590. Este parámetro es opcional. El nombre de unidad predeterminado es 3590. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

## DEFINE DEVCLASS (Definir una clase de dispositivo 3592 para el servidor de medios de z/OS)

---

Para utilizar un servidor de medios de z/OS para acceder a los dispositivos 3592, debe definir una clase de dispositivo 3592. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRARY----biblioteca_medio_zos--DEVType-----3592----->
.-FORMAT----Drive-----.-WORM-----No-----.
```

```

>----->
'-FORMAT-----+DRIVE---+' '-WORM-----+Yes-+-'
      +-3592-----+
      +-3592C---+
      +-3592-2---+
      +-3592-2C--+
      +-3592-3---+
      +-3592-3C--+
      +-3592-4---+
      '-3592-4C-'

.-ESTCAPacity----300G---.
>----->
'-ESTCAPacity----tamaño-'

.-PREFIX----ADSM------.
>----->
'-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention----60-----. .-MOUNTWait----60-----.
>----->
'-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'

.-MOUNTLimit----2------. .-COMpression----Yes-----.
>----->
'-MOUNTLimit----+DRIVES-+-' '-COMpression----+Yes-+-'
      +-número-+
      '-0-----'
      '-No--'

>----->
+-EXpiration----yyyddd-+
'-RETention----días-----'

.-PROtection----No------.
>----->
'-PROtection----+No-----+'
      +-Yes-----+
      '-Automatic-'

.-UNIT----3592------.
>-----<
'-UNIT----nombre_unidad-'

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=3592 (Necesario)

Especifica que se asigna el tipo de dispositivo 3592 a la clase de dispositivo.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3592

Formato	Descripción
3592	Formato sin comprimir (básico)
3592C	Formato comprimido
3592-2	Formato sin comprimir (básico), similar al formato 3592
3592-C	Formato comprimido, similar al formato 3592C

Formato	Descripción
3592-3	Formato sin comprimir (básico), similar al formato 3592
3592-3C	Formato comprimido, similar al formato 3592C
3592-4	Formato sin comprimir (básico), similar al formato 3592
3592-4C	Formato comprimido, similar al formato 3592C
DRIVE	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser distinta del valor que aparece en la lista.	

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades. Para un resultado óptimo, no mezcle las generaciones de unidades en la misma biblioteca. Si una biblioteca contiene una mezcla de generaciones, pueden darse problemas en los medios. Por ejemplo, las unidades de primera generación y segunda generación no pueden leer medios de tercera generación. Si es posible, actualice todas las unidades a 3592 de tercera generación. Si no puede actualizar todas las unidades a 3592 de tercera generación, debe utilizar una configuración especial.

#### WORM

Especifica si las unidades utilizan medios WORM (una sola grabación, varias lecturas). Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los valores siguientes:

Yes

Especifica que las unidades utilizan medios WORM.

No

Especifica que las unidades no utilizan medios WORM.

Consejo: El servidor de IBM Spectrum Protect no suprime automáticamente volúmenes reutilizables en las agrupaciones de almacenamiento WORM después de que se vacíen los volúmenes por caducidad u otros procesos. Para suprimir estos volúmenes y eliminarlos de las agrupaciones de almacenamiento WORM, debe utilizar el comando DELETE VOLUME. IBM Spectrum Protect no puede volver a utilizar volúmenes WORM grabados por el servidor y luego suprimidos de una agrupación de almacenamiento.

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

#### COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

#### RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

## PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

### No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

### Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

## Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

## UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cintas que dé soporte a la cinta 3592. Este parámetro es opcional. El valor predeterminado es 3592. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

## DEFINE DEVCLASS (Definir una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)

---

Para utilizar un servidor de medios de z/OS para acceder a los dispositivos StorageTek como, por ejemplo, StorageTek T9840 o T10000, debe definir una clase de dispositivo ECARTRIDGE. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```

>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--LIBRary----biblioteca_medio_zos--DEVType----ECARTridge---->
.-FORMAT-----DRIVE----- .-ESTCAPacity----9G-----
>-----+-----+-----+-----+-----+-----+----->
'-FORMAT-----+DRIVE-----+' '-ESTCAPacity----tamaño-'
      +-T9840C-----+
      +-T9840C-C--+
      +-T9840D-----+
      +-T9840D-C--+
      +-T10000A-----+
      +-T10000A-C+
      +-T10000B-----+
      +-T10000B-C+
      +-T10000C-----+
      +-T10000C-C+
      +-T10000D-----+
      +-T10000D-C-'

.-PREFIX----ADSM-----
>-----+-----+-----+-----+-----+-----+----->
'-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

.-MOUNTRetention----60----- .-MOUNTWait----60-----
>-----+-----+-----+-----+-----+-----+----->
'-MOUNTRetention----minutos-' '-MOUNTWait----minutos-'

.-MOUNTLimit----2----- .-COMpression----Yes-----
>-----+-----+-----+-----+-----+-----+----->
'-MOUNTLimit----+DRIVES--++' '-COMpression----+Yes+-'
      +-número+
      +-0-----+'
      '-No--'

>-----+-----+-----+-----+-----+-----+----->
+-EXpiration----yyyddd+
'-RETention----dias-----'

.-PROtection----No-----
>-----+-----+-----+-----+-----+-----+----->
'-PROtection----+No-----+'
      +-Yes-----+
      '-Automatic-'

.-UNIT----9840-----
>-----+-----+-----+-----+-----+-----+-----><
'-UNIT----nombre_unidad-'

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

DEVType=ECARTridge (Necesario)

Especifica que se asigna el tipo de dispositivo ECARTRIDGE a la clase de dispositivo. El tipo de dispositivo ECARTRIDGE es para las unidades StorageTek como, por ejemplo, StorageTek T9840 o T10000.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
---------	--------------------	-------------



Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. DRIVE es el valor predeterminado. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Nota:</p> <ul style="list-style-type: none"> <li>Algunos formatos utilizan una función de compresión del hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional. La capacidad estimada predeterminada es de 9 GB.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: **K** (KB), **M** (MB), **G** (GB) o **T** (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. El valor predeterminado es de 60 minutos. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la solicitud de montaje no se cumple en el tiempo especificado, la solicitud de montaje falla. Si un dispositivo se asigna satisfactoriamente y la solicitud de abrir dispositivo no se realiza en el tiempo especificado, la solicitud de abrir dispositivo finaliza y la solicitud de montaje falla.

Este parámetro es opcional. El valor predeterminado es 60. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 2.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

#### COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional. No existe un valor predeterminado.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

#### RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

#### PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

#### Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

#### UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que den soporte a las cintas ECARTRIDGE. Utilice el nombre de la unidad que representa el subconjunto de unidades de la biblioteca que están conectadas al sistema z/OS. Este parámetro es opcional. El valor predeterminado es 9840. El nombre de unidad puede tener hasta 8 caracteres.

## Ejemplo: definir una clase de dispositivo con el tipo de dispositivo ECARTRIDGE

Defina una clase de dispositivo denominada E1 con el tipo de dispositivo ECARTRIDGE y con una protección RACF activa para todos los volúmenes de cinta asignados a esta clase de dispositivo. Para esta clase de dispositivo se comprimen todos los datos. La clase de dispositivo es para una biblioteca del servidor de medios de z/OS denominada ZOSELIB.

```
define devclass e1 devtype=ecartridge library=zoselib compression=yes
  protection=yes
```

## DEFINE DEVCLASS (Definir una clase de dispositivo FILE para el servidor de medios de z/OS)

Para utilizar un servidor de medios de z/OS para acceder a los volúmenes de almacenamiento en los dispositivos de disco magnético, debe definir una clase de dispositivo FILE. En la definición de clase de dispositivo, especifique una biblioteca definida con el parámetro LIBTYPE=ZOSMEDIA.

Un volumen en esta clase de dispositivo es un conjunto de datos lineal VSAM (Virtual Storage Access Method) al que accede el servidor de medios de z/OS. Se pueden utilizar los volúmenes reutilizables con la clase de dispositivo y el servidor de medios de z/OS puede asignar dinámicamente el conjunto de datos lineal VSAM. No es necesario definir volúmenes para que el servidor utilice la clase de dispositivo. Si define volúmenes, establezca el calificador de alto nivel (HLQ) para que SMS reconozca la solicitud de asignación del servidor de medios de z/OS. Si utiliza volúmenes definidos, la función formatear volúmenes no se admite para el servidor al utilizar esta clase de dispositivo. El servidor de medios de z/OS utiliza una característica FormatWrite del gestor de medios DFSMS al llenar los volúmenes FILE.

Puede definir los volúmenes para la clase de dispositivo FILE utilizando el mandato DEFINE VOLUME. No obstante, el servidor de medios de z/OS no asigna espacio para un volumen definido hasta que se abra el volumen para su primer uso.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine DEVclass--nombre_clase_dispositivo----->
>--DEVType-----FILE--LIBRary-----nombre_biblioteca----->
. -MAXCAPacity-----10G----. .-PRIMARYalloc-----2600M--.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -MAXCAPacity-----tamaño- ' ' -PRIMARYalloc-----tamaño- '
. -SECONDARYalloc-----2600M--.
>+-----+-----+-----+-----+-----+-----+-----+----->
' -SECONDARYalloc-----tamaño- '
. -PREFIX-----ADSM-----
>+-----+-----+-----+-----+-----+-----+-----+----->
' -PREFIX-----prefijo_volumen_archivo- '
. -MOUNTLimit-----20-----
>+-----+-----+-----+-----+-----+-----+-----+-----><
' -MOUNTLimit-----número- '
```

### Parámetros

DEVType=FILE (Necesario)

Especifica que se asigna el tipo de dispositivo FILE a la clase de dispositivo.

LIBRary (Obligatorio)

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. servidor de medios de z/OS accede al almacenamiento de disco que utiliza esta clase de dispositivo y SMS controla dicho almacenamiento.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes de archivos definidos en una agrupación de almacenamiento de esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado son 10 GB (MAXCAPACITY=10G).

Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G).

PRIMARYalloc

Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen. Debe haber disponible suficiente espacio para satisfacer la cantidad de asignación primaria. La política SMS (Storage Management Subsystem) determina si se pueden utilizar varios volúmenes físicos para satisfacer la petición de asignación primaria.

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El tamaño mínimo es 100 KB (PRIMARYALLOC=100K). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G). El tamaño predeterminado es 2600 MB (PRIMARYALLOC=2600M). Todos los valores se redondean al siguiente múltiple superior de 256 K.

Para evitar espacio desaprovechado, la operación de asignación dinámica utiliza el menor de los valores especificados en los dos parámetros PRIMARYALLOC y MAXCAPACITY.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

#### SECONDARYalloc

Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado. El conjunto de datos de un volumen de archivos se amplía al tamaño establecido por el parámetro MAXCAPACITY y, a continuación, el volumen se marca como lleno.

Como la asignación secundaria de un conjunto de datos lineal no puede ocupar un volumen físico, tenga en cuenta el tamaño del volumen físico al seleccionar un tamaño de asignación secundaria. Por ejemplo, los volúmenes físicos de un modelo 3 de 3390 tienen aproximadamente 2,8 GB. Para garantizar que cada petición ocupe prácticamente un volumen físico completo, pero no más, utilice un tamaño de asignación secundario que sea un poco menor de 2,8 GB. Una cantidad de asignación secundaria de 2600 MB permite suficiente espacio para el conjunto de datos de volumen VSAM (VVDS), la etiqueta de volumen y la tabla de índice de volumen (VTOC).

Este parámetro es opcional. Especifique este valor como un entero seguido de K (KB), M (MB), G (GB) o T (TB). El valor mínimo es 0 KB (SECONDARYALLOC=0K). El valor predeterminado es 2600 MB. El valor máximo es 16384 GB. Excepto 0, todos los valores se redondean al siguiente múltiple superior de 256 K.

Si se especifica 0 (SECONDARYALLOC=0), el volumen de archivo no se puede ampliar más allá de la cantidad de asignación primaria.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

Si especifica un valor para el parámetro SECONDARYALLOCATION que no es 0, o si permite que el valor tome como valor predeterminado 2600M, la DATACLAS SMS asociada al identificador PREFIX (por ejemplo, calificador de alto nivel) debe tener especificado el atributo Extended Addressability (EA). Sin el atributo EA, la DATACLAS SMS limita la asignación del volumen FILE del conjunto de datos lineal VSAM a la ampliación primaria. (Consulte la descripción del parámetro PRIMARYALLOCATION). Con el conjunto de datos limitado al tamaño de asignación primario, el servidor de medios de z/OS no puede ampliar el conjunto de datos y el volumen se marca como FULL antes de que se alcance la capacidad máxima.

Restricción: Asegúrese de que los valores especificados para los parámetros PRIMARYALLOC y SECONDARYALLOC entren en los límites prácticos del dispositivo de almacenamiento. El servidor no puede comprobar si los valores exceden los límites prácticos del dispositivo y tampoco comprueba si los dos valores exceden conjuntamente el valor de MAXCAPACITY actual.

Consejo: Para rellenar los volúmenes cuando especifica un valor elevado para el parámetro MAXCAPACITY, especifique valores elevados para los parámetros PRIMARYALLOC y SECONDARYALLOC. Utilice tamaños de volumen de MVS mayores para reducir la posibilidad de anomalías de ampliación.

#### PREFIX

Especifica el calificador de nivel superior del nombre del conjunto de datos que se utiliza para asignar conjuntos de datos de volúmenes reutilizables. Para todos los volúmenes de archivos reutilizables creados en esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. El valor predeterminado es ADSM. La longitud máxima del prefijo, incluidos los puntos, es de 32 caracteres.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de conjunto de datos de volumen de archivo que utilice el prefijo predeterminado es

ADSM.B0000021.BFS.

Si tiene un convenio de denominación de conjunto de datos, utilice un prefijo que se ajuste a sus convenios de denominación. Por ejemplo, el siguiente valor es aceptable: `TSM.SERVER2.VSAMFILE`.

Si ejecuta varias instancias de servidor para IBM Spectrum Protect o Tivoli Storage Manager for z/OS Media, debe utilizar un valor exclusivo para el parámetro `PREFIX` en cada clase de dispositivo que defina.

#### MOUNTLimit

Especifica el número máximo de volúmenes `FILE` que se pueden abrir simultáneamente para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es 20.

Si utiliza dispositivos IBM® 3995 que emulan dispositivos 3390, establezca el valor en un número menor que el número de corrientes de entrada y salida concurrentes que pueden existir en el medio físico.

El valor que especifique en este parámetro es importante si existe una importante penalización al conmutar de un volumen a otro. Por ejemplo, la conmutación puede llevarse a cabo cuando se utilizan dispositivos IBM 3995 que emulan dispositivos 3390. El valor que especifique no puede ser mayor que el número de unidades físicas disponibles en el dispositivo.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro `MOUNTLIMIT` de una clase de dispositivo, la transacción fallará.

## DEFINE DOMAIN (Definir un nuevo dominio de políticas)

Utilice este comando para definir un nuevo dominio de políticas. Un dominio de políticas contiene juegos de políticas, clases de gestión y grupos de copia. Se asigna un cliente a un dominio de políticas. El juego de políticas `ACTIVE` del dominio de políticas determina las reglas para los clientes asignados al dominio. Las reglas controlan los servicios de archivado, copia de seguridad y gestión de espacio proporcionados para los clientes.

Debe activar un juego de políticas del dominio para que los clientes asignados al dominio de políticas puedan ejecutar operaciones de copia de seguridad, archivado o migración de archivos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine Domain--nombre_dominio----->
>--+-----+----->
  '-DESCRiption----descripción-'
  .-BACKRETention----30---.  .-ARCHRETention----365--.
>--+-----+----->
  '-BACKRETention----días-'  '-ARCHRETention----días-'
>--+-----+-----><
  |                               .-,-----|
  |                               v           |
  '-ACTIVEDESTination-----nombre_agrupación_datos_activos---+-'
```

### Parámetros

#### nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

#### DESCRIPTION

Especifica una descripción del dominio de políticas. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### BACKRETention

Especifica el número de días (a partir de la fecha en que quedaron inactivas las versiones de copia de seguridad) que deben retenerse las versiones de copia de seguridad de los archivos que ya no están en el sistema de archivos del cliente. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 30. El servidor utiliza el valor de retención de copia de seguridad para gestionar las versiones inactivas de archivos cuando se producen cualquiera de las condiciones siguientes:

- Un archivo se vuelve a vincular a una nueva clase de gestión, pero ni la nueva clase de gestión ni la clase de gestión predeterminada contienen un grupo de copia de seguridad.
- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia de seguridad.

#### ARCHRETention

Especifica el número de días (desde la fecha de archivado) que se han de retener las copias archivadas. Este parámetro es opcional. Puede especificar un entero entre el 0 y el 30000. El valor predeterminado es 365. El servidor utiliza el valor de retención de copias archivadas para gestionar las copias archivadas cuando se produce una de las condiciones siguientes:

- La clase de gestión a la que está vinculado un archivo ya no existe. La clase de gestión predeterminada no contiene un grupo de copia archivada.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está vinculado un archivo. La clase de gestión predeterminada no contiene un grupo de copia archivada.

#### ACTIVEDESTination

Este parámetro opcional especifica los nombres de las agrupaciones de datos activos que almacenan versiones activas de datos de copias de seguridad para nodos asignados al dominio. Puede especificar hasta diez agrupaciones de datos activos para un dominio, separadas por comas. No se pueden utilizar espacios entre los nombres.

Antes de que el servidor de IBM Spectrum Protect grabe datos en una agrupación de datos activos, verifica si el nodo que posee los datos se ha asignado a un dominio que tiene la agrupación de datos activos que se indica en la lista ACTIVEDESTINATION. Si el servidor comprueba que el nodo cumple estos criterios, los datos se almacenarán en la agrupación de datos activos. Si el nodo no cumple los requisitos, los datos no se almacenarán en la agrupación de datos activos. Si la función de grabación simultánea se utiliza para grabar datos en una agrupación de datos activos, el servidor verifica que el nodo cumpla los criterios durante las operaciones de copia de seguridad de clientes de archivado y copia de seguridad de IBM Spectrum Protect o de clientes de aplicación mediante la API de IBM Spectrum Protect. La verificación también se realiza cuando se copian datos activos con el mandato COPY ACTIVE DATA.

## Ejemplo: definir un dominio de políticas

Definir un dominio de políticas con el nombre PROG1 y la descripción Programming Group Domain. Se especificará que las copias archivadas deben retenerse 90 días cuando las clases de gestión o los grupos de copia archivada se suprimen y la clase de gestión predeterminada no contiene un grupo de copia archivada. También se especificará que las versiones de copia de seguridad deben retenerse 60 días cuando se suprimen las clases de gestión o los grupos de copia y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

```
define domain prog1
description="Programming Group Domain"
backretention=60 archretention=90
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DEFINE DOMAIN

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

## DEFINE DRIVE (Definir una unidad en una biblioteca)

Utilice este comando para definir una unidad. Cada unidad se asigna a una biblioteca, por lo que debe definirse la biblioteca antes de emitir este comando.





Si SERIAL=*número\_serie*, el número de serie especificado se utiliza para verificar que la ruta de la unidad es correcta cuando se define la ruta.

Nota: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.

#### ONLine

Especifica si la unidad está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES.

Yes

Especifica que la unidad está disponible para utilizarla.

No

Especifica que la unidad no está disponible para utilizarla.

#### ELEMeNT

Especifica la dirección del elemento de una unidad dentro de una biblioteca de cintas virtual (VTL) o SCSI. El servidor utiliza la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI o VTL de la unidad. El valor predeterminado es AUTODETECT.

Si ELEMENT=AUTODETECT, cuando se defina la ruta de la unidad, el servidor detecta automáticamente el número de elemento.


Para localizar la dirección del elemento para la configuración de la biblioteca, consulte la información del fabricante.

Restricción:

- El parámetro ELEMENT solo es válido para unidades de bibliotecas SCSI o VTL cuando el tipo de unidad no es una unidad NAS (SCSI conectado a red).
- Este parámetro no es efectivo si se emite desde un servidor cliente de biblioteca (es decir, si el tipo de biblioteca es SHARED).
- En función de las posibilidades de la biblioteca, puede que ELEMENT=AUTODETECT no esté admitido. En este caso, debe proporcionar la dirección de elemento.

#### ACS DRV ID

Especifica el ID de la unidad a la que se accede en una biblioteca SCSI. El identificador de unidad es un conjunto de números que indica la ubicación física de una unidad dentro de una biblioteca ACSLS. Este identificador de unidad debe especificarse como *a,l,p,d*, siendo *a* el ACSID, *l* el LSM (módulo de almacenamiento de biblioteca, *p* el número de panel y *d* el ID de unidad. El servidor necesita el identificador de unidad para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Consulte la documentación de StorageTek para obtener más detalles.

 Sistemas operativos Windows Restricción: Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

#### CLEANFREQuency

Especifica la frecuencia con que el servidor activa la limpieza de la unidad. Este parámetro es opcional. Para conseguir el grado de automatización de limpieza más completo para una biblioteca automatizada, deberá tener un cartucho limpiador que esté incorporado en el inventario de volúmenes de la biblioteca.

Si va a utilizar una limpieza basada en la biblioteca, se recomienda NONE cuando el tipo de biblioteca es compatible con esta función.

Este parámetro no es válido para las bibliotecas gestionadas externamente, por ejemplo las bibliotecas 3494 o las bibliotecas StorageTek que se gestionan bajo ACSLS.

Importante: Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades activada por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

NONE

Especifica que el servidor no hace el seguimiento de la limpieza de esta unidad. Puede utilizar este valor para las bibliotecas que tengan su propio sistema de limpieza automática.

ASNEEDED

Especifica que el servidor sólo carga la unidad con un cartucho limpiador dado de alta cuando una unidad notifica al controlador de dispositivo que es necesaria la limpieza.

El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo para ver información detallada de la unidad. Si ASNEEDED no está soportado, puede utilizar el valor gigabytes para la limpieza automática.

Con los controladores IBM 3592 e LTO, se recomienda la limpieza basada en la biblioteca. Si no se da soporte a la limpieza basada en la biblioteca, debe utilizarse ASNEEDED. Gigabytes no es recomendable.

Restricción: IBM Spectrum Protect no controla las unidades conectadas al servidor de archivos NAS. Si hay una unidad conectada sólo a un servidor de archivos NAS (no a un servidor o agente de almacenamiento), no especifique ASNEEDED como frecuencia de limpieza.

gigabytes

Especifica, en gigabytes, la cantidad de datos procesada en la unidad antes de que el servidor cargue la unidad con un cartucho limpiador. El servidor restablece el contador de gigabytes procesados cada vez que carga un cartucho limpiador en la unidad.

Importante: Cuando CLEANFREQUENCY=gigabyte, se puede producir la limpieza de unidad antes de que se alcance el valor de gigabytes, si la unidad notifica al controlador de dispositivo que es necesaria una limpieza.

Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si la información ofrece las recomendaciones para la frecuencia de limpieza en términos de horas de uso, convierta el valor en gigabytes realizando lo siguiente:

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor en gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.

Si se utiliza la frecuencia de limpieza recomendada por IBM® para las unidades de IBM, se garantiza que las unidades no se limpien más de lo necesario.


Para unidades IBM 3590, especifique un valor en gigabytes para la frecuencia de limpieza con el fin de garantizar que las unidades reciben la limpieza adecuada.

## Ejemplo: definir una unidad en la biblioteca

---

Definir una unidad en una biblioteca manual con el nombre de biblioteca LIB01 y el nombre de unidad DRIVE01.

```
define drive lib01 drive01
```

 Sistemas operativos AIX

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/rmt0
```

 Sistemas operativos Linux

```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=/dev/tsm SCSI/mt0
```

 Sistemas operativos Windows


```
define path server01 drive01 srctype=server desttype=drive  
library=lib01 device=mt3.0.0.0
```

## Ejemplo: definir una unidad en una biblioteca ACSLS

---

Definir una unidad en una biblioteca ACSLS con un nombre de biblioteca de ACSLIB y un nombre de unidad de ACSDRV1 .

```
define drive acslib acsdrv1 acsdrv1=1,2,3,4
```

 Sistemas operativos AIX

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/rmt0
```

 Sistemas operativos Linux

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=/dev/tsm SCSI/mt0
```

 Sistemas operativos Windows

```
define path server01 acsdrv1 srctype=server desttype=drive  
library=acslib device=mt3.0.0.0
```

## Ejemplo: definir una unidad en una biblioteca automática

---

Definir una unidad en una biblioteca automatizada cuyo nombre de biblioteca sea AUTO8MMLIB y el nombre de unidad DRIVE01.

```
define drive auto8mmlib drive01 element=82
```

### Sistemas operativos AIX

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/rmt0
```

### Sistemas operativos Linux

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=/dev/tmscsi/mt0
```

### Sistemas operativos Windows

```
define path server01 drive01 srctype=server desttype=drive
library=auto8mmlib device=mt3.0.0.0
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con DEFINE DRIVE

Comando	Descripción
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## DEFINE EVENTSERVER (Definir un servidor como el servidor de eventos)

---

Utilice este comando para identificar un servidor como el servidor de eventos.

Si define un servidor de eventos, un servidor de IBM Spectrum Protect puede enviar eventos a otro servidor de IBM Spectrum Protect que anotará dichos eventos.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

---

```
>>-DEFine EVENTSErVer--nombre_servidor-----<<
```

### Parámetros

---

nombre\_servidor (Obligatorio)

Especifica el nombre del servidor de eventos. El servidor que especifique ya deberá haberse definido con el comando DEFINE SERVER.

### Ejemplo: designar el servidor de eventos

---

Designar ASTRO como el servidor de eventos.

```
define eventserver astro
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DEFINE EVENTSERVER

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE EVENTSERVER	Suprime la referencia a un servidor de eventos.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
PING SERVER	Prueba las conexiones entre servidores..
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.
QUERY SERVER	Muestra información sobre servidores.

**Información relacionada:**

🔗 Anotaciones de eventos de empresa: anotaciones de eventos en otro servidor

## DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)

Utilice este comando para agregar un servidor como miembro de un grupo de servidores. También se puede agregar un grupo de servidores a otro grupo de servidores. Un grupo de servidores permite direccionar comandos a varios servidores especificando sólo el nombre del grupo de servidores.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

      .-|-----|
      v |
>>-DEFine GRPMEMber--nombre_grupo----nombre_miembro+----->>

```

### Parámetros

nombre\_grupo (Obligatorio)

Especifica el nombre del grupo de servidores al que se agregará el miembro.

nombre\_miembro (Obligatorio)

Especifica los nombres de los servidores o grupos que se agregan al grupo. Para especificar varios servidores y grupos, debe separarlos con comas y sin espacios intercalados. Los servidores o grupos de servidores deben estar ya definidos en el servidor.

### Ejemplo: definir un servidor para un grupo de servidores

Definir el servidor SANJOSE en el grupo de servidores CALIFORNIA.

```
define grpmember california sanjose
```

### Ejemplo: definir un servidor y un grupo de servidores para un grupo de servidores

Definir el servidor TUCSON y el grupo de servidores CALIFORNIA en el grupo de servidores WEST\_COMPLEX.

```
define grpmember west_complex tucson,california
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE GRPMEMBER

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.



Comando	Descripción
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## DEFINE LIBRARY (Definir una biblioteca)




Utilice este comando para definir una biblioteca. Una biblioteca es una colección de una o más unidades, y posiblemente dispositivos mecánicos, (dependiendo del tipo de biblioteca), los cuales se pueden utilizar para acceder a los volúmenes de almacenamiento.

A una biblioteca solo puede acceder un origen: un servidor de IBM Spectrum Protect o un transportador de datos. Sin embargo, las unidades de la biblioteca pueden accederse desde varios orígenes.

En el servidor pueden definirse los siguientes tipos de bibliotecas. Se proporcionan descripciones de sintaxis y parámetros para cada tipo.

- DEFINE LIBRARY (Definir una biblioteca 349X)
- DEFINE LIBRARY (Definir una biblioteca ACSLS)
- DEFINE LIBRARY (Definir una biblioteca externa)
- DEFINE LIBRARY (Definir una biblioteca FILE)
- DEFINE LIBRARY (Definir una biblioteca manual)
- DEFINE LIBRARY (Definir una biblioteca SCSI)
- DEFINE LIBRARY (Definir una biblioteca compartida)
- DEFINE LIBRARY (Definir una biblioteca VTL)
-  Sistemas operativos AIX  Sistemas operativos Linux DEFINE LIBRARY (Definir un tipo de biblioteca ZOSMEDIA)

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

 Sistemas operativos Windows

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los comandos DEFINE LIBRARY y UPDATE LIBRARY. Con este parámetro se evita tener que etiquetar previamente un conjunto de cintas. También es más eficaz que utilizar el comando LABEL LIBVOLUME, para lo que es necesario montar los volúmenes por separado. Si utiliza el parámetro AUTOLABEL, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows porque IBM Spectrum Protect no proporciona programas de utilidad para formatear o etiquetar estos tipos de soporte. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el comando label.

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE LIBRARY

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

Comando	Descripción
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## DEFINE LIBRARY (Definir una biblioteca 349X)

Utilice esta sintaxis para definir una biblioteca 349X.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType---349X----->
. -SHARed-----No----- . -RESEtDrives-----No----- .
>-----+-----+-----+-----+-----+-----+----->
' -SHARed-----+Yes-+- ' | (1) |
      '-No--'      '-RESEtDrives-----+Yes-+-'
                          '-No--'

. -AUTOLabel-----Yes----- .
>-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel-----+No-----+- '
      +-Yes-----+
      '-OVERWRITE- '

. -SCRATCHCAtegory-----301---- .
>-----+-----+-----+-----+-----+-----+----->
' -SCRATCHCAtegory-----número- '

. -PRIVATECAtegory-----300---- .
>-----+-----+-----+-----+-----+-----+----->
' -PRIVATECAtegory-----número- '

>-----+-----+-----+-----+-----+-----+-----><
' -WORMSCRatchcategory-----number- '

```



Notas:


1. El valor predeterminado para el parámetro RESEtDRIVES es condicional. Si el parámetro SHARed está definido como NO, el valor del parámetro RESEtDRIVES es NO. Si el parámetro SHARed está definido como YES, el valor del parámetro RESEtDRIVES es YES.

### Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.  
LIBType=349X (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica que la biblioteca es un servidor de datos de biblioteca de cintas IBM 3494 ó 3495.

 Sistemas operativos Windows Especifica que la biblioteca es un servidor de datos de biblioteca de cintas IBM 3494 o un gestor de biblioteca de sistema de cintas IBM que emula un servidor de datos de biblioteca de cinta 3494.

Restricción: Las bibliotecas IBM 3494 solamente admiten un tipo de dispositivo exclusivo a la vez.

SHAREd

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARED=NO es necesario si la biblioteca se controla mediante comandos pasados a través de un servidor de archivos NAS.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor sólo grabará encima de las etiquetas existentes si la etiqueta existente y también la etiqueta de código de barras todavía no se han definido en ninguna agrupación de almacenamiento del servidor o lista de histórico de volúmenes.

SCRATCHCategory

Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables en la biblioteca. Este parámetro es opcional. El valor predeterminado es 301 (se convierte en X'12D' en la biblioteca IBM 3494, pues ésta utiliza valores hexadecimales). Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca.

PRIVATECategory

Especifica el número de categoría para los volúmenes privados que deben montarse por nombre. Este parámetro es opcional. El valor predeterminado es 300 (este valor pasa a ser X'12C' en IBM 3494 porque utiliza valores hexadecimales). Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca.



WORMSCRatchcategory


Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables WORM en la biblioteca. Este parámetro es necesario si utiliza volúmenes WORM. Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca. Este parámetro sólo es válido cuando se utilizan volúmenes WORM 3592.

Restricción: Si no se ha definido WORMSCRATCHCATEGORY y el parámetro WORM está establecido en YES para la clase de dispositivo, aparece un mensaje de error durante la operación de montaje.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect , la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

## Ejemplo: definir una biblioteca 3494

Defina una biblioteca denominada `mi3494` con un número de categoría reutilizable 550, un número de categoría privado 600 y un número de categoría reutilizable de WORM igual a 400

```
define library my3494 libtype=349x scratchcategory=550
privatecategory=600 wormscratchcategory=400
```

## DEFINE LIBRARY (Definir una biblioteca ACSLS)

Utilice esta sintaxis para definir una biblioteca ACSLS.

### Clase de privilegio

 Sistemas operativos Windows Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.





Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

ACSID (Obligatorio)

Especifica el número de esta biblioteca StorageTek asignado por el ACSSA (Automatic Cartridge System System Administrator). Este un número puede ser del 0 al 126. Emita QUERY ACS en el sistema para obtener el número del identificador de la biblioteca. Este parámetro es necesario.

Para obtener más información, consulte la documentación de StorageTek.

## Ejemplo: definir una biblioteca ACSLS compartida

Definir una biblioteca denominada ACSLIB con el tipo de biblioteca ACSLS y el ACSID 1.

```
define library acslib libtype=acsls acsid=1 shared=yes
```

## DEFINE LIBRARY (Definir una biblioteca externa)

Utilice esta sintaxis para definir una biblioteca externa.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType---EXTernal----->
. -AUTOLabel-----Yes-----
>-----+-----+-----+-----<
'-AUTOLabel-----+No-----+-'
      +-Yes-----+
      '-OVERWRITE-'
```

## Parámetros



---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=EXtErnal (Obligatorio)

Especifica que la biblioteca está gestionada con un sistema de gestión de medios externos. Este tipo de biblioteca no da soporte a las definiciones de unidades con el comando DEFINE DRIVE. En su lugar, el sistema externo de gestión de medios identifica la unidad adecuada para las operaciones de acceso a los medios.

 Sistemas operativos AIX  Sistemas operativos Windows En un entorno IBM Spectrum Protect para redes de área de almacenamiento, este parámetro especifica que el software ACSLS (Automated Cartridge System Library Software) de StorageTek o el software de estación de biblioteca controla la biblioteca. Existe software, como Gresham EDT-DistribuTAPE, que permite que varios servidores puedan compartir la biblioteca. Las unidades de esta biblioteca no están definidas en IBM Spectrum Protect. ACSLS identifica la unidad para las operaciones de medios.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es YES.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.




OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.




## Ejemplo: definir una biblioteca EXTERNAL para una configuración SAN

---

Para una configuración de IBM Spectrum Protect para redes de área de almacenamiento, definir una biblioteca denominada EXTLIB de tipo EXTERNAL. Si utiliza Gresham Enterprise DistribuTAPE, el archivo ejecutable del gestor de bibliotecas externo se encuentra en el directorio siguiente:

-  Sistemas operativos AIX/usr/lpp/dtelm/bin/elm
-  Sistemas operativos Linux/opt/OMIdtelm/bin/elm
-  Sistemas operativos Windows:c:\program files\GES\EDT\bin\elm.exe

Si va a utilizar IBM® Tape System Library Manager, el archivo ejecutable del gestor de bibliotecas externo se encuentra en el directorio siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux/opt/IBM/TSLM/client/tsm/elm
-  Sistemas operativos Windows...\IBM\rmm\client\tsm\elm.exe

Para tener más información, consulte la publicación *IBM Tape System Library Manager User's Guide* en <http://www.ibm.com/support/docview.wss?uid=ssg1S7004001>.

## 1. Defina una biblioteca:

```
define library extlib libtype=external
```

## 2. Defina la ruta:

### Sistemas operativos AIX

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/usr/lpp/dtelm/bin/elm"
```

### Sistemas operativos Linux

```
define path server1 extlib srctype=server desttype=library  
externalmanager="/opt/OMIdtelm/bin/elm"
```

### Sistemas operativos Windows

```
define path server1 extlib srctype=server desttype=library  
externalmanager="c:\program files\GES\EDT\bin\elm.exe"
```

## DEFINE LIBRARY (Definir una biblioteca FILE)

---

Utilice esta sintaxis para definir una biblioteca FILE.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType---FILE----->  
.-SHAREd-----No-----.  
>-----<<  
'-SHAREd-----+Yes-+-'  
  '-No--'
```

### Parámetros

---

#### nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

#### LIBType=FILE (Obligatorio)

Indica que se crea una pseudobiblioteca para volúmenes de archivos secuenciales. Cuando emite el comando DEFINE DEVCLASS con los parámetros DEVTYPE=FILE y SHARED=YES, esto se produce automáticamente. Las bibliotecas FILE sólo son necesarias cuando se comparten volúmenes de archivos secuenciales entre el servidor y uno o más agentes de almacenamiento. Para utilizar las bibliotecas FILE es necesario el compartimento de bibliotecas. Las bibliotecas FILE compartidas se admiten para su uso en las configuraciones de copia de seguridad sin LAN solo. No puede utilizar una biblioteca FILE compartida en un entorno en el que se utiliza un gestor de biblioteca para gestionar los clientes de biblioteca.

#### SHARED

Especifica si esta biblioteca está compartida con otros servidores de IBM Spectrum Protect en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

#### YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

#### NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARED=NO es necesario si la biblioteca se controla mediante comandos pasados a través de un servidor de archivos NAS.

### Ejemplo: definir una biblioteca FILE compartida

---

Definir una biblioteca FILE con shared=yes.

```
define library file1 libtype=file shared=yes
```



- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

## Ejemplo: definir una biblioteca manual

Definir una biblioteca denominada MANUALMOUNT con el tipo de biblioteca MANUAL.

```
define library manualmount libtype=manual
```

## DEFINE LIBRARY (Definir una biblioteca SCSI)

Utilice esta sintaxis para definir una biblioteca SCSI.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType---SCSI----->
. -SHARed-----No----- . -RESEtDrives---No-----
>-+-----+-----+-----+-----+-----+-----+----->
' -SHARed-----+Yes-+- ' | (1) |
      '-No--'      '-RESEtDrives---+Yes-+-'
                                '-No--'

. -AUTOLabel---No-----
>-+-----+-----+-----+-----+-----+-----+----->
' -AUTOLabel---+No-----+- '
      +-Yes-----+
      '-OVERWRITE-'

. -RELABELSCRatch---No-----
>-+-----+-----+-----+-----+-----+-----+----->
' -RELABELSCRatch---+No-+- '
      '-Yes-'

. -SERial---AUTODetect-----
>-+-----+-----+-----+-----+-----+-----+-----><
' -SERial---+AUTODetect---+- '
      '-número_serie-'
```

Notas:

1. El valor predeterminado para el parámetro RESETDRIVES es condicional. Si el parámetro SHARED está definido como NO, el valor del parámetro RESETDRIVES es NO. Si el parámetro SHARED está definido como YES, el valor del parámetro RESETDRIVES es YES.

## Parámetros

---

### nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

### LIBType=SCSI (Obligatorio)

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, el servidor utiliza el dispositivo cambiador de medios.

### SHARED

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

#### YES

Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.

#### NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARED=NO es necesario si la biblioteca se controla mediante comandos pasados a través de un servidor de archivos NAS.

### AUTOlabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es NO.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

#### No

Especifica que el servidor no intenta etiquetar ningún volumen.

#### Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

### OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

### RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando este parámetro se define con el valor SÍ, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta de volumen existente. Este parámetro es opcional y está pensado para utilizarse con una biblioteca de cintas virtual (VTL).

Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede influir en el rendimiento.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

#### No



Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.


#### Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

### RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect , la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.
El dispositivo de biblioteca está conectado al dispositivo NAS, NDMP (protocolo de gestión de datos de red) accede indirectamente a él, y a las unidades de cintas solo se accede desde el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

SERIAL

Especifica el número de serie de la biblioteca que se está definiendo. Este parámetro es opcional. El valor predeterminado es AUTODETECT.

Si SERIAL=AUTODETECT, cuando defina la ruta a la biblioteca se utiliza como número de serie el indicado por la biblioteca.

Si SERIAL=número\_serie, el número que ha entrado se compara con el número detectado por el servidor.

Atención: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.




## Ejemplo: definir una biblioteca SCSI

Definir una biblioteca llamada SCSELIB con un tipo de biblioteca de SCSI.




```
define library scsilib libtype=scsi
```

La biblioteca requiere una ruta. El nombre de dispositivo para la biblioteca es:

-  Sistemas operativos AIX/dev/lb0
-  Sistemas operativos Linux/dev/tmsmscsi/lb0
-  Sistemas operativos Windows1b3.0.0.0

Defina la ruta:

 Sistemas operativos AIX

```
define path server1 scsilib srctype=server desttype=library  
device=/dev/lb0
```

 Sistemas operativos Linux

```
define path server1 scsilib srctype=server desttype=library  
device=/dev/tmsmscsi/lb0
```

 Sistemas operativos Windows

```
define path server1 scsilib srctype=server desttype=library  
device=1b3.0.0.0
```

## DEFINE LIBRARY (Definir una biblioteca compartida)

---

Utilice esta sintaxis para definir una biblioteca compartida.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType---SHARED----->  
>--PRIMarylibmanager---nombre_servidor-----<<
```

### Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType=SHARED (Obligatorio)

Especifica que la biblioteca está compartida con otro servidor de IBM Spectrum Protect por una red de área de almacenamiento (SAN) o una conexión SCSI dual con unidades de biblioteca.

Importante: Especifique este tipo de biblioteca cuando se defina la biblioteca en un cliente de bibliotecas.

PRIMarylibmanager

Especifica el nombre del servidor de IBM Spectrum Protect responsable del control del acceso a los recursos de biblioteca. Debe definir este servidor con el comando DEFINE SERVER para poder utilizarlo como gestor de bibliotecas. Este parámetro sólo es necesario y válido si LIBTYPE=SHARED.

### Ejemplo: definir una biblioteca compartida

---

En una SAN, defina una biblioteca denominada SHAREDTSM en un servidor de cliente de biblioteca denominado LIBMGR1

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

## DEFINE LIBRARY (Definir una biblioteca VTL)

---

Utilice esta sintaxis para definir una biblioteca que tenga un dispositivo cambiador de medios controlado por SCSI que se representa mediante una biblioteca de cintas virtual (VTL).

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-DEfINE LIBRARY--nombre_biblioteca--LIBType----VTL----->
  .-SHAREd----No----- . -RESEtDrives----No----- .
>+-----+-----+-----+-----+-----+-----+----->
  '-SHAREd----+Yes-+-' |                               (1) |
      '-No--'       '-RESEtDrives----+Yes-+-----'
                        '-No--'

  .-AUTOLabel----No----- .
>+-----+-----+-----+-----+-----+-----+----->
  '-AUTOLabel----+No-----+-'
                +-Yes-----+
                '-OVERWRITE-'

  .-RELABELSCRatch----Yes----- .
>+-----+-----+-----+-----+-----+-----+----->
  '-RELABELSCRatch----+No-+-'
                        '-Yes-'

  .-SERial----AUTODetect----- .
>+-----+-----+-----+-----+-----+-----+-----><
  '-SERial----+AUTODetect-+-'
                '-número_serie-'
```

### Notas:

1. El valor predeterminado para el parámetro RESEtDRIVES es condicional. Si el parámetro SHARED está definido como NO, el valor del parámetro RESEtDRIVES es NO. Si el parámetro SHARED está definido como YES, el valor del parámetro RESEtDRIVES es YES.

## Parámetros

### nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

### LIBType=VTL (Obligatorio)

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, el servidor utiliza el dispositivo cambiador de medios.

Si está definiendo una biblioteca VTL, el entorno no debe incluir ningún medio mixto y se deben definir rutas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento que utiliza la biblioteca. Si no se cumple alguna de estas características, el rendimiento general puede disminuir a los mismos niveles que el tipo de biblioteca SCSI; especialmente en momentos de gran actividad.

### SHAREd

Especifica si esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Este parámetro es necesario cuando se define una biblioteca para el gestor de bibliotecas.

#### YES



Especifica que esta biblioteca puede compartirse con otros servidores. Si especifica YES, el servidor gestor de bibliotecas monta los volúmenes según lo solicitan otros servidores y realiza un seguimiento de la asignación de unidades y volúmenes en otros servidores.


#### NO

Especifica que esta biblioteca no puede compartirse con otros servidores. SHARED=NO es necesario si la biblioteca se controla mediante comandos pasados a través de un servidor de archivos NAS.

### RESEtDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento. Si, por ejemplo, no hay disponible un agente de almacenamiento pero aún se conserva la ruta a una unidad, la reserva persistente permite al servidor romper la reserva del agente de almacenamiento y acceder a la unidad.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect , la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. NO es el valor predeterminado para una biblioteca definida con SHARED=NO. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente. YES es el valor predeterminado para una biblioteca definida con SHARED=YES.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente. NO es el valor predeterminado para una biblioteca definida con SHARED=NO.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional. El valor predeterminado es NO.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando se establece este parámetro en YES, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta del volumen existente.

Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede influir en el rendimiento.

Restricción: Si va a definir una biblioteca con unidades conectadas a un dispositivo de almacenamiento adjunto de red (NAS), debe utilizar el mandato LABEL LIBVOLUME para etiquetar los volúmenes para esta biblioteca.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar. YES es el valor predeterminado.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

#### SERIAL

Especifica el número de serie de la biblioteca que se está definiendo. Este parámetro es opcional. El valor predeterminado es AUTODETECT.

Si SERIAL=AUTODETECT, cuando defina la ruta a la biblioteca se utiliza como número de serie el indicado por la biblioteca.

Si SERIAL=*número\_serie*, el número que ha entrado se compara con el número detectado por el servidor.

Atención: En función de las posibilidades del dispositivo, puede que SERIAL=AUTODETECT no esté admitido. En este caso, el número de serie se notifica como en blanco.




## Ejemplo: definir una biblioteca VTL

---


Definir una biblioteca denominada VTLLIB cuyo tipo de biblioteca sea VTL.

```
define library vtllib libtype=vtl
```

La biblioteca requiere una ruta. El nombre de dispositivo para la biblioteca es:

-  Sistemas operativos AIX/dev/lb0
-  Sistemas operativos Linux/dev/tmscsi/lb0
-  Sistemas operativos Windowslb3.0.0.0


Defina la ruta:

 Sistemas operativos AIX

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/lb0
```

 Sistemas operativos Linux

```
define path server1 vtllib srctype=server desttype=library  
device=/dev/tmscsi/lb0
```

 Sistemas operativos Windows

```
define path server1 vtllib srctype=server desttype=library  
device=lb3.0.0.0
```

 Sistemas operativos AIX  Sistemas operativos Linux

## DEFINE LIBRARY (Definir un tipo de biblioteca ZOSMEDIA)

---

Utilice esta sintaxis para definir una biblioteca que represente un recurso de almacenamiento TAPE o FILE mantenido por Tivoli Storage Manager for z/OS Media.

Defina una biblioteca de tipo ZOSMEDIA cuando desee que la biblioteca esté gestionada exclusivamente por Tivoli Storage Manager for z/OS Media. La biblioteca aparece para el servidor de IBM Spectrum Protect como un dispositivo de almacenamiento lógico que no requiere definiciones de DRIVE. Se necesita una definición de PATH para el servidor y los agentes de almacenamiento que necesitan acceso al recurso de biblioteca ZOSMEDIA.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-DEFine LIBRary--nombre_biblioteca--LIBType-----ZOSMEDIA-----<<
```

### Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir.

LIBType=ZOSMEDIA (Obligatorio)

Especifica que el tipo de biblioteca es ZOSMEDIA, que representa un recurso de almacenamiento TAPE o FILE mantenido por Tivoli Storage Manager for z/OS Media.

## Ejemplo: configurar una biblioteca ZOSMEDIA

---

El siguiente ejemplo muestra los pasos necesarios para definir y configurar una biblioteca zosmedia. La configuración incluye estos componentes:

- Un servidor denominado sahara
- Una biblioteca definida como de tipo zosmedia denominada zebra
- Un servidor de medios de z/OS denominado oasis
- Un agente de almacenamiento denominado mirage

Defina una biblioteca denominada ZEBRA con un tipo de biblioteca ZOSMEDIA:

```
define library zebra libtype=zosmedia
```

Defina el servidor de medios de z/OS:

```
define server oasis serverpassword=sanddune  
hladdress=9.289.19.67 lladdress=1777
```

El servidor requiere una ruta al recurso de biblioteca gestionado por Tivoli Storage Manager for z/OS Media:

```
define path sahara zebra srctype=server  
desttype=library zosmediaserver=oasis
```

El agente de almacenamiento requiere una ruta al recurso de biblioteca gestionado por Tivoli Storage Manager for z/OS Media:

```
define path mirage zebra srctype=server  
desttype=library zosmediaserver=oasis
```

## DEFINE MACHINE (Definir información de máquina para la recuperación ante siniestro)

---

Utilice este comando para guardar la información de recuperación ante siniestro para una máquina servidor o nodo cliente. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

---

```
>>-DEFine MACHine--nombre_máquina----->  
>--+-----+--+-----+----->  
  '-DESCRiption----descripción-'  '-BUilding--==edificio-'  
>--+-----+--+-----+----->  
  '-FLoor----planta-'  '-ROom----sala-'  
  
  .-PRIority----50-----  .-ADSMServer--==No-----.  
>--+-----+--+-----+-----><  
  '-PRIority----número--'  '-ADSMServer--==+No--+-'  
                               '-Yes-'
```

### Parámetros

---

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina. El nombre puede estar formado por 64 caracteres como máximo.

DESCRiption

Especifica la descripción de una máquina. Este parámetro es opcional. El texto puede tener hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

BUilding

Especifica el edificio donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Floor

Especifica la planta donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Room

Especifica la sala donde está la máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Priority

Especifica la prioridad de restauración de la máquina en forma de un entero del 1 al 99. La prioridad más alta es 1. Este parámetro es opcional. El valor predeterminado es 50.

ADSMServer

Especifica si la máquina es un servidor de IBM Spectrum Protect. Solo puede definirse una máquina como servidor de IBM Spectrum Protect. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Esta máquina no es un servidor de IBM Spectrum Protect.

Yes

Esta máquina es un servidor de IBM Spectrum Protect.

## Ejemplo: definir la información de recuperación ante siniestro de una máquina

Definir una máquina denominada DISTRICT5 y especificar un nombre de ubicación, de planta y de sala. Esta máquina contiene datos esenciales y tiene la prioridad más alta.

```
define machine district5 building=101 floor=27  
room=datafacilities priority=1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE MACHINE

Comando	Descripción
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.
UPDATE MACHINE	Cambia la información para una máquina.

## DEFINE MACHNODEASSOCIATION (Asociar un nodo a una máquina)

Utilice este mandato para asociar nodos cliente a una máquina. Durante la recuperación ante siniestro, puede utilizar esta información para identificar los nodos cliente que residían en las máquinas destruidas.

La máquina debe definirse y los nodos registrarse en IBM Spectrum Protect.

Para recuperar la información, emita el mandato QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Un nodo permanece asociado a una máquina mientras no se suprima el nodo, la máquina o la asociación.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DEFine MACHNODEAssociation--nombre_máquina----->  
.,-----.
```

```

      v
>-----nombre_nodo-----><

```

## Parámetros

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina.

nombre\_nodo (Obligatorio)

Especifica los nombres de nodo. Únicamente se puede asociar un nodo a una máquina. Para especificar varios nodos, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

## Ejemplo: asociar un nodo a una máquina

Asociar el nodo denominado ACCOUNTSPAYABLE a la máquina denominada DISTRICT5.

```
define machnodeassociation district5 accountspayable
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE MACHNODEASSOCIATION

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
DELETE MACHNODEASSOCIATION	Suprime la asociación entre una máquina y un nodo.
QUERY MACHINE	Muestra información sobre máquinas.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.

## DEFINE MGMTCLASS (Definir una clase de gestión)

Utilice este comando para definir una nueva clase de gestión de un juego de políticas. Para que los clientes puedan utilizar la nueva clase de gestión, debe activar el juego de políticas que contiene la nueva clase.

Puede definir una o más clases de gestión para cada juego de políticas de un dominio de políticas. Una clase de gestión puede contener un grupo de copia de seguridad, un grupo de copia archivada, o ambos. El usuario de un nodo cliente puede seleccionar cualquier clase de gestión del juego de políticas activo o utilizar la clase de gestión predeterminada.

Atención: El mandato DEFINE MGMTCLASS no se ejecutará correctamente si se especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la clase de gestión.

## Sintaxis

```

>>-DEFine Mgmtclass--domain_name--policy_set_name--class_name--->
      .-SPACEMGTEchnique-----NONE-----
>+-----+----->
      '-SPACEMGTEchnique-----+--AUTOMATIC--'
          +-SElective+
          '-NONE-----'

      .-AUTOMIGNOnuse-----0----.
>+-----+----->
      '-AUTOMIGNOnuse-----días-'

```

```

.-MIGREQUIRESBkup-----Yes----- .
>-----+----->
'-MIGREQUIRESBkup-----+Yes--+-'
'-No--'

.-MIGDESTination-----SPACEMGPOOL----- .
>-----+----->
'-MIGDESTination-----nombre_agrupación-'

>-----+-----><
'-DESCRiption-----descripción-'

```

## Parámetros

### nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

### nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas al que pertenece la clase de gestión. No puede definir una clase de gestión en el juego de políticas ACTIVE.

### nom\_clase (Necesario)

Especifica el nombre de la nueva clase de gestión. La longitud máxima de este nombre es de 30 caracteres. No puede utilizar *default* ni *grace\_period* como nombre de clase.

### SPACEMGTECHnique

Especifica si un archivo que utiliza esta clase de gestión se puede seleccionar para una operación de migración. Este parámetro es opcional. El valor predeterminado es NONE. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

#### AUTOMATIC

Especifica que se puede seleccionar el archivo para la migración automática y para la migración selectiva.

#### SElective

Especifica que el archivo se puede seleccionar únicamente para la migración selectiva.

#### NONE

Especifica que el archivo no se puede seleccionar para la operación de migración.

### AUTOMIGNOnuse

Especifica el número de días que deben transcurrir desde que se accedió por última vez a un archivo hasta que pueda seleccionarse para la migración automática. Este parámetro es opcional. El valor predeterminado es 0. Si SPACEMGTECHNIQUE no es AUTOMATIC, el servidor no tiene en cuenta este atributo. Puede especificar un entero en el rango 0 – 9999.

Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

### MIGREQUIRESBkup

Especifica si debe existir una versión de copia de seguridad de un archivo antes de que pueda migrarse un archivo. Este parámetro es opcional. El valor predeterminado es YES. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

#### Yes

Especifica que debe existir una versión de copia de seguridad.

#### No

Especifica que la versión de copia de seguridad es opcional.

### MIGDESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los archivos migrados mediante clientes de IBM Spectrum Protect for Space Management. Este parámetro sólo es efectivo para los clientes IBM Spectrum Protect for Space Management, y no es efectivo para los clientes de copia de seguridad/archivado ni los clientes de aplicación. El valor predeterminado es SPACEMGPOOL.

La elección del destino puede depender de factores tales como los siguientes:

- El número de nodos cliente que se migran a la agrupación de almacenamiento. Cuando hay un gran número de archivos de usuario que se almacenan en la misma agrupación de almacenamiento, puede producirse la contención de volúmenes cuando los usuarios intentan migrar archivos a la agrupación de almacenamiento o recuperarlos de ésta.
- La velocidad con la que se deben recuperar los archivos. Si necesita acceso inmediato a las versiones migradas, puede especificar una agrupación de almacenamiento de disco como destino.

El mandato falla si especifica una agrupación de almacenamiento de copia o una agrupación de datos activos como destino.



## DESCRiption

Especifica una descripción de la clase de gestión. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

## Ejemplo: definir una clase de gestión para un juego de políticas y un dominio de políticas específicos

Defina una clase de gestión que se denomina MCLASS1 para el conjunto de políticas SUMMER en el dominio de políticas PROG1. Para los clientes IBM Spectrum Protect for Space Management, se permitirá la migración automática y la migración selectiva, y los archivos migrados se almacenarán en la agrupación de almacenamiento SMPPOOL. Agregue la descripción, "Technical Support Mgmt Class."

```
define mgmtclass prog1 summer mclass1
spacemgtechnique=automatic migdestination=smpool
description="technical support mgmt class"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE MGMTCLASS

Comando	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

## DEFINE NODEGROUP (Definir un grupo de nodos)

Utilice este comando para definir un grupo de nodos. Un *grupo de nodos* es un grupo de nodos cliente a los que se trata como si fuesen una única entidad. Un nodo puede ser un miembro de uno o más grupos de nodos.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

## Sintaxis

```
>>-DEFine NODEGrouP--nombre_grupo----->
>--+-----+-----><
  '-DESCRiption----descripción-'
```

## Parámetros

### nombre\_grupo

Especifica el nombre del grupo de nodos que desea crear. La longitud máxima del nombre es de 64 caracteres. El nombre especificado podría no ser igual al de cualquier otro nombre de nodo de cliente existente.

### DESCRiption

Especifica una descripción del grupo de nodos. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

## Ejemplo: definir un grupo de nodos

Definir un grupo de nodos denominado `group1`.

```
define nodegroup group1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE NODEGROUP

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## DEFINE NODEGROUPMEMBER (Definir un miembro de grupo de nodos)

Utilice este comando para agregar un nodo cliente a un grupo de nodos. Un *grupo de nodos* es un grupo de nodos cliente a los que se trata como si fuesen una única entidad.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

## Sintaxis

```
DEFINE NODEGROUPMEMBER nombre_grupo [nombre_nodo]+
```

## Parámetros

`nombre_grupo`

Especifica el nombre del grupo de nodos al que desea agregar un nodo cliente.

`nombre_nodo`

Especifica el nombre del nodo cliente que desea agregar al grupo de nodos. Puede especificar uno o más nombres. Separe varios nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín al especificar varios nodos.

## Ejemplo: definir miembros de grupo de nodos

Definir dos miembros, `node1` y `node2`, para un grupo de nodos, `group1`.

```
define nodegroupmember group1 node1,node2
```

## Comandos relacionados



Tabla 1. Comandos relacionados con DEFINE NODEGROUPMEMBER

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.




## DEFINE PATH (Definir una ruta)

Utilice este mandato para definir una ruta para el acceso de un origen a un destino. Deben definirse un origen y un destino antes de definir una ruta. Por ejemplo, si se necesita una ruta entre un servidor y una unidad, primero deberá emitir el comando DEFINE DRIVE y, a continuación, el comando DEFINE PATH. Después de haber emitido el comando DEFINE DRIVE, debe especificarse una ruta con el fin de que el servidor pueda utilizar la unidad.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de ruta.

- DEFINE PATH (Definir una ruta cuando el destino es una unidad)
- DEFINE PATH (Definir una ruta cuando el destino es una biblioteca)
-  Sistemas operativos AIX  Sistemas operativos Linux DEFINE PATH (Definir una ruta cuando el destino es una biblioteca ZOSMEDIA)

Si quiere obtener información detallada y actual sobre soporte de dispositivos, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

## Comandos relacionados

Tabla 1. Mandatos relacionados con DEFINE PATH

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## DEFINE PATH (Definir una ruta cuando el destino es una unidad)

Utilice esta sintaxis cuando defina una ruta a una unidad.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine PATH--nombre_origen--nombre_destino----->
>--SRCType-----+DATAMover-+-+-----+----->
      '-SERVer----'   '-AUTODetect-----+No-+-'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY----nombre_biblioteca----->
>----DEVIce-----+nombre_dispositivo+----->
      '-FILE-----'
      .-GENERICTAPE-----No----- .-ONLine-----Yes-----
>--+-----+-----+-----+----->
      '-GENERICTAPE-----+Yes-+-'   '-ONLine-----+Yes-+-'
                          '-No--'   '-No--'
      .-DIRectory-----nombre_directorio_actual-.
>--+-----+-----+-----+----->
      |           .-',-----'
      |           v           |
      | '-DIRectory-----nombre_directorio-+-----'
```

### Parámetros

nombre\_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre\_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

AUTODetect

Especifica si se actualiza automáticamente en la base de datos el número de serie de una unidad en el momento en que se defina la ruta. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente. El número de serie se sigue comparando con lo que ya hay en la base de datos correspondiente al dispositivo. El servidor emite un mensaje si existe una discrepancia.

Yes

Especifica que el número de serie no se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica al servidor.

Importante:

1. Si no ha establecido el número de serie al definir la unidad, el servidor siempre intenta detectar el número de serie, y AUTODETECT toma el valor YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. El uso de AUTODETECT=YES en este comando significa que el número de serie establecido en la definición de unidad se actualiza con el número de serie detectado.
3. Si establece DESTTYPE=DRIVE y AUTODETECT=YES, el número de elemento de la unidad que se encuentra en la base de datos cambia automáticamente para reflejar el mismo número de elemento que corresponde al número de serie de esa unidad. Esto se aplica a las unidades de una biblioteca SCSI. Para obtener más información acerca del número de elemento, consulte DEFINE DRIVE.
4. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

DESTType=DRive (Obligatorio)

Especifica que el destino es una unidad. Cuando el destino es una unidad, debe especificar un nombre de biblioteca.

**LIBRARY**

Especifica el nombre de la biblioteca a la que se asigna la unidad. La biblioteca debe estar ya definida en el servidor. Si la ruta es de un transportador de datos NAS a una biblioteca, la biblioteca debe tener el LIBTYPE establecido en SCSI, 349X o ACSLS.

**DEVICE**

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.





 Sistemas operativos AIX  Sistemas operativos Windows El origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos AIX /dev/mt3  Sistemas operativos Windows mt3
De un agente de almacenamiento (en un sistema Windows) a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM® System Storage Serie N: rst01





 Sistemas operativos Linux El origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 2 para obtener ejemplos.


Tabla 2. Ejemplos de nombres de dispositivos


De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	/dev/tmscsi/mt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	/dev/tmscsi/mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM System Storage Serie N: rst01

Importante:

-  Sistemas operativos AIX  Sistemas operativos Linux Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf.  Sistemas operativos Windows Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo c:\winnt\ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el comando SYSCONFIG. Utilice este comando para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```

 Sistemas operativos Windows GENERICTAPE

 Sistemas operativos Windows Indica si la unidad de cintas que se va a utilizar es un tipo de clase de dispositivo GENERICTAPE. Si el dispositivo es una unidad de cintas y no recibe soporte de IBM Spectrum Protect, pero es compatible para el sistema operativo Windows, puede utilizarlo con el formato de cinta genérico. Para utilizar la unidad, especifique GENERICTAPE=Yes al definir una ruta a la unidad. El valor predeterminado es No. Los valores posibles son:

Yes

Indica que la unidad de cintas que se va a utilizar es un tipo de clase de dispositivo GENERICTAPE.

No

Indica que la unidad de cintas que se va a utilizar no es un tipo de clase de dispositivo GENERICTAPE.

#### ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Por ejemplo, si la ruta desde un transportador de datos a una unidad está en línea, pero el transportador de datos o la unidad está fuera de línea, no puede utilizar la ruta.

#### DIRectory

Especifique las ubicaciones en las que el agente de almacenamiento lee y graba los archivos que representan volúmenes de almacenamiento para la clase de dispositivo FILE asociada a la biblioteca FILE. El parámetro DIRECTORY también se utiliza para los dispositivos de tipo REMOVABLEFILE. Para los dispositivos REMOVABLEFILE, el parámetro DIRECTORY proporciona información para el servidor (no un agente de almacenamiento) junto con el parámetro DRIVE para describir acceso al dispositivo. Este parámetro es opcional.


Para una ruta desde un agente de almacenamiento a un dispositivo FILE, este parámetro sólo es válido cuando se cumplen *todas* las condiciones siguientes:

- El tipo de origen es SERVER (lo que significa que se ha definido como servidor un agente de almacenamiento en este servidor).
- El nombre de origen es el nombre del agente de almacenamiento y *no* del servidor.
- El destino es una unidad lógica que forma parte de una biblioteca FILE creada cuando se definió la clase de dispositivo.

Si ha especificado varios directorios para la clase de dispositivo asociada a la biblioteca FILE, debe especificar el mismo número de directorios para cada ruta de la biblioteca FILE. No cambie o mueva los directorios existentes en el servidor que está utilizando el agente de almacenamiento, para que la clase de dispositivo y la ruta permanezcan sincronizadas. Está permitido agregar directorios. Si se especifica un número no coincidente de directorios, se puede producir una anomalía de tiempo de ejecución.

El valor predeterminado de DIRECTORY es el directorio del servidor en el momento en que se emite el mandato. El registro de Windows se utiliza para ubicar el valor predeterminado.

Utilice un convenio de denominación que le permita asociar el directorio a una unidad física determinada. Esto ayuda a garantizar que la configuración es válida para compartir la biblioteca FILE entre el servidor y el agente de almacenamiento. Si el agente de almacenamiento se encuentra en un sistema Windows, utilice un nombre del convenio de denominación universal (UNC). Cuando el agente de almacenamiento no dispone de permiso para acceder al almacenamiento remoto, experimenta anomalías de montaje.

 Sistemas operativos Windows La cuenta asociada con el servicio del agente de almacenamiento debe ser una cuenta del grupo de administradores local o una cuenta del grupo de administradores del dominio. Si la cuenta está en el grupo de administradores local, el identificador de usuario y la contraseña deben corresponderse con los de la cuenta con autorización para acceder al almacenamiento, tal como fueron proporcionados por el sistema que administra los elementos compartidos remotos. Por ejemplo, si un servidor SAMBA proporciona acceso al almacenamiento remoto, el identificador de usuario y la contraseña de la configuración SAMBA deben coincidir con los del identificador de usuario y la contraseña del administrador local asociado al servicio del agente de almacenamiento.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
define path stal file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```

En el ejemplo anterior, el mandato DEFINE DEVCLASS establece el sistema de archivos compartidos en el directorio al que accede el servidor como D:\FILEDIR\DIR1. Sin embargo, el agente de almacenamiento utiliza un nombre UNC \\192.168.1.10\FILEDIR\DIR1. Esto implica que el sistema con la dirección TCP/IP 192.168.1.10 está compartiendo el mismo directorio, que utiliza FILEDIR como nombre compartido. Asimismo, el servicio de agente de almacenamiento tiene una cuenta que puede acceder a este almacenamiento. Puede acceder a éste porque está asociado a una cuenta local con el mismo identificador de usuario y contraseña que 192.168.1.10 o a una cuenta de dominio disponible tanto en el agente de almacenamiento como en 192.168.1.10. Si es adecuado para la instalación, puede sustituir 192.168.1.10 por un nombre simbólico como:

example.yourcompany.com

Atención:

1. Los agentes de almacenamiento acceden a los volúmenes FILE sustituyendo un nombre de directorio de un nombre de volumen por un nombre de directorio de un directorio de la lista proporcionada por el comando DEFINE PATH. Los directorios especificados en este parámetro no están validados en el servidor.
2. IBM Spectrum Protect no crea recursos compartidos, permisos ni monta el sistema de archivos destino. Debe realizar estas acciones antes de iniciar el agente de almacenamiento.

## Ejemplo: definir una ruta desde un servidor hasta una unidad

---

Definir una ruta de un servidor a una unidad. En este caso, el nombre de servidor es *NET1*, el nombre de unidad es *TAPEDRV6*, la biblioteca es *NETLIB* y el nombre de dispositivo es *mt4*. Establecer AUTODETECT en NO.


```
define path net1 tapedrv6 srctype=server autodetect=no desttype=drive
library=netlib device=mt4
```

## Ejemplo: definir una ruta desde un servidor de transportador de datos hasta una unidad para la realización de la copia de seguridad y la restauración

---

Definir una ruta desde un transportador de datos, que es un servidor de archivos NAS, hasta la unidad que el servidor de archivos NAS utilizará para operaciones de copia de seguridad y restauración. En este ejemplo, el transportador de datos NAS es *NAS1*, el nombre de unidad es *TAPEDRV3*, la biblioteca es *NASLIB* y el nombre de dispositivo para la unidad es *rst01*.

```
define path nas1 tapedrv3 srctype=datamover desttype=drive library=naslib
device=rst01
```

 Sistemas operativos Linux

## Ejemplo: definir una ruta desde un agente de almacenamiento hasta una unidad para la realización de la copia de seguridad y la restauración

---

Definir una ruta desde el agente de almacenamiento *SA1* hasta la unidad que el agente de almacenamiento utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, la biblioteca es *TSMLIB*, la unidad es *TAPEDRV4* y el nombre de dispositivo para la unidad es */dev/tmscsi/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
device=/dev/tmscsi/mt3
```

 Sistemas operativos AIX  Sistemas operativos Windows

## Ejemplo: definir una ruta desde un agente de almacenamiento hasta una unidad para la realización de la copia de seguridad y la restauración

---

Definir una ruta desde el agente de almacenamiento *SA1* hasta la unidad que el agente de almacenamiento utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, la biblioteca es *TSMLIB*, la unidad es *TAPEDRV4* y el nombre de dispositivo para la unidad es */dev/mt3*.

```
define path sa1 tapedrv4 srctype=server desttype=drive library=tsmlib
device=/dev/mt3
```

 Sistemas operativos AIX  Sistemas operativos Windows

## Ejemplo: definir una ruta para otorgar al agente de almacenamiento acceso al almacenamiento de disco compartido

---

Definir una ruta que otorgue al agente de almacenamiento acceso a los archivos del almacenamiento de disco compartido con el servidor. La unidad *FILE9* se define para la biblioteca *FILE1* del servidor. El agente de almacenamiento *SA1* accede a *FILE9*. En el agente de almacenamiento, estos datos se encuentran en el directorio *\\192.168.1.10\filedata*.


 Sistemas operativos AIX Los datos para *FILE9* residen en el servidor, en */tsmdata/filedata*.

 Sistemas operativos Windows Los datos para *FILE9* residen en el servidor, en *d:\tsmdata\filedata*.

```
define path sa1 file9 srctype=server desttype=drive library=file1 device=file
directory="\\192.168.1.10\filedata"
```

## Ejemplo: configurar un agente de almacenamiento para que utilice una biblioteca FILE


El siguiente ejemplo muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:  Sistemas operativos Windows

- c:\server
- d:\server
- e:\server

 Sistemas operativos AIX  Sistemas operativos Linux


- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Utilice el siguiente comando para configurar una biblioteca FILE denominada CLASSA con una unidad denominada CLASSA1 en SERVER1:  Sistemas operativos Windows

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

 Sistemas operativos AIX  Sistemas operativos Linux


```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```



2. Quiere que el agente de almacenamiento STA1 pueda utilizar la biblioteca FILE, para poder definir la siguiente ruta para el agente de almacenamiento STA1:  Sistemas operativos Windows


```
define path stal classal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
define path stal classal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

 Sistemas operativos Windows En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio c:\server por el nombre de directorio \\192.168.1.10\c\server para poder acceder a los volúmenes FILE que se encuentran en el directorio c:\server del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio /opt/tivoli1 por el nombre de directorio /opt/ibm1/ para poder acceder a los volúmenes FILE que se encuentran en el directorio /opt/tivoli1 del servidor.

3.  Sistemas operativos Windows SERVER1 crea el volumen de archivo c:\server\file1.dsm. Si cambia más adelante el primer directorio de la clase de dispositivo con el comando siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

SERVER1 todavía puede acceder al volumen de archivo c:\server\file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

4. Si se crea el volumen de archivo /opt/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /opt/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el



agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

## DEFINE PATH (Definir una ruta cuando el destino es una biblioteca)

Utilice esta sintaxis cuando defina una ruta a una biblioteca.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DEFine PATH--nombre_origen--nombre_destino----->
                                     (1)
>--SRCType-----+-DATAMover-----+-----+----->
      '-SERVer-----'    '-AUTODetect---+-No--+-'
                                     '-Yes-'
>--DESTType-----LIBRARY--+-DEVIce-----nombre_dispositivo---+----->
      '-EXTERNALManager-----nombre_ruta-'
      .-ONLine-----Yes-----
>+-----+-----+-----+-----><
      '-ONLine-----+-Yes-+-'
      '-No--'
```

Notas:

1. DATAMOVER sólo se aplica a dispositivos NAS.

### Parámetros

nombre\_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre\_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

Atención: Para definir una ruta de un transportador de datos NAS a una biblioteca, la biblioteca debe tener LIBTYPE establecido en SCSI, 349x o ACSLS.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

AUTODetect

Especifica si se actualizará automáticamente en la base de datos el número de serie de una unidad o biblioteca en el momento en que se defina la ruta. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad o a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente. El número de serie se sigue comparando con lo que ya hay en la base de datos correspondiente al dispositivo. El servidor emite un mensaje si existe una discrepancia.

Yes

Especifica que el número de serie se actualizará automáticamente para reflejar el mismo número de serie que la unidad reporta a IBM Spectrum Protect.

Importante:

1. Si no ha establecido el número de serie al definir la unidad o la biblioteca, el servidor siempre intenta detectar el número de serie, y AUTODETECT toma el valor YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.

2. El uso de AUTODETECT=YES en este comando significa que el número de serie establecido en la definición de unidad o biblioteca se actualiza con el número de serie detectado.
3. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

#### DESTType=LIBRARY (Obligatorio)

Especifica que el destino es una biblioteca. Este parámetro es necesario.

#### DEVICE

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.






 Sistemas operativos AIX  Sistemas operativos Windows El origen utiliza el nombre de dispositivo para acceder a la biblioteca. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos AIX /dev/lb4  Sistemas operativos Linux /dev/tmscsi/lb4  Sistemas operativos Windows lb4.1
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una biblioteca	mc0





 Sistemas operativos Linux El origen utiliza el nombre de dispositivo para acceder a la biblioteca. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	/dev/tmscsi/lb4
De un transportador de datos NAS a una biblioteca	mc0

Importante:


-  Sistemas operativos AIX  Sistemas operativos Linux Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf.  Sistemas operativos Windows Para las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo c:\winnt\ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM® Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el comando SYSCONFIG. Utilice este comando para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```

Utilice este comando para determinar el nombre de dispositivo para una biblioteca:

```
sysconfig -m
```

#### EXTERNALManager

Especifica la ubicación del gestor de bibliotecas externo donde IBM Spectrum Protect puede enviar peticiones de acceso a medio. Especifique el valor de este parámetro entre comillas simples. Por ejemplo, especifique:  Sistemas operativos AIX

/usr/lpp/GESedt-acsls/bin/elmdt

 Sistemas operativos Linux

/opt/GESedt-acsls/bin/elmdt

 Sistemas operativos Windows

C:\Archivos de programa\GES\EDT-ACSLs\bin\elmdt.exe

Este parámetro es necesario cuando el nombre de la biblioteca es una biblioteca externa.

## ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

### Yes

Especifica que la ruta está disponible para utilizarla.


### No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Atención: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.


## Ejemplo: definir una ruta desde un servidor hasta una biblioteca

Defina una ruta desde el servidor SATURN hacia la biblioteca de tipos SCSI SCSILIB:  Sistemas operativos AIX

```
define path saturn scsilib srctype=server
desttype=library device=/dev/lb3
```

 Sistemas operativos Linux

```
define path saturn scsilib srctype=server
desttype=library device=/dev/tmscsi/lb3
```

 Sistemas operativos Windows

```
define path saturn scsilib srctype=server
desttype=library device=lb3.0.0.0
```

 Sistemas operativos AIX  Sistemas operativos Linux

## DEFINE PATH (Definir una ruta cuando el destino es una biblioteca ZOSMEDIA)

Utilice esta sintaxis cuando defina una ruta a una biblioteca ZOSMEDIA. Debe definir el servidor de medios de z/OS en la configuración con el comando DEFINE SERVER.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-DEfINE PATH--nombre_origen--nombre_destino----->
>--SRCType-----SERVer--DESTType-----LIBRary----->
                                     .-ONLine-----Yes-----.
>--ZOSMEDIASERVER-----server_name--+-----+----->>
                                     '-ONLine-----+Yes+-'
                                     '-No--'
```

## Parámetros

nombre\_origen (Obligatorio)

Especifica el nombre del origen de la ruta.

nombre\_destino (Obligatorio)

Especifica el nombre de la biblioteca ZOSMEDIA.

SRCType=SERVer (Obligatorio)

Especifica que el origen es un servidor o un agente de almacenamiento.

DESTType=LIBRary (Obligatorio)

Especifica que el destino es una biblioteca.

ZOSMEDIAServer (Obligatorio)

Especifica el nombre del servidor que representa un servidor de Tivoli Storage Manager for z/OS Media.

#### ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

#### Yes

Especifica que la ruta está disponible para utilizarla.

#### No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Atención: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.

Si no se puede acceder a servidor de medios de z/OS durante la inicialización del servidor de IBM Spectrum Protect, se establecerá la ruta a la biblioteca en fuera de línea. Utilice el mandato UPDATE PATH y especifique ONLINE=YES para variar la biblioteca ZOSMEDIA de nuevo a en línea.

## DEFINE POLICYSET (Definir un juego de políticas)

---

Utilice este comando para definir un juego de políticas de un dominio de políticas. Un juego de políticas contiene clases de gestión, que contienen grupos de copia. Puede definir uno o varios juegos de políticas para cada dominio de políticas.

Para que un juego de políticas entre en vigor, debe activar el juego de políticas con el comando ACTIVATE POLICYSET. Sólo puede haber un juego de políticas activo en un dominio de políticas. Los grupos de copia y las clases de gestión del juego de políticas activo determinan las reglas que siguen los nodos cliente para realizar las operaciones de copia de seguridad, archivado y gestión de espacio, y el modo en que se gestionan los archivos de cliente.

Utilice el comando VALIDATE POLICYSET para verificar que un juego de políticas está completo y es válido antes de activarlo con el comando ACTIVATE POLICYSET.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

### Sintaxis

---

```
>>-DEFine Policyset--nombre_dominio--nombre_juego_políticas----->  
>--+-----+-----><  
'-DESCRiption-----descripción-'
```

### Parámetros

---

#### nombre\_dominio (Necesario)

Especifica el nombre del juego de políticas al que pertenece el juego de políticas.

#### nombre\_juego\_políticas (Necesario)

Especifica el nombre del juego de políticas. La longitud máxima de este nombre es de 30 caracteres. No puede definir un juego de políticas denominado ACTIVE.

#### DESCRiption

Especifica la descripción del nuevo juego de políticas. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

### Ejemplo: definir un juego de políticas

---

Definir un juego de políticas denominado SUMMER para el dominio de políticas PROG1 e incluir la descripción, "Programming Group Policies".

```
define policyset prog1 summer  
description="Programming Group Policies"
```

### Comandos relacionados

---

Tabla 1. Comandos relacionados con DEFINE POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## DEFINE PROFASSOCIATION (Definir una asociación de perfil)

Utilice este comando en un gestor de configuración para asociar uno o varios objetos con un perfil de configuración para distribuirlos a los servidores gestionados suscritos. Cuando un servidor gestionado se suscribe a un perfil, el gestor de configuración envía las definiciones de objeto asociadas con el perfil al servidor gestionado donde están almacenadas en la base de datos. Los objetos que se crean de este modo en la base de datos de un servidor gestionado se convierten en objetos gestionados. Un objeto se puede asociar a varios perfiles.

Puede utilizar este comando para definir un conjunto inicial de asociaciones de perfiles y para agregarlo a asociaciones existentes.

Puede asociar a un perfil los tipos de objetos siguientes:

- Registros y autorizaciones de administrador
- Dominios de políticas, que incluyen los juegos de políticas, las clases de gestión, los grupos de copia y las planificaciones de cliente de los dominios.
- Planificaciones de administración
- Scripts de comandos de servidor
- Conjuntos de opciones de cliente
- Definiciones del servidor
- Definiciones de grupos de servidores

Consejo: El gestor de configuración no distribuye información de estado sobre un objeto a los servidores gestionados. Por ejemplo, información como el número de días que han transcurrido desde la última vez que el administrador accedió al servidor no se distribuye a los servidores gestionados. Este tipo de información se mantiene en las bases de datos de cada servidor gestionado.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DEFine PROFASSOCIation--nombre_perfil----->
>+-----+-----+-----+-----+----->
  '-ADMinS-----+*-----+-'
      | .-,----- . |
      | V             | |
      '---nombre_admin+--'
>+-----+-----+-----+-----+----->
  '-DOmains-----+*-----+-'
      | .-,----- . |
      | V             | |
      '---nombre_dominio+--'
>+-----+-----+-----+-----+----->
  '-ADScheds-----+*-----+-'
```



- Si utiliza una definición de coincidencia con todos y ya existe una lista de dominios, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de dominios y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para eliminar la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro DOMAINS=\*.

Importante: Las operaciones de cliente como, por ejemplo, copia de seguridad y copia archivada no se ejecutarán si no existen las agrupaciones destino. Por lo tanto, los servidores gestionados suscritos a este perfil deben tener definiciones para todas las agrupaciones de almacenamiento especificadas como destino en los dominios asociados. Utilice el comando RENAME STGPOOL para cambiar el nombre de las agrupaciones de almacenamiento existentes de modo que coincidan con los nombres de destino distribuidos.

#### ADScheds

Especifica las planificaciones de administración que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (\*) solo, para especificar todas las planificaciones de administración que están definidas en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otras planificaciones de administración, éstas se distribuirán automáticamente mediante el perfil.

Consejo: Las planificaciones de administración no están activas cuando las distribuye un gestor de configuración. Un administrador de un servidor gestionado debe activar todas las planificaciones para que puedan ejecutarse en ese servidor. Si el perfil ya tiene planificaciones de administración asociadas, será aplicable lo siguiente:

- Si especifica una lista de planificaciones de administración y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de planificaciones de administración, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de planificaciones de administración y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro ADSCHEDS=\*.

#### SCRipts

Especifica los scripts de comandos que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (\*) solo, para especificar todos los scripts que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros scripts, éstos se distribuirán automáticamente mediante el perfil.

Si el perfil ya tiene scripts asociados, será aplicable lo siguiente:

- Si especifica una lista de scripts y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de scripts, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de scripts y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro SCRIPTS=\*.

#### CLOptsets

Especifica los conjuntos de opciones de cliente que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (\*) solo, para especificar todos los conjuntos de opciones de cliente que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros conjuntos de opciones de cliente, éstos se distribuirán automáticamente mediante el perfil.

Si el perfil ya tiene conjuntos de opciones de cliente asociados, será aplicable lo siguiente:

- Si especifica una lista de conjuntos de opciones de cliente y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de conjuntos de opciones de cliente, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de conjuntos de opciones de cliente y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para eliminar la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro CLOPSETS=\*.

#### SERVers

Especifica las definiciones de servidor que se van a asociar al perfil. Las definiciones se distribuyen en los servidores gestionados que se inscriben en este perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (\*) solo, para especificar todos los servidores que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros servidores, éstos se distribuirán automáticamente mediante el perfil.

El gestor de configuración distribuye los siguientes atributos de servidor: el método de comunicaciones, la dirección IP, la dirección de puerto, la contraseña del servidor, el URL y la descripción. Las definiciones de servidor distribuidas siempre tienen el atributo ALLOWREPLACE establecido en YES en el servidor gestionado, independientemente del valor que tenga este parámetro en el gestor de configuración. En el servidor gestionado, puede utilizar el comando UPDATE SERVER para establecer todos los demás atributos.

Si el perfil ya tiene servidores asociados, será aplicable lo siguiente:

- Si especifica una lista de servidores y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de servidores, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de servidores y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro SERVERS=\*

Importante:

1. Una definición de servidor en un servidor gestionado no se sustituye por una definición del gestor de configuración a menos que se haya permitido sustituir la definición del servidor gestionado. Para permitir la sustitución, en el servidor gestionado, actualice la definición del servidor con el comando UPDATE SERVER con ALLOWREPLACE=YES.
2. Si un gestor de configuración distribuye una definición de servidor a un servidor gestionado y existe un grupo de servidores con el mismo nombre en el servidor gestionado, la definición de servidor distribuida sustituye la definición del grupo de servidores.

#### SERVERGroups

Especifica los grupos de servidores que se van a asociar al perfil. Puede utilizar caracteres comodín en los nombres. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice la definición de coincidencia con todos, un asterisco (\*) solo, para especificar todos los grupos de servidores que están definidos en el gestor de configuración. Si especifica la definición de coincidencia con todos y más adelante agrega otros grupos de servidores, éstos se distribuirán automáticamente mediante el perfil.

Consejo: Un gestor de configuración no distribuye una definición de grupo de servidores a un servidor gestionado si el servidor gestionado tiene un servidor definido con el mismo nombre que el grupo de servidores.

Si el perfil ya tiene grupos de servidores asociados, será aplicable lo siguiente:

- Si especifica una lista de grupos de servidores y ya existe una lista, IBM Spectrum Protect combina la lista nueva con la existente.
- Si utiliza una definición de coincidencia con todos y ya existe una lista de grupos de servidores, IBM Spectrum Protect sustituye la lista con la definición de coincidencia con todos.
- Si especifica una lista de grupos de servidores y se ha especificado previamente una definición de coincidencia con todos, IBM Spectrum Protect no tiene en cuenta la lista. Para suprimir la definición de coincidencia con todos, emita el comando DELETE PROFASSOCIATION con el parámetro SERVERGROUPS=\*

## Ejemplo: asociar un dominio específico a un perfil específico

Asociar un dominio denominado MARKETING con un perfil denominado DELTA.

```
define profassociation delta domains=marketing
```

## Ejemplo: asociar todos los dominios a un perfil específico

Ya tiene una lista de dominios asociada al perfil denominado GAMMA. Ahora asocie todos los dominios definidos en el gestor de configuración con el perfil.

```
define profassociation gamma domains=*
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE PROFASSOCIATION

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.



Comando	Descripción
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## DEFINE PROFILE (Definir un perfil)

Utilice este comando en un gestor de configuración para definir un perfil (un conjunto de información de configuración) que se podrá distribuir a los servidores gestionados.

Después de haber definido un perfil, puede utilizar el comando DEFINE PROFASSOCIATION para especificar los objetos que han de distribuirse a los servidores gestionados mediante la suscripción al perfil.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine PROFIle--nombre_perfil----->
>--+-----+-----><
  '-DESCription---descripción-'
```

### Parámetros

nombre\_perfil (Obligatorio)

Especifica el nombre del perfil. La longitud máxima del nombre es de 30 caracteres.

DESCription

Especifica la descripción del perfil. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Este parámetro es opcional.

### Ejemplo: definir un nuevo perfil

Defina un perfil de nombre ALPHA con una descripción de "Centro de programación".

```
define profile alpha
description="Programming Center"
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.

Comando	Descripción
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## DEFINE RECMEDMACHASSOCIATION (Asociar medio de recuperación con una máquina)

Utilice este comando para asociar un medio de recuperación a una o varias máquinas. Una máquina se asocia al medio de recuperación para que la ubicación del medio de arranque y la lista de nombres de volúmenes esté disponible para recuperar la máquina. Para recuperar la información, emita el comando QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

Para asociar una máquina a un medio de recuperación, la máquina y el medio deben estar definidos en IBM Spectrum Protect. Una máquina permanece asociada al medio mientras no se suprime la asociación, el medio o la máquina.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine RECMEDMACHAssociation--nombre_medio----->
      .-,-----
      v          |
>----nombre_máquina-+----->>
```

### Parámetros

nombre\_soporte (Obligatorio)

Especifica el nombre del medio de recuperación al que se asociarán una o varias máquinas.

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina que se ha de asociar al medio de recuperación. Una máquina puede asociarse a varios medios de recuperación. Para especificar una lista de máquinas, separe los nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

### Ejemplo: asociar máquinas a medios de recuperación

Asociar las máquinas DISTRICT1 y DISTRICT5 al medio de recuperación DIST5RM.

```
define recmedmachassociation dist5rm
district1,district5
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE RECMEDMACHASSOCIATION

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE MACHINE	Suprime una máquina.
DELETE RECMEDMACHASSOCIATION	Suprime la asociación entre un medio de recuperación y una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY MACHINE	Muestra información sobre máquinas.

Comando	Descripción
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

## DEFINE RECOVERYMEDIA (Definir medio de recuperación)

Utilice este comando para definir el medio necesario para recuperar una máquina. El mismo medio puede estar asociado a varias máquinas. Para que se visualice la información, utilice el comando QUERY MACHINE. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine RECOVERYMedia--nombre_medio----->
>+-----+
|           .-,----- . |
|           v           | |
'-VOLumenames-----nombre_volumen-+-'
>+-----+
'-DESCRiption-----descripción-'
>+-----+
               .-Type-----Other----- .
'-LORcation-----ubicación-' '-Type-----+--Other-+-'
                               '-BOot--'
>+-----+
'-PRORduct-----nombre_producto-'
>+-----+-----+-----><
'-PRORDUCTInfo-----información_producto-'
```

### Parámetros

**nombre\_soporte** (Obligatorio)

Especifica el nombre del medio de recuperación que se ha de definir. El nombre puede tener hasta 30 caracteres.

**VOLumenames**

Especifica los nombres de volúmenes que contienen datos recuperables (por ejemplo, copias de imágenes del sistema operativo). Este parámetro es necesario si especifica el tipo de medio BOOT. Los nombres de volúmenes de medios de arranque deben especificarse en el orden en que se insertarán en la máquina al efectuar la recuperación. La longitud máxima de la lista de nombres de volúmenes es de 255 caracteres. La lista debe estar delimitada por comillas si contiene algún carácter en blanco.

**DESCRiption**

Especifica la descripción del medio de recuperación. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

**LORcation**

Especifica la ubicación del medio de recuperación. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

**Type**

Especifica el tipo de medio de recuperación. Este parámetro es opcional. El valor predeterminado es OTHER.

**BOot**

Especifica que este es un medio de arranque. Debe especificar los nombres de los volúmenes si el tipo es BOOT.

**ORther**

Especifica que éste no es un medio de arranque. Por ejemplo, un CD que contiene los manuales del sistema operativo.

**PRORduct**

Especifica el nombre del producto que se ha grabado en este medio. Este parámetro es opcional. La longitud máxima son 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

**PRORDUCTInfo**

Especifica la información sobre el producto que se ha grabado en el medio. Esta información puede ser necesaria para restaurar la máquina. Este parámetro es opcional. La longitud máxima son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

## Ejemplo: definir los medios necesarios para realizar la recuperación de una máquina

Definir el medio de recuperación denominado DIST5RM. Se incluirá la descripción y la ubicación.

```
define recoverymedia dist5rm
description="district 5 base system image"
location="district 1 vault"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE RECOVERYMEDIA

Comando	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

## DEFINE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)

Utilice este comando para crear una planificación de cliente o de comando de administración.

El mandato DEFINE SCHEDULE tiene dos formatos: uno si la planificación se aplica a las operaciones de cliente y el otro si la planificación se aplica a mandatos administrativos. En estos dos formatos, puede seleccionar las planificaciones de estilo clásico o mejorado. La sintaxis y los parámetros de cada formato se definen por separado.

Para cada planificación, se especifica un margen de puesta en marcha. El margen de puesta en marcha es el período de tiempo durante el cual debe iniciarse la planificación. La planificación no completará necesariamente el proceso dentro de este margen. Si el servidor no está ejecutándose cuando se arranca este margen, pero se arranca antes de que se alcance el final del margen definido, la planificación se ejecutará cuando se vuelva a arrancar el servidor. Las opciones asociadas a cada estilo de planificación (clásico y mejorado) determinan cuándo deben comenzar las ventanas de inicio de sesión.

Tabla 1. Comandos relacionados con DEFINE SCHEDULE

Comando	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un comando planificado.
SET MAXSCHEDSESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- DEFINE SCHEDULE (Definir una planificación de cliente)  
Utilice el comando DEFINE SCHEDULE para definir una planificación de cliente. IBM Spectrum Protect utiliza esta planificación para realizar automáticamente diversas operaciones de cliente para la estación de trabajo cliente en los intervalos o días

especificados. Después de haber definido una planificación, utilice el mandato DEFINE ASSOCIATION para asociar el cliente a la planificación.

- DEFINE SCHEDULE (Definir una planificación para un comando de administración)

Utilice el comando DEFINE SCHEDULE para crear una nueva planificación para procesar un comando de administración.

## DEFINE SCHEDULE (Definir una planificación de cliente)

Utilice el comando DEFINE SCHEDULE para definir una planificación de cliente. IBM Spectrum Protect utiliza esta planificación para realizar automáticamente diversas operaciones de cliente para la estación de trabajo cliente en los intervalos o días especificados. Después de haber definido una planificación, utilice el mandato DEFINE ASSOCIATION para asociar el cliente a la planificación.

Debe iniciar el planificador de cliente en la estación de trabajo cliente para que IBM Spectrum Protect procese la planificación.

No todos los clientes pueden ejecutar todas las operaciones planificadas, aunque pueda definir la planificación en el servidor y asociar ésta al cliente. Por ejemplo, un cliente Macintosh no puede ejecutar una planificación cuando la acción sea restaurar o recuperar archivos o ejecutar un script ejecutable. En los diferentes sistemas operativos cliente, un script ejecutable, también se conoce como un archivo de comandos, un archivo por lotes o un script.

IBM Spectrum Protect no puede ejecutar varias planificaciones al mismo tiempo para el mismo nodo cliente.

### Clase de privilegio

Para definir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado al dominio de políticas al que pertenece la planificación.

### Sintaxis

Planificación de cliente clásica

```
>>-DEFine SCHEDULE--domain_name--schedule_name----->
>--+-----+-----+-----+-----+-----+-----+-----+----->
>'-Type---Client-' '-DESCRIPTION---descripción-'
. ACTION---Incremental-----.
>--+-----+-----+-----+-----+-----+-----+-----+----->
'-ACTION---+Incremental-----+'
  +Selective-----+
  +Archive-----+
  |                 |                 |                 |                 |
  |                 | '-SUBACTION---+'                 |
  |                 |                 | '-FASTBack-' |
  +Backup-----+
  |                 |                 |                 |                 |
  |                 | '-SUBACTION---+'                 |
  |                 |                 | '+FASTBack----+' |
  |                 |                 | '+SYSTEMState+' |
  |                 |                 | '+VApp-----+' |
  |                 |                 | '-VM-----+' |
  +RESTore-----+
  +RETRieve-----+
  +IMAGEBACkup-----+
  +IMAGERESTore-----+
  +Command-----+
  +Macro-----+
  '-Deploy-----+'

>--+-----+-----+-----+-----+-----+-----+-----+----->
'-OPTions---serie_opción-'

. -PRIority---5-----.
>--+-----+-----+-----+-----+-----+-----+-----+----->
|                 (1) |                 | '-PRIority---número-'
'-OBJects-----serie_objeto-'

. -STARTDate---fecha_actua-.
>--+-----+-----+-----+-----+-----+-----+-----+----->
'-STARTDate---fecha-----'

. -STARTTime---hora_actua-. . -DURation---1-----.
>--+-----+-----+-----+-----+-----+-----+-----+----->
```

```

'-STARTTime----hora-----' '-DURATION ---numero-'

.-DURUnits----Hours----- .-MAXRUNtime----0-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-DURUnits----+Minutes----+' '-MAXRUNtime----numero-'
    +-Hours-----+
    +-Days-----+
    '-INDefinite-'

.-SCHEDStyle----Classic-. .-PERiod----1-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-SCHEDStyle----Classic-' '-PERiod----numero-'

.-PERUnits----Days----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-PERUnits----+Hours---+'
    +-Days----+
    +-Weeks---+
    +-Months---+
    +-Years---+
    '-Onetime-'

.-DAYofweek----ANY----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-DAYofweek----+ANY-----+'
    +-WEEKDay---+
    +-WEEKEnd---+
    +-SUNday----+
    +-MONday----+
    +-TUESday---+
    +-WEDnesday+
    +-THURsday--+
    +-FRIDay----+
    '-SATURday--'

.-EXPIration----Never----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+<
'-EXPIration----+Never---+'
    '-date--'

```

**Notas:**

1. El parámetro OBJECTS es opcional cuando ACTION=INCREMENTAL, pero es necesario para otras acciones.

## Sintaxis

---

Planificación de cliente mejorada

```

>>-DEFine SCHEDULE--domain_name--schedule_name----->
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-Type----Client-' '-DESCRiption----descripci3n-'

.-ACTion----Incremental----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-ACTion----+Incremental-----+'
    +-Selectiva-----+
    +-Archive--+-+-----+-----+-----+-----+-----+
    |               '-SUBACTion----FASTBack-'             |
    +-Backup--+-+-----+-----+-----+-----+-----+
    |               | .-"----- . | |
    |               '-SUBACTion----+-----+-----+-----+' |
    |               +-FASTBack----+ |
    |               +-SYSTEMState+ |
    |               +-VApp-----+ |
    |               '-VM-----+' |
    +-REStore-----+
    +-RETrievE-----+
    +-IMAGEBACKup-----+
    +-IMAGERESTore-----+
    +-Command-----+
    '-Macro-----+'

>+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

```

'-OPTions-----serie_opción-'
                                .-PRIority-----5-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
|              (1)              |  '-PRIority-----número-'
'-OBJects-----serie_objeto-'

.-STARTDate-----fecha_actual-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'| -STARTDate-----fecha-----'

.-STARTTime-----hora_actual-.  .-DURation-----1-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'| -STARTTime-----hora-----'  '| -DURATION  ----número-'

.-DURUnits-----Hours----- .-MAXRUNtime-----0-----.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'| -DURUnits-----+Minutes+-'  '| -MAXRUNtime-----número-'
      +-Hours-----
      '-Days-----'

                                .-MONth-----ANY----- .
>--SCHEDStyle-----Enhanced+-----+-----+-----+-----+-----+----->
                                '| -MONth-----+ANY-----+'
                                    +-JANuary---+
                                    +-February--+
                                    +-MARch-----+
                                    +-APRil-----+
                                    +-May-----+
                                    +-JUNe-----+
                                    +-JULy-----+
                                    +-AUGust---+
                                    +-September--+
                                    +-October---+
                                    +-November--+
                                    '| -December--'

.-DAYOFMonth-----ANY----- .  .-WEEKofmonth-----ANY----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'| -DAYOFMonth-----+ANY--+-'  '| -WEEKofmonth-----+ANY-----+'
      '-Day-'                   +-First--+
                                +-Second--+
                                +-Third--+
                                +-FOurth--+
                                '| -Last---'

.-DAYofweek-----ANY----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'| -DAYofweek-----+ANY-----+'
      +-WEEKDay---+
      +-WEEKEnd---+
      +-SUNday----+
      +-Monday----+
      +-TUESday---+
      +-Wednesday--+
      +-THursday---+
      +-Friday----+
      '| -SATurday--'

.-EXPIration-----Never----- .
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----><
'| -EXPIration-----+Never--+-'
      '-date--'

```

Notas:

1. El parámetro OBJECTS es opcional cuando ACTION=INCREMENTAL, pero es necesario para otras acciones.

## Parámetros

---

nombre dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de definir. Puede especificar hasta 30 caracteres para el nombre.

Type=Client

Especifica que se define una planificación para un cliente. Este parámetro es opcional.

DESCription

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACTion

Especifica la acción que se produce cuando se procesa esta planificación. Los valores posibles son:

Incremental

Especifica que la planificación hace copia de seguridad de todos los archivos que son nuevos o que se han modificado desde la última copia de seguridad incremental. La copia de seguridad incremental también hace copia de seguridad de todos los archivos para el que se hayan podido caducar todas las copias de seguridad existentes.

Selective

Especifica que la planificación sólo hace copia de seguridad de los archivos especificados con el parámetro OBJECTS.

Archive

Especifica que la planificación hace copia archivada de los archivos especificados con el parámetro OBJECTS.

Backup

Especifica que la planificación realiza una copia de seguridad de los archivos especificados con el parámetro OBJECTS.

REStore

Especifica que la planificación restaura los archivos especificados con el parámetro OBJECTS.

Cuando especifique ACTION=RESTORE para una operación planificada y se define la opción REPLACE como PROMPT, no se efectúa ninguna petición. Si establece la opción en PROMPT, se ignoran los archivos.

Si se especifica una segunda especificación de archivo, ésta actúa como destino de la restauración. Si necesita restaurar varios grupos de archivos, planifique una restauración para cada especificación de archivo que necesita restaurar.

RETRieve

Indica que la planificación recupera los archivos especificados con el parámetro OBJECTS.

Recuerde: Un segundo archivo especificado actúa como el destino de recuperación. Si necesita recuperar varios grupos de archivos, cree una planificación distinta para cada grupo de archivos.

IMAGEBACKup

Especifica que la planificación hace copia de seguridad de los volúmenes lógicos especificados con el parámetro OBJECTS.

IMAGEREStore

Especifica que la planificación restaura los volúmenes lógicos especificados con el parámetro OBJECTS.

Comando

Indica que la planificación procesa un comando de un sistema operativo de cliente o un script, especificado con el parámetro OBJECTS.

Macro

Especifica que un cliente procesa una macro cuyo nombre de archivo se especifica con el parámetro OBJECTS.

SUBACTion

Puede especificar uno de los siguientes valores:

""

Cuando una serie vacía (dos dobles comillas) se especifica con ACTION=BACKUP, la copia de seguridad es incremental.

FASTBACk

Especifica que una operación de cliente FastBack identificada por el parámetro ACTION se va a planificar para procesar. El parámetro ACTION debe ser ARCHIVE o BACKUP.

SYSTEMState

Especifica que se ha programado una copia de seguridad del estado del sistema.

VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

VM

Especifica que se ha programado una copia de seguridad VMware del cliente.

Deploy

Especifica si se actualizarán las estaciones de trabajo del cliente con paquetes de despliegue especificados con el parámetro OBJECTS. El parámetro OBJECTS debe contener dos especificaciones: los archivos del paquete que se deben recuperar y de dónde recuperarlos. Asegúrese de que los objetos están en orden *ubicación\_archivos*. Por ejemplo:

```
define schedule standard deploy_1 action=DEPLOY objects=  
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\  
..\IBM_ANR_WIN\"
```



Los valores de las siguientes opciones estarán restringidos si se especifica ACTION=DEPLOY:

#### PERUNITS

Especifique PERUNITS=ONETIME. Si especifica PERUNITS=PERIOD, el parámetro se omitirá.

#### DURUNITS

Especifique MINUTES, HOURS o DAYS para el parámetro DURUNITS. No especifique INDEFINITE.

#### SCHEDSTYLE

Especifique el estilo predeterminado, CLASSIC.


El comando SCHEDULE falla si los parámetros no coinciden con los valores de parámetro necesarios, como V.R.M.F.

### OPTions

Especifica las opciones que se especifican en el comando planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el comando planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de comandos. Todas las opciones que se describen como válidas solamente en la línea de comandos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el comando planificado:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el comando DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el comando planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:
  - `options='-subdir=yes -domain="all-local -c: -systemobject"'`
- Para especificar `domain all-local -c: -d:`, escriba:
  - `options='-domain="all-local -c: -d:"'`

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

### OBJects

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando ACTION=INCREMENTAL. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un comando o una macro, el objeto será el nombre del comando o macro que debe ejecutarse.

Si especifica ACTION=INCREMENTAL sin especificar ningún valor para este parámetro, el comando planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de
destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número
excesivo de argumentos de línea de
comandos
```

Si especifica ACTION=ARCHIVE, INCREMENTAL o SELECTIVE para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.


Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofes. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofes. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar C:\ARCHIVO 2, D:\ARCHIVOS GIF y E:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="C:\ARCHIVO 2" "D:\ARCHIVOS GIF" "E:\ARCHIVO DE PRUEBA"
- Para especificar D:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="D:\ARCHIVO DE PRUEBA"
- Para especificar D:\PRUEBA,ARCHIVO:
  - OBJECTS="D:\PRUEBA,ARCHIVO"

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar /home/archivo 2, /home/archivos gif y /home/archivo de prueba, escriba:
  - OBJECTS="/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba"
- Para especificar /home/archivo de prueba, escriba:
  - OBJECTS="/home/archivo de prueba"

 Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

#### PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

#### STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.

Valor	Descripción	Ejemplo
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este comando a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

#### DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

Consejo: Defina las planificaciones con duraciones de más de 10 minutos. Con ello, el planificador de IBM Spectrum Protect dispondrá de tiempo suficiente para procesar la planificación y avisar al cliente.

#### DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

#### Minutes

Especifica que la duración del margen se define en minutos.

#### Hours

Especifica que la duración del margen se define en horas.

#### Days

Especifica que la duración del margen se define en días.

#### INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

#### MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejo: El tiempo máximo de ejecución se calcula desde el principio de la ventana de inicio y no desde la hora en que se inician las sesiones en la ventana de inicio.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. El valor predeterminado es 0. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y no se emite ningún mensaje de aviso. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de una operación planificada son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todas las sesiones de cliente para esta operación deben finalizar a la 1:00 del mediodía. Si se siguen ejecutando una o varias sesiones después de la 1:00 del mediodía, el servidor emite un mensaje de aviso.

Consejo: También puede especificar un valor para *Alerta de tiempo de ejecución* de 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

#### SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se puede ejecutar una planificación, o los días en los que se ejecuta. El valor predeterminado es la sintaxis clásica.

Los valores posibles son:

##### Classic

Los parámetros de la sintaxis Classic son: PERIOD, PERUNITS y DAYOFWEEK. No puede utilizar estos parámetros: MONTH, DAYOFMONTH y WEEKOFMONTH.

##### Enhanced

Los parámetros de la sintaxis Enhanced son: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No puede utilizar estos parámetros: PERIOD y PERUNITS.

#### PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

#### PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

##### Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

##### Days

Especifica que el período entre márgenes de puesta en marcha es en días.

##### Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

#### Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

#### Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

#### Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

#### DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

##### Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

##### Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

##### ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

##### WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

##### WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

##### SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

##### Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

##### TUESday

Especifica que el margen de puesta en marcha comienza en Martes.

##### Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

##### THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

##### Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

#### SAturday

Especifica que el margen de puesta en marcha comienza en Sábado.

#### MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada mes del año.

#### DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es el -1, el penúltimo es el -2, etc. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecuta una vez ese día.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

#### WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecuta una vez durante esa semana.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

#### EXpiration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

#### Never

Especifica que la planificación no caduca nunca.

#### fecha\_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

## Ejemplo: definir una planificación para una copia de seguridad incremental mensual

---

Definir una planificación denominada MONTHLY\_BACKUP que inicia una copia de seguridad incremental de todos los nodos asociados. Especifique martes 1 de mayo de 2001 como fecha de inicio. Esta fecha no concuerda con el día de la semana especificado (domingo), por lo tanto el margen de puesta en marcha empieza en el primer domingo después del 1 de mayo de 2001 (05/01/2001). Los márgenes de puesta en marcha de esta planificación abarcan de las 01:00 a las 03:00. Esta planificación mensual inicia la copia de seguridad de los espacios de archivos c: y d: para todos los nodos asociados.

```
define schedule standard monthly_backup
description="Copia de seguridad mensual de las unidades c: y d:"
objects="c:\* d:\*"
startdate=05/01/2001 starttime=01:00
duration=2 durunits=hours period=1
perunits=months dayofweek=sunday
```

## Ejemplo: definir una planificación para una copia de seguridad incremental semanal

---

Definir una planificación denominada WEEKLY\_BACKUP que inicia una copia de seguridad incremental de todos los nodos asociados. El margen de puesta en marcha inicial para esta planificación abarca desde las 23:00:00 del sábado, 7 de junio de 1997 (07/06/1997), a las 03:00:00 del domingo, 8 de junio de 1997 (08/06/1997). Los márgenes siguientes comienzan a las 23:00:00, cada sábado. Cuando se ejecuta esta planificación, no se devuelve ningún mensaje al nodo cliente.

```
define schedule employee_records weekly_backup
startdate=06/07/1997 starttime=23:00 duration=4
durunits=hours perunits=weeks
dayofweek=saturday options=-quiet
```

## Ejemplo: definir una planificación que archive un directorio específico trimestralmente

---

Actualizar una planificación de las copias específicas archivadas trimestralmente el último viernes del mes.

```
define schedule employee_records quarterly_archive
starttime=20:00 action=archive
object=/home/employee/records/*
duration=1 durunits=hour schedstyle=enhanced
month=mar,jun,sep,dec weekofmonth=last dayofweek=fri
```

## DEFINE SCHEDULE (Definir una planificación para un comando de administración)

Utilice el comando DEFINE SCHEDULE para crear una nueva planificación para procesar un comando de administración.

Puede incluir scripts en una planificación de comando de administración para que se procesen automáticamente.

Nota:

1. No puede planificar el comando MACRO ni el comando QUERY ACTLOG.
2. Si va a planificar un comando que especifique el parámetro WAIT, el parámetro debe establecerse en YES para que el proceso proporcione un código de retorno a la sesión que lo ha iniciado. Para obtener más información acerca del parámetro WAIT, consulte el apartado Proceso de comandos de servidor.

### Clase de privilegio

Para definir una planificación de comandos de administración, debe tener privilegio de sistema.

### Sintaxis

Planificación de administración clásica

```
>>-DEFine SChedule--nombre_planificación----->
>--+-----+--CMD---comando----->
  '-Type---Administrative-'
  .-ACTIVE---No--.
>--+-----+-----+----->
  '-ACTIVE---Yes-' '-DEscription---descripción-'
  .-PRIority---5----- .-STARTDate---fecha_actual-.
>--+-----+-----+----->
  '-PRIority---numero-' '-STARTDate---fecha-----'
  .-STARTTime---hora_actual-. .-DURation---1-----.
>--+-----+-----+----->
  '-STARTTime---hora-----' '-DURation ---numero-'
  .-DURUnits---Hours----- .-MAXRUNtime---0-----.
>--+-----+-----+----->
  '-DURUnits---+Minutes---+' '-MAXRUNtime---numero-'
    +-Hours-----+
    +-Days-----+
    '-INDefinite-'
  .-SCHEDStyle---Classic-. .-PERiod---1-----.
>--+-----+-----+----->
  '-SCHEDStyle---Classic-' '-PERiod---numero-'
  .-PERUnits---Days----- .
>--+-----+----->
  '-PERUnits---+Hours---+'
    +-Days-----+
    +-Weeks---+
    +-Months---+
    +-Years---+
    '-Onetime-'
  .-DAYofweek---ANY----- .
>--+-----+----->
  '-DAYofweek---+ANY---+'
    +-WEEKDay---+
    +-WEEKEnd---+
```







Valor	Descripción	Ejemplo
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.  Si emite este comando a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o - HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.  Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

#### DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

#### DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

##### Minutes

Especifica que la duración del margen se define en minutos.

##### Hours

Especifica que la duración del margen se define en horas.

##### Days

Especifica que la duración del margen se define en días.

##### INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

#### MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales se deben completar los procesos del servidor que se han iniciado mediante los mandatos planificados. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejos:

- Es posible que los procesos no finalicen inmediatamente después de que los haya cancelado el planificador central. Finalizan cuando registran la notificación de cancelación del planificador central.
- El tiempo de ejecución máximo se calcula comenzando desde el momento en que se inicia el servidor. Si el mandato de planificación inicia más de un proceso, se calcula tiempo máximo de ejecución de cada proceso a partir del inicio del proceso.
- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.
- Este parámetro no se aplica si el mandato planificado no inicia un proceso de servidor.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. El valor predeterminado es 0. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y el planificador central no cancela procesos. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de un mandato planificado son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todos los procesos de servidor aplicables iniciados por el mandato se deben finalizar a la 1:00 del mediodía. Si uno o varios procesos aplicaciones continúan ejecutándose pasadas la 1:00 del mediodía, el planificador central cancela los procesos.

Consejo: También puede especificar como *hora de finalización* la 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

#### SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se debe ejecutar una planificación, o los días en los que se debe ejecutar. El estilo puede ser clásica o mejorada. El valor predeterminado es la sintaxis clásica.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten para las planificaciones mejoradas los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS.

#### PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

#### PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

#### Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

#### Days

Especifica que el período entre márgenes de puesta en marcha es en días.

#### Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

#### Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

#### Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

#### Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

#### DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

##### Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

##### Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

#### ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

#### WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

#### WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

#### SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

#### Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

#### TUesday

Especifica que el margen de puesta en marcha comienza en Martes.

#### Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

#### THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

#### Friday

Especifica que el margen de puesta en marcha comienza en Viernes.  
Saturday  
Especifica que el margen de puesta en marcha comienza en Sábado.

#### MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY. Esto significa que la planificación se ejecutará todos los meses del año.

#### DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es -1, el penúltimo es -2, etc. Puede especificar varios valores separados mediante comas, sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecutará una vez ese día.

El valor predeterminado es ANY. Esto significa que la planificación se ejecutará cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

#### WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecutará una vez durante esa semana.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

#### EXpiration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

##### Never

Especifica que la planificación no caduca nunca.

##### fecha\_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

## Ejemplo: definir una planificación para que se realice la copia de seguridad de la agrupación de almacenamiento primaria cada dos días

---

Definir una planificación denominada BACKUP\_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. La copia de seguridad se ejecuta a las 8 p.m. cada dos días.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
active=yes starttime=20:00 period=2
```

## Ejemplo: definir una planificación para que se realice la copia de seguridad de la agrupación de almacenamiento primaria dos veces al mes

---

Definir una planificación denominada BACKUP\_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. Seleccionar una planificación mejorada y ejecutarla el día uno y el quince de cada mes.

```
define schedule backup_archivepool type=administrative
cmd="backup stgpool archivepool recoverypool"
schedstyle=enhanced dayofmonth=1,15
```

## DEFINE SCRATCHPADENTRY (Definir una entrada de registro)

---

Utilice este mandato para introducir datos en una línea nueva en el registro. La anotación es una tabla de base de datos que aloja el servidor. Puede utilizar el registro para almacenar información diversa en formato de tabla.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-DEFine SCRATCHPAdentry--major_category--minor_category----->  
>--subject--Line ---número--Data-----datos-----><
```

## Parámetros

---

major\_category (obligatorio)

Especifica la categoría principal en la se almacenarán los datos. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

minor\_category (obligatorio)

Especifica la categoría secundaria en la se almacenarán los datos. Las categorías secundarias son secciones dentro de categorías principales. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)

Especifica el tema bajo el que se almacenarán los datos. Los asuntos son secciones en categorías secundarias. Entre una serie de texto de como máximo 100 caracteres alfanuméricos. Este parámetro distingue entre mayúsculas y minúsculas.

Line (obligatorio)

Especifica el número de la línea en la que se almacenarán los datos. Las líneas son secciones dentro de los asuntos. Especifique un entero en el rango 1 – 1000.

Data (obligatorio)

Especifica los datos que se almacenarán en la línea. Puede entrar un máximo de 1000 caracteres. Ponga los datos entre comillas si los datos contienen uno o más espacios en blanco. Los datos distinguen entre mayúsculas y minúsculas.

## Ejemplo: Definir una entrada de registro

---

Entre las fechas de vacaciones de un administrador, Jane, en una tabla que almacena información sobre la ubicación de todos los administradores.

```
define scratchpentry admin_info location jane line=2 data=  
"Fuera de la oficina del 1-15 Nov."
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con DEFINE SCRATCHPADENTRY

Comando	Descripción
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

## DEFINE SCRIPT (definir un script de IBM Spectrum Protect)

---

Utilice este comando para definir un script de IBM Spectrum Protect o para crear un nuevo script de IBM Spectrum Protect con el contenido de otro script.

La primera línea del script se puede definir con este comando. Para agregar más líneas al script, utilice el mandato UPDATE SCRIPT.

Consejos:

- Si direcciona mandatos dentro de los scripts, delimite el servidor o el grupo de servidores con paréntesis y omita los dos puntos. De otro modo, si la sintaxis incluye el carácter de los dos puntos, el mandato no se redirecciona al emitirse el mandato RUN. En lugar de ello, el comando sólo se ejecuta en el servidor desde el que se emite el comando RUN.

- No puede redirigir la salida de un mandato desde un script de IBM Spectrum Protect. En su lugar, ejecute el script, y luego especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de operador, políticas, almacenamiento o sistema.

## Sintaxis

```
>>-DEFine SCript--nombre_script----->
                                     .-Line----001----.
>--+línea_comandos--+----->
|           '-Line ---número-' |
| '-File----nombre_archivo-----' |
>+-----<
  '-DESCRiption----descripción-'
```

## Parámetros

nombre\_script (Obligatorio)

Especifica el nombre del script que se va a definir. Puede especificar hasta 30 caracteres para el nombre.

línea\_comandos

Especifica el primer comando de un script que se procesará. Debe especificar este parámetro (y el parámetro LINE de forma opcional) o el parámetro FILE.

El comando que especifique puede contener variables de sustitución y se puede continuar en varias líneas si especifica un carácter de continuación (-) como último carácter del comando. Las variables de sustitución se especifican con el carácter '\$', seguido de un número que indica el valor del parámetro al procesarse el script. Puede especificar hasta 1200 caracteres para la línea de comandos. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco.

Puede ejecutar comandos en serie, en paralelo o en serie y en paralelo, especificando los comandos de script SERIAL o PARALLEL para el parámetro COMMAND\_LINE . Puede ejecutar varios comandos en paralelo y esperar a que finalicen antes de proceder con el comando siguiente. Los comandos se ejecutan en serie hasta que se encuentre un comando en paralelo.

Pueden utilizarse sentencias de flujo lógico condicional. Estas sentencias incluyen IF, EXIT y GOTO.

Line

Especifica el número de línea de la línea de comandos. Ya que los mandatos se especifican en varias líneas, los números de línea se utilizan para determinar el orden en que se procesan al ejecutar el script. La primera línea, o línea 001, es el valor predeterminado. Este parámetro es opcional.

File

Especifica el nombre del archivo cuyo contenido se lee en el script que se va a definir. El archivo debe residir en el servidor donde se ejecuta este comando. Si especifica el parámetro FILE, no puede especificar una línea de comandos ni un número de línea.

Puede crear un script consultando otro script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene al consultar el script se dirige al archivo que especifique con el parámetro OUTPUTFILE. Para crear el nuevo script, el contenido del script que se va a definir se leerá del archivo que especifique con el parámetro OUTPUTFILE.

DESCRiption

Especifica la descripción del script. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Este parámetro es opcional.

## Ejemplo: escribir un script para que se visualicen los clientes de AIX

Defina un script que muestre todos los clientes de AIX.

```
define script qaixc "select node_name from nodes
where platform_name='AIX'"
desc='Display aix clients'
```

## Ejemplo: escribir y ejecutar un script para que se redireccione un mandato a un grupo de servidores

Defina y ejecute un script que direcciona el comando QUERY STGPOOL a un grupo de servidores denominado DEV\_GROUP.

```
define script qu_stg "(dev_group) query stgpool"
run qu_stg
```

## Ejemplo: crear un script a partir de un script existente

Defina un script cuyas líneas de comandos se lean de un archivo denominado MY.SCRIPT y especifique que el nuevo script se denomine AGADM. El archivo debe residir en el servidor y éste debe leerlo.

```
define script agadm file=my.script
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE SCRIPT

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

### Conceptos relacionados:

Uso de sentencias de flujo lógico en un script

### Tareas relacionadas:

Definición de un script del servidor

Ejecución de mandatos en paralelo o en serie

Realización de tareas simultáneamente en varios servidores



### Referencia relacionada:

Códigos de retorno de los scripts para IBM Spectrum Protect

## DEFINE SERVER (Definir un servidor para las comunicaciones de servidor a servidor)

Utilice este mandato para definir un servidor para utilizar funciones, tales como volúmenes virtuales, replicación de nodos, direccionamiento de mandatos y el movimiento de datos libre de la LAN, entre otros.

Utilice este comando para definir un servidor para las funciones siguientes:

- Configuración de Enterprise
- Anotación de eventos Enterprise
- Direccionamiento de comandos
- Volúmenes virtuales
- movimiento de datos sin LAN
- Réplica de nodo
-  Sistemas operativos AIX  Sistemas operativos Linux Movimiento de datos utilizando servidor de medios de z/OS
- Supervisión del estado de los servidores remotos
- Supervisión de alerta de los servidores remotos
- Exportación de servidor a servidor

Si utiliza un servidor de directorios LDAP para autenticar contraseñas, los servidores de destino deben estar configurados para las contraseñas autenticadas por LDAP. Los datos que se replican de un nodo que se autentica con un servidor de directorios LDAP son inaccesible si el servidor de réplica de destino no está configurado correctamente. Si el servidor de réplica de destino no está configurado, los datos replicados de un nodo LDAP todavía pueden seguir allí. Sin embargo, el servidor de réplica de destino debe estar configurado para que utilice LDAP si desea acceder a los datos.



El uso de volúmenes virtuales no está soportado si el servidor de origen y el servidor de destino residen en el mismo servidor de IBM Spectrum Protect.

Este mandato también se utiliza para definir un agente de almacenamiento de IBM Spectrum Protect como si fuese un servidor.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

Para:

- Direccionamiento de comandos
- Supervisión del estado de los servidores remotos
- Supervisión de alerta de los servidores remotos
- Exportación de servidor a servidor



Consejo: El direccionamiento de mandatos utiliza el ID y la contraseña del administrador que emite el mandato.

```
>>-DEfine--SERver--nombre_servidor--HLAddress-----ip_address---->
>--LLAddress-----puerto_tcp--+-----+----->
      '-COMMmethod-----TCPIP-'
>--+-----+-----+-----+----->
      '-URL-----url-' '-DESCRiption-----descripci3n-'
      .-SSL-----No-----
>--+-----+-----+-----+----->
      '-SSL-----+No--+-'
      '-Yes-'
      .-SESSiONSECurity-----TRANSiTiONal-----
>--+-----+-----+-----+-----<
      '-SESSiONSECurity-----+STRiCT-----+-'
      '-TRANSiTiONal-'
```

## Sintaxis

---

Para:

- Configuraci3n de Enterprise
- Anotaci3n de eventos Enterprise
- Agente de almacenamiento
- Servidores de origen y destino de r3plica de nodo
-  Sistemas operativos AIX  Sistemas operativos Linuxservidor de medios de z/OS

```
>>-DEfine--SERver--nombre_servidor----->
>--SERVERPAssword-----contrase1a--HLAddress-----ip_address---->
>--LLAddress-----puerto_tcp--+-----+----->
      '-COMMmethod-----TCPIP-'
>--+-----+-----+-----+----->
      '-URL-----url-' '-DESCRiption-----descripci3n-'
      (1)
      .-CROSSDEfine-----No----- (2)
>--+-----+-----+-----+----->
      '-CROSSDEfine-----+No--+-'
      '-Yes-'
      .-VALIdateprotocol-----No----- .-SSL-----No-----
>--+-----+-----+-----+----->
      '-VALIdateprotocol-----+No--+-' '-SSL-----+No--+-'
      '-All-' '-Yes-'
      .-SESSiONSECurity-----TRANSiTiONal-----
```



## URL

Especifica la dirección URL de este servidor. El parámetro es opcional.

## DELgraceperiod

Especifica un número de días en que el objeto permanece en el servidor de destino después de haber sido marcado para suprimirlo. Puede especificar un valor de 0 a 9999. El valor predeterminado es 5. Este parámetro es opcional.

## NODENAME




Especifica un nombre de nodo que ha de utilizar el servidor para conectarse con el servidor destino. Este parámetro es opcional. Si especifica el parámetro NODENAME, debe especificar también el parámetro PASSWORD. Si especifica el parámetro PASSWORD sin especificar el parámetro NODENAME, el nombre de nodo toma de forma predeterminada el nombre de servidor especificado con el comando SET SERVERNAME.

## DESCRIPTION

Especifica la descripción del servidor. El parámetro es opcional. La descripción puede tener hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

## CROSSDEFINE

Especifica si el servidor que ejecuta este mandato se define a sí mismo en el servidor que se especifica mediante este mandato. Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **Importante:** Este parámetro no se aplica a las definiciones del agente de almacenamiento.

Si se incluye este parámetro, también deberá emitir los mandatos SET SERVERNAME, SET SERVERPASSWORD, SET SERVERHLADDRESS, SET CROSSDEFINE y SET SERVERLLADDRESS. El valor predeterminado es NO.

Recuerde:

- Para las operaciones de réplica, los nombres de los servidores de réplica de origen y destino deben coincidir con los nombres especificados en este comando.
- CROSSDEFINE puede utilizarse con SSL=YES si todas las condiciones especificadas para el parámetro SSL=YES existen en el servidor de origen y destino.

Puede especificar uno de los siguientes valores:

No

La definición cruzada no se ha completado.

Yes

La definición cruzada se ha completado.

## VALIDATEprotocol (en desuso)

Especifica una comprobación de redundancia cíclica para validar los datos enviados entre el agente de almacenamiento y el servidor de IBM Spectrum Protect. El parámetro es opcional. El valor predeterminado es NO.

**Importante:** A partir de IBM Spectrum Protect Versión 8.1.2, la validación que estaba habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

## SSL

Especifica la modalidad de comunicación del servidor. El valor predeterminado es NO.

**Importante:** A partir de V8.1.2, el parámetro SSL utiliza SSL para cifrar ciertas comunicaciones con el servidor especificado, incluso si se especifica SSL=NO.

Las siguientes condiciones y consideraciones se aplican cuando especifica el parámetro SSL:

- Antes de iniciar los servidores, los certificados autofirmados de los servidores asociados deben estar en el archivo de base de datos de claves (cert.kdb) de cada uno de los servidores.
- Puede definir varios nombres de servidor con distintos parámetros en el mismo servidor de destino.
- Los agentes de almacenamiento puede emitir el mandato DSMSTA SETSTORAGESERVER e incluir los parámetros SSL para crear la base de datos clave.

Puede especificar uno de los siguientes valores:

No

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, excepto si el servidor envía o recibe datos de objeto. Los datos de objeto se envían y se reciben mediante TCP/IP. Si elige no cifrar los objetos de datos, el rendimiento del servidor será similar a la comunicación mediante una sesión TCP/IP y la sesión es segura.

Yes

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, incluso si el servidor envía o recibe datos de objeto.

## SESSIONSECURITY

Especifica si el servidor que está definiendo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

#### STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el servidor que se define. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor especificado y un servidor IBM Spectrum Protect.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el servidor especificado pueda autenticarse en el servidor IBM Spectrum Protect:

- Tanto el servidor que se define como el servidor IBM Spectrum Protect deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el servidor que está definiendo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre él mismo y el servidor IBM Spectrum Protect.


Los servidores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en IBM Spectrum Protect.

#### TRANSitional

Especifica que se aplican los valores de seguridad existentes para el servidor. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el servidor no cumplen nunca los requisitos para el valor STRICT, el servidor continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un servidor cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el servidor ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un servidor que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, el direccionamiento de mandatos o la exportación entre servidores, cuando un nodo o un administrador se autentica en el servidor IBM Spectrum Protect como nodo o administrador de otro servidor.

#### Sistemas operativos Linux TRANSFERMethod

 Sistemas operativos Linux Especifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

#### Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN).

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, las operaciones de transferencia de datos fallan.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Si especifica TRANSFERMETHOD=FASP en el mandato PROTECT STGPOOL o REPLICATE NODE, ese valor altera temporalmente el parámetro TRANSFERMETHOD en los mandatos DEFINE SERVER y UPDATE SERVER.

## Ejemplo: configurar dos servidores que utilicen SSL para comunicarse (configuración manual)

Consejo: Si ambos servidores están utilizando V8.1.2 o un software posterior, SSL se configura automáticamente entre los servidores y no se necesita configuración manual.

Si ninguno de los servidores está utilizando el software V8.1.2, debe configurar manualmente los dos servidores para utilizar SSL para comunicarse.

Las direcciones de servidor son las siguientes:

- ServerA está en `bfa.tucson.ibm.com`
- ServerB está en `bfb.tucson.ibm.com`

Complete los pasos siguientes para configurar los dos servidores para SSL:

1. Especifique la opción TCPPOPT 1500 para ambos servidores en el archivo de opciones dsmserv.opt.
2. Inicie los dos servidores.

3. Concluya los dos servidores para importar el certificado de socio cert256. Para ServerA, el certificado está en el directorio de instancia /tsma. Para ServerB, el certificado está en el directorio de instancia /tsmb.
4. Inicie los dos servidores. El archivo /tsma/cert256.arm se copia en /tsmb/cert256.bfa.arm en la dirección bfb.tucson.ibm.com. El archivo /tsmb/cert256.arm se copia en /tsmb/cert256.bfb.arm en la dirección bfa.tucson.ibm.com.
5. Emita el comando siguiente:
  - o Desde ServerA:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label "bfb" -file /tsma/cert256.bfb.arm
```

- o En ServerB:

```
gsk8capicmd_64 -cert -add -db cert.kdb -stashed -format ascii
-label "bfa" -file /tsmb/cert256.bfa.arm
```

En cada servidor, puede ver los certificados de la base de datos de claves con el mandato siguiente:

```
gsk8capicmd_64 -cert -list -db cert.kdb -stashed
```

6. Reinicie los servidores.
7. Consulte el mandato DEFINE SERVER. Para ServerA, emita el mandato de ejemplo siguiente:

```
DEFINE SERVER BFB hla=bfb.tucson.ibm.com lla=1542
serverpa=passwordforbfb SSL=YES
```

Para ServerB, emita el mandato de ejemplo siguiente:

```
DEFINE SERVER BFA hla=bfa.tucson.ibm.com lla=1542
serverpa=passwordforbfa SSL=YES
```

Si no utiliza SSL, emita el siguiente mandato de ejemplo DEFINE SERVER en ServerA:

```
DEFINE SERVER BFBTCP hla=bfb.tucson.ibm.com lla=1500
serverpa=passwordforbfb SSL=NO
```

Si no utiliza SSL, emita el siguiente mandato de ejemplo DEFINE SERVER en ServerB:

```
DEFINE SERVER BFATCP hla=bfa.tucson.ibm.com lla=1500
serverpa=passwordforbfa SSL=NO
```

## Ejemplo: Definir un servidor para comunicarse con otro servidor utilizando la seguridad de sesión estricta.

---

Defina un nombre de servidor de SERVER1 para utilizar los parámetros de seguridad más estrictos para autenticarse con el servidor IBM Spectrum Protect.

```
define server server1 sessionsecurity=strict
```

## Ejemplo: definir un servidor de destino

---

Un servidor destino tiene la dirección de alto nivel 9.116.2.67 y la dirección de bajo nivel 1570. Defina dicho servidor destino ante el servidor origen, denomínelo SERVER2 y establezca la contraseña en SECRET. Especifique que los objetos permanezcan en el servidor de destino durante siete días después de que se hayan marcado para la supresión.

```
define server server2 password=secret
hladdress=9.115.3.45 lladdress=1570 delgraceperiod=7
```

## Ejemplo: definir un servidor para que reciba mandatos de otros servidores

---

Definir un servidor que pueda recibir mandatos direccionados desde otros servidores. Denomine al servidor WEST\_COMPLEX. Establezca la dirección de alto nivel en 9.172.12.35, la dirección de bajo nivel en 1500 y la dirección URL en http://west\_complex:1580/.

```
define server west_complex
hladdress=9.172.12.35 lladdress=1500
url=http://west_complex:1580/
```

## Ejemplo: establecer una definición cruzada para los dos servidores

---

Utilizar la definición cruzada para definir SERVER\_A y SERVER\_B.

1. En SERVER\_B, especificar el nombre de servidor, la contraseña y las direcciones de alto y bajo nivel de SERVER\_B. Especifica que se admite la definición cruzada.

```
set servername server_b
set serverpassword mylife
set serverhladdress 9.115.20.80
set serverlladdress 1860
set crossdefine on
```

2. En SERVER\_A, especificar el nombre de servidor, la contraseña y las direcciones de alto y bajo nivel de SERVER\_A.









```
set servername server_a
set serverpassword yourlife
set serverhladdress 9.115.20.97
set serverlladdress 1500
```

3. En SERVER\_A, defina SERVER\_B:

```
define server server_b hladdress=9.115.20.80 lladdress=1860
serverpassword=mylife crossdefine=yes
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE SERVER

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE PATH	 Sistemas operativos AIX  Sistemas operativos Linux Define una ruta cuando el destino es un servidor de medios de z/OS.
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
 Sistemas operativos AIX  Sistemas operativos Linux UPDATE PATH	 Sistemas operativos AIX  Sistemas operativos Linux Define una ruta cuando el destino es un servidor de medios de z/OS.
UPDATE SERVER	Actualiza la información sobre un servidor.

## DEFINE SERVERGROUP (Definir un grupo de nodo)

Utilice este mandato para definir un grupo de servidores. Con un grupo de servidores, puede direccionar mandatos a varios servidores especificando sólo el nombre del grupo. Después de haber definido el grupo de servidores, agregue servidores al grupo con el mandato DEFINE GRPMEMBER.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DEFine SERVERGroup--nombre_grupo----->
>--+-----+-----><
  '-DESCRiption-----descripción-'
```

## Parámetros

nombre\_grupo (Obligatorio)

Especifica el nombre del grupo de servidores. La longitud máxima del nombre es de 64 caracteres.

DESCRiption

Especifica una descripción del grupo de servidores. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

## Ejemplo: definir un grupo de servidores

Definir un grupo de servidores denominado WEST\_COMPLEX.

```
define servergroup west_complex
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE SERVERGROUP

Comando	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## DEFINE SPACETRIGGER (Definir desencadenante de espacio)

Utilice este mandato para definir los valores de los desencadenantes que determinan cuándo y cómo ha de preparar el servidor espacio adicional cuando se han excedido los umbrales predeterminados en las agrupaciones de almacenamiento que utilizan las clases de dispositivo FILE y DISK. Los desencadenantes de espacio no estarán activados para las agrupaciones de almacenamiento con un parámetro RECLAMATIONTYPE=SNAPLOCK.

El servidor IBM Spectrum Protect asigna más espacio cuando la utilización de espacio alcanza un valor especificado. Después de haber asignado espacio adicional, el servidor añade espacio a la agrupación especificada (disco de acceso aleatorio o de acceso secuencial).

Importante: Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Un cálculo no preciso puede dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar desactivado.

Por ejemplo, si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calculará el espacio añadiendo valores que representan el espacio que resta en cada directorio. Estos cálculos de espacio

serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione el directorio que se ha especificado para la clase de dispositivo y que se produzca una condición de insuficiencia de espacio de forma prematura.

Para evitar posibles problemas y garantizar la obtención de un cálculo preciso, debe asociar cada directorio a un sistema de archivos distinto. Si un desencadenante se ha desactivado porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a activar el desencadenante especificando el mandato siguiente: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---

```
.-Fullpct----80-----.  
>>-DEFine SPACETrigger---STG---+-----+----->  
                                '-Fullpct----porcentaje-'  
  
. -SPACEexpansion---20-----.  
>--+-----+----->  
    '-SPACEexpansion---porcentaje-'  
  
>--+-----+----->  
    '-EXPansionprefix---prefijo-'  
  
>--+-----+-----<<  
    '-STGPOOL---nombre_agrupación_almacenamiento-'
```

## Parámetros

---

### STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

### Fullpct

Este parámetro especifica el porcentaje de utilización de la agrupación de almacenamiento. Este parámetro es opcional. Especifique un valor entero de 0 a 99. El valor predeterminado es 80. Un valor de cero (0) inactiva el desencadenante de espacio. Cuando se sobrepasa este valor, el desencadenante de espacio crea nuevos volúmenes. El hecho de haberse excedido el umbral podría no generar la creación de nuevos volúmenes hasta que se realice la siguiente petición de espacio.



Puede determinar la utilización de la agrupación de almacenamiento ejecutando el mandato `QUERY STGPOOL` con `FORMAT=DETAILED`. El porcentaje de utilización de la agrupación de almacenamiento se visualiza en el campo "Util. desencadenante espacio". El cálculo de este porcentaje no incluye volúmenes reutilizables potenciales. El cálculo de la utilización del porcentaje que se utiliza para la migración y la reclamación, no obstante, sí incluye los volúmenes reutilizables potenciales.

### SPACEexpansion

Para las agrupaciones de almacenamiento de tipo `FILE` de acceso secuencial, este parámetro se utiliza para determinar el número de volúmenes adicionales que se crean en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es 20. Los volúmenes se crean utilizando el valor `MAXCAPACITY` de la clase de dispositivo de la agrupación de almacenamiento. Para las agrupaciones de almacenamiento `DISK` de acceso aleatorio, el desencadenante de espacio crea un único volumen utilizando `EXPANSIONPREFIX`.

### EXPansionprefix

Para las agrupaciones de almacenamiento `DISK` de acceso aleatorio, este parámetro especifica el prefijo que el servidor utiliza para crear nuevos archivos de agrupación de almacenamiento. Este parámetro es opcional y sólo se aplica a la clase de dispositivo `DISK` de acceso aleatorio. El prefijo predeterminado es la ruta de instalación del servidor.



El prefijo puede incluir uno o varios caracteres de separación de directorios; por ejemplo:  Sistemas operativos AIX  
 Sistemas operativos Linux


/opt/tivoli/tsm/server/bin/

 Sistemas operativos Windows

c:\Archivos de programa\tivoli\tsm\



 Sistemas operativos AIX  Sistemas operativos Linux Puede especificar hasta 250 caracteres. Si especifica un prefijo erróneo, es posible que la ampliación automática no se ejecute.

 Sistemas operativos Windows Puede especificar hasta 200 caracteres. Si especifica un prefijo erróneo, es posible que la ampliación automática no se ejecute. Si el servidor se ejecuta como servicio de Windows, el prefijo predeterminado es el directorio c:\wnnt\system32.

Este parámetro no es válido para desencadenantes de espacio de agrupaciones de almacenamiento de acceso secuencial FILE. Los prefijos se obtienen de los directorios que se han especificado con la clase de dispositivo asociada.

#### STGPOOL

Especifica la agrupación de almacenamiento que está asociada con este desencadenante de espacio. Este parámetro es opcional para los desencadenantes de espacio de agrupación de almacenamiento. Si especifica el parámetro STG pero no se especifica el parámetro STGPOOL, se crea un desencadenante de espacio que se aplica a todas las agrupaciones de almacenamiento DISK (de acceso aleatorio) y FILE (de acceso secuencial) que no tienen un desencadenante de espacio específico.

Este parámetro no se aplica a agrupaciones de almacenamiento con el parámetro RECLAMATIONTYPE=SNAPLOCK.

## Ejemplo: definir un desencadenante de espacio que incremente el espacio de la agrupación de almacenamiento un 25 por ciento

Establecer un desencadenante de espacio de agrupación de almacenamiento para que la cantidad de espacio de una agrupación de almacenamiento se incremente un 25 por ciento cuando se alcance un porcentaje de utilización de los volúmenes existentes equivalente al 80 por ciento. El espacio se crea en los directorios asociados con la clase de dispositivo.

```
define spacetrigger stg spaceexpansion=25 stgpool=file
```

## Ejemplo: definir un desencadenante de espacio que incremente el espacio de la agrupación de almacenamiento un 40 por ciento

Establecer un desencadenante de espacio para la agrupación de almacenamiento WINPOOL1 para que la cantidad de espacio de la agrupación de almacenamiento se incremente un 40 por ciento cuando se alcance un porcentaje de utilización de los volúmenes existentes equivalente al 80 por ciento.

```
define spacetrigger stg spaceexpansion=40 stgpool=winpool1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE SPACETRIGGER

Comando	Descripción
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

## DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)

Utilice este mandato para definir un nuevo umbral de supervisión de estado.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.



Especifica el número de agrupaciones de almacenamiento definidas que no se pueden leer o en las que no se puede escribir.

**STGPOOLINUSEANDDEFINED**

Especifica el número total de volúmenes definidos que se están utilizando.

**ACTIVELOGUTIL**

Especifica el porcentaje de utilización actual del registro activo. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

**ARCHLOGUTIL**

Especifica la utilización actual del registro de archivado. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

**CPYSTGPOOLUTIL**

Especifica el porcentaje de utilización para una agrupación de almacenamiento de copia. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

**PMRYSTGPOOLUTIL**

Especifica el porcentaje de utilización para una agrupación de almacenamiento primario. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

**DEVCLASSPCTDRVOFFLINE**

Especifica el porcentaje de utilización de las unidades que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTDRVPOLLING**

Especifica el sondeo de unidades, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTLIBPATHSOFFLINE**

Especifica las rutas de biblioteca que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTPATHSOFFLINE**

Especifica el porcentaje de rutas de clase de dispositivo que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTDISKSNOTRW**

Especifica el porcentaje de discos que no se pueden grabar para la clase de dispositivo de disco. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTDISKSUNAVAILABLE**

Especifica el porcentaje de volúmenes de disco que no están disponibles, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**FILEDEVCLASSPCTSCRUNALLOCATABLE**

Especifica el porcentaje de volúmenes reutilizables que el servidor no puede asignar para una determinada clase de dispositivo de archivo no compartido. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**Condition**

Especifica la condición que se utiliza para comparar la salida de actividad con el valor especificado. El valor predeterminado es EXISTS. Especifique uno de los siguientes valores:

**EXists**

Crea un indicador de supervisión de estado si existe la actividad.

**GT**

Crea un indicador de supervisión de estado si la salida de actividad es mayor que el valor especificado.

**GE**

Crea un indicador de supervisión de estado si la salida de actividad es mayor que o igual al valor especificado.

**LT**

Crea un indicador de supervisión de estado si la salida de actividad es menor que el valor especificado.

**LE**

Crea un indicador de supervisión de estado si la salida de actividad es menor que o igual al valor especificado.

**EQual**

Crea un indicador de supervisión de estado si la salida de actividad es igual al valor especificado.

**Value (necesario)**

Especifica el valor que se compara con la salida de actividad para la condición especificada. Debe especificar este parámetro, a menos que CONDITION esté establecido en EXISTS. Puede especificar un entero en el rango 0 – 9999999999999999.

**Status**

Especifica que se cree el indicador de estado en la supervisión de estado si pasa la condición que se está evaluando. Este parámetro opcional tiene un valor predeterminado de NORMAL. Especifique uno de los siguientes valores:

**Normal**

Especifica que el indicador de estado tiene un valor de estado normal.

Aviso

Especifica que el indicador de estado tiene un valor de estado de aviso.

Error

Especifica que el indicador de estado tiene un valor de estado de error.

## Definir umbral de estado

Defina un umbral de estado para el porcentaje medio de utilización de agrupación de almacenamiento emitiendo el mandato siguiente:

```
define statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=85 condition=gt status=warning
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DEFINE STATUSTHRESHOLD

Comando	Descripción
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## DEFINE STGPOOL (Definir una agrupación de almacenamiento)

Utilice este mandato para definir una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia, una agrupación de datos activos, una agrupación de almacenamiento de contenedor de directorio, una agrupación de almacenamiento de copia de contenedor, o una agrupación de almacenamiento de contenedor en un entorno de nube.

Una agrupación de almacenamiento primaria proporciona un destino para copias de seguridad de los archivos, copias archivadas o archivos que se han migrado desde los nodos de cliente. Una agrupación de almacenamiento de copia proporciona un destino para copias de los archivos que se encuentran en agrupaciones de almacenamiento primarias. Una agrupación de datos activos proporciona un destino para las versiones activas de datos de copia de seguridad que se encuentran en las agrupaciones de almacenamiento primarias. Una agrupación de almacenamiento de contenedor proporciona un destino para los archivos con duplicados eliminados. Una agrupación de almacenamiento en la nube proporciona el almacenamiento en un entorno de nube. Una agrupación de almacenamiento de copia de contenedor proporciona una copia en cinta de una agrupación de almacenamiento de contenedor de directorio. El número máximo de agrupaciones de almacenamiento que puede definir para un servidor es 999.

Todos los volúmenes de una agrupación de almacenamiento pertenecen a la misma clase de dispositivo. Las agrupaciones de almacenamiento de acceso aleatorio utilizan el tipo de dispositivo DISK. Después de definir una agrupación de almacenamiento de acceso aleatorio, debe definir los volúmenes de la agrupación para crear el espacio de almacenamiento.

Las agrupaciones de almacenamiento de acceso secuencial utilizan las clases de dispositivo definidas para dispositivos de cinta, archivos en disco (tipo de dispositivo FILE) y el almacenamiento en otro servidor (tipo de dispositivo SERVER). Para crear espacio de almacenamiento en una agrupación de almacenamiento de acceso secuencial debe permitir los volúmenes reutilizables para la agrupación al definirla o actualizarla, o bien definir volúmenes para la agrupación después de definirla. También puede hacer ambas cosas.

Restricción: Si un cliente utiliza la función de escritura simultánea y la deduplicación de datos, la función de deduplicación de datos se desactiva durante el proceso de copia de seguridad en una agrupación de almacenamiento.

El mandato DEFINE STGPOOL tiene seis formatos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con DEFINE STGPOOL

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
MOVE MEDIA	Mueve los volúmenes de agrupaciones de almacenamiento gestionados por una biblioteca automatizada.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RENAME STGPOOL	Redenomina una agrupación de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.

Comando	Descripción
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de contenedores en la nube)  
Utilice este mandato para definir una agrupación de almacenamiento de contenedor en un entorno de nube. Este tipo de agrupación de almacenamiento se utiliza para la eliminación de duplicados de datos. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de contenedores de directorio)  
Utilice este mandato para definir una agrupación de almacenamiento de contenedores de directorio que se utilice para la deduplicación de datos.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de copia de contenedor)  
Utilice este mandato para definir una agrupación de almacenamiento de copia de contenedor para que contenga una copia de datos de una agrupación de almacenamiento de contenedor de directorios.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio)  
Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial)  
Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso secuencial.
- **DEFINE STGPOOL** (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial)  
Utilice este mandato para definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial.
- **DEFINE STGPOOL** (Definir una agrupación de datos activos asignada a dispositivos de acceso secuencial)  
Utilice este comando para definir una agrupación de almacenamiento de datos asignada a dispositivos de acceso secuencial.

## DEFINE STGPOOL (Definir una agrupación de almacenamiento de contenedores en la nube)

Utilice este mandato para definir una agrupación de almacenamiento de contenedor en un entorno de nube. Este tipo de agrupación de almacenamiento se utiliza para la eliminación de duplicados de datos. No se admiten las agrupaciones de almacenamiento de contenedores en la nube en Linux on System z.

Consejo: Para optimizar el rendimiento de archivado y copia de seguridad, configure uno o varios directorios de almacenamiento local para contener temporalmente los datos que IBM Spectrum Protect está transfiriendo a la nube. Después de utilizar un mandato DEFINE STGPOOL para definir una agrupación de almacenamiento de contenedores en la nube, utilice el mandato DEFINE STGPOOLDIRECTORY para asignar directorios de almacenamiento local a la agrupación de almacenamiento de contenedores en la nube. Para obtener más información, consulte el apartado Optimización del rendimiento para el almacenamiento de objetos en la nube.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--STGType----Cloud----->
    .-Pooltype----Primary-.
>--+-----+-----+-----+-----+-----+-----+----->
    '-Pooltype----Primary-' '-DESCRIPTION----descripción-'
    .-CLOUDType----Swift-----
>--+-----+-----+-----+-----+-----+-----+----->
    '-CLOUDType----+Azure-----+'
                    +-S3-----+
                    +-Softlayer--+
                    +-Swift-----+
                    '-V1Swift--'

                                (1)
>>-IDentity----identidad_nube-----PAssword----contraseña----->
    .-CLOUDLocation----Offpremise----.
>--+-----+-----+-----+-----+-----+-----+----->
    '-CLOUDLocation----+Offpremise-+-'
                    '-ONpremise--'
```



Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

Este parámetro es opcional. Si no especifica el parámetro, se utiliza el valor predeterminado SWIFT.

#### CLOUDUrl

Especifica el URL del entorno de nube donde está configurando la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un punto final de servicio blob, una URL de punto final de región, una dirección IP de accesor, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo `https://` o `http://` al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL no se valida hasta que empieza la primera copia de seguridad.

Para obtener más información sobre cómo encontrar estos valores, seleccione su proveedor de servicios en la nube de la lista que aparece en la página Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos.

Consejo: Para utilizar más de una aplicación de accesos de IBM Cloud Object Storage, liste las direcciones IP de las aplicaciones de accesos separadas por una barra vertical (`|`), sin espacios, como `CLOUDURL=<accesser_URL1>|<accesser_URL2>|<accesser_URL3>`. Si va a utilizar el centro de operaciones, escriba una dirección IP de aplicación de acceso en el campo URL del asistente Añadir agrupación de almacenamiento y, a continuación, pulse Intro para añadir direcciones IP adicionales. Utilice varias aplicaciones de acceso para mejorar el rendimiento.

Este parámetro es necesario si especifica el parámetro CLOUDTYPE.

- Azure
- S3 (Simple Storage Service)
- Softlayer
- Swift
- V1Swift

#### Identity

Especifica el ID de usuario para la nube que se ha especificado en el parámetro STGTYPE=CLOUD. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si ha especificado CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

#### PASSword (Obligatorio)

Especifica la contraseña para la nube especificada en el parámetro STGTYPE=CLOUD. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres. Los parámetros IDENTITY y PASSWORD no se validan hasta que empieza la primera copia de seguridad.

#### CLOUDLocation

Especifica la ubicación física de la nube especificada en el parámetro CLOUD. Este parámetro es opcional. El valor predeterminado es OFFPREMISE. Puede especificar uno de los siguientes valores:

- OFFpremise
- ONpremise

#### BUCKETName

Especifica el nombre de un grupo de AWS S3 o una caja fuerte de IBM Cloud Object Storage que se van a utilizar con esta agrupación de almacenamiento, en lugar de utilizar el nombre de grupo o el nombre de caja fuerte predeterminados. Este parámetro es opcional y sólo es válido si especifica CLOUDTYPE=S3. Si no existe el nombre que especifica, el servidor crea un grupo o caja fuerte con el nombre especificado antes de utilizar el grupo o caja fuerte. Siga las restricciones de asignación de nombres de su proveedor de nube cuando especifique este parámetro. Revise los permisos del grupo o caja fuerte y asegúrese de que las credenciales de esta agrupación de almacenamiento tienen permiso de lectura, grabación, lista y supresión de objetos en este grupo o caja fuerte. Si no tiene la posibilidad de cambiar o ver los permisos, y todavía no ha grabado datos en esta agrupación de almacenamiento, utilice el mandato UPDATE STGPPOOL con el parámetro BUCKETNAME para utilizar un grupo o caja fuerte diferente.

#### ACCess

Especifica cómo acceden los nodos cliente y los procesos de servidor a la agrupación de almacenamiento en la nube. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar uno de los siguientes valores:

##### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en la agrupación de almacenamiento en la nube. Este es el valor predeterminado.

##### READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en la agrupación de almacenamiento en la nube.

##### UNAVailable



Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento en la nube.

#### MAXWriters

Especifica el número máximo de sesiones de grabación que se pueden ejecutar simultáneamente en la agrupación de almacenamiento en la nube. Especifique un número máximo de sesiones de grabación para controlar que el rendimiento de la agrupación de almacenamiento en la nube no afecte negativamente a otros recursos del sistema. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

#### NOLimit

Especifica que no existe un límite de tamaño máximo para el número de grabadores que puede utilizar. Este es el valor predeterminado.

#### máximo\_grabadores

Limita el número máximo de grabadores que puede utilizar. Especifique un número entero del 1 al 99999.

#### REUsedelay

Especifica el número de días que deben transcurrir después de que se hayan eliminado todas las extensiones deduplicadas de una agrupación de almacenamiento en la nube. Este parámetro controla la duración con que las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento en la nube. Cuando caduca el valor especificado para este parámetro las extensiones deduplicadas se suprimen de la agrupación de almacenamiento en la nube. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

#### 1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento en la nube pasado un día. Este es el valor predeterminado.

#### días

Puede especificar un entero en el rango 0 – 9999.

Consejo: Defina este parámetro en un valor que sea mayor que el número especificado para el mandato SET DRMDBBACKUPEXPIREDDAYS. Si establece este parámetro en un valor superior, puede garantizar que restaura la base de datos a un nivel anterior, las referencias a los archivos en la agrupación de almacenamiento en la nube siguen siendo válidas.

#### ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

#### Yes

Especifica que el servidor cifra los datos de cliente.

#### No

Especifica que el servidor no cifra los datos de cliente.

Este parámetro es opcional. El valor predeterminado depende de la ubicación física de la nube, que se especifica mediante el parámetro CLOUDLOCATION. Si la nube está fuera de las instalaciones, el servidor cifra los datos de forma predeterminada. Si la nube está en las instalaciones, el servidor no cifra los datos de forma predeterminada.

#### COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

#### Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

## Ejemplo 1: definir una agrupación de almacenamiento en la nube OpenStack Swift

---

Defina una agrupación de almacenamiento en la nube OpenStack Swift denominada STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password description="OpenStack Swift cloud"
```

## Ejemplo 2: definir una agrupación de almacenamiento primario en la nube

---

Defina una agrupación de almacenamiento primario en la nube denominada STGPOOL1.

```
define stgpool stgpool1 stgtype=cloud
cloudtype=swift cloudurl=http://123.234.123.234:5000/v2.0
identity=admin:admin password=password pooltype=primary
```





almacenamiento son 5 GB. Puede utilizar una de las siguientes unidades de medida:

Tabla 1. Factor de escala para el tamaño de archivo máximo

Factor de escala	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

Consejo: Si no especifica una unidad de medida para el tamaño máximo de archivo, el valor se especifica en bytes.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 2. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

Agrupación especificada	Resultado
No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor no almacena el archivo.
Se ha especificado una agrupación como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor almacena el archivo en la agrupación de almacenamiento que ha especificado.

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos durante el proceso de deduplicación de datos, el servidor considera que el tamaño del proceso de deduplicación de datos es el tamaño de archivo. Si el tamaño total de todos los archivos del proceso es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

#### MAXWriters

Especifica el número máximo de hebras de E/S para los siguientes procesos:

- El número de hebras de E/S que se pueden ejecutar simultáneamente en la agrupación de almacenamiento de contenedores de directorio.
- El número de hebras de E/S que se graban simultáneamente en la agrupación de almacenamiento de contenedores de directorio.

Este parámetro es opcional. Como práctica recomendada, utilice el valor predeterminado NOLIMIT. Puede especificar los valores siguientes:

#### NOLimit

Especifica que no se graba ningún número máximo de hebras de E/S en la agrupación de almacenamiento máximo\_grabadores

Limita el número máximo de hebras de E/S que puede utilizar. Especifique un número entero del 1 al 99999.

Consejo: El servidor de IBM Spectrum Protect gestiona el número de hebras de E/S de forma automática en función de los recursos que hay disponibles y la carga del servidor.

#### NEXTstgpool

Especifica el nombre de una agrupación de almacenamiento secuencial primaria o de acceso aleatorio en la que se almacenan los archivos cuando la agrupación de almacenamiento de contenedores de directorio está llena. Este parámetro es opcional.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

#### PROTECTstgpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino donde se realiza la copia de seguridad de los datos cuando utiliza el mandato PROTECT STGPOOL para esta agrupación de almacenamiento. Este parámetro es opcional.

#### PROTECTLOCstgpools

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor en un dispositivo local en el que se realiza la copia de seguridad de los datos. Esta agrupación de almacenamiento de copia de contenedor será una agrupación de almacenamiento de destino local cuando utilice el mandato PROTECT STGPOOL. Puede especificar un máximo de dos nombres de agrupación de almacenamiento de copia de contenedor. Puede separar varios nombres con comas y sin espacios intercalados. La longitud máxima de cada nombre es de 30 caracteres. Este parámetro es opcional.

#### REUsedelay

Especifica el número de días que deben transcurrir antes de que se eliminen todas las extensiones con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio. Este parámetro controla el tiempo durante el cual las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento de contenedores de directorio después de que ya no se haga referencia a ellas. Cuando expira el período de tiempo especificado para el parámetro, las extensiones con duplicados eliminados se suprimen de la agrupación de almacenamiento de contenedores de directorio. Especifique un número entero del 0 al 9999. El valor predeterminado para las agrupaciones de almacenamiento de contenedores de directorio es 1, lo que significa que las extensiones con duplicados eliminados a las que ya no se hace referencia se suprimen de una agrupación de almacenamiento de contenedores de directorio al cabo de 1 día.

Establezca este parámetro en un valor mayor que el número especificado como periodo de copia de seguridad de base de datos, para asegurarse de que las extensiones de datos continúan siendo válidas cuando restaura la base de datos a otro nivel.

#### ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente.

#### COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

## Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio configurada para almacenamiento de desbordamiento para cuando la agrupación de almacenamiento está llena

---

Definir una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL1. La agrupación de almacenamiento está configurada para que el almacenamiento se desborde en una agrupación de almacenamiento de cinta cuando la agrupación de almacenamiento este llena.

```
define stgpool stgpool1 stgtype=directory nextstgpool=overflow_tape_pool
```

## Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio que especifique el tamaño máximo de archivo

---

Defina una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL2. La agrupación de almacenamiento especifica el tamaño máximo de archivo que el servidor puede almacenar en la agrupación de almacenamiento en 100 megabytes.

```
define stgpool stgpool2 stgtype=directory maxsize=100M
```

## Ejemplo: Definir una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de origen con una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino para hacer copia de seguridad de los datos

---

Defina una agrupación de almacenamiento de contenedores de directorio llamada STGPOOL3. Se hace una copia de seguridad de los datos de la agrupación de almacenamiento STGPOOL3 en una agrupación de almacenamiento de contenedores de directorio, TARGET\_STGPOOL3, en el servidor de réplica de destino.

```
define stgpool stgpool3 stgtype=directory protectstgpool=target_stgpool3
```





El tiempo que es necesario para realizar la operación de copia se puede reducir utilizando varios procesos paralelos. Sin embargo, en algunos casos, cuando se ejecutan varios procesos, uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso distinto.

Cuando especifique este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a la operación de copia. Para acceder a un volumen de cinta, el servidor utiliza un punto de montaje y una unidad. El número de puntos de montaje y unidades disponibles depende del límite de montaje de la clase de dispositivo de la agrupación de almacenamiento y de otra actividad del servidor y del sistema.

Este parámetro se ignora si utiliza la opción PREVIEW=YES en el mandato PROTECT STGPOOL. En ese caso, sólo se utiliza un proceso y no se necesitan puntos de montaje ni unidades.

#### REClaim

Especifica cuando un volumen pasa a ser seleccionable para la reclamación y la reutilización. Especifica la elegibilidad como el porcentaje de espacio de un volumen que está ocupado por las extensiones que ya no se almacenan en la agrupación de almacenamiento de contenedor de directorios. La reclamación mueve cualesquiera extensiones que sigan almacenadas en la agrupación de almacenamiento de contenedor de directorios de volúmenes elegibles a otros volúmenes. La reclamación se produce sólo cuando un mandato PROTECT STGPOOL almacena datos en esta agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero en el rango 1 - 100. El valor predeterminado es 100, lo que significa que los volúmenes de esta agrupación de almacenamiento no se reclaman.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Al establecer un valor de reclamación de 50 o superior, los datos que se mueven de dos volúmenes reclamados no utilizan más del equivalente de un nuevo volumen.

Tenga cuidado al utilizar la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Por lo tanto, para fines de recuperación ante siniestro, asegúrese de que planifica las copias de seguridad de bases de datos para que se ejecuten después de que se hayan ejecutado las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM, y asegúrese de que todos los volúmenes de copia de seguridad de bases de datos se trasladen fuera del local junto con los volúmenes de DRM.

Consejo: Establezca diferentes valores de reclamación para las agrupaciones de almacenamiento de copia de contenedor fuera del local y dentro del local. Debido a que las agrupaciones de almacenamiento de copia de contenedor almacenan datos de eliminación de duplicados, las extensiones de datos abarcan varios volúmenes de cinta. Cuando seleccione un umbral de reclamación para una copia fuera del local, tenga en cuenta el número de puntos de montaje disponibles y el número de volúmenes de cinta que debe recuperar en caso de siniestro. Establecer un umbral más alto, significa que se deberán recuperar más volúmenes que si se establece la reclamación en un valor inferior. Si se utiliza un umbral más bajo se reduce el número de puntos de montaje necesarios en caso de siniestro. El método preferido consiste en definir el valor de reclamación para copias externas en 60 y, para copias internas, en el intervalo 90 - 100.

#### RECLAIMLIMIT

Especifica el número máximo de volúmenes que reclama el servidor cuando se emite el mandato PROTECT STGPOOL y se especifican las opciones RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED. Este parámetro solo es válido para las agrupaciones de almacenamiento de copia de contenedor. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

##### NOLimit

Especifica que todos los volúmenes de la agrupación de almacenamiento de copia de contenedor se procesen para la reclamación.

##### límite\_vol

Especifica el número máximo de volúmenes de la agrupación de almacenamiento de copia de contenedor que se reclaman. El valor que se especifique determinará cuántas nuevas cintas reutilizables están disponibles una vez completado el proceso de reclamación. Puede especificar un número comprendido entre 1 y 100000.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todas las extensiones de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva al estado reutilizable. Este parámetro es opcional. Puede especificar un entero en el rango 0 – 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo al estado reutilizable, tan pronto como se han suprimido todas las extensiones del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a extensiones de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. Si utiliza gestor



recuperación ante siniestro, el número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

## Ejemplo: Definir una agrupación de almacenamiento de copia de contenedor con una clase de dispositivo LTO7A

Definir una agrupación de almacenamiento de copia de contenedor, CONTAINER1\_COPY2, en la clase de dispositivo LTO7A. Se permitirán hasta 50 volúmenes reutilizables en esta agrupación. La reutilización de volúmenes se retardará 45 días.

```
define stgpool container1_copy2 lto7a pooltype=copycontainer
maxscratch=50 reusedelay=45
```

Tabla 1. Mandatos relacionados con DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia de contenedor)

Comando	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (copia de contenedor)	Actualizar una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (contenedor de directorios)	Actualizar una agrupación de almacenamiento de contenedores de directorios.

## DEFINE STGPOOL (Definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio)

Utilice este mandato para definir una agrupación de almacenamiento primaria asignada a dispositivos de acceso aleatorio.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine STGpool--nombre_agrupación--DISK----->
. -Pooltype----Primary-. .-STGType----Devclass-.
>--+-----+-----+-----+----->
' -Pooltype----Primary-' '-STGType----Devclass-'

>--+-----+-----+-----+----->
' -DESCription----descripción-'

. -ACCess----READWrite----- .
>--+-----+-----+-----+----->
' -ACCess----+READWrite----+'
+ -READOnly----+
' -UNAVailable-'

. -MAXSize----NOLimit----- .
>--+-----+-----+-----+----->
' -MAXSize----tamaño_máximo_archivo-'

. -CRCDATA----No----- .
>--+-----+-----+-----+----->
' -CRCDATA----+Yes--+'
```



Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

**READWrite**

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

**READOnly**

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

**UNAVailable**

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

**MAXSize**

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

**NOLimit**

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

**tamaño\_máximo\_archivo**

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo para esta agrupación de almacenamiento son 5 GB. Puede utilizar una de las siguientes unidades de medida:

Factor de escala	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
----------------------	-------------------------	-----------

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSize=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

#### CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

##### Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se produce una carga general adicional para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

##### No

Especifica que los datos se almacenan sin información de CRC.

#### NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. Este parámetro es opcional. Si no especifica ninguna agrupación de almacenamiento siguiente, se producen las acciones siguientes:

- El servidor no puede migrar los archivos de esta agrupación de almacenamiento
- El servidor no puede almacenar archivos que superen el tamaño máximo de esta agrupación de almacenamiento en otra agrupación de almacenamiento

#### Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

#### HIghmig

Especifica que el servidor inicia la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 100. El valor predeterminado es 90.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por nodo a la siguiente agrupación de almacenamiento. El parámetro NEXTSTGPOOL define este valor. Puede especificar HIGHMIG=100 para impedir que se produzca la migración en esta agrupación de almacenamiento.

#### LOWmig

Especifica que el servidor detiene la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 99. El valor predeterminado es 70.

Cuando la migración se realiza por nodo o espacio de archivos, en función de la proximidad, el nivel de ocupación de la agrupación de almacenamiento puede caer por debajo del valor que ha especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0.

#### CAChe

Especifica si el proceso de migración deja una copia en caché de un archivo en esta agrupación de almacenamiento una vez migrado el archivo a la siguiente agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

Yes

Especifica que está activada la función de caché.

No

Especifica que está desactivada la función de caché.

Si se utiliza la función de caché se puede mejorar la posibilidad de recuperar archivos, pero puede afectar al rendimiento de otros procesos.

#### MIGProcess

Especifica el número de procesos que utiliza el servidor para migrar los archivos de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero del 1 al 999. El valor predeterminado es 1.

Durante la migración, estos procesos se ejecutan en paralelo para proporcionar el potencial de mejorar los índices de migración.

Consejos:

- El número de procesos de migración depende de los siguientes valores:
  - El parámetro MIGPROCESS
  - El valor de proximidad de la agrupación siguiente
  - El número de nodos o el número de grupos de proximidad con datos en la agrupación de almacenamiento que se está migrando

Por ejemplo, supongamos que tenemos `MIGPROCESS = 6`, el parámetro `COLLOCATE` de la siguiente agrupación está establecido en `NODE`, pero solo hay dos nodos con datos en la agrupación de almacenamiento. El proceso de migración consta solo de dos procesos, no de seis. Si el parámetro `COLLOCATE` está establecido en `GROUP` y ambos nodos están en el mismo grupo, el proceso de migración consta solamente de un proceso. Si el parámetro `COLLOCATE` está establecido en `NO` o `FILESPACE`, y cada nodo tiene dos espacios de archivos con datos de copia de seguridad, el proceso de migración consta de cuatro procesos.

- Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

#### MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Para calcular un valor para comparar con el valor `MIGDELAY` especificado, el servidor cuenta los elementos siguientes:

- El número de días que el archivo ha estado en la agrupación de almacenamiento
- El número de días, si hay alguno, desde que un cliente recuperó el archivo

El menor de ambos valores se compara con el valor de `MIGDELAY` especificado. Por ejemplo, si se cumplen todas las condiciones siguientes, no se migrará un archivo:

- Un archivo ha permanecido en una agrupación de almacenamiento durante cinco días.
- Un cliente ha accedido al archivo en los tres últimos días.
- El valor especificado para el parámetro `MIGDELAY` es cuatro días.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración.

Si desea que el servidor cuente el número de días basándose tan solo en el momento en que se almacenó un archivo y no en el momento en el que se recuperó, utilice la opción del servidor `NORETRIEVEDATE`.

#### MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional. El valor predeterminado es YES.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

#### AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. El valor predeterminado es CLIENT. Este parámetro es opcional y afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPools. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPools.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea está inhabilitada.

Client

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRATION

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

#### COPYSTGPools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. El parámetro COPYSTGPools es opcional. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Al especificar un valor para el parámetro COPYSTGPools, también puede especificar un valor para el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPools y ACTIVEDATAPools no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricción: No se admite la función de grabación simultánea en las siguientes operaciones de almacenamiento:

- Cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
- Operaciones de copias de seguridad de NAS. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia:
  - Las agrupaciones de almacenamiento de copia se ignoran
  - Los datos solo se almacenan en la agrupación de almacenamiento primaria

Atención: La función que proporciona el parámetro COPYSTGPOLLS no tiene como finalidad sustituir el mandato BACKUP STGPOLLS. Si utiliza el parámetro COPYSTGPOLLS, continúe utilizando el mandato BACKUP STGPOLLS para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

#### COPYContinue

Especifica cómo reacciona normalmente el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOLLS. Este parámetro es opcional. El valor predeterminado es YES. Si especifica el parámetro COPYCONTINUE, también debe especificar el parámetro COPYSTGPOLLS.

Puede especificar los siguientes valores:

#### Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

#### No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

#### Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

#### ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEDATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOLLS y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro solamente está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos "NATIVE" o "NONBLOCK". Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - o NETAPPDUMP
  - o CELERRADUMP
  - o NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria especificada en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos:
  - o Las agrupaciones de datos activos se ignoran
  - o Los datos solo se almacenan en la agrupación de almacenamiento primaria
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el mandato COPY ACTIVE DATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVE DATA POOLS no tiene como finalidad sustituir al mandato COPY ACTIVE DATA. Si utiliza el parámetro ACTIVE DATA POOLS, utilice el mandato COPY ACTIVE DATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

#### SHRED

Especifica si los datos se van a sobregrabar físicamente cuando se supriman. Este parámetro es opcional. Puede especificar un entero del 0 al 10. El valor predeterminado es 0.

Si especifica un valor de cero, el servidor suprime los datos de la base de datos. Sin embargo, el almacenamiento que se utiliza para contener los datos no se sobregraba, y los datos existirán en el almacenamiento hasta que se reutilice el almacenamiento para otros datos. Los datos se podrían descubrir y reconstruir tras haberlos suprimido.

Si especifica un valor mayor que cero, el servidor suprime los datos lógicamente y físicamente. El servidor sobregraba el almacenamiento utilizado para contener los datos el número especificado de veces. Esta sobregrabación aumenta la dificultad de descubrir y reconstruir los datos tras su supresión.

Para asegurarse de que todas las copias de los datos se destruyen, especifique un valor SHRED superior a cero para la agrupación de almacenamiento especificada en el parámetro NEXT STG POOL. No especifique ni COPY STG POOLS ni ACTIVE DATA POOLS. Normalmente la especificación de valores relativamente altos para el recuento de sobregrabación mejora el nivel de seguridad, pero podría afectar negativamente al rendimiento.

La sobregrabación de datos suprimidos se realiza de forma asíncrona tras completarse la operación de supresión. Por lo tanto, el espacio ocupado por los datos suprimidos permanecerá ocupado durante algún tiempo. El espacio no está disponible como espacio libre para nuevos datos.

No se puede utilizar un valor SHRED superior a cero si el valor del parámetro CACHE es YES.

Importante: Después de que haya finalizado una operación de exportación y se hayan identificado los archivos para la exportación, los cambios que se realicen en el valor SHRED se ignorarán. Una operación de exportación que se ha suspendido retiene el valor de SHRED original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor SHRED de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el comando de exportación después de realizar la operación de limpieza necesaria.

## Ejemplo: definir una agrupación de almacenamiento primaria para una clase de dispositivo DISK

Definir una agrupación de almacenamiento primaria, POOL1, que utilice la clase de dispositivo DISK, con la función de caché activada. Limitar el tamaño de archivo máximo a 5 MB. Almacenar los archivos de más de 5 MB en agrupaciones de almacenamiento subordinadas, que empiezan con la agrupación de almacenamiento PROG2. El umbral superior de migración se establecerá en el 70 % y el umbral inferior de migración en el 30 %.

```
define stgpool pool1 disk
description="main disk storage pool" maxsize=5m
```







'-IDENTIFYProcess-----número-----'

#### Notas:

1. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos NETAPPDUMP, CELERRADUMP o NDMPDUMP.
2. Este parámetro no está disponible o se pasa por alto en el caso de agrupaciones de almacenamiento CENTERA.
3. El valor RECLAMATIONTYPE=SNAPLOCK sólo es válido para las agrupaciones de almacenamiento definidas en los servidores que están activados para IBM Spectrum Protect para retención de datos. La agrupación de almacenamiento debe estar asignada a una clase de dispositivo FILE y los directorios especificados en la clase de dispositivo deben ser volúmenes NetApp SnapLock.
4. Los valores NETAPPDUMP, CELERRADUMP y NDMPDUMP no son válidos para las agrupaciones de almacenamiento definidas con una clase de dispositivo FILE-type.
5. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
6. Este parámetro sólo está disponible cuando el valor del parámetro DEDUPLICATE es YES.

## Parámetros

---

#### nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de definir. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

#### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo a la que pertenece el grupo de copia que se ha de suprimir. Puede especificar cualquier clase de dispositivo excepto la clase de dispositivo DISK.

#### POoltype=Primary

Especifica que desea definir una agrupación de almacenamiento primaria. Este parámetro es opcional. El valor predeterminado es PRIMARY.

#### STGType

Especifica el tipo de almacenamiento que desea definir para una agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es DEVCLASS.

#### Devclass

Especifica que se asigna un tipo de clase de dispositivo de agrupación de almacenamiento a la agrupación de almacenamiento.

#### DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

#### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

#### READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

#### UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

#### MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar uno de los siguientes valores:

#### NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

#### tamaño\_máximo\_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSize=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

Restricción:

Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

#### NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. No puede migrar datos de una agrupación de almacenamiento de acceso secuencial a una agrupación de almacenamiento de acceso aleatorio. Este parámetro es opcional.

Si esta agrupación de almacenamiento no tiene una agrupación de almacenamiento que le siga, el servidor no puede migrar los archivos de esta agrupación de almacenamiento y no puede almacenar en otra agrupación de almacenamiento los archivos que sobrepasan el tamaño máximo de esta agrupación de almacenamiento.

Cuando no hay suficiente espacio disponible en la agrupación de almacenamiento actual, el parámetro NEXTSTGPOOL para las agrupaciones de almacenamiento de acceso secuencial no permite que los datos se almacenen en la agrupación siguiente. En este caso, el servidor emite un mensaje y la transacción no se efectúa correctamente.

Para las siguientes agrupaciones de almacenamiento con un tipo de dispositivo FILE, el servidor realiza una comprobación preliminar para determinar si hay disponible espacio suficiente. Si no hay espacio disponible, el servidor salta a la siguiente agrupación de almacenamiento de la jerarquía. Si hay espacio disponible, el servidor intenta almacenar datos en esa agrupación. No obstante, es posible que falle la operación de almacenamiento porque cuando se intenta realmente realizar la operación de almacenamiento el espacio ya no está disponible.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor de nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.
- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

#### HIghmig

Especifica que el servidor inicia la migración cuando la utilización de la agrupación de almacenamiento alcanza este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes

de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 100. El valor predeterminado es 90.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por volumen, a la siguiente agrupación de almacenamiento definida para la agrupación. Puede establecer el umbral superior de migración en 100 para impedir la migración en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### LOwmig

Especifica que el servidor detiene la migración cuando la utilización de la agrupación de almacenamiento es igual o inferior a este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 99. El valor predeterminado es 70.

Cuando la agrupación de almacenamiento alcanza el umbral inferior de migración, el servidor no inicia la migración de los archivos de otro volumen. Puede establecer el umbral inferior de migración en 0 para permitir que la migración vacíe la agrupación de almacenamiento.



Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es 60, excepto para agrupaciones de almacenamiento que utilicen dispositivos WORM.

 Sistemas operativos AIX  Sistemas operativos Windows Para las agrupaciones de almacenamiento que utilizan dispositivos WORM, se puede bajar el valor predeterminado 100. Al bajar el valor, el servidor puede consolidar los datos en menos volúmenes cuando sea necesario. Los volúmenes que se vacían por la operación de reclamación se pueden dar de baja de la biblioteca, con lo que quedan ranuras libres para nuevos volúmenes. Los volúmenes no se pueden reutilizar porque son de una sola operación de grabación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1. Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento primaria de acceso secuencial.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que no se ha especificado el parámetro RECLAIMSTGPOOL o que la agrupación de almacenamiento de reclamación tiene la misma clase de dispositivo que la agrupación de almacenamiento que se reclama, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMSTGpool

Especifica otra agrupación de almacenamiento primaria como destino de los datos reclamados de esta agrupación de almacenamiento. Este parámetro es opcional. Cuando el servidor reclama volúmenes para la agrupación de almacenamiento, el servidor traspasa los datos sin caducar de los volúmenes que se están reclamando a la agrupación de almacenamiento indicada en este parámetro.

Una agrupación de almacenamiento de reclamación tiene la mayor utilidad para una agrupación de almacenamiento que sólo tenga una unidad en su biblioteca. Al especificar este parámetro, el servidor traspasa todos los datos de los volúmenes reclamados a la agrupación de almacenamiento de reclamación independientemente del número de unidades de la biblioteca.

Para volver a traspasar los datos de la agrupación de almacenamiento de reclamación a la agrupación de almacenamiento original, utilice la jerarquía de agrupaciones de almacenamiento. Especifique la agrupación de almacenamiento original como la siguiente agrupación de almacenamiento de la agrupación de almacenamiento de reclamación.

Restricción:

- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAMATIONtype

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

##### THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

##### SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención por medio del software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido para agrupaciones de almacenamiento que están definidos en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El mandato DEFINE puede fallar si el parámetro RECLAMATIONTYPE especificado es distinto del que está definido para las agrupaciones de almacenamiento que ya están definidas en el nombre de clase de dispositivo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional. El valor predeterminado es GROUP.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario. La función de proximidad también pueden afectar al número de procesos de migración de discos a agrupación secuencial.

Puede especificar una de las opciones siguientes:

#### No

Especifica que la función de proximidad está desactivada. Durante la migración de disco, los procesos se crean a un nivel de espacio de archivos.

#### GGroup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no añade nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para nodos agrupados, y en el nivel de nodo para nodos no agrupados.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos que se denominan A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para espacios de archivos agrupados.



Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

#### NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Para COLLOCATE=NODE, el servidor crea procesos en el nivel de nodo cuando se migran datos del disco.

#### FILESPACE

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

Para COLLOCATE=FILESPACE, el servidor crea procesos en el nivel de espacio de archivos al migrar datos del disco.

#### MAXSCRATCH (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables, se evita tener que definir cada volumen que se va a utilizar.

El valor especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Cuando se suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el comando SET DRMDBBACKUPEXPIREDDAYS.

#### OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el mandato. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco. Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Todos los archivos de un volumen deben poder seleccionarse para una operación de migración antes de que el servidor seleccione el volumen para migración. Para calcular un valor para comparar con el valor MIGDELAY especificado, el servidor cuenta el número de días que el archivo ha permanecido en la agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración. Si desea que el servidor cuente el número de días sólo basándose en el momento en que se almacenó un archivo y no en el momento en que se recuperó, utilice la opción del servidor NORETRIEVEDATE.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional. El valor predeterminado es YES.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

#### Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

#### No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

#### MIGProcess

Especifica el número de procesos paralelos que se utilizará para migrar los archivos de los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta el número de agrupaciones de almacenamiento secuenciales que participarán en la migración y el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la migración.

Por ejemplo, supongamos que desea migrar los volúmenes de dos agrupaciones de almacenamiento secuencial primarias simultáneamente y que desea especificar tres procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que la agrupación de almacenamiento a la que se están migrando los archivos tienen la misma clase de dispositivo que la agrupación de almacenamiento de la que se migran, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una unidad corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar simultáneamente seis procesos de migración, necesita como mínimo un total de 12 puntos de montaje y 12 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 12 como mínimo.

Si el número de procesos de migración especificados es mayor que el número de puntos de montaje o unidades disponibles, los procesos que no obtengan puntos de montaje o unidades esperarán a que haya puntos de montaje o unidades disponibles. Si las unidades o los puntos de montaje no pasan a estar disponibles dentro del tiempo MOUNTWAIT, los procesos de migración finalizarán. Para obtener información acerca de la especificación del tiempo MOUNTWAIT, consulte el apartado DEFINE DEVCLASS (Definir una clase de dispositivo).

El servidor de IBM Spectrum Protect iniciará el número especificado de procesos de migración independientemente del número de volúmenes elegibles para la migración. Por ejemplo, si especifica diez procesos de migración y sólo seis volúmenes son elegibles para migración, el servidor iniciará diez procesos y cuatro de ellos terminarán sin que se procesen volúmenes.

Consejo: Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### DATAFormat

Especifica el formato de datos que debe utilizarse para hacer copia de seguridad de archivos en esta agrupación de almacenamiento y restaurarlos de la misma. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

##### NATIVE

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

##### NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

##### NETAPPDump

Especifica que los datos tienen un formato de vuelco NetApp. Este formato de datos se debe especificar para imágenes del sistema de archivos que están en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos NetApp o IBM System Storage N Series que utiliza NDMP. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NETAPPDUMP. Puede utilizar el mandato MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

##### CELERRADump

Especifica que los datos tienen un formato de vuelco EMC Celerra. Este formato de datos debe especificarse para las imágenes de sistema de archivos que tienen un formato de vuelco y de las que se realizó una copia de seguridad a partir de un servidor de archivos EMC Celerra que utiliza NDMP. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=CELERRADUMP. Puede utilizar el comando MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

##### NDMPDump

Especifica que los datos tienen un formato de copia de seguridad específico del fabricante del NAS. Utilice este formato de datos para las imágenes de sistemas de archivos de las que se hizo una copia de seguridad desde un servidor de archivos NAS que no sea NetApp o EMC Celerra. El servidor no realiza la migración, la reclamación ni la ejecución de AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NDMPDUMP. Puede utilizar el comando MOVE DATA para traspasar datos desde una agrupación de almacenamiento primaria hasta otra o bien para extraerlos de un volumen si el volumen debe volver a utilizarse.

#### AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. El valor predeterminado es CLIENT. Este parámetro es opcional y afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si la opción AUTOCOPY se establece en ALL o CLIENT y existe como mínimo una agrupación de almacenamiento que aparece listada en las opciones COPYSTGPools o ACTIVEDataPools, la eliminación de duplicados del lado del cliente está inhabilitada.

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento

fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPools. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPools.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea esta inhabilitada.

Client

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRATION

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

COPYSTGPools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. El parámetro COPYSTGPools es opcional. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Al especificar un valor para el parámetro COPYSTGPools, también puede especificar un valor para el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPools y ACTIVEDATAPools no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento definida con una lista de agrupaciones de almacenamiento de copia.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. No se da soporte a la grabación simultánea en agrupaciones de almacenamiento de copia cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se da soporte a la grabación simultánea en las siguientes operaciones de almacenamiento. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia, éstas se pasarán por alto y los datos se almacenarán únicamente en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.

Atención: La función que proporciona el parámetro COPYSTGPOOLS no tiene como finalidad sustituir el mandato BACKUP STGPOOL. Si utiliza el parámetro COPYSTGPOOLS, continúe utilizando el mandato BACKUP STGPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

#### COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOOLS. Este parámetro es opcional. El valor predeterminado es YES. Si especifica el parámetro COPYCONTINUE, también debe especificar el parámetro COPYSTGPOOLS.

El parámetro COPYCONTINUE no afecta a la función de grabación simultánea durante la migración.

Puede especificar los siguientes valores:

#### Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

#### No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEDATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEDATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento principal a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los

formatos de datos siguientes:

- o NETAPPDUMP
  - o CELERRADUMP
  - o NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
  3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria que se ha especificado en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos, las agrupaciones de datos activos se pasarán por alto y los datos sólo se almacenarán en la agrupación de almacenamiento primaria.
  4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
  5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el comando COPY ACTIVE DATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVE DATA POOLS no tiene como finalidad sustituir al mandato COPY ACTIVE DATA. Si utiliza el parámetro ACTIVE DATA POOLS, utilice el mandato COPY ACTIVE DATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

#### DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE. El valor predeterminado es NO.

#### IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50. El valor predeterminado es 1. Si el valor del parámetro DEDuplicate es NO, el valor predeterminado de IDENTIFYPROCESS no tiene ningún efecto.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

## Ejemplo: definir una agrupación de almacenamiento primaria con una clase de dispositivo 8MMTAPE

---

Definir una agrupación de almacenamiento primaria que se denomine 8MMPOOL para la clase de dispositivo 8MMTAPE (con el tipo de dispositivo 8MM) y un tamaño de archivo máximo de 5 MB. Almacenar los archivos de más de 5 MB en agrupaciones subordinadas, a partir de POOL1. Se activará la función de proximidad de los archivos de los nodos cliente. Se permitirán hasta 5 volúmenes reutilizables en esta agrupación de almacenamiento.

```
define stgpool 8mmpool 8mmtape maxsize=5m
nextstgpool=pool1 collocate=node
maxscratch=5
```

#### Referencia relacionada:

SET DRMDBBACKUPEXPIREDDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

## DEFINE STGPOOL (Definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial)

---

Utilice este mandato para definir una agrupación de almacenamiento de copia asignada a dispositivos de acceso secuencial.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

---

```

>>-DEFine STGpool--nombre_agrupación--nombre_clase_dispositivo-->
>--Pooltype-----Copy--+-----+----->
      '-DESCRIPTION----descripción-'

      .-ACCESS-----READWrite-----
>--+-----+----->
      '-ACCESS-----+READWrite---+'
            +READOnly-----+
            '-UNAVailable-'

      .-COLlocate----No-----
>--+-----+----->
      '-COLlocate----+No-----+'
            +-GRoup-----+
            +-NODE-----+
            '-Filespace-'

      .-REclaim----100----- .-RECLAIMProcess----1-----
>--+-----+----->
      '-REclaim----porcentaje-' '-RECLAIMProcess----number-'

      .-RECLAMATIONType----THRESHold-----
>--+-----+----->
      |                                     (1) |
      '-RECLAMATIONType----+THRESHold+-----'
            '-SNAPlock--'

      .-OFFSITERECLAIMLimit----NOLimit-.
>--+-----+-----+--MAXSCRatch----número-->
      '-OFFSITERECLAIMLimit----number--'

      .-REUsedelay----0----
>--+-----+-----+----->
      '-REUsedelay----días-' '-OVFLocation----ubicación-'

      .-DATAFormat----NATive-----
>--+-----+----->
      |                                     (2) |
      '-DATAFormat----+NATive-----+'
            +-NONblock-----+
            +-NETAPPDump--+
            +-CELERRADump+
            '-NDMPDump----'

      .-CRCDData----No----- .-DEDuplicate----No-----
>--+-----+-----+----->
      '-CRCDData----+Yes-+-' '-DEDuplicate----+No-----+'
            '-No--' | (3) |
                   '-Yes-----'

      .-IDENTIFYProcess----0-----
>--+-----+-----+----->
      |                                     (4) |
      '-IDENTIFYProcess----número-----'

```

#### Notas:

1. El valor RECLAMATIONTYPE=SNAPLOCK sólo es válido para las agrupaciones de almacenamiento definidas en los servidores que están activados para IBM Spectrum Protect para retención de datos. La agrupación de almacenamiento debe estar asignada a una clase de dispositivo FILE y los directorios especificados en la clase de dispositivo deben ser volúmenes NetApp SnapLock.
2. Los valores NETAPPDUMP, CELERRADUMP y NDMPDUMP no son válidos para las agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.
3. Este parámetro sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.
4. Este parámetro sólo está disponible cuando el valor del parámetro DEDUPLICATE es YES.

## Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de definir. El nombre debe ser exclusivo y la longitud máxima permitida es de 30 caracteres.

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo de acceso secuencial a la que se asigna esta agrupación de almacenamiento de copia. Puede especificar cualquier clase de dispositivo definida con el comando DEFINE DEVCLASS.

POoltype=COpy (Necesario)

Especifica que desea definir una agrupación de almacenamiento de copia.

DESCRiption

Especifica la descripción de la agrupación de almacenamiento de copia. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor acceder a los archivos de la agrupación de almacenamiento de copia. Este parámetro es opcional. El valor predeterminado es READWRITE. Puede especificar los valores siguientes:

READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de almacenamiento de copia.

READOnly

Especifica que los nodos cliente sólo pueden leer los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional. El valor predeterminado es NO.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.



- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

#### NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

#### Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

#### RECLAIM

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es de 100, lo cual significa que no se lleva a cabo la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de copia que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos sin caducar del volumen reclamable desde una agrupación de almacenamiento de copia o primaria que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de almacenamiento de copia original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de almacenamiento de copia.

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento de copia. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de copia de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

#### RECLAMATIONType

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

##### THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

##### SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención utilizando el software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido para agrupaciones de almacenamiento que se definen en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El comando DEFINE no se ejecutará correctamente si el parámetro RECLAMATIONTYPE especificado es distinto del valor definido para las agrupaciones de almacenamiento ya definidas para el nombre de clase de dispositivo.

#### OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

##### NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

##### número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, suponga que una agrupación de almacenamiento de copias contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclamarán los tres volúmenes cuando se ejecute la reclamación. Si se especifica un valor de 2, sólo se reclamarán VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclamará VOL1.

#### MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se ha especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento de copia y la capacidad correspondiente estimada para la agrupación de almacenamiento de copia.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de almacenamiento de copia mientras no se cambie la modalidad de acceso. A continuación, un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento de copia seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el comando SET DRMDBBACKUPEXPIREDDAYS.

#### OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el comando. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

#### DATAFormat

Especifica el formato de datos que debe utilizarse para hacer copia de seguridad de archivos en esta agrupación de almacenamiento y restaurarlos de la misma. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

##### NATive

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

##### NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

##### NETAPPDump

Especifica que los datos tienen un formato de vuelco NetApp. No especifique este formato de datos para imágenes de sistema de archivos que se encuentran en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos NetApp utilizando NDMP. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NETAPPDUMP. Puede

utilizar el comando MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

#### CELERRADump

Especifica que los datos tienen un formato de vuelco EMC Celerra. No especifique este formato de datos para imágenes de sistema de archivos que se encuentran en un formato de vuelco y de las que se ha realizado una copia de seguridad desde un servidor de archivos EMC Celerra utilizando NDMP. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=CELERRADUMP. Puede utilizar el comando MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

#### NDMPDump

Especifica que los datos tienen un formato de copia de seguridad específico del fabricante del NAS. No especifique este formato de datos para imágenes del sistema de archivos de las que se ha hecho copia de seguridad desde un servidor de archivos NAS que no sea NetApp o EMC Celerra. El servidor no realizará la reclamación de la agrupación de almacenamiento o AUDIT VOLUME para una agrupación de almacenamiento con DATAFORMAT=NDMPDUMP. Puede utilizar el mandato MOVE DATA para extraer los datos generados por NDMP de un volumen si el volumen debe volver a utilizarse.

#### CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

##### Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

##### No

Especifica que los datos se almacenan sin información de CRC.

#### Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

#### DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE. El valor predeterminado es NO.

#### IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50.

El valor predeterminado para este parámetro es 0. Los procesos de eliminación de duplicados para una agrupación de almacenamiento de copias no son necesarios si se especifican procesos de eliminación de duplicados para la agrupación de almacenamiento primaria. Si IBM Spectrum Protect analiza un archivo de una agrupación de almacenamiento, IBM Spectrum Protect también analiza el archivo que se encuentra en todas las demás agrupaciones de almacenamiento.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los





La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

No

Especifica que la función de proximidad está desactivada.

GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

NODe

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

FIlespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación produce que el espacio fragmentado y el espacio que ocupan los archivos de copia de seguridad inactivos en los volúmenes pueda volver a utilizarse traspasando los restantes archivos no caducados y los archivos de copia de seguridad activos desde un volumen hasta otro volumen. Esta acción hace que el volumen original esté disponible para su reutilización. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor predeterminado es 60.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de datos activos que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación primaria o de datos activos que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de datos activos original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de datos activos.

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. El valor predeterminado es 1.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de datos activos. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de datos activos de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

#### RECLAMATIONType

Especifica el método según el cual se reclaman y se gestionan los volúmenes. Este parámetro es opcional. El valor predeterminado es THRESHOLD. Los siguientes son los valores posibles:

##### THRESHold

Especifica que los volúmenes que pertenecen a esta agrupación de almacenamiento se reclaman en función del valor del umbral del atributo RECLAIM de esta agrupación de almacenamiento.

##### SNAPlock

Especifica que los volúmenes FILE que pertenecen a esta agrupación de almacenamiento serán gestionados para su retención utilizando el software de NetApp Data ONTAP y los volúmenes NetApp SnapLock. Este parámetro sólo es válido para agrupaciones de almacenamiento que se definen en un servidor que tiene la protección de retención de datos activada y que está asignada a una clase de dispositivo FILE. Los volúmenes de esta agrupación de almacenamiento no se reclaman en función del umbral; se omite el valor RECLAIM para la agrupación de almacenamiento.

Todos los volúmenes de esta agrupación de almacenamiento se crean como volúmenes FILE. Se establece una fecha de retención, que se deriva de los atributos de retención del grupo de copias archivadas de la agrupación de almacenamiento, en los metadatos para el volumen FILE utilizando la función SnapLock del sistema operativo de NetApp Data ONTAP. Hasta que la fecha de retención haya caducado, no se puede suprimir el volumen FILE ni todos los datos contenidos en él del volumen físico SnapLock en el que está almacenado.

El parámetro RECLAMATIONTYPE para todas las agrupaciones de almacenamiento que se definan debe ser el mismo definido para el mismo nombre de clase de dispositivo. El comando DEFINE no se ejecutará correctamente si el parámetro RECLAMATIONTYPE especificado es distinto del valor definido para las agrupaciones de almacenamiento ya definidas para el nombre de clase de dispositivo.

#### OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Puede especificar los valores siguientes:

##### NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.



número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, imaginemos que una agrupación de datos activos contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica un valor para este parámetro OFFSITERECLAIMLIMIT, se reclaman los tres volúmenes cuando se ejecute la reclamación. Si especifica un valor de 2, sólo se reclaman VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclama VOL1.

#### MAXSCRatch (Obligatorio)

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se especifica para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de datos activos y la capacidad correspondiente estimada para la agrupación de datos activos.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de datos activos mientras no se cambie la modalidad de acceso. A continuación, un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, lo que significa que se puede volver a grabar en un volumen o devolverlo a la agrupación de reutilizables, tan pronto como se han suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de datos activos seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el comando SET DRMDBBACKUPEXPIREDDAYS.

#### OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca con el comando. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

#### DATAFormat

Especifica el formato de datos que ha de utilizarse para copiar archivos en esta agrupación de almacenamiento y restaurar los archivos de esta agrupación de almacenamiento. El formato predeterminado es el formato de servidor NATIVE. Puede especificar los valores siguientes:

NATIVE

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect e incluye encabezamientos de bloque.

#### NONblock

Especifica que el formato de datos es el formato nativo del servidor de IBM Spectrum Protect y no incluye encabezamientos de bloque.

En un volumen asociado a una clase de dispositivo FILE, el tamaño de bloque mínimo predeterminado es de 256 KB, con independencia de la cantidad de datos que se graben en el volumen. Para la realización de determinadas tareas, puede minimizar la existencia de espacio desaprovechado en los volúmenes de almacenamiento especificando el formato de datos NONBLOCK. Por ejemplo, puede especificar el formato de datos NONBLOCK para las siguientes tareas:

- Uso de productos de gestión de contenidos
- Uso de la opción de cliente DIRMC para almacenar información de directorios
- Migración de archivos muy pequeños utilizando IBM Spectrum Protect for Space Management o IBM Spectrum Protect HSM para Windows

Sin embargo, en la mayoría de las situaciones, el formato preferido es NATIVE.

#### CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

#### Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

#### No

Especifica que los datos se almacenan sin información de CRC.

#### Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

#### DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. El valor predeterminado es NO.

#### IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Entre un valor de 0 – 50.

El valor predeterminado para este parámetro es 0. Los procesos de eliminación de duplicados para una agrupación de almacenamiento de copias no son necesarios si se especifican procesos de eliminación de duplicados para la agrupación de almacenamiento primaria. Si IBM Spectrum Protect analiza un archivo de una agrupación de almacenamiento, IBM Spectrum Protect también analiza el archivo que se encuentra en todas las demás agrupaciones de almacenamiento.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

## Ejemplo: definir una agrupación de datos activos con una clase de dispositivo DC500

Definir una agrupación de datos activos, TAPEPOOL2, para la clase de dispositivo DC500. Se permitirán hasta 50 volúmenes reutilizables en esta agrupación. La reutilización de volúmenes se retardará 45 días.

```
define stgpool tapepool3 dc500 pooltype=activedata
maxscratch=50 reusedelay=45
```

### Referencia relacionada:

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

## DEFINE STGPOOLDIRECTORY (Definición de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para definir uno o varios directorios en una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.

Consejo: Después de definir una agrupación de almacenamiento de contenedor en la nube, cree uno o varios directorios que se utilicen para el almacenamiento local. Temporalmente puede almacenar los datos en el almacenamiento local durante la ingesta de datos, y antes de mover los datos a la nube. De este modo, puede mejorar el rendimiento de la copia de seguridad y el archivado. Para obtener más información, consulte el apartado Optimización del rendimiento para el almacenamiento de objetos en la nube.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

```
>>-DEFine STGPOOLDIrectory--nombre_agrupación-----nombre_directorio+----><
```

## Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Este parámetro es obligatorio.

nombre\_directorio (Obligatorio)

Especifica el directorio que debe definirse en la agrupación de almacenamiento. Este parámetro es necesario. Puede especificar más de un nombre de directorio separando cada nombre con una coma y sin espacios intercalados.

Si utiliza el cliente administrativo y el nombre de directorio contiene una coma o una barra inclinada invertida ("\"), especifique el nombre entre comillas.

## Ejemplo: Definición de un directorio de agrupación de almacenamiento

Defina un directorio de agrupación de almacenamiento que se denomine DIR1 utilizando una agrupación de almacenamiento de contenedores de directorios que se denomine POOL1.

 Sistemas operativos AIX  Sistemas operativos Linux

```
define stgpooldirectory pool1 /storage/dir1
```

 Sistemas operativos Windows

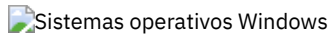
```
define stgpooldirectory pool1 c:\storage\dir1
```

## Ejemplo: Definir varios directorios de agrupaciones de almacenamiento

Defina directorios de agrupaciones de almacenamiento que se denominen DIR1 y DIR2 utilizando una agrupación de almacenamiento de contenedores de directorios que se denomine POOL1.

 Sistemas operativos AIX  Sistemas operativos Linux

```
define stgpooldirectory pool1 /storage/dir1,/storage/dir2
```



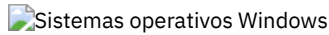
```
define stgpooldirectory pool1 e:\storage\dir1,f:\storage\dir2
```

## Ejemplo: definir un almacenamiento local para una agrupación de almacenamiento de contenedor de nubes

Cree un directorio de agrupación de almacenamiento denominado DIR3 en una agrupación de almacenamiento de contenedor de nubes que se llame CLOUDLOCALDISK1.



```
define stgpooldirectory cloudlocaldisk1 /storage/dir3
```



```
define stgpooldirectory cloudlocaldisk1 c:\storage\dir3
```

Tabla 1. Mandatos relacionados con DEFINE STGPOOLDIRECTORY

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

## DEFINE SUBSCRIPTION (Definir una inscripción en un perfil)

Utilice este comando en un servidor gestionado para suscribir dicho servidor a un perfil.

Cuando un servidor se suscribe a su primer perfil, también se crea una suscripción al perfil predeterminado (si existe) del gestor de configuración. Entonces, el servidor establece contacto periódicamente para actualizar la configuración.

Restricciones:

1. Un servidor no se puede suscribir a perfiles de más de un gestor de configuración.
2. Si un servidor se suscribe a un perfil con un objeto asociado que ya está definido en el servidor, la definición local se sustituye por la definición del gestor de configuración. Por ejemplo, si un servidor tiene una planificación de administración denominada WEEKLY\_BACKUP, y después se suscribe en un perfil que también tiene una planificación de administración denominada WEEKLY\_BACKUP, se sustituirá la definición local.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DEFine SUBSCRIPtion--nombre_perfil----->
>--+-----+-----><
  '-SERVer----nombre_servidor-'
```

### Parámetros

nombre\_perfil (Obligatorio)

Especifica el nombre del perfil en el que se suscribe el servidor.

SERVer

Especifica el nombre del gestor de configuración del que se obtiene la información de configuración. Este parámetro es necesario si el servidor gestionado no tiene una suscripción como mínimo. Si el servidor gestionado tiene una suscripción, puede omitir

este parámetro y se tomará el gestor de configuración como valor predeterminado para dicha suscripción.

## Ejemplo: definir una suscripción de perfil

Suscribir un perfil denominado BETA que reside en un gestor de configuración denominado TOM.

```
define subscription beta server=tom
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DEFINE SUBSCRIPTION

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGREFRESH	Especifica un intervalo de tiempo para que los servidores gestionados entren en contacto con los gestores de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## DEFINE VIRTUALFSMAPPING (Definir una correlación de espacios de archivos virtuales)

Utilice este mandato para definir una correlación de espacios de archivos virtuales.

En las operaciones de datos NAS BACKUP NODE y RESTORE NODE, pueden utilizarse nombres de espacios de archivos virtuales similares a un nombre del sistema de archivos. Consulte la documentación sobre el dispositivo NAS para obtener orientación acerca de cómo especificar los parámetros de este comando.

Nota: El nodo NAS debe tener una definición de transportador de datos asociada porque, cuando el servidor de IBM Spectrum Protect actualiza una correlación de espacios de archivos virtuales, el servidor intenta ponerse en contacto con el dispositivo NAS para validar el sistema de archivos virtuales y el nombre del sistema de archivos.

## Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

## Sintaxis

```
>>-DEFine VIRTUALFSmapping -nombre_nodo----->  
>--nombre_espacio_archivos_virtual--nombre_sistema_archivos----->
```

```

.-NAMEType---SERVER-----
>--ruta-----<
'-NAMEType---SERVER-----'
'-HEXadecimal-'

```

## Parámetros

### nombre\_nodo (Necesario)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

### nombre\_espacio\_archivos\_virtual (Obligatorio)

Especifica el nombre que hace referencia a esta definición de espacio de archivos virtual. El nombre de espacio de archivos virtual es sensible a las mayúsculas y minúsculas y el primer carácter debe ser una barra inclinada /. La longitud del nombre no puede ser mayor que 64 caracteres, incluida la barra inclinada necesaria. Los nombres de los espacios de archivos virtuales están limitados al mismo juego de caracteres establecido para el resto de objetos del servidor, excepto el carácter de barra inclinada /, que también está permitido.

El nombre del espacio de archivos virtual no puede ser idéntico a ningún sistema de archivos en el nodo NAS. Al seleccionar un nombre de espacio de archivos virtual, tenga en cuenta las restricciones siguientes:

- Si se crea un sistema de archivos en el dispositivo NAS con el mismo nombre que un sistema de archivos virtual, se producirá un conflicto de nombres en el servidor al realizarse la copia de seguridad del nuevo espacio de archivos. Utilice una cadena de caracteres para el nombre de espacio de archivos virtual que es poco probable que se utilice en el futuro como un nombre de sistema de archivos real en el dispositivo NAS.

Por ejemplo: un usuario sigue un convenio de denominación para crear espacios de archivos en un dispositivo NAS con los nombres de formato /vol1, /vol2, /vol3. El usuario define un espacio de archivos virtual en el servidor con el nombre /vol9. Si continúa utilizando los mismos convenios de denominación, es muy probable que el nombre del espacio de archivos virtual entre en conflicto con un nombre de espacio de archivos real en algún momento del futuro.

- Durante las operaciones de copia de seguridad y restauración, el servidor verifica que no se produzca ningún conflicto de nombres antes de iniciar la operación.
- El nombre del espacio de archivos virtual aparecerá como un espacio de archivos en la salida del comando QUERY FILESPACE, así como en los paneles de copia de seguridad y restauración del cliente web de IBM Spectrum Protect. Por lo tanto, debe considerar la posibilidad de seleccionar un nombre que identifique sin ningún tipo de ambigüedad este objeto como una ruta de directorio en el dispositivo NAS.

### nombre\_sistema\_archivos (Obligatorio)

Especifica el nombre del sistema de archivos en el que se encuentra la ruta. El nombre del sistema de archivos debe existir en el nodo NAS especificado. El nombre del sistema de archivos no puede contener caracteres comodín.

### ruta (Obligatorio)

Especifica la ruta de la raíz del sistema de archivos al directorio. La ruta sólo puede hacer referencia a un directorio. La longitud máxima de la ruta es de 1024 caracteres. El nombre de ruta es sensible a las mayúsculas y minúsculas.

### NAMEType

Especifica la forma en la que el servidor debe interpretar el nombre de ruta especificado. Este parámetro es útil cuando una ruta contiene caracteres que no forman parte de la página de códigos en que se ejecuta el servidor. El valor predeterminado es SERVER.

Los valores posibles son:

#### SERVER

El servidor utiliza la página de códigos del servidor para interpretar el nombre de ruta.

#### HEXadecimal

El servidor interpreta el nombre de ruta que ha entrado como la representación hexadecimal de la ruta. Esta opción debe utilizarse cuando una ruta contenga caracteres que no se pueden entrar. Esto podría ocurrir si el sistema de archivos NAS se establece en un idioma diferente de aquél en que se ejecuta el servidor.

## Ejemplo: definir una correlación de espacios de archivos virtuales

Definir el nombre de correlación de espacios de archivos virtuales /mikeshomedir para la ruta /home/mike en el sistema de archivos /vol/vol1 del nodo NAS denominado NAS1.

```
define virtualfsmapping nas1 /mikeshomedir /vol/vol1 /home/mike
```

## Comandos relacionados



Tabla 1. Comandos relacionados con DEFINE VIRTUALFSMAPPING

Comando	Descripción
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

## DEFINE VOLUME (Definir un volumen en una agrupación de almacenamiento)

Utilice este comando para asignar un volumen de acceso secuencial o aleatorio a una agrupación de almacenamiento.

Cuando se defina un volumen de agrupación de almacenamiento de acceso aleatorio (DISK) o un volumen de agrupación de almacenamiento de acceso secuencial asociado a una clase de dispositivo FILE, puede utilizar el servidor para que éste cree el volumen antes de que se asigne. O bien puede utilizar los desencadenantes de espacio para crear volúmenes preasignados cuando se hayan excedido los umbrales de utilización de espacio predeterminados. Para obtener detalles sobre los desencadenantes de espacio, consulte el apartado DEFINE SPACETRIGGER (Definir desencadenante de espacio). Para obtener volúmenes asociados con clases de dispositivos diferentes a DISK o tipos de dispositivos diferentes a FILE, puede utilizar el mandato DEFINE VOLUME para asignar un volumen ya creado a una agrupación de almacenamiento.


 Sistemas operativos AIX  Sistemas operativos Linux Cuando se utiliza una clase de dispositivo FILE para el almacenamiento gestionado por el servidor de medios de z/OS, no es necesario formatear o definir volúmenes. Si define un volumen para este tipo de clase de dispositivo FILE utilizando el comando DEFINE VOLUME, el servidor de medios de z/OS no asigna espacio para el volumen hasta que se abra el volumen para su primer uso.


Atención: Los volúmenes para el servidor de medios de z/OS que se crean mediante el comando DEFINE VOLUME permanecen llenos físicamente o asignados después de que el servidor vacía el volumen, por ejemplo, después de la caducidad o la reclamación. Para los volúmenes FILE, el espacio DASD no se cede al sistema cuando se vacía el volumen. Si una agrupación de almacenamiento requiere un volumen de relleno o vacío, se puede utilizar el volumen FILE. En comparación, los volúmenes de cinta que se vacían lógicamente son igual que si estuvieran vacíos físicamente. Los volúmenes de cinta y FILE permanecen definidos en el servidor. En comparación, los volúmenes reutilizables, incluido el almacenamiento físico que se asigna para los volúmenes de archivo reutilizables, se devuelven al sistema cuando se vacían.

Para crear espacio en las agrupaciones de almacenamiento de acceso secuencial, puede definir volúmenes o permitir al servidor solicitar volúmenes reutilizables según sea necesario, tal y como especifica el parámetro MAXSCRATCH para la agrupación de almacenamiento. En el caso de agrupaciones de almacenamiento asociadas a la clase de dispositivo FILE, el servidor puede crear volúmenes privados según sea necesario por medio de los desencadenantes de espacio de la agrupación de almacenamiento. En el caso de agrupaciones de almacenamiento DISK, el mecanismo reutilizable no está disponible. No obstante, puede crear espacio si crea volúmenes y, a continuación, los define en el servidor. O bien, puede hacer que el servidor cree los volúmenes que utilizan desencadenantes de espacio de agrupación de almacenamiento.

El servidor no valida la existencia de un nombre de volumen al definir un volumen en una agrupación de almacenamiento asociada a una biblioteca. El volumen definido tiene una capacidad estimada "0" hasta que se graban datos en él.

Atención: El tamaño de un volumen de agrupación de almacenamiento no se puede cambiar después de que se ha definido en el servidor.

 Sistemas operativos AIX Si cambia el tamaño de los volúmenes de IBM Spectrum Protect ampliando los volúmenes lógicos con formato RAW mediante SMIT o modificando el tamaño de los archivos de los volúmenes con comandos o programas de utilidad de sistema operativo, es posible que el servidor no se inicialice correctamente y se pierdan datos.

 Sistemas operativos Windows Si cambia el tamaño de los volúmenes modificando el tamaño de los archivos de los volúmenes con mandatos o programas de utilidad de sistema operativo, es posible que el servidor no se inicialice correctamente y se pierdan datos.

Restricciones:

- Este mandato no puede utilizarse para definir volúmenes en agrupaciones de almacenamiento con el valor de parámetro RECLAMATIONTYPE=SNAPLOCK. Los volúmenes de este tipo de agrupación de almacenamiento se han asignado utilizando el





- Sistemas operativos AIX Sistemas operativos Linux Tabla 3: FILE para el servidor de medios de z/OS
- Tabla 4: cinta
- Sistemas operativos AIX Sistemas operativos Linux Tabla 5: cinta para servidor de medios de z/OS
- Tabla 6: REMOVABLEFILE

Tabla 1. Requisitos de nombre de volumen para DISK

Requisitos de nombre de volumen	Ejemplo
<p>El nombre del archivo que contendrá los datos de volumen bien con un nombre de ruta completo o bien un nombre de ruta relativo al directorio de funcionamiento actual.</p> <p> Si un nombre contiene espacios en blanco intercalados, signos de igual u otros caracteres especiales, delimite la lista con comillas.</p>	<p> Sistemas operativos AIX  Sistemas operativos Linux</p> <pre>/usr/storage/sbkup01.dsm</pre> <p> Si está utilizando un volumen lógico de AIX, especifique el nombre de ruta de la siguiente manera:</p> <pre>/dev/rxxx</pre> <p>donde xxx es el nombre del volumen lógico.</p> <p> Sistemas operativos Windows</p> <pre>"c:\archivos de programa\tivoli\tsm\server\data3.dsm"</pre>

Tabla 2. Requisitos de nombre de volumen para FILE

Requisitos de nombre de volumen	Ejemplo
<p>El nombre del archivo que contendrá los datos del volumen, con el nombre de ruta totalmente calificado o con el nombre de ruta relativo al directorio identificado en el parámetro DIRECTORY para la clase de dispositivo.</p> <p> Si un nombre contiene espacios en blanco intercalados, signos de igual u otros caracteres especiales, delimite la lista con comillas.</p> <p>Coloque los volúmenes FILE en uno de los directorios que se especifican con el parámetro DIRECTORY del mandato DEFINE DEVCLASS. De lo contrario, es posible que los agentes de almacenamiento no tengan acceso a los volúmenes. Para obtener detalles, consulte el apartado DEFINE PATH (Definir una ruta).</p>	<p> Sistemas operativos AIX  Sistemas operativos Linux</p> <pre>/data/fpool01.dsm</pre> <p> Sistemas operativos Windows</p> <pre>"f:\data storage\fpool01.dsm"</pre>

Sistemas operativos AIX Sistemas operativos Linux

Tabla 3. servidor de medios de z/OS: requisitos de nombre de volumen para FILE

Requisitos de nombre de volumen	Ejemplo
---------------------------------	---------

Requisitos de nombre de volumen	Ejemplo
<p>Para los volúmenes FILE utilizados con el servidor de servidor de medios de z/OS, especifique un nombre de conjunto de datos. El nombre del conjunto de datos puede constar de uno o más calificadores delimitados por un punto. Los calificadores pueden contener un máximo de 8 caracteres. La longitud máxima del nombre del conjunto de datos es de 44 caracteres. La primera letra de cada calificador debe ser un carácter alfabético o nacional (@#\$), seguido de caracteres alfabéticos, nacionales, numéricos o guiones.</p> <p>Para asignar el conjunto de datos lineal VSAM asociado cuando se presenta el volumen en el sistema z/OS, el calificador de alto nivel (HLQ) se suele filtrar mediante rutinas de selección automática de clases específicas en las restricciones de política de SMS en el sistema donde se ejecuta el servidor de medios de z/OS.</p> <p>El comportamiento del calificador de alto nivel es similar al del nombre PREFIX en una solicitud reutilizable. El calificador de alto nivel suele utilizarlo DFSMS para afectar los atributos de asignación, como Extended Addressability para los conjuntos de datos que se espera que se amplíen cuando el espacio que ya está asignado al volumen de archivo se ha agotado.</p> <p>Si no existe el conjunto de datos, el servidor lo crea cuando se utiliza el volumen para una operación de almacenamiento de IBM Spectrum Protect específica. El conjunto de datos no se crea cuando se define el volumen. Se puede producir una pérdida de datos al definir volúmenes porque el servidor de medios de z/OS reutiliza el volumen o el conjunto de datos lineal VSAM si existe en el momento del tiempo de asignación. Importante: Para permitir que el servidor genere nombres de volumen, considere utilizar volúmenes reutilizables.</p>	 Sistemas operativos AIX  Sistemas operativos Linux  SERVER1.BFS.POOL3.VOLA

Tabla 4. Requisitos de nombre de volumen para cinta

Requisitos de nombre de volumen	Ejemplo
<p>Uso de 1 a 32 caracteres alfanuméricos.</p> <p>El nombre de volumen no puede contener espacios en blanco intercalados ni signos de igual.</p>	DSMT01

 Sistemas operativos AIX  Sistemas operativos Linux

Tabla 5. servidor de medios de z/OS: requisitos de nombre de volumen para cinta

Requisitos de nombre de volumen	Ejemplo
---------------------------------	---------

Requisitos de nombre de volumen	Ejemplo
<p>Para los cartuchos de cinta, especifique un nombre de volumen de cinta con 1 a 6 caracteres alfanuméricos. El servidor convierte en mayúsculas los nombres de volumen de cinta.</p> <p>El nombre de volumen no puede contener espacios en blanco intercalados ni signos de igual.</p> <p>Los volúmenes que el servidor utiliza para cualquier fin debe tener un nombre exclusivo. Este requisito es válido para todos los volúmenes, tanto si se utilizan para las agrupaciones de almacenamiento como si se emplean para operaciones como una copia de seguridad o exportación de base de datos. El requisito se aplica también a los volúmenes que residen en distintas bibliotecas de medios de z/OS pero que utiliza el mismo servidor.</p>	DSMT01

Tabla 6. Requisitos de nombre de volumen para REMOVABLEFILE

Requisitos de nombre de volumen	Ejemplo
<p>1-6 caracteres alfanuméricos</p> <p>El servidor convierte en mayúsculas los nombres de volumen.</p>	DSM01

#### ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor (como, por ejemplo, migración) acceder a los archivos del volumen de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es READWRITE. Los valores posibles son:

#### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en el volumen.

#### READOnly

Especifica que los nodos de cliente y los procesos de servidor sólo pueden realizar operaciones de lectura en los archivos almacenados en el volumen.

#### UNAVailable

Especifica que ni los nodos de cliente ni los procesos de servidor pueden acceder a los archivos almacenados en el volumen.

Si define un volumen de acceso aleatorio como UNAVAILABLE, no podrá activar el volumen.

Si define un volumen de acceso secuencial como UNAVAILABLE, el servidor no intentará acceder al volumen.

#### Offsite

Especifica que el volumen está en una ubicación fuera de local desde la que no se puede montar. Este valor sólo se puede especificar para los volúmenes de agrupaciones de almacenamiento de copia o de datos activos.

Utilice este valor para poder localizar los volúmenes de las ubicaciones de fuera del local. El servidor trata los volúmenes que están designados como fuera del local de forma diferente:

- El servidor no genera peticiones de montaje para los volúmenes designados como fuera de local.
- El servidor reclama o traspasa datos de los volúmenes fuera de local recuperando los archivos de otras agrupaciones de almacenamiento.
- El servidor no suprime automáticamente de una agrupación de almacenamiento de copia o de datos activos los volúmenes reutilizables de fuera de local vacíos.

#### LOcation

Especifica la ubicación del volumen. Este parámetro es opcional. Este parámetro únicamente puede especificarse para los volúmenes de agrupaciones de almacenamiento de acceso secuencial. La información de ubicación puede tener una longitud máxima de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco.

#### Formatsize

Especifica el tamaño del volumen de acceso aleatorio o volumen FILE que se crea y formatea en un paso. El valor se especifica en megabytes. El tamaño máximo es de 8.000.000 MB (8 terabytes). Este parámetro es necesario si se da alguna de las condiciones siguientes:

- Se especifica un solo volumen FILE o DISK que se crea y formatea en un paso.

- El valor del parámetro NUMBEROFVOLUMES es superior a 1 y se están creando volúmenes DISK.
- El valor del parámetro NUMBEROFVOLUMES es mayor que 1 y el valor del parámetro FORMATSIZES es igual o menor que el parámetro MAXCAPACITY del comando DEFINE DEVCLASS.

Si está asignando volúmenes en un servidor de medios de z/OS, este parámetro no es válido.

Para un volumen FILE, debe especificar un valor menor o igual que el valor del parámetro MAXCAPACITY de la clase de dispositivo asociada a la agrupación de almacenamiento.

No puede utilizar este parámetro para varios volúmenes predefinidos. A menos que se especifique `WAIT=YES`, la operación se realizará como un proceso en segundo plano.

#### Numberofvolumes

Especifica el número de volúmenes que se crean y formatean en un paso. Este parámetro sólo se aplica a agrupaciones de almacenamiento con clases de dispositivo DISK o FILE. Este parámetro es opcional. El valor predeterminado es 1. Si especifica un valor mayor que 1, también debe especificar un valor para el parámetro FORMATSIZES. Especifique un número de 1 a 256.

Si está asignando volúmenes en un servidor de medios de z/OS, el único valor que admite este parámetro es el valor predeterminado de 1.

Si el valor del parámetro NUMBEROFVOLUMES es mayor que 1, se agregará un sufijo numérico al nombre del volumen que ha especificado para crear cada nombre ,por ejemplo, tivolivol001 y tivolivol002. Asegúrese de elegir un nombre de volumen para crear un nombre de archivo válido para el sistema de archivos de destino cuando se agrega el sufijo.

Importante: Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para obtener más información, consulte el apartado DEFINE PATH (Definir una ruta).

#### Wait

Especifica si se realiza una operación de creación y formato de volumen de modo subordinado o en primer plano. Este parámetro es opcional. No se tiene en cuenta excepto si se especifica también el parámetro FORMATSIZES.






#### No

Especifica que se realiza una operación de creación y formato de volumen de modo subordinado. El valor NO es el valor predeterminado cuando se especifica también un tamaño de formato.

#### Yes

Especifica que la operación de creación y formateo de un volumen se ejecuta en primer plano. Recuerde: No se puede especificar `WAIT=YES` desde la consola del servidor.

## Ejemplo: utilizar un proceso subordinado para definir un nuevo volumen de 100 MB para una agrupación de almacenamiento de disco

Crear un volumen de 100 MB en la agrupación de almacenamiento de disco denominada BACKUPPOOL.   El nombre del volumen es /var/storage/bf.dsm.  El nombre de volumen es j:\storage\bf.dsm. El volumen se creará como proceso subordinado.  

```
define volume backuppool
/var/storage/bf.dsm formatsize=100
```

```
define volume backuppool j:\storage\bf.dsm formatsize=100
```






## Ejemplo: definir un volumen para una agrupación de almacenamiento de disco con acceso de lectura y grabación

La agrupación de almacenamiento denominada POOL1 está asignada a una clase de dispositivo de cinta. Definir el volumen denominado TAPE01 en esta agrupación de almacenamiento, con acceso READWRITE.

```
define volume pool1 tape01 access=readwrite
```

## Ejemplo: definir un volumen para una agrupación de almacenamiento de archivo

La agrupación de almacenamiento que se denomina FILEPOOL está asignada a una clase de dispositivo con el tipo de dispositivo FILE.

  Definir un volumen que se denomina filepool\_vol01 para esta agrupación de almacenamiento.  Definir un volumen que se denomina fp\_vol01.dsm para esta agrupación de almacenamiento.  

```
define volume filepool /usr/storage/filepool_vol01
```

```
define volume filepool j:\storage\fp_vol01.dsm
```

## Ejemplo: utilizar un proceso en segundo plano para definir 10 volúmenes para una agrupación de almacenamiento de archivo con una capacidad máxima de 5 GB de clase de dispositivo

Defina 10 volúmenes en una agrupación de almacenamiento secuencia que utiliza una clase de dispositivo FILE. La agrupación de almacenamiento se denomina FILEPOOL. El valor del parámetro MAXCAPACITY para la clase de dispositivo asociada a esta agrupación de almacenamiento es 5 GB. La creación debe realizarse en segundo plano.

```
define volume filepool filevol numberofvolumes=10 formatsize=5000
```

El servidor crea los nombres de volumen filevol001 a filevol010.

Los volúmenes se crean en el directorio o directorios que se han especificado con el parámetro DIRECTORY de la clase de dispositivo que está asociada con la agrupación de archivos de la agrupación de almacenamiento. Si ha especificado varios directorios para la clase de dispositivo, los volúmenes individuales se pueden crear en cualquiera de los directorios de la lista.

## Comandos relacionados

Tabla 7. Comandos relacionados con DEFINE VOLUME

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

## Comandos DELETE

Utilice los mandatos DELETE para suprimir o eliminar un objeto de IBM Spectrum Protect.

- DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)
- DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)
- DELETE BACKUPSET (Suprimir un juego de copias de seguridad)
- DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)
- DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)
- DELETE COLLOGROUP (Suprimir un grupo de proximidad)
- DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)
- DELETE COPYGROUP (Suprimir un grupo de copias de seguridad o de archivado)
- DELETE DATAMOVER (Suprimir un transportador de datos)
- DELETE DEDUPSTATS (Suprimir las estadísticas de eliminación de duplicados de datos)
- DELETE DEVCLASS (Suprimir una clase de dispositivo)
- DELETE DOMAIN (Suprimir un dominio de políticas)
- DELETE DRIVE (Suprimir una unidad de una biblioteca)
- DELETE EVENT (Suprimir registros de eventos)
- DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)
- DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)
- DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)
- DELETE LIBRARY (Suprimir una biblioteca)
- DELETE MACHINE (Suprimir información de una máquina)
- DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)
- DELETE MGMTCLASS (Suprimir una clase de gestión)
- DELETE NODEGROUP (Suprimir un grupo de nodos)
- DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)
- DELETE PATH (Suprimir una ruta)
- DELETE POLICYSET (Suprimir un juego de políticas)

- DELETE PROFASSOCIATION (Suprimir una asociación de perfil)
- DELETE PROFILE (Suprimir un perfil)
- DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)
- DELETE RECOVERYMEDIA (Suprimir medio de recuperación)
- DELETE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)
- DELETE SCRIPT (Suprimir líneas de comandos de un script o suprimir todo el script)
- DELETE SERVER (Suprimir una definición de servidor)
- DELETE SERVERGROUP (Suprimir un grupo de servidores)
- DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)
- DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)
- DELETE STGPOOL (Suprimir una agrupación de almacenamiento)
- DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)
- DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)
- DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)
- DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)
- DELETE VOLHISTORY (Suprimir información histórica de volúmenes)
- DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

## DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)

Utilice este mandato para suprimir un mensaje de la lista de desencadenantes de alerta.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

      .-n-----
      v               |
>>-DELeTe ALERtTriggeR-+--número_mensaje-+-----><

```

### Parámetros

número\_mensaje (Obligatorio)

Especifica el número de mensajes que desea eliminar de la lista de desencadenantes de alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres. Puede utilizar caracteres comodín para especificar números de mensajes.

### Suprimir desencadenante de alerta

Suprima dos números de mensaje que se han designado como alertas, emitiendo el mandato siguiente:

```
delete alerttrigger ANR1067E,ANR1073E
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con DELETE ALERTTRIGGER

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.

Comando	Descripción
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

## DELETE ASSOCIATION (Suprimir la asociación de nodo con una planificación)

Utilice este comando para suprimir la asociación que hay entre un nodo cliente y una planificación de cliente. IBM Spectrum Protect ya no ejecuta la planificación en el nodo cliente.

Si intenta suprimir la asociación entre un cliente y una planificación a la que no está asociado, este comando no tendrá vigor alguno para dicho cliente.

### Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que pertenece la planificación

### Sintaxis

```
>>-DELeTe ASSOCIation--nombre_dominio--nombre_planificación----->
      .-,-----
      v          |
>----nombre_nodo-+-----<<
```

### Parámetros

nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre\_planificación (Obligatorio)

Especifica el nombre de la planificación de la que se deben disociar los clientes.

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo cliente que ya no está asociado a la planificación de cliente. Puede especificar una lista de clientes que dejarán de estar asociados con la planificación especificada. Los elementos de la lista se separan con comas, sin espacios intercalados. También puede utilizar un carácter comodín para especificar un nombre. Todos los clientes coincidentes dejarán de estar asociados con la planificación especificada.

### Ejemplo: suprimir una asociación de nodo con una planificación

Para suprimir la asociación del nodo JEFF, asignado al dominio de políticas DOMAIN1, con la planificación WEEKLY\_BACKUP, emita el comando siguiente:

```
delete association domain1 weekly_backup jeff
```

### Ejemplo: suprimir una asociación de nodo con una planificación con un comodín para la selección de los nodos

Suprimir la asociación de los clientes seleccionados, asignados al dominio de políticas DOMAIN1, con la planificación WEEKLY\_BACKUP para que estos clientes ya no puedan ejecutar esta planificación. Los nodos que dejan de estar asociados con la planificación contienen ABC o XYZ en el nombre de nodo. Emita el comando:

```
delete association domain1
weekly_backup *abc*,*xyz*
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE ASSOCIATION

Comando	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.

## DELETE BACKUPSET (Suprimir un juego de copias de seguridad)

Utilice este mandato para suprimir manualmente un juego de copias de seguridad antes de que caduque su período de retención.

Cuando el servidor crea un juego de copias de seguridad, el período de retención asignado al juego de copias de seguridad determina el tiempo en que el juego de copias de seguridad permanece en la base de datos. Una vez transcurrida dicha fecha, el servidor suprime automáticamente el juego de copias de seguridad cuando se ejecuta el proceso de caducidad. Sin embargo, también puede suprimir manualmente del servidor el juego de copias de seguridad del cliente antes de la fecha de caducidad planificada mediante el comando DELETE BACKUPSET.

Atención: Si los volúmenes contienen varios juegos de copias de seguridad, no volverán a establecerse en estado de reutilización hasta que todos los juegos de copias de seguridad hayan caducado o se hayan suprimido.

### Clase de privilegio

Si la opción del servidor REQSYSAUTHOUTFILE se establece en YES (el valor predeterminado), el administrador deberá disponer de privilegio de sistema. Si la opción del servidor REQSYSAUTHOUTFILE se establece en NO, el administrador deberá disponer de privilegio de sistema o de privilegio de políticas para el dominio al que se ha asignado el nodo cliente.

### Sintaxis

```

      .-,------.
      v          |
>>-DELeTe BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'
      .-,------.
      v          |
>---nombre_juego_copias_seguridad-+-----+----->
      '-BEGINDate----fecha-'
>+-----+-----+-----+----->
      '-BEGINTime----hora-' '-ENDDate----fecha-'
      .-WHEREDataTpe----ALL-----
>+-----+-----+-----+----->
      '-ENDTime----hora-' |          .-,------. |
      |          |          v          | |
      '-WHEREDataTpe-----+FILE-+--+-'
      '-IMAGE-'
>+-----+-----+-----+----->
      '-WHEREREtention----+días--+-'
      '-NOLimit-'
>+-----+-----+-----+----->
      '-WHEREDEScRiption----+descripción-'
      .-Preview ----No-----
>+-----+-----+-----+-----<
      '-Preview----+No--+-'
      '-Yes-'
  
```

### Parámetros

nombre\_nodo o nombre\_grupo\_nodos (Necesario)

Especifica el nombre de los nodos cliente o grupos de nodos cuyos datos se incluyen en los volúmenes de juegos de copias de seguridad especificados. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo que especifique pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener caracteres comodín. Si volúmenes de juegos de copias de seguridad contienen juegos de



copias de seguridad de varios nodos, cada juego de copias de seguridad cuyo nombre de nodo coincida con uno de los nombres de nodo especificados se suprimirá.

nombre\_juego\_copias\_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a suprimir. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

BEGINDate

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional.

Utilice este parámetro junto con el parámetro BEGINDATE para especificar un rango para la fecha y la hora. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

ENDDate

Especifica la fecha final en la que se creó el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro junto con el parámetro ENDTIME para especificar un rango para la fecha y la hora. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final del rango en que se ha creado el juego de copias de seguridad que se va a suprimir. Este parámetro es opcional. Puede utilizar este parámetro junto con el parámetro ENDDATE para especificar un rango para la fecha y la hora. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-02:00 o -02:00.

#### WHEREDATType

Especifica que se van a suprimir los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben suprimir. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

##### ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben suprimir. Este es el valor predeterminado.

##### FILE

Especifica que se va a suprimir un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen copias de seguridad de archivos y directorios realizadas por el cliente de copia de seguridad/archivado.

##### IMAGE

Especifica que se va a suprimir un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el comando BACKUP IMAGE del cliente de copia de seguridad/archivado.

#### WHERERETention

Especifica el valor de retención, especificado en días, asociado a los juegos de copias de seguridad que se van a suprimir. Puede especificar un entero entre el 0 y el 30000. Los valores son:

##### días

Especifica que los juegos de copias de seguridad que permanecen retenidos durante este número de días, se suprimirán.

##### NOLimit

Especifica que los juegos de copias de seguridad que permanecen retenidos indefinidamente, se suprimirán.

#### WHEREDEscription

Especifica la descripción asociada al juego de copias de seguridad que se va a suprimir. La descripción que especifique puede contener caracteres comodín. Este parámetro es opcional. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### Preview

Especifica si se previsualiza la lista de los juegos de copias de seguridad que se van a suprimir, sin suprimir realmente los juegos de copias de seguridad. Este parámetro es opcional. El valor predeterminado es NO. Los valores son:

##### No

Especifica que los juegos de copias de seguridad se suprimirán.

##### Yes

Especifica que el servidor visualiza la lista de los juegos de copias de seguridad que se van a suprimir, sin suprimir realmente los juegos de copias de seguridad.

## Ejemplo: suprimir un juego de copias de seguridad

Suprimir el juego de copias de seguridad PERS\_DATA.3099 que pertenece al nodo cliente JANE. El juego de copias de seguridad se generó el día 19/11/1998 a las 10:30:05 horas, y la descripción es "Documentation Shop".

```
delete backupset pers_data.3099  
begindate=11/19/1998 begintime=10:30:05  
wheredescription="documentation shop"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE BACKUPSET

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## DELETE CLIENTOPT (Suprimir una opción de un conjunto de opciones)

Utilice este comando para suprimir una opción de cliente de un conjunto de opciones.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas sin restringir o privilegio de políticas restringido.

### Sintaxis

```
>>-DELeTe CLIENTOpt--nombre_conjunto_opciones--nombre_opción---->  
>--+-----+-----<  
  '-SEQnumber--++-número-+-'  
    '-ALL----'
```

### Parámetros

nombre\_conjunto\_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones del cliente.

nombre\_opción (Obligatorio)

Especifica una opción cliente válida.

SEQnumber

Especifica un número de secuencia cuando se especifica un nombre de opción más de una vez. Este parámetro es opcional. Los valores válidos son:

- n  
Especifica un número entero igual o mayor que 0.
- ALL  
Especifica todos los números de secuencia.

## Ejemplo: suprimir la opción de formato de fecha

Suprimir la opción de formato de fecha en un conjunto de opciones denominado *ENG*.

```
delete clientopt eng dateformat
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE CLIENTOPT

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

## DELETE CLOPTSET (Suprimir un conjunto de opciones de cliente)

Utilice este comando para suprimir un conjunto de opciones de cliente.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas sin restringir o privilegio de políticas restringido.

## Sintaxis

```
>>-DELeTe CLOptset--nombre_conjunto_opciones-----><
```

## Parámetros

nombre\_conjunto\_opciones (Obligatorio)  
Especifica el nombre del conjunto de opciones del cliente que se va a suprimir.

## Ejemplo: suprimir un conjunto de opciones de cliente

Suprimir el conjunto de opciones de cliente denominado *ENG*.

```
delete cloptset eng
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE CLOPTSET

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.

Comando	Descripción
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.

## DELETE COLLOGROUP (Suprimir un grupo de proximidad)

Utilice este comando para suprimir un grupo de proximidad. No puede suprimir un grupo de proximidad si incluye algún miembro.

Puede eliminar todos los miembros del grupo de proximidad mediante la emisión del comando DELETE COLLOCMEMBER con un comodín en el parámetro nombre\_nodo.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de almacenamiento sin restricciones.

### Sintaxis

```
>>-DElete COLLOGroup--nombre_grupo-----<<
```

### Parámetros

nombre\_grupo  
Especifica el nombre del grupo de proximidad que desea suprimir.

### Ejemplo: suprimir un grupo de proximidad

Suprimir un grupo de proximidad denominado group1.

```
delete collogroup group1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE COLLOGROUP

Comando	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.

Comando	Descripción
UPDATE COLLOCGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## DELETE COLLOCMEMBER (Suprimir un miembro de grupo de proximidad)

Utilice este mandato para suprimir un nodo de cliente o espacio de archivos de un grupo de proximidad.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de almacenamiento sin restricciones.

### Sintaxis

Suprimir un nodo de un grupo de proximidad

```

      .-,------.
      v              |
>>-DElete COLLOCMember--nombre_grupo---nombre_nodo+-----><

```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad del que desea suprimir un nodo de cliente.

nombre\_nodo

Especifica el nombre del nodo de cliente que desea suprimir del grupo de proximidad. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nodos.

Suprimir un espacio de archivos de un grupo de proximidad de espacio de archivos

```

>>-DElete COLLOCMember--nombre_grupo--nombre_nodo----->
      .-,------.
      v              |
>>-Filespace-----nombre_espacio_archivos+----->
      .-NAMEType----SERVER-----
>+-----+-----+----->
  '-NAMEType----+-SERVER--+'
      +-UNICODE-+
      '-FSID---- '
      .-CODEType----BOTH-----
>+-----+-----+-----><
  '-CODEType----+-BOTH-----+'
      +-UNICODE----+
      '-NONUNICODE-'

```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad del que desea suprimir un espacio de archivos.

nombre\_nodo

Especifica el nodo de cliente donde se encuentra el espacio de archivos.

Filespace

Especifica el *nombre\_espacio\_archivos* del nodo de cliente que desea suprimir del grupo de proximidad. Puede especificar uno o más nombres de espacio de archivos que se encuentren en un nodo de cliente específico. Si especifica varios nombres de espacio de archivos, sepárelos con comas, no utilice espacios intercalados. También puede utilizar caracteres comodín al especificar varios nombres de espacio de archivos.

NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Un cliente de copia de seguridad/archivado con soporte de Unicode solamente está disponible para Windows, Macintosh OS 9, Macintosh OS X y NetWare. Utilice este parámetro cuando especifique un nombre de espacio de archivos que no sea un único comodín. Puede especificar un nombre de espacio de archivos cualificado al completo que no contenga un comodín. O bien puede especificar un nombre de espacio de archivos parcialmente cualificado, que puede tener un comodín, pero debe contener otros caracteres. El valor predeterminado es SERVER. Los valores posibles son:

#### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

#### UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen realmente los nombres y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

#### FSID

El servidor interpreta los nombres de espacios de archivos por sus ID de espacio de archivos (FSID).

#### CODETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro solamente cuando especifique un único carácter comodín para el nombre de espacio de archivos. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Los valores siguientes están disponibles:

#### BOTH

Incluir los espacios de archivos independientemente del tipo de página de códigos.

#### UNICODE

Incluir solo espacios de archivos que están en Unicode.

#### NONUNICODE

Incluir los espacios de archivos que no están en Unicode.

## Suprimir miembros de grupo de proximidad

---

Suprimir dos nodos, NODE1 y NODE2, de un grupo de proximidad, GROUP1.

```
delete collocmember group1 node1,node2
```

## Suprimir un espacio de archivos de un grupo de proximidad de espacio de archivos

---

Emita el mandato siguiente para suprimir el espacio de archivos *cap\_27400* del grupo de proximidad *collgrp\_2* en el nodo *hp\_4483*:

```
delete collocmember collgrp_2 hp_4483 filespace=cap_27400
```

## Suprimir un miembro de grupo de proximidad de espacio de archivos de un nodo que utiliza Unicode

---

Si el espacio de archivos se encuentra en un nodo que utiliza Unicode, puede especificarlo en el mandato. Emita el mandato siguiente para suprimir el espacio de archivos *cap\_257* del grupo de proximidad *collgrp\_3* del nodo *win\_4687*:

```
delete collocmember collgrp_3 win_4687 filespace=cap_257 codetype=unicode
```

## Suprimir un espacio de archivos con un nombre parcial designado

---

Si el espacio de archivos tiene un nombre parcial, puede utilizar un comodín para suprimirlo. Emita el mandato siguiente para suprimir el espacio de archivos *cap\_* del grupo de proximidad *collgrp\_4* del nodo *win\_4687*:

```
delete collocmember collgrp_4 win_4687 filespace=cap_* codetype=unicode
```

Si hay más de un espacio de archivos cuyo nombre empieza por *cap\_*, estos espacios de archivos también se suprimen.

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DELETE COLLOCMEMBER

Comando	Descripción
---------	-------------





Especifica el dominio de políticas al que pertenece el grupo de copia.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas al que pertenece el grupo de copia.

nom\_clase (Necesario)

Especifica la clase de gestión a la que pertenece el grupo de copia.

STANDARD

Especifica el grupo de copias, que siempre es STANDARD. Este parámetro es opcional. El valor predeterminado es STANDARD.

Type

Especifica el tipo del grupo de copia que se va a suprimir. Este parámetro es opcional. El valor predeterminado es BACKUP. Los valores posibles son:

Backup

Especifica que se suprime el grupo de copia de seguridad.

Archive

Especifica que se suprime el grupo de copia archivada.

## Ejemplo: suprimir un grupo de copias de seguridad

Suprimir el grupo de copia de seguridad de la clase de gestión ACTIVEFILES que está en el juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS.

```
delete copygroup employee_records  
vacation activefiles
```

## Ejemplo: suprimir un grupo de copias archivadas

Suprimir el grupo de copia archivada de la clase de gestión MCLASS1 que está en el juego de políticas SUMMER del dominio de políticas PROG1.

```
delete copygroup progl summer mclass1 type=archive
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE COPYGROUP

Comando	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

## DELETE DATAMOVER (Suprimir un transportador de datos)

Utilice este comando para suprimir un transportador de datos. No es posible suprimir un transportador de datos si hay rutas definidas en este transportador de datos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DELeTe DATAMover--nombre_transportador_datos-----><
```

### Parámetros

nombre\_transportador\_datos (Obligatorio)

Especifica el nombre del transportador de datos.

Nota: Con este comando se suprime el transportador de datos aunque haya datos del nodo NAS correspondiente.

## Ejemplo: suprimir un transportador de datos



Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que se incluye en las estadísticas de deduplicación de datos. Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el comando falla.

Restricción: Sólo puede especificar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de nube.

nombre\_nodo

Especifica el nombre del nodo de cliente que se notifica en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Si no especifica un valor para este parámetro, se visualizarán todos los nodos. Puede especificar hasta 64 caracteres para el nombre de nodo. Si especifica más de 64 caracteres, el comando falla.

nombre\_espacio\_de\_archivos o FSID

Especifica el nombre o el ID de espacio de archivos (FSID) de uno o varios espacios de archivos que se notifican en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. El asterisco es el valor predeterminado. Especifique uno de los siguientes valores:

\*

Especifique un asterisco (\*) para mostrar todos los espacios de archivos o ID.

nombre\_espacio\_de\_archivos

Especifica el nombre del espacio de archivos. Especifique varios nombres separándolos con comas y sin espacios intercalados. FSID especifica el identificador del espacio de archivos. Este parámetro es válido para los clientes con espacios de archivos que están en formato Unicode. Especifique varios nombres separándolos con comas y sin espacios intercalados.

Para los clientes con espacios de archivos en formato Unicode, puede especificar un nombre de espacio de archivos o un FSID. Si especifica un nombre de espacio de archivos, es posible que el servidor deba convertir el nombre de espacio de archivos que especifique. Por ejemplo, puede que el servidor deba convertir el nombre que especifique de la página de códigos del servidor a Unicode.

Restricciones: Se aplican las siguientes restricciones a los nombres de espacio de archivos y los identificadores de espacio de archivos (FSID):

- Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.
- No especifique FSID y nombres de espacio de archivos en el mismo comando.

CODEType

Especifica qué tipo de espacios de archivos se van a incluir en el informe. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un asterisco para visualizar información sobre todos los espacios de archivos. Este parámetro es opcional. Especifique uno de los siguientes valores:

UNICODE

Incluir los espacios de archivos que están en formato Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en formato Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos. Este es el valor predeterminado.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro cuando los clientes de IBM Spectrum Protect tengan espacios de archivos en formato Unicode y estén en sistemas operativos Windows, NetWare o Macintosh OS X. Este parámetro es opcional.

Este parámetro es necesario si especifica un nombre de nodo y un nombre de espacio de archivos o un FSID.

Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un asterisco.

Especifique uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

TODate

Especifica la fecha más reciente de las estadísticas que se van a suprimir. IBM Spectrum Protect elimina únicamente las estadísticas cuya fecha sea la misma o sea anterior a la fecha que especifique. Este parámetro es opcional.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	15/10/2015  Si especifica una fecha, se evaluarán todos los registros candidatos que se grabaron en dicha fecha (que finaliza a las 11:59:59 pm).
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1.  Para visualizar la información creada hasta ayer, puede especificar TODATE=TODAY-1 o TODATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los registros que estaban activos el día 10 del mes actual.

TOTime

Especifica que desea suprimir las estadísticas de eliminación de duplicados de datos creadas hasta esa hora inclusive en la fecha indicada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada.	12:30:22
NOW	La hora actual en la fecha especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada.	NOW+03:00 o +03:00.  Si emite el comando DELETE DEDUPSTATS a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect suprime los registros con la hora 12:00 o anterior en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada.	NOW-03:30 o -03:30.  Si emite el comando DELETE DEDUPSTATS a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect suprime los registros con la hora 5:30 o anterior en la fecha especificada.

## Ejemplo: suprimir estadísticas de eliminación de duplicados de datos para un espacio de archivos




Suprimir estadísticas de deduplicación de datos de un espacio de archivos llamado /srvr que pertenece a una agrupación de almacenamiento de contenedores de directorio, POOL1, que está almacenada en el nodo de cliente NODE1.

```
delete dedupstats pool1 node1 /srvr
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE DEDUPSTATS

Comando	Descripción
---------	-------------

Comando	Descripción
GENERATE DEDUPSTATS	Genera las estadísticas de eliminación de duplicados de datos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DEDUPSTATS	Muestra las estadísticas de eliminación de duplicados de datos.

## DELETE DEVCLASS (Suprimir una clase de dispositivo)

Utilice este comando para suprimir una clase de dispositivo.

Para utilizar este mandato, antes debe suprimir todas las agrupaciones de almacenamiento asignadas a la clase de dispositivo y, si es necesario, cancelar todos los procesos de exportación o importación de la base de datos que estén utilizando la clase de dispositivo.

No se puede suprimir la clase de dispositivo DISK, que se predefine en la instalación, pero se pueden suprimir todas las clases de dispositivo que haya definido un administrador de IBM Spectrum Protect.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DELeTe DEVclass--nombre_clase_dispositivo-----<<
```

### Parámetros

nombre\_clase\_dispositivo (Necesario)  
Especifica el nombre de la clase de dispositivo que se ha de suprimir.









### Ejemplo: suprimir una clase de dispositivo

Suprimir la clase de dispositivo denominada MYTAPE. No existen agrupaciones de almacenamiento asignadas a la clase de dispositivo.

```
delete devclass mytape
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE DEVCLASS

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux DEFINE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
 Sistemas operativos AIX  Sistemas operativos Linux UPDATE DEVCLASS (servidor de medios de z/OS)	 Sistemas operativos AIX  Sistemas operativos Linux Cambia los atributos de una clase de dispositivo para el almacenamiento gestionado por un servidor de medios de z/OS.

## DELETE DOMAIN (Suprimir un dominio de políticas)

Utilice este comando para suprimir un dominio de políticas. Todos los conjuntos de políticas, incluido el conjunto de políticas ACTIVE, clases de gestión y grupos de copia se suprimen junto con el dominio de políticas.

No se puede suprimir un dominio de políticas en el que haya nodos inscritos. Para determinar si hay nodos cliente inscritos para un dominio de políticas, emita el mandato QUERY DOMAIN o QUERY NODE. Traspase todos los nodos cliente a otro dominio de políticas o suprima los nodos.

Puede suprimir el dominio de políticas STANDARD predefinido. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-DELeTe Domain--nombre_dominio-----><
```

## Parámetros

---

*nombre\_dominio* (Necesario)  
Especifica el dominio de políticas que se suprime.

## Ejemplos: suprimir un dominio de políticas

---

Suprimir el dominio de políticas EMPLOYEE\_RECORDS.

```
delete domain employee_records
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DELETE DOMAIN

Comando	Descripción
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

## DELETE DRIVE (Suprimir una unidad de una biblioteca)

---

Utilice este comando para suprimir una unidad de una biblioteca. No se puede suprimir una unidad que se está utilizando.

Todas las rutas relacionadas con una unidad deben suprimirse para que la propia unidad pueda suprimirse.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---

```
>>-DELeTe DRive--nombre_biblioteca--nombre_unidad-----><
```

## Parámetros

---

*nombre\_biblioteca* (Necesario)  
Especifica el nombre de la biblioteca donde está situada la unidad.  
*nombre\_unidad* (Obligatorio)  
Especifica el nombre de la unidad que se ha de suprimir.

## Ejemplo: suprimir una unidad de una biblioteca

---

Suprimir la unidad DRIVE3 de la biblioteca denominada AUTO.

```
delete drive auto drive3
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE DRIVE

Comando	Descripción
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE DRIVE	Cambia los atributos de una unidad.

## DELETE EVENT (Suprimir registros de eventos)

Utilice este mandato para suprimir registros de eventos de la base de datos. Se crea un registro de eventos cuando se arranca o falla el proceso de un mandato planificado.

Este mandato suprime únicamente los registros de eventos que existen a la hora que se ejecuta el mandato. Un registro de eventos no se encontrará:

- Si el registro de eventos no se ha creado nunca (el evento se ha planificado para el futuro).
- Si el evento se ha pasado y el registro de eventos ya se ha suprimido.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

## Sintaxis

```

>>-DELeTe EVent-- fecha--+-00:00-.-----+----->
                        '-hora--'

.-TYPE---Client-----
>--+-----+-----<
'-TYPE---+Client-----+'
      +-Administrative+
      '-All-----'
```

## Parámetros

fecha (Obligatorio)

Especifica la fecha que se utiliza para determinar qué registros de eventos se han de suprimir. El número máximo de días que puede especificar es de 9999.

Utilice este parámetro junto con el parámetro TIME para especificar una fecha y hora en que suprimir los registros de eventos. Se suprimirá cualquier registro cuyo inicio planificado sea anterior a la fecha y hora especificadas. Sin embargo, no se suprimirán los registros de eventos cuyo margen de puesta en marcha no haya transcurrido todavía.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

hora

Especifica la hora que se utiliza para determinar qué registros de eventos se han de suprimir. Utilice este parámetro junto con el parámetro DATE para especificar una fecha y hora en que suprimir los registros de eventos. Se suprimirá cualquier registro cuyo inicio planificado sea anterior a la fecha y hora especificadas. Sin embargo, no se suprimirán los registros de eventos cuyo margen de puesta en marcha no haya transcurrido todavía. El valor predeterminado es 00:00.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+03:00 o +03:00 Atención: Si emite este comando a las 9:00 utilizando NOW+03:00 o +03:00, IBM Spectrum Protect suprimirá los registros que tengan una hora a partir de las 12:00 en la fecha que se especifique.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-03:00 o -03:00

TYPE

Especifica el tipo de eventos que se ha de suprimir. Este parámetro es opcional. El valor predeterminado es CLIENT. Los valores posibles son:

Client

Especifica que se suprimen los registros de eventos de las planificaciones de cliente.

ADministrative

Especifica que se suprimen los registros de eventos de las planificaciones de comandos de administración.

ALL

Especifica que se suprimen los registros de eventos de las planificaciones de mandatos de administración y de cliente.

## Ejemplo: suprimir registros de eventos

Suprimir registros para eventos con horas de inicio planificadas anteriores a las 08:00 del 26 de Mayo de 1998 (26/05/1998), y cuyo margen de puesta en marcha ya haya transcurrido. Los registros de estos eventos se suprimirán, con independencia de si ha transcurrido o no el período de retención de los registros de eventos, tal como se ha especificado con el mandato SET EVENTRETENTION.

```
delete event 05/26/1998 08:00
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE EVENT

Comando	Descripción
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.

## DELETE EVENTSERVER (Suprimir la definición del servidor de eventos)



Utilice este comando para suprimir la definición del servidor de eventos. Debe emitir este comando antes de emitir el comando DELETE SERVER. Si especifica el servidor que se ha definido como el servidor de eventos en el comando DELETE SERVER, recibirá un mensaje de error.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-DELeTe EVENTSErVer-----><
```

## Ejemplo: suprimir una definición de servidor de eventos

---

Suprimir la definición del servidor de eventos ASTRO.

```
delete eventserver
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DELETE EVENTSERVER

Comando	Descripción
DEFINE EVENTSERVER	Define un servidor como un servidor de eventos.
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.

## DELETE FILESPACE (Suprimir datos del nodo cliente del servidor)

---

Utilice este comando para suprimir espacios de archivos del servidor. Los archivos que pertenecen al espacio de archivos se suprimen de las agrupaciones de almacenamiento primaria, datos activos y de copia, y de los grupos de proximidad de espacio de archivos.

IBM Spectrum Protect suprime uno o varios espacios de archivos como una serie de transacciones de base de datos de proceso por lotes, con lo que impide que se ejecute una operación de retrotracción o validación para todo un espacio de archivos como una sola acción. Si se cancela el proceso o se produce un problema en el sistema, puede realizarse una supresión parcial. Un comando DELETE FILESPACE posterior para el mismo nodo o propietario puede suprimir los datos restantes.

Si este mandato se aplica a un volumen WORM (una sola grabación, varias lecturas), el volumen se hará reutilizable de nuevo si le queda espacio en el cual se puedan grabar datos. Los datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el comando CHECKOUT LIBVOLUME.

Consejos:

- Si la protección de retención de archivado está activada, el servidor suprime las copias archivadas con periodos de retención caducados. Para obtener más información, consulte el mandato SET ARCHIVERETENTIONPROTECTION.
- El servidor no suprimirá las copias archivadas que están en espera de supresión hasta que se libere la retención.
- La reclamación no se inicia mientras el mandato DELETE FILESPACE se está ejecutando.
- Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se elimina del grupo de proximidad.
- Si suprime un espacio de archivo en una agrupación de almacenamiento de duplicados eliminados, el nombre del espacio de archivo DELETED aparece en la salida del mandato QUERY OCCUPANCY hasta que se hayan eliminado las dependencias de eliminación de duplicados.
- Cuando se configura la réplica en un espacio de archivos, el mandato DELETE FILESPACE solo suprime el espacio de archivos en el servidor cuando emite el mandato. Si emite el mandato REPLICATE NODE, el espacio de archivos no se suprime en el otro servidor de réplica.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.



Se suprimen todas las copias archivadas de todos los espacios de archivos de un nodo inscrito como TYPE=SERVER.

#### DATA

Especifica los objetos a suprimir. Este parámetro es opcional. El valor predeterminado es ANY. Puede especificar uno de los siguientes valores:

##### ANY

Se suprimen archivos, directorios e imágenes.

##### FILES

Se suprimen archivos y directorios.

##### IMAGES

Se suprimen objetos de imágenes. Puede utilizar este parámetro solamente si ha especificado TYPE=ANY o TYPE=BACKUP.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Puede especificar uno de los siguientes valores:

##### No

Especifica que el servidor procesa este comando en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

##### Yes

Especifica que el servidor procesa este mandato en primer plano. Espere a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida al cliente de administración cuando finaliza el comando.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### OWNER

Restringe los datos que se suprimen a los archivos que pertenecen al propietario. Este parámetro es opcional y se hace caso omiso cuando TYPE=SPACEMANAGED. Este parámetro sólo se aplica a los sistemas cliente de varios usuarios, como AIX, Linux y Solaris OS.

#### NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Un cliente de archivado y copia de seguridad con soporte Unicode solamente está disponible para los siguientes sistemas operativos: Windows, Macintosh OS X y NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

##### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

##### UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

##### FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

#### CODETYPE

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

##### UNICODE

Incluir los espacios de archivos que están en Unicode.

##### NONUNICODE

Incluir los espacios de archivos que no están en Unicode.

##### BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

## Suprimir un espacio de archivos

---

Suprima el espacio de archivo C\_Drive que pertenece al nodo cliente HTANG.

```
delete filespace htang C_Drive
```

## Suprimir todos los archivos gestionados por espacio para un nodo de cliente

Suprimir todos los archivos migrados del nodo de cliente APOLLO (esto es, todos los archivos gestionados por espacio).

```
delete filespace apollo * type=spacemanaged
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE FILESPACE

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
RENAME FILESPACE	Redenomina un espacio de archivos de cliente en el servidor.

## DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)

Utilice este comando para suprimir de un grupo de servidores un servidor o un grupo de servidores.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
      .-|-----|  
      v          |  
>>>DELeTe GRPMEMber--nombre_grupo----nombre_miembro+----->>
```

### Parámetros

nombre\_grupo (Obligatorio)

Especifica el grupo.

nombre\_miembro (Obligatorio)

Especifica el servidor o el grupo que se suprime del grupo. Para especificar varios nombres, debe separarlos con comas y sin espacios intercalados.

### Ejemplo: suprimir un servidor de un grupo de servidores

Suprimir el miembro PHOENIX del grupo WEST\_COMPLEX.

```
delete grpmember west_complex phoenix
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE GRPMEMBER

Comando	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.

Comando	Descripción
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVER	Suprime la definición de un servidor.
DELETE SERVERGROUP	Suprime un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## DELETE LIBRARY (Suprimir una biblioteca)

Utilice este comando para suprimir una biblioteca. Antes de suprimir la biblioteca, deberá eliminar otros objetos asociados, por ejemplo la ruta.

Utilice este comando para suprimir una biblioteca. Antes de suprimir una biblioteca, suprima la ruta y todas las unidades asociadas.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DElete LIBRary--nombre_biblioteca-----<<
```

### Parámetros

nombre\_biblioteca (Necesario)  
Especifica el nombre de la biblioteca que se ha de suprimir.

### Ejemplo: suprimir una biblioteca manual

Suprimir la biblioteca manual denominada LIBR1.

```
delete library libr1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE LIBRARY

Comando	Descripción
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

Comando	Descripción
UPDATE PATH	Cambia los atributos asociados con una ruta.

## DELETE MACHINE (Suprimir información de una máquina)

Utilice este comando para suprimir la información de descripción de una máquina. Para sustituir la información existente, emita este comando y, a continuación, emita el comando INSERT MACHINE.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DELeTe MACHine--machine_name----->
. -Type---All-----
>+-----+-----><
' -Type---All-----'
    +-RECOVERYInstructions-+
    '-Characteristics-----'
```

### Parámetros

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina cuya información debe suprimirse.

Type

Especifica el tipo de información de la máquina. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

All

Especifica toda la información.

RECOVERYInstructions

Especifica las instrucciones de recuperación.

CHaracteristics

Especifica las características de la máquina.

### Ejemplo: suprimir la información de una máquina específica

Suprimir las características de máquina asociadas a la máquina DISTRICT5.

```
delete machine district5 type=characteristics
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE MACHINE

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE MACHINE	Cambia la información para una máquina.

## DELETE MACHNODEASSOCIATION (Suprimir la asociación entre una máquina y un nodo)

Utilice este comando para suprimir la asociación que hay entre una máquina y uno o varios nodos. Este comando no suprime el nodo de IBM Spectrum Protect.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
      .-|-----|  
      v          |  
>>-DElete MACHNODEAssociation--machine_name----nombre_nodo-+---><
```

## Parámetros

---

nombre\_máquina (Obligatorio)

Especifica el nombre de una máquina que está asociada a uno o varios nodos.

nombre\_nodo (Obligatorio)

Especifica el nombre de un nodo asociado a una máquina. Si especifica una lista de nombres de nodos, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Si un nodo no está asociado a la máquina, se omite ese nodo.

## Ejemplo: suprimir una asociación entre un nodo y una máquina

---

Suprimir la asociación entre la máquina DISTRICT5 y el nodo ACCOUNTSPAYABLE.

```
delete machnodeassociation district5 accountspayable
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DELETE MACHNODEASSOCIATION

Comando	Descripción
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
QUERY MACHINE	Muestra información sobre máquinas.

## DELETE MGMTCLASS (Suprimir una clase de gestión)

---

Utilice este comando para suprimir una clase de gestión. No puede suprimir una clase de gestión del juego de políticas ACTIVE. Junto con la clase de gestión, se suprimen todos los grupos de copia de la clase de gestión.

Puede suprimir la clase de gestión asignada como valor predeterminado para un juego de políticas, pero un juego de políticas no se puede activar si no tiene una clase de gestión predeterminada.

Puede suprimir la clase de gestión predefinida STANDARD del dominio de políticas STANDARD. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas sin restricciones, o privilegio de políticas limitado al dominio de políticas al que pertenece la clase de gestión.

## Sintaxis

---

```
>>-DElete Mgmtclass--nom_dominio--nom_conjunto_políticas--nom_clase-><
```

## Parámetros

---

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre\_juego\_políticas (Necesario)  
Especifica el juego de políticas al que pertenece la clase de gestión.  
nom\_clase (Necesario)  
Especifica la clase de gestión que se suprime.

## Ejemplo: suprimir una clase de gestión

Suprimir la clase gestión ACTIVEFILES del juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS.

```
delete mgmtclass employee_records  
vacation activefiles
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE MGMTCLASS

Comando	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

## DELETE NODEGROUP (Suprimir un grupo de nodos)

Utilice este comando para suprimir un grupo de nodos. No puede suprimir un grupo de nodos si incluye algún miembro.

Atención: Puede eliminar todos los miembros del grupo de nodos ejecutando el comando DELETE NODEGROUPMEMBER con un carácter comodín en el parámetro nombre\_nodo.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

## Sintaxis

```
>>-DELeTe NODEGrouP--nombre_grupo-----<<
```

## Parámetros

nombre\_grupo  
Especifica el nombre del grupo de nodos que desea suprimir.

## Ejemplo: suprimir un grupo de nodos

Suprimir un grupo de nodos denominado group1.

```
delete nodegroup group1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE NODEGROUP

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.



Comando	Descripción
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## DELETE NODEGROUPMEMBER (Suprimir un miembro de grupo de nodos)

Utilice este comando para suprimir un nodo cliente de un grupo de nodos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

### Sintaxis

```

      .-,-,-----
      v          |
>>-DELeTe NODEGROUPMember--nombre_grupo----nombre_nodo-+-----><

```

### Parámetros

nombre\_grupo

Especifica el nombre del grupo de nodos del que desea suprimir un nodo cliente.

nombre\_nodo

Especifica el nombre del nodo cliente que desea suprimir del grupo de nodos. Puede especificar uno o más nombres. Al especificar varios nombres, separe los nombres con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nodos.

### Ejemplo: suprimir miembros de grupo de nodos

Suprimir dos nodos, `node1` y `node2`, de un grupo de nodos, `group1`.

```
delete nodegroupmember group1 node1,node2
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE NODEGROUPMEMBER

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.

Comando	Descripción
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## DELETE PATH (Suprimir una ruta)

Utilice este comando para suprimir una definición de ruta.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DElete PATH--nombre_origen--nombre_destino----->
                                     (1)
>--SRCType-----+--DATAMover-----+----->
      '-SERVer-----'
                                     (2)
>--DESTType-----+--DRive-----LIBRary-----nombre_biblioteca+---->>
      '-LIBRary-----'

```

Notas:

1. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.
2. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.

### Parámetros

nombre\_origen (Obligatorio)

Especifica el origen de la ruta que se va a suprimir. Este parámetro es necesario.

El nombre especificado debe ser el nombre de un servidor o transportador de datos que ya se haya definido para el servidor.

nombre\_destino (Obligatorio)

Especifica el nombre del destino de la ruta que se va a suprimir. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen de la ruta que se va a suprimir. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un agente de almacenamiento.

DESTType (Obligatorio)

Especifica el tipo de destino. Los valores posibles son:

DRive LIBRary=library\_name

Especifica que el destino es una unidad. Los parámetros DRIVE y LIBRARY son necesarios si el tipo de destino es una unidad.

LIBRary

Especifica que el destino es una biblioteca.

Atención: Si se suprime la ruta de un transportador de datos a una biblioteca, o se suprime la ruta del servidor a una biblioteca, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia en este estado, no se inicializará la biblioteca.

### Ejemplo: suprimir una ruta de transportador de datos NAS

Suprimir una ruta de un transportador de datos NAS denominado NAS1 a la biblioteca NASLIB.

```
delete path nas1 naslib srctype=datamover desttype=library
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE PATH

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE PATH	Define una ruta de un origen a un destino.
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## DELETE POLICYSET (Suprimir un juego de políticas)

Utilice este comando para suprimir un juego de políticas. Al suprimir un juego de políticas, también se suprimen todas las clases de gestión y los grupos de copia que pertenecen al juego de políticas.

El conjunto de políticas ACTIVE de un dominio de políticas no se puede suprimir. Puede sustituir el contenido del conjunto de políticas ACTIVE activando otro conjunto de políticas. De lo contrario, el único modo de eliminar el conjunto de políticas ACTIVE es suprimir el dominio de políticas que contiene el conjunto de políticas.

Puede suprimir el juego de políticas STANDARD predefinido. Sin embargo, si más adelante reinstala el servidor de IBM Spectrum Protect, el proceso restaurará todos los objetos de política STANDARD.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

### Sintaxis

```
>>-DElete Policyset--nombre_dominio--nombre_juego_políticas----><
```

### Parámetros

nombre\_dominio (Necesario)  
Especifica el dominio de políticas al que pertenece el juego de políticas.

nombre\_juego\_políticas (Necesario)  
Especifica el juego de políticas que se va a suprimir.

### Ejemplo: suprimir un juego de políticas

Suprima el conjunto de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS emitiendo el mandato siguiente:

```
delete policyset employee_records vacation
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.



Especifica los administradores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (\*) para suprimir del perfil todos los administradores. Si especifica una lista de administradores y para el perfil existe una definición que coincide con todos, el comando no se ejecutará. Las definiciones de administrador no se modifican en el gestor de configuración. Sin embargo, se suprimen automáticamente de todos los servidores gestionados suscritos en la siguiente renovación de la configuración, con las excepciones siguientes:

- Un administrador no se suprime si tiene una sesión abierta en el servidor.
- Un administrador no se suprime si, como consecuencia, el servidor gestionado se queda sin administradores con la clase de privilegio de sistema.

#### DOMains

Especifica los dominios cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (\*) para suprimir del perfil todos los dominios. Si especifica una lista de dominios y para el perfil existe una definición que coincide con todos los dominios, el comando no se ejecutará.

La información de dominio se suprime automáticamente de todos los servidores gestionados suscritos. Sin embargo, no se suprimirá un dominio de políticas que tenga nodos cliente asignados. Para suprimir el dominio en el servidor gestionado, asigne esos nodos cliente a otro dominio de políticas.

#### ADSHeds

Especifica una lista de planificaciones de administración cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Si especifica una lista de planificaciones de administración y para el perfil existe una definición que coincide con todas las planificaciones de administración, el comando no se ejecutará. Utilice el carácter de coincidencia con todos (\*) para suprimir del perfil todas las planificaciones de administración.

Las planificaciones de administración se suprimen automáticamente de todos los servidores gestionados suscritos. Sin embargo, una planificación de administración no se suprime si está activa en el servidor gestionado. Para suprimir una planificación activa, debe convertir la planificación en inactiva.

#### SCRipts

Especifica los scripts de comandos del servidor cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (\*) para suprimir del perfil todos los scripts. Si especifica una lista de dominios y para el perfil existe una definición que coincide con todos los scripts, el comando no se ejecutará. Los scripts de comandos del servidor se suprimen automáticamente de todos los servidores gestionados suscritos.

#### CLOptsets

Especifica los conjuntos de opciones de cliente cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Utilice el carácter de coincidencia con todos (\*) para suprimir del perfil todos los conjuntos de opciones de cliente. Si especifica una lista de conjuntos de opciones de cliente y para el perfil existe una definición que coincide con todos los conjuntos de opciones de cliente, el comando no se ejecutará. Los conjuntos de opciones de cliente se suprimen automáticamente de todos los servidores gestionados suscritos.

#### SERVers

Especifica los servidores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Puede utilizar el carácter de coincidencia con todos (\*) para suprimir del perfil todos los servidores. Si especifica una lista de servidores y para el perfil existe una definición que coincide con todos los servidores, el comando no se ejecutará. Las definiciones de servidor se suprimen automáticamente de todos los servidores gestionados suscritos con las excepciones siguientes:

- Una definición de servidor no se suprime si el servidor gestionado tiene una conexión abierta con otro servidor.
- Una definición de servidor no se suprime si el servidor gestionado tiene una clase de dispositivo de tipo SERVER que hace referencia al otro servidor.
- Una definición de servidor no se suprime si el servidor es el servidor de eventos para el servidor gestionado.

#### SERVERGroups

Especifica los grupos de servidores cuya asociación al perfil se suprime. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Puede utilizar el carácter de coincidencia con todos (\*) para suprimir del perfil todos los grupos de servidores. Si especifica una lista de grupos de servidores y para el perfil existe una definición que coincide con todos los grupos, el comando no se ejecutará. Las definiciones de grupo de servidores se suprimen automáticamente de todos los servidores gestionados suscritos.

## Ejemplo: suprimir las asociaciones de dominio de un perfil específico

---

Suprimir todas las asociaciones de dominios del perfil denominado MIKE.

```
delete profassociation mike domains=*
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE PROFASSOCIATION

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## DELETE PROFILE (Suprimir un perfil)

Utilice este comando en un gestor de configuración para suprimir un perfil y detener su distribución a los servidores gestionados.

No se puede suprimir un perfil bloqueado. Primero debe desbloquear el perfil con el comando UNLOCK PROFILE.

Al suprimir un perfil de un gestor de configuración no se suprimen de los servidores gestionados los objetos asociados con ese perfil. Puede utilizar el comando DELETE SUBSCRIPTION con el parámetro DISCARDOBJECTS=YES en cada servidor gestionado suscrito para suprimir suscripciones al perfil y objetos asociados. De este modo también se evita que los servidores gestionados soliciten actualizaciones adicionales del perfil.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DELEte PROFIle--nombre_perfil--+-Force-----No-----+-----><
                                     '-Force-----+No--+-'
                                     '-Yes-'
```

## Parámetros

nombre\_perfil (Obligatorio)

Especifica el perfil que se suprime.

Force

Especifica si se suprime el perfil en caso de que uno o más servidores gestionados estén suscritos a dicho perfil. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que no se suprime el perfil si uno o más servidores gestionados están suscritos a dicho perfil. Se pueden suprimir las suscripciones en cada servidor gestionado con el comando DELETE SUBSCRIPTION.

Yes

Especifica que se suprime el perfil aunque uno o más servidores gestionados estén suscritos a dicho perfil. Cada servidor inscrito continúa solicitando actualizaciones del perfil suprimido hasta que se suprima la inscripción.

## Ejemplo: suprimir un perfil

Suprimir un perfil denominado BETA, aunque se inscriban en él uno o varios servidores gestionados.

```
delete profile beta force=yes
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## DELETE RECMEDMACHASSOCIATION (Suprimir asociación de medio de recuperación y máquina)

Utilice este comando para suprimir la asociación de una o varias máquinas a un medio de recuperación. Este comando no suprime la máquina de IBM Spectrum Protect.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DELeTe RECMEDMACHAssociation--nombre_medio----->
      .-,-----
      v          |
>----nombre_máquina-+-----<<
```

### Parámetros

nombre\_soporte (Obligatorio)

Especifica el nombre del medio de recuperación que está asociado a una o varias máquinas.

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina asociada al medio de recuperación. Para especificar una lista de nombres de máquinas, debe separar los nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Si una máquina no está asociada al medio de recuperación, la máquina no se tiene en cuenta.

### Ejemplo: suprimir la asociación de una máquina a los medios de recuperación

Suprimir la asociación entre el medio de recuperación DIST5RM y las máquinas DISTRICT1 y DISTRICT5.

```
delete recmedmachassociation
dist5rm district1,district5
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE RECMEDMACHASSOCIATION

Comando	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
QUERY MACHINE	Muestra información sobre máquinas.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

## DELETE RECOVERYMEDIA (Suprimir medio de recuperación)

Utilice este comando para suprimir una definición de medio de recuperación de IBM Spectrum Protect.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DELeTe RECOVERYMedia--nombre_medio-----><
```

### Parámetros

nombre\_soporte (Obligatorio)  
Especifica el nombre del medio de recuperación.

### Ejemplo: suprimir la definición de los medios de recuperación

Suprimir el medio de recuperación DIST5RM.

```
delete recoverymedia dist5rm
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE RECOVERYMEDIA

Comando	Descripción
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

## DELETE SCHEDULE (Suprimir una planificación de cliente o de comando de administración)

Utilice este comando para suprimir planificaciones de la base de datos.

El mandato DELETE SCHEDULE tiene dos formatos: uno si la planificación se aplica a las operaciones de cliente y el otro si la planificación se aplica a mandatos administrativos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con DELETE SCHEDULE

Comando	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.



Comando	Descripción
QUERY SCHEDULE	Muestra información sobre planificaciones.
UPDATE SCHEDULE	Cambia los atributos de una planificación.

- DELETE SCHEDULE (Suprimir una planificación de cliente)  
Utilice el mandato DELETE SCHEDULE para suprimir de la base de datos una o varias planificaciones de cliente. Cuando se elimina la planificación, se suprimen todas las asociaciones de cliente con dicha planificación.
- DELETE SCHEDULE (Suprimir una planificación de administración)  
Utilice este comando para suprimir de la base de datos una o varias planificaciones de comando de administración.

## DELETE SCHEDULE (Suprimir una planificación de cliente)

Utilice el mandato DELETE SCHEDULE para suprimir de la base de datos una o varias planificaciones de cliente. Cuando se elimina la planificación, se suprimen todas las asociaciones de cliente con dicha planificación.

### Clase de privilegio

Para suprimir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado para el dominio de políticas al que pertenece la planificación.

### Sintaxis

```
>>-DELeTe SCHedule--nombre_dominio--nombre_planificación----->
      .-Type-----Client-.
>--+-----+-----<<
```

### Parámetros

- nombre\_dominio (Necesario)  
Especifica el nombre del dominio de políticas al que pertenece la planificación.
- nombre\_planificación (Obligatorio)  
Especifica el nombre de la planificación que se va a suprimir. Puede utilizar un carácter comodín para especificar este nombre.
- Type=Client  
Especifica que se suprimirá una planificación de cliente. Este parámetro es opcional. El valor predeterminado es CLIENT.

### Ejemplo: suprimir una planificación específica de un dominio de políticas específico

Suprimir la planificación WEEKLY\_BACKUP, la cual pertenece al dominio de políticas EMPLOYEE\_RECORDS.

```
delete schedule employee_records weekly_backup
```

## DELETE SCHEDULE (Suprimir una planificación de administración)

Utilice este comando para suprimir de la base de datos una o varias planificaciones de comando de administración.

### Clase de privilegio

Para suprimir una planificación de comandos de administración, debe tener autorización del sistema.

### Sintaxis

```
>>-DELeTe SCHedule--schedule_name--Type-----Administrative-----<<
```

### Parámetros

- nombre\_planificación (Obligatorio)  
Especifica el nombre de la planificación que se va a suprimir. Puede utilizar un carácter comodín para especificar este nombre.
- Type=Administrative (Necesario)

Especifica que se suprimirá una planificación de comando de administración.

## Ejemplo: suprimir una planificación de comandos de administración

Suprimir la planificación de comando de administración denominada DATA\_ENG.

```
delete schedule data_eng type=administrative
```

## DELETE SCRATCHPADENTRY (Suprimir una entrada de registro)

Utilice este mandato para suprimir una o varias líneas de datos de un área de registro.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DELeTe SCRATCHPadentry--major_category--minor_category----->  
  
      .-Line-----*-----.  
>--subject--+-----+-----<<  
      '-Line ---número-'
```

### Parámetros

major\_category (obligatorio)

Especifica la categoría de la que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

minor\_category (obligatorio)

Especifica la categoría secundaria de la que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)

Especifica el asunto del que se suprimirán una o varias líneas de datos. Este parámetro distingue entre mayúsculas y minúsculas.

Line

Especifica una línea de datos que se suprimirá. Para número, entre el número de la línea que se suprimirá. Todos los datos en la línea se suprimirán. La numeración de otras líneas en la sección de asunto no se ve afectada. Puede suprimir todas las líneas de datos de una sección de asunto omitiendo el parámetro Line en este mandato.

## Ejemplo: Suprima todas las líneas de datos de un asunto en el registro

Suprima todas las líneas de datos acerca de la ubicación de un administrador, Jane, de la base de datos que almacena información sobre administradores:

```
delete scratchpadentry admin_info location jane
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con DELETE SCRATCHPADENTRY

Comando	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

## DELETE SCRIPT (Suprimir líneas de comandos de un script o suprimir todo el script)

Utilice este mandato para suprimir una única línea de un script de IBM Spectrum Protect o para suprimir el script de IBM Spectrum Protect completo.

## Clase de privilegio

---

Para emitir este comando, el administrador debe haber definido el script con anterioridad o debe tener privilegio de sistema.

## Sintaxis

---

```
>>-DELeTe SCRipt--nombre_script--+-----+-----><
                               '-Line -==--número-'
```

## Parámetros

---

nombre\_script (Obligatorio)

Especifica el nombre del script que se va a suprimir. Se suprime el script si no se especifica un número de línea.

Line

Especifica el número de la línea que se va a suprimir del script. Si no especifica ningún número de línea, se suprime todo el script.

## Ejemplo: suprimir una línea específica de un script

---

Mediante la utilización del siguiente script, denominado QSAMPLE, emitir un comando para suprimir de éste la línea 005.

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY PROCESS

delete script qsampl line=5
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con DELETE SCRIPT

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

## DELETE SERVER (Suprimir una definición de servidor)

---

Utilice este comando para suprimir una definición de servidor.

El comando no se ejecutará si el servidor:

- Está definido como el servidor de eventos.
- Está especificado en una definición de clase de dispositivo cuyo tipo de dispositivo es SERVER.
- Tiene una conexión abierta con otro servidor.
- Es un servidor de destino para los volúmenes virtuales.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-DELeTe--SERver--nombre_servidor-----><
```

## Parámetros

nombre\_servidor (Obligatorio)  
Especifica el nombre de un servidor.

## Ejemplo: suprimir la definición de un servidor

Suprimir la definición del servidor denominado SERVER2.

```
delete server server2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE SERVER

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY EVENTSERVER	Muestra el nombre del servidor de eventos.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
UPDATE SERVER	Actualiza la información sobre un servidor.

## DELETE SERVERGROUP (Suprimir un grupo de servidores)

Utilice este mandato para suprimir un grupo de servidores. Si el grupo que se suprime es miembro de otros grupos de servidores, IBM Spectrum Protect también elimina el grupo de los otros grupos.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DELeTe SERVERGroup--nombre_grupo-----><
```

## Parámetros

nombre\_grupo (Obligatorio)  
Especifica el grupo de servidores que se suprime.

## Ejemplo: suprimir un grupo de servidores

Suprimir un grupo de servidores denominado WEST\_COMPLEX.

```
delete servergroup west_complex
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE SERVERGROUP

Comando	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
MOVE GRPMEMBER	Mueve un miembro del grupo de servidores.

Comando	Descripción
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## DELETE SPACETRIGGER (Suprimir los desencadenantes de espacio de agrupación de almacenamiento)

Utilice este comando para suprimir la definición del desencadenante de espacio de agrupación de almacenamiento.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-DELeTe SPACETriGger--STG----->
>--+-----+-----<
  '-STGPOOL----nombre_agrupación_almacenamiento-'
```

### Parámetros

STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

STGPOOL

Especifica el desencadenante de la agrupación de almacenamiento que se suprimirá. Si se especifica STG sin especificar STGPOOL, el desencadenante de espacio de la agrupación de almacenamiento predeterminado es el destino de supresión.

### Ejemplo: suprimir una definición de desencadenante de espacio

Suprimir la definición del desencadenante de espacio para la agrupación de almacenamiento WINPOOL1.

```
delete spacetrigger stg stgpool=winpool1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE SPACETRIGGER

Comando	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

## DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)

Utilice este mandato para suprimir un umbral de supervisión de estado existente.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DELeTe STATusthreshold--nombre_umbral-----><
```

## Parámetros

nombre\_umbral (Necesario)  
Especifica el nombre de umbral que desea suprimir.

## Suprimir un umbral de estado existente

Suprima un umbral de estado existente emitiendo el mandato siguiente:

```
delete statusthreshold avgstgpl
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DELETE STATUSTHRESHOLD

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## DELETE STGPOOL (Suprimir una agrupación de almacenamiento)

Utilice este comando para suprimir una agrupación de almacenamiento. Para suprimir una agrupación de almacenamiento, antes debe suprimir todos los volúmenes que están asignados a la agrupación de almacenamiento.

No se puede suprimir una agrupación de almacenamiento que se identifica como la próxima agrupación de almacenamiento para otra agrupación de almacenamiento. Para obtener más información acerca de la jerarquía de las agrupaciones de almacenamiento, consulte el parámetro NEXTSTGPOOL en el comando DEFINE STGPOOL.

Restricciones:

- Para las agrupaciones de almacenamiento de contenedor, suprima todos los directorios de agrupación de almacenamiento antes de suprimir la agrupación de almacenamiento.
- No suprima una agrupación de almacenamiento que se especifique como un destino de clase de gestión o grupo de copia del juego de políticas ACTIVE. Es posible que como consecuencia no puedan ejecutarse las operaciones de cliente.
- Cuando suprime una agrupación de almacenamiento de copia que anteriormente se había incluido en una definición de agrupación de almacenamiento primaria (específicamente en la lista COPYSTGPOOLS), debe eliminar la agrupación de almacenamiento de copia de la lista antes de suprimirla. De otro modo, el comando DELETE STGPOOL no se ejecutará correctamente hasta que se hayan eliminado todas las referencias a esa agrupación de copia. Para cada agrupación de

almacenamiento primaria que tenga una referencia a la agrupación de almacenamiento de copia que va a suprimirse, elimine la referencia, mediante la especificación del comando UPDATE STGPOOL con el parámetro COPYSTGPOOLS, que se hace a todas las agrupaciones de almacenamiento de copia anteriores, a excepción de la agrupación de almacenamiento de copia que va a suprimirse.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DELeTe STGpool--nombre_agrupación-----<<
```

## Parámetros

nombre\_agrupación (Obligatorio)  
Especifica la agrupación de almacenamiento que se suprime.

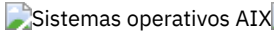

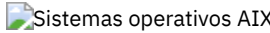
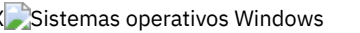
## Ejemplo: suprimir una agrupación de almacenamiento

Suprimir la agrupación de almacenamiento denominada POOLA.

```
delete stgpool poola
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE STGPOOL

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
  SET DRMCOPYSTGPOOL	  Especifica que DRM gestiona las agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

## DELETE STGPOOLDIRECTORY (Suprimir un directorio de agrupación de almacenamiento)

Utilice este comando para suprimir una definición de un directorio de agrupación de almacenamiento.

Es posible que desee suprimir un directorio de agrupación de almacenamiento por las siguientes razones:

- Para poner fuera de servicio un almacenamiento anterior.
- Para dejar de utilizar el disco local antes de mover datos a la nube.
- Para no mantener los datos en el directorio de agrupación de almacenamiento porque no hay necesidad de hacerlo.

Restricciones:

- Sólo puede emitir este mandato cuando no haya ningún contenedor asignado al directorio de agrupación de almacenamiento. Emita el mandato QUERY CONTAINER para determinar si hay algún contenedor asignado al directorio de agrupación de almacenamiento.
- Para eliminar contenedores de un directorio de agrupación de almacenamiento, debe emitir el mandato UPDATE STGPOOLDIRECTORY y especificar el parámetro ACCESS=DESTROYED. A continuación, emita el mandato AUDIT CONTAINER y especifique el parámetro ACTION=REMOVEDAMAGED. Verifique que la máquina se ha eliminado. El parámetro ACTION=REMOVEDAMAGED elimina la información de inventario de los objetos de los que se ha efectuado una copia de seguridad o que han sido archivados. Solo debe eliminar la información de inventario si no necesita las copias de seguridad.

Si el hardware genera algún error o una pérdida del directorio, consulte los mandatos relevantes AUDIT y REPAIR. Debería realizar las reparaciones necesarias en el entorno de IBM Spectrum Protect antes de suprimir la agrupación de almacenamiento.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DELeTe STGPOOLDIRectory--nombre_agrupación--directorio-----><
```

## Parámetros

nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que contiene el directorio que se debe suprimir. Este parámetro es necesario.

directorio (Obligatorio)

Especifica el directorio del sistema de archivos de la agrupación de almacenamiento que se debe suprimir. Este parámetro es necesario.

## Ejemplo: actualizar un directorio de agrupación de almacenamiento para preparar la supresión

Actualice un directorio de agrupación de almacenamiento que se denomina DIR1 en la agrupación de almacenamiento POOLA para marcarlo como destruido. Cuando una agrupación de almacenamiento se marca como destruida, puede suprimirla.

 Sistemas operativos AIX  Sistemas operativos Linux

```
update stgpooldirectory poola /storage/dir1 access=destroyed
```

 Sistemas operativos Windows

```
update stgpooldirectory poola e:\storage\dir1 access=destroyed
```

## Ejemplo: suprimir un directorio de agrupación de almacenamiento

Suprima el directorio de agrupación de almacenamiento denominado DIR1 en la agrupación de almacenamiento POOLA.

 Sistemas operativos AIX  Sistemas operativos Linux

```
delete stgpooldirectory poola /storage/dir1
```

 Sistemas operativos Windows

```
delete stgpooldirectory poola e:\storage\dir1
```

Tabla 1. Comandos relacionados con DELETE STGPOOLDIRECTORY

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.



Comando	Descripción
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.
QUERY EXTENTUPDATES	Muestra información sobre las actualizaciones de las extensiones de datos en agrupaciones de almacenamiento de contenedores de directorio.

## DELETE SUBSCRIBER (Suprimir las inscripciones de la base de datos del gestor de configuración)

Utilice este comando en un gestor de configuración para suprimir de la base de datos del gestor de configuración suscripciones del servidor gestionado. Utilice este comando cuando ya no exista un servidor gestionado o no pueda enviar notificaciones al gestor de configuración después de suprimir una suscripción.

Atención: Utilice este comando sólo en las escasas situaciones en las que la base de datos del gestor de configuración contenga una entrada para una suscripción, pero el servidor gestionado no tenga dicha suscripción. Por ejemplo, utilice este comando si ya no existe un servidor gestionado o no puede enviar notificaciones al gestor de configuración tras suprimir una suscripción.

En circunstancias normales, utilice el comando DELETE SUBSCRIPTION para suprimir una suscripción del servidor gestionado. El servidor gestionado envía la notificación al gestor de configuración, que entonces suprime la suscripción de su base de datos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DELeTe SUBSCRIBer--nombre_servidor-----<<
```

### Parámetros

nombre\_servidor (Obligatorio)  
Especifica el nombre del servidor gestionado con entradas de suscripción que se deben suprimir.

### Ejemplo: suprimir entradas de suscripción para un servidor gestionado específico

Suprimir todas las entradas de suscripción para un servidor gestionado denominado DAN.

```
delete subscriber dan
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE SUBSCRIBER

Comando	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

## DELETE SUBSCRIPTION (Suprimir una inscripción en un perfil)

Utilice este comando en un servidor gestionado para suprimir una suscripción a un perfil. También puede suprimir del servidor gestionado todos los objetos asociados al perfil.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DElete SUBSCRIPtion--nombre_perfil----->
.-DISCARDobjects----No-----
>-+-----+-----><
'-DISCARDobjects----++-No-+-'
'-Yes-'
```

### Parámetros

nombre\_perfil (Obligatorio)

Especifica el nombre del perfil cuya inscripción se suprime.

DISCARDobjects

Especifica si los objetos asociados con el perfil se van a suprimir en el servidor gestionado. Este parámetro es opcional. El valor predeterminado es NO.

No

Especifica que los objetos no se suprimirán.

Yes

Especifica que se suprimirán los objetos, excepto si están asociados a otro perfil para el que hay una inscripción definida.

### Ejemplo: suprimir una suscripción de perfil

Suprimir una suscripción a un perfil denominado ALPHA y sus objetos asociados de un servidor gestionado.

```
delete subscription alpha discardobjects=yes
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DELETE SUBSCRIPTION

Comando	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

## DELETE VIRTUALFSMAPPING (Suprimir una correlación de espacios de archivos virtuales)

Utilice este comando para suprimir una definición de correlación de espacios de archivos virtuales. Los espacios de archivos virtuales que contienen datos no puede suprimirse a menos que primero se utilice el comando DELETE FILESPACE.

### Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

## Sintaxis

```
>>-DElete VIRTUALFSmapping  -nombre_nodo----->
>--nombre_espacio_archivos_virtual-----<
```

## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre\_espacio\_archivos\_virtual (Obligatorio)

Especifica el nombre de la definición de correlación de espacios de archivos virtuales que se eliminará. Se permite el uso de caracteres comodín.

## Ejemplo: suprimir una correlación de espacios de archivos virtuales

Suprimir la definición de correlación de espacios de archivos virtuales /mikeshomedir para el nodo NAS denominado NAS1.

```
delete virtualfsmapping nas1 /mikeshomedir
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE VIRTUALFSMAPPING

Comando	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

## DELETE VOLHISTORY (Suprimir información histórica de volúmenes)

Utilice este mandato para suprimir los registros del archivo histórico de volúmenes que ya no son necesarios (por ejemplo, los registros de volúmenes de copia de seguridad de la base de datos obsoletos).

Cuando suprime registros de volúmenes que no se encuentran en las agrupaciones de almacenamiento (por ejemplo, volúmenes de copia de seguridad de la base de datos o de exportación), los volúmenes volverán al estado reutilizable aunque IBM Spectrum Protect los haya adquirido como volúmenes privados. Se eliminarán los volúmenes reutilizables con el tipo de dispositivo FILE. Al suprimir los registros de volúmenes de agrupación de almacenamiento, los volúmenes permanecen en la base de datos de IBM Spectrum Protect. Al suprimir registros de objetos de archivo del plan de recuperación de un servidor origen, los objetos del servidor destino se marcan para suprimirlos.

Restricción: No utilice el mandato DELETE VOLHISTORY para suprimir del archivo histórico de volúmenes la información sobre volúmenes correspondiente al conjunto de copias de seguridad. En su lugar, utilice el mandato DELETE BACKUPSET para ello.

Los usuarios de DRM, deben controlar la caducidad de la copia de seguridad de base de datos con el mandato SET DRMDBBACKUPEXPIREDDAYS y no con este mandato DELETE VOLHISTORY. Utilice el mandato DELETE VOLHISTORY para eliminar un registro del volumen. Esto puede provocar la pérdida de los volúmenes gestionados con el mandato MOVE DRMEDIA. Utilice el mandato SET DRMDBBACKUPEXPIREDDAYS para gestionar la caducidad automática de los volúmenes de copia de seguridad de base de datos DRM.

Consejos:

- No se suprimen los volúmenes de la serie de copia de seguridad de la base de datos más reciente.
- Los archivos históricos de volúmenes existentes no se actualizan automáticamente con este mandato.
- Puede utilizar el mandato DEFINE SCHEDULE para suprimir registros del archivo histórico de forma periódica.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-DElete VOLHistory--TODate---- fecha----->
. -Totime-----23:59:59-
>-----+----->
' -Totime----- hora-----'

>--Type----+All-----<
+DBBackup--+-----+
| '-DEVclass----class_name-' |
+DBSnapshot--+-----+
| '-DEVclass----class_name-' |
+DBRpf-----+
+EXPort-----+
| .-DELETEDatest---No-----|
+RPFfile--+-----+
| '-DELETEDatest---+No--+' |
| '-Yes-' |
| .-DELETEDatest---No-----|
+RPFSnapshot--+-----+
| '-DELETEDatest---+No--+' |
| '-Yes-' |
+STGNew-----+
+STGReuse-----+
'-STGDelete-----'
```

## Parámetros

### TODate (Obligatorio)

Especifica la fecha a utilizar para seleccionar la información histórica de volúmenes secuenciales que se ha de suprimir. Solo puede suprimir los registros cuya fecha sea la misma o sea anterior a la fecha que especifique. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	01/23/1999
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-30 o -30. Para suprimir los registros con 30 días de antigüedad o más, puede especificar TODAY-30 o simplemente -30.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

### TOTime

Especifica que desea suprimir los registros creados hasta esa hora inclusive en la fecha indicada. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:30:22
NOW	La hora actual en la fecha especificada	NOW

Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha especificada	NOW+03:00 o +03:00.  Si emite el comando DELETE VOLHISTORY a las 9:00 con TOTIME=NOW+03:00 o TOTIME=+03:00, IBM Spectrum Protect suprime los registros con la hora 12:00 o anterior en la fecha especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha especificada	NOW-03:30 o -03:30.  Si emite el comando DELETE VOLHISTORY a las 9:00 con TOTIME=NOW-3:30 o TOTIME=-3:30, IBM Spectrum Protect suprime los registros con la hora 5:30 o anterior en la fecha especificada.

#### Type (Necesario)

Especifica el tipo de los registros, que también cumplen los criterios de fecha y hora, que se suprimirán del archivo histórico de volúmenes. Los valores posibles son:

##### All

Especifica que se suprimirán todos los registros.

Restricción: El comando DELETE VOLHISTORY no suprime los registros de los volúmenes remotos.

##### DBBackup

Especifica que sólo se suprimirán los registros que contienen información sobre los volúmenes utilizados para copias de seguridad incrementales y completas de la base de datos, es decir, con los tipos de volumen BACKUPFULL y BACKUPINCR, y que cumplen los criterios de fecha y hora especificados. No se suprimirán los registros de la última serie de copia de seguridad incremental y completa de la base de datos.

##### DEVclass=nombre\_clase

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear copias de seguridad de la base de datos. Este parámetro opcional se puede utilizar para suprimir copias de seguridad de la base de datos creadas utilizando una clase de dispositivo de volúmenes virtuales de servidor a servidor. El tipo de clase de dispositivo debe ser SERVER. Este parámetro sólo se puede utilizar para suprimir entradas históricas de volumen del tipo BACKUPFULL, BACKUPINCR o DBSNAPSHOT.

Un volumen de copia de seguridad de base de datos completa o incremental puede seleccionarse para suprimirse si se cumplen todas las condiciones siguientes :

- La clase de dispositivo utilizada para crear el volumen de copia de seguridad de base de datos coincide con la clase de dispositivo especificada.
- El volumen se ha creado en la fecha y hora especificadas o antes.
- El volumen no forma parte de la serie de copias de seguridad de base de datos completa más incremental más reciente.
- El volumen no forma parte de una serie de copias de seguridad completa más incremental con una copia de seguridad de base de datos incremental creada después de una fecha y hora especificadas.

##### DBSnapshot

Especifica que sólo se suprimirán los registros que contienen información sobre los volúmenes utilizados para copias de seguridad de instantánea de base de datos y que cumplen los criterios de fecha y hora especificados. Los registros relacionados con la última copia de seguridad de base de datos de instantáneas no se suprimirán.

##### DEVclass=nombrecalse

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear copias de seguridad de la base de datos. Este parámetro opcional se puede utilizar para suprimir copias de seguridad de la base de datos creadas utilizando una clase de dispositivo de volúmenes virtuales de servidor a servidor. El tipo de clase de dispositivo debe ser SERVER. Este parámetro sólo se puede utilizar para suprimir entradas históricas de volumen del tipo BACKUPFULL, BACKUPINCR o DBSNAPSHOT.

Un volumen de copia de seguridad de instantánea de base de datos puede seleccionarse para suprimirse si se cumplen todas las condiciones siguientes:

- La clase de dispositivo utilizada para crear el volumen de copia de seguridad de base de datos coincide con la clase de dispositivo especificada
- El volumen se ha creado en la fecha y hora especificadas o antes
- El volumen no forma parte de la última serie de copias de seguridad de base de datos de instantáneas

##### DBRpf

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos y los volúmenes de archivo del plan de recuperación.

#### EXPort

Especifica que sólo se suprimen los registros que contienen información sobre volúmenes de exportación.

#### RPFfile

Especifica que sólo se suprimen los registros que contienen información sobre los objetos de archivos del plan de recuperación que están almacenados en el servidor destino y que cumplen los criterios de fecha y hora especificados.

#### DELETEDlatest

Especifica si el archivo del plan de recuperación más reciente es elegible para ser suprimido. Este parámetro opcional puede utilizarse para suprimir los archivos más recientes del plan de recuperación creados utilizando la clase de dispositivo de volúmenes virtuales de servidor a servidor.

Este parámetro sólo puede utilizarse para suprimir entradas históricas de volumen del tipo RPFfile (por ejemplo, los archivos del plan de recuperación creados con el parámetro DEVCLASS y el mandato PREPARE). Si no se especifica este parámetro, no se suprimirán las entradas RPFfile más recientes.

No

Especifica que el último archivo RPFfile no se suprime.

Sí

Especifica que el archivo RPFfile más reciente se suprime si cumple los criterios de fecha y hora especificados.

#### RPFSnapshot

Especifica que sólo han de suprimirse los registros que contienen información acerca de los objetos de archivo de plan de recuperación que se han creado para las copias de seguridad de base de datos de instantáneas, que están almacenados en un servidor de destino y que cumplen los criterios de fecha y hora especificados. El último archivo RPFsnapshot no se suprimirá a menos que cumpla los criterios de fecha y hora especificados y el parámetro DELETE se establezca en Yes.

#### DELETEDlatest

Especifica si el archivo del plan de recuperación más reciente es elegible para ser suprimido. Este parámetro opcional puede utilizarse para suprimir los archivos más recientes del plan de recuperación creados utilizando la clase de dispositivo de volúmenes virtuales de servidor a servidor.

Este parámetro sólo puede utilizarse para suprimir entradas históricas de volumen del tipo RPFsnapshot (por ejemplo, los archivos del plan de recuperación creados con el parámetro DEVCLASS y el mandato PREPARE). Si no se especifica este parámetro, no se suprimirán las entradas RPFsnapshot más recientes.

No

Especifica que el último archivo RPFsnapshot no se suprime.

Sí

Especifica que el archivo RPFsnapshot más reciente se suprime si cumple los criterios de fecha y hora especificados.

#### STGNew

Especifica que sólo se suprimen los registros que contienen información sobre los nuevos volúmenes de almacenamiento de acceso secuencial.

#### STGReuse

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de almacenamiento de acceso secuencial reutilizados.

#### STGDelete

Especifica que sólo se suprimen los registros que contienen información sobre los volúmenes de almacenamiento de acceso secuencial suprimidos.

## Ejemplo: suprimir información de archivo de plan de recuperación

Suprimir toda la información del archivo de plan de recuperación que se crea en o antes del 28/03/2016.

```
delete volhistory type=rpfile todate=03/28/2016
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DELETE VOLHISTORY

Comando	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.

Comando	Descripción
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFIL	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.
SET DRMDBBACKUPEXPIREDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.

## DELETE VOLUME (Suprimir un volumen de agrupación de almacenamiento)

Utilice este comando para suprimir un volumen de agrupación de almacenamiento y, de forma opcional, los archivos almacenados en el volumen.

Si el volumen tiene datos, para suprimir el volumen debe hacer una de las posibilidades siguientes:

- Antes de suprimir el volumen, utilice el comando MOVE DATA para traspasar todos los archivos a otro volumen.
- Solicite explícitamente que se descarten todos los archivos del volumen al suprimir el volumen (especificando DISCARDDATA=YES).

Si suprime varios volúmenes, debe suprimirlos de uno en uno. Si suprime varios volúmenes a la vez, el rendimiento del servidor puede resultar afectado de modo negativo.

No se pueden suprimir volúmenes de agrupación de almacenamiento si están utilizándose. Por ejemplo, no se puede suprimir un volumen si hay un usuario restaurando o recuperando un archivo que reside en el volumen, si el servidor está grabando información en el volumen o si hay un proceso de reclamación utilizando el volumen.

Si emite el mandato DELETE VOLUME, la información del volumen se suprime de la base de datos de IBM Spectrum Protect. Sin embargo, los archivos físicos que están asignados al mandato DEFINE VOLUME no se eliminan del espacio de archivos.

Si este mandato se aplica a un volumen WORM (una sola grabación, varias lecturas), el volumen se hará reutilizable si le queda espacio en el cual se pueden grabar datos. Los datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el comando CHECKOUT LIBVOLUME.

El comando DELETE VOLUME actualiza automáticamente el inventario de bibliotecas del servidor correspondiente a los volúmenes secuenciales si el volumen vuelve a establecerse en el estado de reutilización cuando queda vacío. Para determinar si un volumen volverá al estado de reutilización, emita el comando QUERY VOLUME y consulte la salida. Si el valor del atributo "¿Volumen reutilizable?" es "Sí", el inventario de bibliotecas del servidor se actualiza automáticamente.

Si el valor es "No," puede emitir el comando UPDATE LIBVOLUME para especificar el estado de reutilización. Se recomienda emitir el comando UPDATE LIBVOLUME después de haber emitido el comando DELETE VOLUME.

El intento de utilizar el comando DELETE VOLUME para suprimir volúmenes de WORM FILE de una agrupación de almacenamiento con RECLAMATIONTYPE=SNAPLOCK no se ejecuta correctamente y se genera un mensaje de error. La supresión de volúmenes de WORM FILE vacíos se realiza sólo a través del proceso de reclamación.

Si emite el comando DELETE VOLUME para un volumen de una agrupación de almacenamiento que tiene un valor de parámetro SHRED mayor que 0, el volumen se establece en estado pendiente hasta que se ejecuta la destrucción. La destrucción es necesaria para que se complete la supresión, aunque el volumen esté vacío.

Si emite el comando DELETE VOLUME para un volumen de una agrupación de almacenamiento configurada para la eliminación de datos duplicados, el servidor destruirá los objetos que hacen referencia a los datos de ese volumen.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento en la que está definido el volumen.

```
.-DISCARDdata-----No-----.
>>-DELEte Volume--nombre_volumen-----+-----+----->
'-DISCARDdata-----+No--+-'
'-Yes-'

.-Wait-----No-----.
>--+-----+-----><
'-Wait-----+No--+-'
'-Yes-'
```

## Parámetros

---

### nombre\_volumen (Necesario)

Especifica el nombre del volumen que se ha de suprimir.

### DISCARDdata

Especifica si se suprimen los archivos almacenados en el volumen. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

#### No

Especifica que no se suprimen los archivos almacenados en el volumen. Si el volumen contiene algún archivo, el volumen no se suprime.

#### Yes

Especifica que se suprimirán todos los archivos almacenados en el volumen. El servidor no necesita montar el volumen para este tipo de supresión.

Recuerde:

1. El servidor no suprime las copias archivadas que están en espera de supresión.
2. Si la protección de retención de archivado está activada, el servidor sólo suprime las copias archivadas cuyo período de retención ha caducado.

Si el volumen que se suprime es un volumen de agrupación de almacenamiento primaria, el servidor comprueba si alguna de las agrupaciones de almacenamiento de copia tiene copias de los archivos que se suprimen. Al suprimir los archivos almacenados en un volumen de agrupación de almacenamiento primaria, también se suprimen todas las copias que hay de esos archivos en las agrupaciones de almacenamiento de copia.

Al suprimir un volumen de disco de una agrupación de almacenamiento primaria, el comando también suprime todos los archivos que son copias en caché (copias de los archivos que se han migrado a la siguiente agrupación de almacenamiento). Al suprimir en caché de los archivos no se suprimen los archivos que ya se han migrado o de los que se ha hecho una copia de seguridad en las agrupaciones de almacenamiento de copia. Solamente estarán afectadas las copias en caché de los archivos.

Si el volumen que se suprime es un volumen de agrupación de almacenamiento de copia, sólo se suprimen los archivos en el volumen de agrupación de copia. Los archivos de la agrupación de almacenamiento primaria no se verán afectados.

No utilice el comando DELETE VOLUME con DISCARDATA=YES si está ejecutándose un proceso de restauración (RESTORE STGPPOOL o RESTORE VOLUME). El comando DELETE VOLUME podría dar lugar a que la restauración no se completara.

Si cancela la operación DELETE VOLUME durante el proceso o si se produce un error del sistema, pueden que hayan quedado varios archivos en el volumen. Puede volver a suprimir el mismo volumen para que el servidor suprima los archivos que quedan y después el volumen.

### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro sólo afecta al proceso si también se ha solicitado que se descarten todos los datos del volumen. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

#### No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

#### Yes



Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Recuerde: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: suprimir un volumen de agrupación de almacenamiento

Suprimir el volumen de agrupación de almacenamiento stgvol.1 de la agrupación de almacenamiento FILEPOOL.

```
delete volume stgvol.1
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DELETE VOLUME

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

## Comandos DISABLE

Utilice los comandos DISABLE para que el servidor no pueda realizar determinados tipos de operaciones.

- DISABLE EVENTS (Desactivar eventos para anotación de eventos)
- DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)
- DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)

## DISABLE EVENTS (Desactivar eventos para anotación de eventos)

Utilice este comando para desactivar el proceso de uno o varios eventos. Si especifica un receptor no admitido en ninguna plataforma o especifica un evento o nombre no válido, IBM Spectrum Protect emitirá un mensaje de error. Sin embargo, los receptores, eventos o nombres válidos que haya especificado seguirán habilitados.

Consejo: Los mensajes de la categoría SEVERE y el mensaje ANR9999D pueden proporcionar una valiosa información de diagnóstico si existen problemas graves en el servidor. Por este motivo, no debe desactivar estos mensajes.

Restricción:

- Determinados mensajes se visualizan en la consola incluso si están desactivados. Entre estos se encuentran algunos mensajes emitidos durante el proceso de arranque y conclusión del servidor y las respuestas a comandos de administración.
- Los mensajes de servidor que se hayan originado en el servidor donde se ha emitido este mandato no se pueden desactivar para las anotaciones de actividades.

ANR1822I indica que las anotaciones de eventos se están finalizando para el receptor especificado. Cuando se emite el comando DISABLE EVENTS este mensaje se anota en el receptor, aunque sea uno de los eventos que se han desactivado. Esto se hace para confirmar que las anotaciones de eventos han finalizado en ese receptor, pero los mensajes ANR1822I siguientes no se anotan en dicho receptor.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
.-,------.
v          |
>>-DISable EVents---+receivers-----+----->
                    +-ALL-----+
                    +-CONSOLE-----+
                    +-ACTLOG-----+
                    +-EVENTSERVER----+
                    +-FILE-----+
                    +-FILETEXT-----+
                    |               |
                    |      (1)     |
                    +-NTEVENTLOG-----+
                    |               |
                    |      (2)     |
                    +-SYSLOG-----+
                    +-TIVOLI-----+
                    '-USEREXIT-----'
```

```
.-,------.
v          |
>---+nombre_evento+----->
    +-ALL-----+
    +-INFO-----+
    +-WARNING-----+
    +-ERROR-----+
    '-SEVERE-----'
```

```
>+-----><
|                                     |
|                                     |
|          .-,------.              |
|          v          |              |
+-NODEname-----+nombre_nodo+-----+
|                                     |
|          .-,------.              |
|          v          |              |
'-SERVername-----+nombre_servidor+--'
```

Notas:

1. NTEVENTLOG sólo está disponible en Windows.
2. SYSLOG sólo está disponible en Linux.

## Parámetros

receptores (Obligatorio)

Especifica el nombre de los receptores cuyos eventos se desactivan. Especifique varios receptores separándolos con comas sin espacios intercalados. Los valores posibles son:

ALL

Todos los receptores, excepto los eventos del servidor en el receptor de anotaciones de actividades (ACTLOG). Para el receptor de anotaciones de actividades únicamente se pueden desactivar los eventos de clientes.

CONSOLE

La consola estándar del servidor como receptor.

ACTLOG

Las anotaciones de actividades como receptor. Sólo puede desactivar los eventos de cliente, no los eventos de servidor, para las anotaciones de actividades.

EVENTSERVER

El servidor de eventos como receptor.

FILE

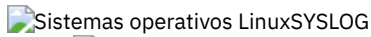
Un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo. Los registros no pueden ser leídos fácilmente por cualquier persona.

FILETEXT

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

NTEVENTLOG

Las anotaciones de aplicaciones de Windows como receptor.



Sistemas operativos LinuxEscribe mensajes directamente al registro del sistema en Linux.

**TIVOLI**

Tivoli Enterprise Console (TEC) como receptor.

**USEREXIT**

Un programa escrito por el usuario como receptor. El servidor escribe información en el programa.

**sucesos (Obligatorio)**

Especifica los eventos que se desactivan. Puede especificar varios eventos separándolos con comas sin espacios intercalados. Los valores posibles son:

**ALL**

Todos los eventos.

**nombre\_evento**

Un número de mensaje de cuatro dígitos que tiene antepuesto ANR para un evento del servidor o ANE para un evento del cliente. Los rangos válidos son de ANR0001 a ANR9999 y de ANE4000 a ANE4999. Especifique el parámetro NODENAMES si los eventos del cliente se van a desactivar para los nodos coincidentes. Especifique el parámetro SERVERNAME si los eventos del servidor se van a desactivar para los servidores coincidentes.

Sólo para el receptor de eventos de TIVOLI, puede especificar los siguientes nombres de eventos para los clientes de la aplicación IBM Spectrum Protect:

cliente de aplicaciones de IBM Spectrum Protect	Prefijo	Rango
Data Protection para Microsoft Exchange Server	ACN	3500–3649
Data Protection para Lotus Domino	ACD	5200–5299
Data Protection para Oracle	ANS	500–599
Data Protection para Informix	ANS	600–699
Data Protection para Microsoft SQL Server	ACO	3000–3999

Recuerde: Si se especifica ALL se desactivan estos mensajes. Sin embargo, las opciones INFO, WARNING, ERROR y SEVERE no tienen ningún efecto sobre los mensajes.

**categorías de gravedad**

Si la lista de eventos contiene una categoría de gravedad, todos los eventos de dicha gravedad se desactivarán para los nodos especificados. Los tipos de mensajes son:

**INFO**

Mensajes informativos (de tipo I).

**WARNING**

Mensajes de aviso (de tipo W).

**ERROR**

Mensajes de error (de tipo E).

**SEVERE**

Mensajes de error grave (de tipo S).

**NODENAME**

Especifica el nombre de uno o varios nodos cuyos eventos se desactivan. Puede utilizar el carácter comodín (\*) para especificar todos los nodos. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, los eventos se desactivan para el servidor donde se ejecuta este comando.

**SERVername**

Especifica el nombre de uno o varios servidores cuyos eventos se desactivan. Puede utilizar el carácter comodín (\*) para especificar todos los servidores excepto el servidor donde se ejecuta este comando. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, los eventos se desactivan para el servidor donde se ejecuta este comando.

## Ejemplo: desactivar categorías específicas de eventos

Desactivar todos los eventos de clientes de las categorías INFO y WARNING para las anotaciones de actividad y receptores de consola para todos los nodos.

```
disable events actlog,console
info,warning nodename=*
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con DISABLE EVENTS

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## DISABLE REPLICATION (Impedir el proceso de réplica de salida en un servidor)

Utilice este comando para impedir que un servidor de réplica de origen inicie nuevos procesos de réplica.

El uso de este comando no detiene la ejecución de procesos de réplica. La ejecución de procesos de réplica continuará hasta que se completen o hasta que finalicen sin completarse. Utilice este comando y el comando ENABLE REPLICATION para controlar el proceso de réplica.

Emita este comando en el servidor que actúe como origen para los datos replicados.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-DISAbLe REPLiCation-----<<
```

### Parámetros

Ninguno.

### Ejemplo: desactivar el proceso de réplica

Desactive el proceso de réplica en un servidor de réplica de origen.

```
disable replication
```

### Comandos relacionados

Tabla 1. Comandos relacionados con DISABLE REPLICATION

Comando	Descripción
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

# DISABLE SESSIONS (Impedir que nuevas sesiones accedan a IBM Spectrum Protect)

Utilice este mandato para impedir el acceso de nuevas sesiones a IBM Spectrum Protect. Las sesiones activas se completarán. Para un determinado servidor, puede especificar si se desactivan las sesiones de entrada, las sesiones de salida o ambas.

Los procesos del servidor como, por ejemplo, operaciones de migración y reclamación, no resultan afectadas cuando se emite el comando DISABLE SESSIONS.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

## Sintaxis

```
>>-DISAbLe SESSions----->
. -CLient-----
>--+-----><
'|++-CLient-----|'
'|++-ALL-----|'
'|++-ADMin-----|'
'|--SERVer-----|'
'|          | .-DIRectioN---Both----- |'
'| -nombre_servidor--+-----+-'
'|          | ++-DIRectioN---Both-----+-'
'|          | ++-DIRectioN---INbound--+-'
'|          | --DIRectioN---OUTbound---'
```

## Parámetros

Especifica el tipo de sesión que se desactiva. Este parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

### CLient

Inhabilita sólo las sesiones de cliente de copia de seguridad y archivado.

### ALL

Inhabilita todos los tipos de sesión.

### ADMin

Inhabilita sólo las sesiones administrativas.

### SERVer

Inhabilita sólo las sesiones de servidor a servidor. Sólo se desactivan los siguientes tipos de sesiones:

- Anotación de eventos de servidor a servidor
- Gestión empresarial
- Inscripción servidor
- Fuera de la LAN: almacenamiento agente - servidor
- Volúmenes virtuales
- Réplica de nodo

También puede especificar si se desactivan las sesiones de entrada, las sesiones de salida o ambas para un determinado servidor.

### nombre\_servidor

Especifica el nombre del servidor cuyas sesiones desea desactivar. Este parámetro es opcional. Si no especifica este parámetro, no se inician nuevas sesiones con otros servidores. Las sesiones en ejecución no se cancelan.

### DIRectioN

Especifica si se desactivan las sesiones de entrada, las sesiones de salida o ambas. Este parámetro es opcional. El valor predeterminado es BOTH. Son posibles los siguientes valores:

#### Both

Especifica que se desactivan las sesiones de entrada desde el servidor especificado y las sesiones de salida hacia el servidor especificado.

#### INbound

Especifica que sólo se desactivan las sesiones de entrada desde el servidor especificado.  
OUTbound  
Especifica que sólo se desactivan las sesiones de salida hacia el servidor especificado.

## Ejemplo: impedir que se establezcan nuevas sesiones de copia de seguridad y archivado de nodo cliente en el servidor

Impedir temporalmente que nuevas sesiones de nodos clientes accedan al servidor.

```
disable sessions
```

## Ejemplo: impedir que puedan establecerse nuevas sesiones en el servidor

Impedir temporalmente que nuevas sesiones accedan al servidor.

```
disable sessions all
```

## Ejemplo: desactivar las sesiones de salida hacia un servidor

Desactive las sesiones de salida hacia un servidor denominado REPLSRV.

```
disable sessions server replsrv direction=outbound
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DISABLE SESSIONS

Comando	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## Comandos DISMOUNT

Utilice el comando DISMOUNT para desmontar un volumen mediante la dirección de dispositivo real o mediante el nombre de volumen.

- DISMOUNT VOLUME (Desmontar un volumen por nombre de volumen)

## DISPLAY OBJNAME (Mostrar un nombre de objeto completo)

Utilice este comando para IBM Spectrum Protect que se visualice un nombre de objeto completo si el nombre que figura en un mensaje o en la salida de una consulta está abreviado por razones de limitación de longitud. Los nombres de objeto que son muy largos pueden ser difíciles de mostrar y usar en funciones normales del sistema operativo. El servidor IBM Spectrum Protect abreviará nombres largos y les asignará un ID de señal que puede utilizarse si el nombre de la ruta del objeto sobrepasa los 1024 bytes. El ID de señal se muestra en una cadena que incluye identificadores para el nodo, el espacio de archivos y el nombre del objeto. El formato es: [TSMOBJ:nID.fsID.objID]. Cuando se especifica con el comando DISPLAY OBJNAME, el ID de señal puede utilizarse para que se muestre el nombre completo del objeto.

## Clase de privilegio

Cualquier administrador puede emitir este comando

## Sintaxis

```
>>-DISplay OBJname--ID_ señal-----<<
```

## Parámetros

ID\_señal (Necesario)

Especifica el ID que se indica en la etiqueta [TSMOBJ:], cuando el nombre de un objeto es demasiado largo para mostrarlo.

## Ejemplo: visualizar el nombre de objeto completo de un ID de señal en un mensaje

Supongamos que se recibe el mensaje siguiente:

```
ANR9999D file.c(1999) Error al manejar archivo [TSMOBJ:1.1.649498]
debido a la falta de recursos de servidor.
```

Para mostrar el nombre de objeto completo del archivo al que se hace referencia en el mensaje de error, especifique el ID de señal en el comando DISPLAY OBJNAME.

```
display obj 1.1.649498
```

## Comandos relacionados

Tabla 1. Comandos relacionados con DISPLAY OBJNAME

Comando	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.

## Comandos ENABLE

Utilice el comando ENABLE para que el servidor pueda realizar algunos tipos de operaciones.

- ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)
- ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)
- ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)

## ENABLE EVENTS (Activar eventos del servidor o del cliente para anotaciones)

Utilice este mandato para activar el proceso de uno o varios eventos. Si especifica un receptor no admitido en ninguna plataforma o especifica un evento o nombre no válido, IBM Spectrum Protect emitirá un mensaje de error. Sin embargo, los receptores, eventos o nombres válidos que haya especificado seguirán habilitados.

Restricción: Algunos eventos, como algunos mensajes emitidos durante el arranque o la conclusión del servidor, van directamente a la consola. No van a otros receptores aunque estén activados.

Los comandos de administración se devuelven al emisor del comando y sólo se registran como sucesos numerados. Estos sucesos numerados no se registran en la consola del sistema, pero sí en los demás receptores, incluidas las sesiones de línea de comandos de administración que se ejecutan en modalidad de consola.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

      .-|-----|
      v
>>-ENable--EEvents---+--ALL-----+----->
      +-CONSOLE-----+
      +-ACTLOG-----+
      +-EVENTSERVER----+
      +-FILE-----+
      +-FILETEXT-----+
      |                (1) |
      +-NTEVENTLOG-----+
      |                (2) |
```

```

+-SYSLOG-----+
+-TIVOLI-----+
'-USEREXIT-----'

.-,-----
V      |
>---+-nombre_evento+----->
+-ALL-----+
+-INFO-----+
+-WARNING-----+
+-ERROR-----+
'-SEVERE-----'

>---+-----<
|               .-,-----|
|               V      |
+-NODEname-----nombre_nodo+-----+
|               .-,-----|
|               V      |
'-SERVERname-----nombre_servidor+--'

```

#### Notas:

1. NTEVENTLOG sólo está disponible en Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

## Parámetros

### receptores (Obligatorio)

Especifica uno o varios receptores para los que se anotan los eventos activados. Puede especificar varios receptores separándolos con comas sin espacios intercalados. Los valores válidos son:

#### ALL

Todos los receptores.

#### CONSOLE

La consola estándar del servidor como receptor.

#### ACTLOG

Las anotaciones de actividades del servidor como receptor.

#### EVENTSERVER

El servidor de eventos como receptor.


#### FILE

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo. Los registros no pueden ser leídos fácilmente por cualquier persona.


#### FILETEXT

Un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

#### Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsLas anotaciones de aplicaciones de Windows como receptor.

#### Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

#### TIVOLI

Tivoli Enterprise Console (TEC) como receptor.

#### USEREXIT

Un programa escrito por el usuario como receptor. El servidor escribe información en el programa.

### sucesos (Obligatorio)

Especifica el tipo de eventos que se activan. Puede especificar varios eventos separándolos con comas sin espacios intercalados. Los valores posibles son:

#### ALL

Todos los eventos.

#### nombre\_evento

Un número de mensaje de cuatro dígitos que tiene antepuesto **ANR** para un evento del servidor o **ANE** para un evento del cliente. Los rangos válidos son de ANR0001 a ANR9999 y de ANE4000 a ANE4999. Especifique el parámetro NODENAME si los eventos del cliente se van a activar para nodos coincidentes. Especifique el parámetro SERVERNAME si los eventos del servidor se van a activar para los servidores coincidentes.

Para el receptor de eventos de TIVOLI, puede especificar los siguientes rangos adicionales para los clientes de la aplicación IBM Spectrum Protect:



cliente de aplicaciones de IBM Spectrum Protect	Prefijo	Rango
Data Protection para Microsoft Exchange Server	ACN	3500–3649
Data Protection para Lotus Domino	ACD	5200–5299
Data Protection para Oracle	ANS	500–599
Data Protection para Informix	ANS	600–699
Data Protection para Microsoft SQL Server	ACO	3000–3999

Restricción: El cliente de aplicación debe tener activado el soporte para Tivoli Event Console ampliado con el fin de poder direccionar estos mensajes a Tivoli Event Console.

Consejo:

- Si se especifica la opción ALL se activan estos mensajes. Sin embargo, las opciones INFO, WARNING, ERROR y SEVERE no tienen ningún efecto sobre los mensajes.
- Debido al número de mensajes, no se deben activar todos los mensajes de un nodo para que se anoten en Tivoli Event Console.

categorías de gravedad

Si la lista de eventos contiene una categoría de gravedad, todos los eventos de dicha gravedad se activarán para los nodos especificados. Los tipos de mensajes son:

INFO

Se activan los mensajes informativos (de tipo I).

WARNING

Se activan los mensajes de aviso (de tipo W).

ERROR

Se activan los mensajes de error (de tipo E).

SEVERE

Se activan los mensajes de error grave (de tipo S).

NODENAME

Especifica uno o varios nodos cliente para los que se activan los eventos. Puede utilizar un carácter comodín para especificar todos los nodos cliente. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, los eventos se activan para el servidor donde se ejecuta este comando.

SERVername

Especifica uno o varios servidores para los que se activan los eventos. Puede utilizar un carácter comodín para especificar todos los servidores excepto el servidor donde se ejecuta este comando. Puede especificar SERVERNAME o NODENAME. Si no se especifica ninguno de los parámetros, los eventos se activan para el servidor donde se ejecuta este comando.

## Ejemplo: activar categorías específicas de eventos

Activar todos los eventos del cliente ERROR y SEVERE para el receptor USEREXIT y el nodo BONZO.

```
enable events userexit error,severe nodename=bonzo
```

## Comandos relacionados

Tabla 1. Comandos relacionados con ENABLE EVENTS

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## ENABLE REPLICATION (Permitir el proceso de réplica de salida en un servidor)

Utilice este comando para permitir que un servidor de réplica de origen inicie el proceso de réplica normal después de una restauración de base de datos. También puede utilizar este comando para reanudar el proceso de réplica después de emitir el comando DISABLE REPLICATION.

Atención: Antes de activar la réplica después de una restauración de base de datos, determine si las copias de los datos que hay en el servidor de destino son necesarias. Si lo son, debe sincronizar los datos del nodo de cliente replicando los datos del servidor de réplica de destino en el servidor de réplica de origen. El proceso de réplica sustituye los datos en el servidor de origen que se han perdido debido a la restauración de base de datos.

Emita este comando en el servidor que actúe como origen para los datos replicados.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-ENable REPLication-----<<
```

### Parámetros

Ninguno.

### Ejemplo: permitir el proceso de réplica

Permita el proceso de réplica en un servidor de réplica de origen.

```
enable replication
```

### Comandos relacionados

Tabla 1. Comandos relacionados con ENABLE REPLICATION

Comando	Descripción
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

## ENABLE SESSIONS (Reanudar la actividad del usuario en el servidor)

Utilice este mandato después de emitir el mandato DISABLE SESSIONS para iniciar nuevas sesiones que puedan acceder a un servidor. Para un determinado servidor, puede especificar si se activan las sesiones de entrada, las sesiones de salida o ambas.

El proceso de este comando no afecta a los procesos del sistema como por ejemplo, migración y reclamación.

Utilice el comando QUERY STATUS para visualizar la disponibilidad del servidor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

## Sintaxis

---

```
>>-ENable SESSions----->
. -CLient-----
>--+-----+><
'|++-CLient-----+'
'|++-ALL-----+'
'|++-ADMin-----+'
'| -SERVer-----+'
'|
'| nombre_servidor .-DIRection---Both-----.'
'|
'|++-DIRection---Both-----+'
'|++-DIRection---INbound---+'
'| -DIRection---OUTbound-'
```

## Parámetros

---

Especifica el tipo de sesión que se activa. Este parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

### CLient

Habilita sólo las sesiones de cliente de copia de seguridad y archivado.

### ALL

Habilita todos los tipos de sesión.

### ADMin

Habilita sólo las sesiones administrativas.

### SERVer

Habilita sólo las sesiones de servidor a servidor. También puede especificar si se activan las sesiones de entrada, las sesiones de salida o ambas para un determinado servidor.

### nombre\_servidor

Especifica el nombre de un determinado servidor cuyas sesiones desea activar. Este parámetro es opcional. Si no especifica este parámetro, se activan nuevas sesiones con los demás servidores.

### DIRection

Especifica si se activan las sesiones de entrada, las sesiones de salida o ambas. Este parámetro es opcional. El valor predeterminado es BOTH. Son posibles los siguientes valores:

#### Both

Especifica que se activan las sesiones de entrada desde el servidor especificado y las sesiones de salida hacia el servidor especificado.

#### INbound

Especifica que sólo se activan las sesiones de entrada hacia el servidor especificado.

#### OUTbound

Especifica que sólo se activan las sesiones de salida desde el servidor especificado.

## Ejemplo: reanudar la actividad del nodo cliente en el servidor

---

Reanudar la operación normal, permite a los nodos clientes acceder al servidor.

```
enable sessions
```

## Ejemplo: reanudar todas las actividades en el servidor

---

Reanudar la operación normal, permite a todas las sesiones acceder al servidor.

```
enable sessions all
```

## Ejemplo: activar las sesiones de salida hacia un servidor

---

Active las sesiones de salida hacia un servidor denominado REPLSRV.

```
enable sessions server replsrv direction=outbound
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con ENABLE SESSIONS

Comando	Descripción
ACCEPT DATE	Acepta la fecha actual en el servidor.
CANCEL SESSION	Cancela las sesiones activas con el servidor.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## ENCRYPT STGPOOL (Cifrar datos en una agrupación de almacenamiento)

Utilice este mandato para cifrar datos en una agrupación de almacenamiento de contenedores de directorio o de contenedores de nube.

### Clase de privilegio

Cualquier administrador puede emitir este mandato.

### Sintaxis

```
>>-ENCRypt STGpool--nombre_agrupación----->
      .-MAXPRocess---4----- .-Preview ---No-----
>--+-----+-----+-----+----->
      '-MAXPRocess---número-' '-Preview---+Yes+-'
                                   '-No--'

      .-Wait---No-----
>--+-----+-----+-----+-----<<
      '-Wait---+No--+-'
                                   '-Yes-'
```

### Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que contiene los datos que se deben cifrar.

Restricciones:

- Solo puede especificar agrupaciones de almacenamiento de contenedores de directorio o agrupaciones de almacenamiento de contenedores de nube.
- Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el mandato falla.

MAXPRocess

Especifica el número máximo de procesos paralelos que pueden tener lugar cuando la agrupación de almacenamiento está cifrando datos. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

Preview

Especifica si se mostrará una vista previa de todos los mandatos que se procesan como parte del mandato ENCRYPT STGPOOL. Este parámetro es opcional. Son posibles los siguientes valores:

No

Especifica que no se mostrará una vista previa de los mandatos. Este es el valor predeterminado.

Yes

Especifica que se mostrará una vista previa de los mandatos.

Wait

Especifica si el cifrado de la agrupación de almacenamiento se producirá en primer plano o en segundo plano. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras se está procesando el mandato. Los mensajes relacionados con el proceso en segundo plano se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Éste es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe finalizar para poder continuar con otras tareas. Los mensajes se muestran en el archivo de registro de actividades o la consola de servidor, o en ambos, en función de la ubicación en la que se registren los mensajes.

Restricción: No puede especificar el parámetro WAIT=YES desde la consola de servidor.

## Ejemplo: cifrar datos en una agrupación de almacenamiento

Cifrar datos en una agrupación de almacenamiento que se denomina POOL1 y especificar un número máximo de 30 procesos paralelos.

```
encrypt stgpool pool1 maxprocess=30
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con ENCRYPT STGPOOL

Comando	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.

## END EVENTLOGGING (Detener eventos de anotaciones)

Utilice este mandato para dejar de anotar los eventos en un receptor activo.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

```
>>-END--EVEntlogging-+-----+-----><
| .-,-----+-----+-----|
| V          |         |         |
'---+--CONSOLE-----+---+'
    +-ACTLOG-----+
    +-EVENTSERVER----+
    +-FILE-----+
    +-FILETEXT-----+
    |               |
    |               | (1) |
    +-NTEVENTLOG----+
    |               | (2) |
    +-SYSLOG-----+
    +-TIVOLI-----+
    '-USEREXIT-----'
```

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

## Parámetros

Especifica un tipo de receptor. Puede especificar varios receptores separándolos con comas sin espacios intercalados. Este parámetro es opcional. El valor predeterminado es ALL. Si especifica ALL o no especifica ningún receptor, se finaliza la anotación para todos los receptores.

ALL

Especifica todos los receptores.

## CONSOLE

Especifica la consola del servidor como receptor.

## ACTLOG

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor. La anotación se puede detener únicamente para eventos del cliente.

## EVENTSERVER

Especifica el servidor de eventos como receptor.


## FILE


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


## FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

## TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

## USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

## Ejemplo: detener las anotaciones de eventos

Finalizar la anotación de eventos en la salida de usuario.

```
end eventlogging userexit
```

## Comandos relacionados

Tabla 1. Comandos relacionados con END EVENTLOGGING

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## EXPIRE INVENTORY (Arrancar manualmente el proceso de caducidad de inventario)

Utilice este comando para iniciar manualmente el proceso de caducidad de inventario. El proceso de caducidad de inventario elimina las copias de los archivos de archivado y de copia de seguridad de cliente del almacenamiento del servidor. La eliminación se basa en las especificaciones de política de los grupos de copia de archivado y de copia de seguridad y archivo de las clases de gestión a las que están vinculados los archivos.

Si tiene la función de gestor de recuperación ante siniestro para el servidor de IBM Spectrum Protect, el proceso de caducidad de inventario también elimina los volúmenes virtuales elegibles que se utilizan para los procesos siguientes:

- Copias de seguridad de base de datos del tipo BACKUPFULL, BACKUPINCR y DBSNAPSHOT. El comando SET DRMDBBACKUPEXPIREDAYS controla cuándo podrán seleccionarse estos volúmenes para su caducidad.
- Archivos del plan de recuperación del tipo RPFILe y RPFNSAPSHOT. El comando SET DRMRPFEXPIREDAYS controla cuándo podrán seleccionarse estos volúmenes para su caducidad.

El proceso de caducidad de inventario que se ejecuta durante la inicialización del servidor no elimina estos volúmenes virtuales.

Tan solo se permite un proceso de caducidad a la vez, pero este proceso se puede distribuir entre un máximo de 40 hebras. Si hay un proceso de caducidad en ejecución, no puede iniciar otro proceso.

Puede configurar el proceso de caducidad automático con la opción de servidor EXPINTERVAL. Si establece la opción EXPINTERVAL en 0, el servidor no ejecutará automáticamente el proceso de caducidad y deberá emitir el mandato EXPIRE INVENTORY para iniciar el proceso.

Este comando crea un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Si se aplica este mandato a un volumen WORM, el volumen vuelve a ser un volumen cero si hay espacio restante en el que se pueden escribir los datos. Los os datos de los volúmenes WORM, incluidos los datos suprimidos y caducados, no se pueden sobrescribir. Por lo tanto, sólo se pueden escribir datos en el espacio que no contiene datos caducados, suprimidos o actuales. Si un volumen WORM no tiene espacio disponible para grabar los datos, seguirá siendo privado. Para eliminar el volumen de la biblioteca, debe utilizar el comando CHECKOUT LIBVOLUME.

Ejecute el mandato EXPIRE INVENTORY para suprimir archivos del almacenamiento del servidor si no se ha suprimido cuando utilizó las operaciones de supresión del cliente.

Si desea más información sobre las operaciones de supresión de cliente, consulte Mandatos y opciones de cliente de archivado y copia de seguridad.

## Clase de privilegio

Para emitir este mandato, debe tener privilegios de sistema.

## Sintaxis

```

      .-Quiet---No-----.
>>-EXPIre Inventory-----+----->
      '-Quiet---+No---+'
              '-Yes-'

      .-Wait---No----- .-Nodes---*-----.
>--+-----+-----+----->
      '-Wait---+No---+' '-Nodes---+nombre_nodo---+'
              '-Yes-'              '-nombre_grupo_nodos-'

>--+-----+-----+----->
      '-EXCLUDENodes---nombre_nodo_excluido-'

      .-Type---All-----.
>--+-----+-----+----->
      '-Domain---domain_name-' '-Type---+All---+'
                                  +-Archive-+
                                  +-Backup--+
                                  '-Other---'

      .-REsource---4----- .-SKipdirs---No-----.
>--+-----+-----+----->
      '-REsource---numero-' '-SKipdirs---+No---+'
                                  '-Yes-'

>--+-----+-----+-----><
      '-DUration---minutos-'
```

## Parámetros

### Quiet

Especifica si el servidor ha de suprimir los mensajes detallados relativos a cambios de políticas durante el proceso de caducidad. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

#### No

Especifica que el servidor envía mensajes informativos detallados.

#### Yes

Especifica que el servidor sólo envía mensajes resumidos. El servidor emite mensajes acerca de los cambios de política únicamente cuando se suprimen los archivos y cuando se utilizó la clase de gestión predeterminada o el periodo de gracia de retención para el dominio para caducar los archivos.

También puede especificar la opción EXPQUIET del archivo de opciones del servidor para determinar automáticamente si el proceso de caducidad se ejecuta con mensajes resumidos.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

##### No

Especifica que el servidor procesa este comando en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

##### Yes

Especifica que el servidor procesa este comando en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### SKIPDIRS

Especifica si el servidor omite los objetos tipo directorio durante el proceso de caducidad. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

##### No

Especifica que el servidor caduca los archivos y directorios según los criterios de la política correspondiente.

##### Yes

Especifica que el servidor omite los objetos tipo directorio y los objetos de archivado durante el proceso de caducidad, aunque los directorios se puedan seleccionar para la caducidad. Si especifica YES, impedirá que se supriman los directorios y el proceso de caducidad puede llevarse a cabo con más rapidez.

Atención: No utilice esta opción todo el tiempo. Con IBM Spectrum Protect Versión 6.0 y posteriores, puede ejecutar varias hebras (recursos) para un proceso de caducidad. Asimismo, si especifica YES con frecuencia, el tamaño de la base de datos aumenta a medida que se acumulan los objetos de directorio y aumenta el período de tiempo utilizado para la caducidad. Ejecute SKIPDIRS=NO periódicamente para que caduquen los directorios y disminuya el tamaño de la base de datos.

#### Nodes

Especifica el nombre de los nodos cliente y de los grupos de nodos cuyos datos van a procesarse. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Este parámetro es opcional.

Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de comando NODES y DOMAIN, y que no coincidan con los criterios para las opciones de comando EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

#### EXCLUDENodes

Especifica el nombre de los nodos de cliente y de los grupos de nodos cuyos datos no van a procesarse. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener dichos caracteres. Este parámetro es opcional.

Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de comando NODES y DOMAIN, y que no coincidan con los criterios para las opciones de comando EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

#### Domain

Especifica que solo van a procesarse los datos para los nodos de cliente asignados al dominio especificado. Este parámetro es opcional. Puede especificar NODES, EXCLUDENODES, DOMAIN, o cualquier combinación de estos. Si especifica más de uno de estos parámetros, sólo se procesarán los nodos que coincidan con los criterios para las dos opciones de comando NODES y DOMAIN, y que no coincidan con los criterios para las opciones de comando EXCLUDENODES. Si no especifica EXCLUDENODES, EXCLUDENODES ni DOMAIN con un valor, se procesan los datos para todos los nodos.

#### Type

Especifica el tipo de datos que se van a procesar. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:



ALL

Procesa todos los tipos de datos que pueden elegirse para la caducidad.

Archive

Procesa solo los datos de archivado de cliente.

Backup

Procesa solo los datos de copia de seguridad de cliente.

Otro

Procesa solo los elementos para las funciones del gestor de recuperación ante siniestro, como los archivos del plan de recuperación y copias de seguridad de bases de datos obsoletas.

REsource

Especifica el número de hebras que se pueden ejecutar en paralelo. Especifique un valor en el rango de 1 a 40. Este parámetro es opcional. El valor predeterminado es cuatro.

La caducidad se ejecuta como un proceso único, aunque los recursos representan el trabajo en paralelo por parte del servidor dentro del proceso de caducidad único. Los datos de archivado de un nodo sólo se ejecutan en un único recurso, pero los datos de copia de seguridad se puede propagar entre recursos de un nivel de espacio de archivos. Por ejemplo, si especifica `NODE=X, Y, Z` cada uno con tres espacios de archivos y `RESOURCE=5`, el proceso de caducidad para los tres nodos de cliente X, Y y Z se ejecuta en paralelo. Al menos un recurso procesa cada nodo y, al menos, un nodo utiliza múltiples recursos para procesar datos de copia de seguridad entre los distintos espacios de archivo.

DUration

Especifica el número máximo de minutos que debe esperarse a que se ejecute el proceso de caducidad. El proceso se detiene cuando transcurre el número de minutos especificado o cuando se han suprimido todos los objetos caducados seleccionables, lo que ocurra primero. Especifique un valor en el rango de 1 a 2880. Este parámetro es opcional. Si este parámetro no se especifica, la duración del proceso de caducidad no queda limitado por la hora.

## Ejemplo: ejecutar el proceso de caducidad de inventario para un período de tiempo específico

Ejecutar el proceso de caducidad en un plazo de dos horas.

```
expire inventory duration=120
```

## Ejemplo: ejecutar el proceso de caducidad de inventario para los datos de copia de seguridad para dos nodos cliente

Ejecutar el proceso de caducidad de inventario para los datos de copia de seguridad para dos nodos cliente, CHARLIE y ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory nodes=charlie,robbie resource=2 type=backup
```

## Ejemplo: ejecutar el proceso de caducidad de inventario para todos los nodos de cliente excepto dos nodos

Ejecute el proceso de caducidad de inventario para todos los nodos de cliente, excepto dos nodos, CHARLIE y ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory excludenodes=charlie,robbie
```

## Ejemplo: ejecutar el proceso de caducidad de inventario para todos los nodos de cliente en un dominio, excepto un nodo

Ejecute el proceso de caducidad de inventario para todos los nodos de cliente en un dominio, excepto un nodo, ROBBIE. Permita que el servidor ejecute el proceso de caducidad hasta que se complete.

```
expire inventory domain=standard excludenodes=robbie
```

## Comandos relacionados

Tabla 1. Comandos relacionados con EXPIRE INVENTORY

Comando	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
CANCEL EXPIRATION	Cancela el proceso de caducidad de inventario.

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## Comandos EXPORT

Utilice el mandato EXPORT para copiar información de un servidor de IBM Spectrum Protect en un medio extraíble secuencial.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

- EXPORT ADMIN (Exportar información del administrador)
- EXPORT NODE (Exportar información de nodos cliente)
- EXPORT POLICY (Exportar información de políticas)
- EXPORT SERVER (Exportar información del servidor)

## EXPORT ADMIN (Exportar información del administrador)

Utilice este comando para exportar definiciones de administrador y de autorización desde un servidor. Se puede exportar la información a medios secuenciales para después importarla a otro servidor, o bien se puede exportar la información directamente a otro servidor para su importación inmediata.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

IBM Spectrum Protect exporta información de administrador como, por ejemplo:

- El nombre, la contraseña y la información de contacto del administrador
- Clases de privilegios de administración que se otorgan al administrador
- Si el ID de administrador tiene bloqueado el acceso del servidor

Puede utilizar el comando QUERY ACTLOG para ver el estado de la operación de exportación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si exporta información a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema,














nombre\_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el comando emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

## Ejemplo: exportar definiciones de administrador a volúmenes de cinta

Desde el servidor, exportar la información de todos los administradores definidos a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Se informa sobre el número y tipo de los objetos a la consola del sistema y a las anotaciones de actividades. Emita el comando:

```
export admin devclass=menu1  
volumenames=tape01,tape02,tape03
```

## Ejemplo: exportar definiciones de administrador a volúmenes de cinta listados en un archivo

Desde el servidor, exporte la información para todos los administradores definidos en los volúmenes de cintas que figuran en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA

Este archivo contiene las líneas siguientes:

```
TAPE01  
TAPE02  
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export admin devclass=menu1 volumenames=file:tapevol
```

```
export admin devclass=menu1 volumenames=file:tapevol.data
```

Se informa sobre el número y tipo de los objetos a la consola del sistema y a las anotaciones de actividades.

## EXPORT ADMIN (Exportar información del administrador directamente a otro servidor)

---

Utilice este comando para exportar definiciones de administrador y de autorización directamente a otro servidor de la red. Así se genera una importación inmediata en el servidor de destino.

Puede emitir el comando QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

### Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema.

### Sintaxis

---

```
>>-EXPort Admin-+-----+----->
      | .-,-----+-----|
      | V          | |
      +---nombre_admin-+-'

>+-----+----->
  '-TOserver---nombre_servidor-'

.-PREVIEWImport---No-----.-Replacedefs---No-----.
>+-----+-----+-----+----->
  '-PREVIEWImport---+No--+-' '-Replacedefs---+No--+-'
      '-Yes-'                  '-Yes-'

.-ENCryptionstrength---AES-----.
>+-----+-----+-----+-----><
  '-ENCryptionstrength---+AES-+-'
      '-DES-'
```

### Parámetros

---

#### nombre\_admin

Especifica los administradores para los que se va a exportar la información. Este parámetro es opcional. El valor predeterminado son todos los administradores.

Debe separar los elementos de la lista con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

#### TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el comando DEFINE SERVER. El administrador que emita el comando de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

#### PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

## Ejemplo: exportar las definiciones del administrador a un servidor de destino

---

Exportar todas las definiciones de administrador al servidor destino definido como OTHERSERVER. Previsualizar las operaciones de importación en el servidor destino. Emita el mandato:

```
export admin * toserver=otherserver previewimport=yes
```

Desde el servidor de destino, OTHERSERVER, puede visualizar las operaciones de importación si emite el comando:

```
proceso de consulta
```

## EXPORT NODE (Exportar información de nodos cliente)

---

Utilice este comando para exportar definiciones de nodos cliente o datos de archivos a medios secuenciales o directamente a otro servidor para su importación inmediata.

Importante: Para los mandatos que exportan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato EXPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

La siguiente información se incluye en cada definición de nodo cliente:

- El ID de usuario, la contraseña y la información de contacto.
- El nombre del dominio de políticas asignado del cliente.
- El estado de compresión de archivos.
- Si el usuario tiene autorización para suprimir copias de seguridad o copias archivadas del almacenamiento del servidor.
- Si el ID de nodo cliente tiene bloqueado el acceso al servidor.

De forma opcional, también puede exportar los elementos siguientes:

- Definiciones de espacio de archivos.
- Copias de seguridad, copias archivadas y archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.
- Información de autorización de acceso que pertenece a los espacios de archivos exportados.
- Los datos de copia archivada cuyo estado es en espera de supresión (dicho estado se conservará). Cuando los datos de copia archivada se importan, permanecerán en espera de retención.

Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores a los que se exportan deben estar configurados para las contraseñas de LDAP. Los datos del nodo que se exportan desde un nodo que se autentica con un servidor de directorios LDAP no son accesible si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos exportados desde un nodo de LDAP todavía se pueden exportar. Pero el servidor de destino debe estar configurado para utilizar LDAP, para acceder a los datos.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.
- Los mandatos EXPORT NODE y EXPORT SERVER no exportan datos de una agrupación de fragmentación a menos que lo permita de forma explícita estableciendo el parámetro ALLOWSHREDDABLE en el valor YES. Si se especifica este valor y los datos exportados incluyen datos de agrupaciones de destrucción, esos datos no se podrán destruir. No se emite ningún aviso si la operación de exportación incluye datos de agrupaciones de fragmentación.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
  - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.
  - Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
  - Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESPPACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

El mandato EXPORT NODE genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si está exportando información de nodo a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Para visualizar información sobre cualquiera de las opciones de exportación de servidor a servidor suspendidas o en ejecución, emita el mandato QUERY EXPORT. El mandato QUERY EXPORT sólo visualiza información acerca de las exportaciones que se han suspendido o que pueden suspenderse. Las operaciones de exportación que pueden suspenderse, y reiniciarse posteriormente, son las exportaciones de servidor a servidor cuyo FILEDATA tiene un valor distinto de NONE. Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de exportación.

Dado que pueden producirse resultados imprevisibles, no ejecute procesos de caducidad, migración, copia de seguridad o archivado cuando emita el mandato EXPORT NODE.

Para un servidor que tenga clientes que admitan Unicode, puede conseguir que el servidor convierta el nombre de espacio de archivos que especifique, o bien utilizar uno de los parámetros siguientes:

- FSID



- UNIFILESPACE

El comando EXPORT NODE ofrece dos posibilidades: exportación directa a otro servidor de la red o bien exportación a un medio secuencial. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con EXPORT NODE

Comando	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

- EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)  
Se pueden exportar definiciones de nodo o datos de archivos de un servidor a un medio secuencial para después importarlas a otro servidor.
- EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)  
Utilice este comando para exportar definiciones de nodos cliente o datos de archivos directamente a otro servidor para su importación inmediata.

## EXPORT NODE (Exportar definiciones de nodo a medios secuenciales)

Se pueden exportar definiciones de nodo o datos de archivos de un servidor a un medio secuencial para después importarlas a otro servidor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

      .-*-----
>>-EXPort Node-----+----->
      | .-,------. |
      | v             | |
      |'---nombre_nodo-+-'

>+-----+----->
      | .-,------. |
      | v             | |
      |'-FILESpace-----nombre_espacio_archivos-+-'

>+-----+----->
      | .-,------. |
      | v             | |
      |'-FSID-----ID_espacio_archivos-+-'

```



nodo especificado, se realizará la búsqueda en todos los espacios de archivos del espacio de archivos, FSID, y en las listas habilitadas para Unicode.

Restricción: Si utiliza caracteres comodín para especificar nombres de nodo o patrones de nodo, el servidor no notifica los nombres o patrones de nodo que no coincidan con ninguna entrada de la base de datos. Compruebe las estadísticas de resumen de las anotaciones de actividades para verificar que el servidor haya exportado todos los nodos previstos.

#### FILESpace

Especifica los espacios de archivos para los que se van a exportar los datos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

Restricción: Si se especifica un espacio de archivos, los espacios de archivos habilitados para Unicode no se exportan.

#### FSID

Especifica los espacios de archivos utilizando sus identificadores de espacios de archivos (FSID). El servidor utiliza los identificadores FSID para encontrar los espacios de archivos que se deben exportar. Para buscar el FSID para un espacio de archivos, utilice el comando QUERY FILESPACE. Puede separar varios identificadores de espacios de archivos con comas y sin espacios intercalados. Este parámetro es opcional.

#### UNIFILESpace

Especifica los espacios de archivos que el servidor reconoce como activados para Unicode. El servidor convierte los nombres entrados de la página de códigos del servidor a la página de códigos UTF-8 para encontrar los espacios de archivos a exportar. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizarse un carácter comodín para especificar un nombre. Este parámetro es opcional.

#### DOmains

Especifica los dominios de políticas desde donde deben exportarse los nodos. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Si especifica dominios, sólo se exportarán los nodos si pertenecen a uno de los dominios especificados. Puede utilizar caracteres comodín para especificar un nombre.

#### FILEData

Especifica el tipo de archivos que se deben exportar para todos los nodos que se están exportando al servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Nota: Si está exportando un nodo que tiene datos de grupo, los datos que no son parte de los objetos de destino podrían exportarse. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. Por ejemplo, si FILEDATA=BACKUPACTIVE cuando se especifican los parámetros FROMDATE o TODATE, es posible incluir datos de copia de seguridad inactivos. La copia de seguridad incremental de los datos puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten.

Si está exportando a un medio secuencial: la clase de dispositivo que utilizan los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para exportar la información del nodo. El límite de montaje para la clase de dispositivo debe ser como mínimo 2.

Importante: Si se van a exportar los nodos cliente inscritos como TYPE=SERVER, debe especificar ALL, ARCHIVE o ALLACTIVE.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad *activas e inactivas*. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Este parámetro admite los valores siguientes:

#### ALL

El servidor exporta todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management.

#### None

El servidor no exporta archivos, sólo las definiciones de los nodos.

#### ARChive

El servidor sólo exporta las copias archivadas.

#### Backup

El servidor sólo exporta las versiones de copia de seguridad, ya sean activas o inactivas.

#### BACKUPActive

El servidor solo exporta las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando EXPORT.

#### ALLActive

El servidor exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando EXPORT.

#### SPacemanaged

El servidor exporta solo los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si se previsualiza el resultado de la operación de exportación, sin exportar la información. Puede utilizar este parámetro para previsualizar cuántos bytes de datos se transfieren de forma que pueda determinar cuántos volúmenes serán necesarios. Este parámetro admite los valores siguientes:

No

Especifica que se ha de exportar la información del nodo. Si especifica este valor, también debe especificar una clase de dispositivo.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades. Si especifica este valor, no es necesario especificar una clase de dispositivo.

Este parámetro es opcional. El valor predeterminado es NO.

#### DEVclass

Especifica la clase de dispositivo donde se han de grabar los datos de exportación. Este parámetro es necesario si especifica PREVIEW=NO.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la exportación, IBM Spectrum Protect cancela las operaciones con prioridad más baja para que haya una unidad disponible.

Consejo: Se pueden exportar los datos a una agrupación de almacenamiento de otro servidor especificando una clase de dispositivo que tenga el tipo de dispositivo SERVER.

#### Scratch

Especifica si se pueden utilizar volúmenes reutilizables. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que se pueden utilizar volúmenes reutilizables para la operación de exportación. Si especifica también una lista de volúmenes, los volúmenes reutilizables sólo se utilizan si no hay suficiente espacio en los volúmenes especificados.

No

Especifica que no pueden utilizarse volúmenes reutilizables para la exportación. Para determinar el número de volúmenes que puede necesitar, puede ejecutar el comando especificando PREVIEW=YES.

#### VOLumenames

Especifica los volúmenes que se utilizarán para contener los datos exportados. Este parámetro es opcional, a no ser que especifique SCRATCH=NO y PREVIEW=NO. Si no especifica ningún nombre de volumen, se utilizan los volúmenes reutilizables.

Puede especificar uno de los siguientes valores:










nombre\_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

#### USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el comando emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

#### FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.

Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, pueden exportarse los datos de los que se ha hecho copia de seguridad después del parámetro TODATE o TOTIME. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia 10 días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este comando a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00.  Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

#### TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

#### ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

#### ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro admite los valores siguientes:

No

Especifica que los datos no se exportarán desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que los datos pueden exportarse desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

Este parámetro es opcional. El valor predeterminado es NO.

## Ejemplo: exportar información de nodo cliente a volúmenes de cinta específicos

Desde el servidor, exportar la información de nodo cliente a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1.

```
export node devclass=menu1 volumenames=tape01,tape02,tape03
```

## Ejemplo: exportar información de nodo de cliente utilizando el FSID

Desde el servidor, utilice el FSID para exportar versiones de copias de seguridad activas de datos de archivos del nodo cliente JOE al volumen de cinta TAPE01. Para determinar el FSID, emita primero un comando QUERY FILESPACE.

1. Para determinar el FSID, emita un comando QUERY FILESPACE.

```
query filespace joe
```

Node Name	Filespace archivos	FSID	Platform forma	Filespace	Is esp. (MB)Util. Unicode?	Capacity	Pct
JOE	\\joe\c\$	1	WinNT	NTFS	Sí	2.502,3	75,2
JOE	\\joe\d\$	2	WinNT	NTFS	Sí	6.173,4	59,6

2. Exporte las versiones de copias de seguridad activas de los datos de archivos y especifique que el volumen de cinta debe ser utilizado por un dispositivo asignado a la clase de dispositivo MENU1.

```
export node joe fsid=1,2  
filedata=backupactive devclass=menu1  
volumenames=tape01
```

## Ejemplo: exportar información de nodo cliente a los volúmenes de cinta que se indican en un archivo

Desde el servidor, exporte la información de nodo de cliente a cinta que figura en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA

El archivo contiene las líneas siguientes:

```
TAPE01  
TAPE02  
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando siguiente:

  Sistemas operativos Linux

```
export node devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export node devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT NODE (Exportar definiciones de nodo o datos de archivo directamente a otro servidor)

Utilice este comando para exportar definiciones de nodos cliente o datos de archivos directamente a otro servidor para su importación inmediata.

Importante: No es posible exportar nodos de tipo NAS. El proceso de exportación excluirá estos nodos.

Puede suspender y reiniciar una operación de exportación de servidor a servidor que tenga un valor de FILEDATA distinto de NONE. El servidor guarda el estado de la operación de exportación para que se pueda reiniciar a partir del punto en que se encontraba cuando falló o se suspendió. La operación de exportación puede reiniciarse más adelante mediante la emisión del comando RESTART EXPORT.

Importante: Una operación de exportación se suspende cuando se detecta una de estas condiciones:

- Se emite un comando SUSPEND EXPORT para la operación de exportación que está en ejecución.
- Operación realizada por adelantado: otro proceso ha suprimido el archivo que se lee para la exportación.
- Errores de comunicaciones en una exportación de servidor a servidor.
- No hay puntos de montaje disponibles.
- Los volúmenes necesarios no están disponibles.
- Se han encontrado errores de E/S.

Emita el comando QUERY EXPORT para que se visualice la información relacionada con las operaciones de exportación que están en ejecución y que se han suspendido.



La operación de exportación no se puede reiniciar si falla antes de transmitir al servidor de destino las definiciones de nodos y espacios de archivos seleccionables. Debe volver a especificar el comando para empezar una nueva operación de exportación.

Puede emitir el comando QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el comando QUERY EXPORT para obtener una lista de todas las operaciones de exportación de servidor a servidor que pueden reiniciarse. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
.-*-----.  
>>-EXPort Node-----+----->  
      '-nombre_nodo-'  
  
>-----+----->  
      '-FILESpace-----nombre_espacio_archivos-'  
  
>-----+----->  
      '-FSID-----identificador_espacio_archivos-'  
  
>-----+----->  
      '-UNIFILESpace-----nombre_espacio_archivos-'  
  
>-----+----->  
      '-DDomains-----nombre_dominio-'  
  
.FILEData-----None-----.  
>-----+----->  
      '-FILEData-----+ALL-----+-'  
                        +-None-----+  
                        +-ARchive-----+  
                        +-Backup-----+  
                        +-BACKUPActive-+  
                        +-ALLActive-----+  
                        '-SPacemanaged-'  
  
>-----+----->  
      |                               .-FROMTime-----00:00:00-. |  
      '-FROMDate-----fecha-----+-----+-'  
                        '-FROMTime-----hora-----'  
  
>-----+----->  
      |                               .-TOTime-----23:59:59-. |  
      '-TODate-----fecha-----+-----+-'  
                        '-TOTime-----hora-----'  
  
>-----+----->  
      '-EXPORTIDentifier-----identificador_exportación-'  
  
>-----+----->  
      '-TOServer-----nombre_servidor-'  
  
.PREVIEWImport-----No-----.  
>-----+----->  
      '-PREVIEWImport-----+No--+-'  
                        '-Yes-'  
  
.MERGEfilespace-----No-----.  
>-----+----->  
      '-MERGEfilespace-----+No--+-'  
                        '-Yes-'  
  
.Replacedefs-----No-----.  
>-----+----->  
      '-Replacedefs-----+No--+-'  
                        '-Yes-'  
  
.PROXynodeassoc-----No-----.  
>-----+----->
```



El servidor no exporta archivos, sólo las definiciones de los nodos.

#### ARchive

El servidor sólo exporta las copias archivadas.

#### Backup

El servidor sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

#### BACKUPActive

El servidor sólo exporta las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando EXPORT.

#### ALLActive

El servidor exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando EXPORT.

#### SPacemanaged

El servidor exporta solo los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

#### FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.

Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Importante: Si tiene datos de grupo en el nodo que está exportando, pueden exportarse los datos de los que se ha hecho copia de seguridad después del parámetro TODATE o TOTIME. Un ejemplo de datos de grupo son los datos de máquina virtual o los datos de copia de seguridad de estado del sistema. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia 10 días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
-------	-------------	---------

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00. Si emite este comando a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00. Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

#### TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00. Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00. Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

#### TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el comando DEFINE SERVER. El administrador que emita el comando de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

#### PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

#### Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

#### No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

#### MERGEfilespace

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

#### Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

#### PROXynodeassoc

Especifica si se exportan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

#### ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

#### ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no exporta datos desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que el servidor realiza la exportación desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

Restricción: Después de que una operación de exportación ha finalizado la identificación de los archivos que han de exportarse, los cambios que se realicen en el valor ALLOWSHREDABLE de la agrupación de almacenamiento se pasarán por alto. Una operación de exportación que se ha suspendido retiene el valor de ALLOWSHREDABLE original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor ALLOWSHREDABLE de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el comando de exportación después de realizar la operación de limpieza necesaria.

#### EXPORTIdentifier

Este parámetro opcional especifica el nombre que ha seleccionado para identificar esta operación de exportación. Si no especifica un identificador, el servidor generará uno automáticamente. El nombre del identificador de exportación no puede tener más de 64 caracteres, no puede contener caracteres comodín y no es sensible a las mayúsculas y minúsculas. Puede utilizar el nombre del identificador para hacer referencia a las operaciones de exportación en los comandos QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT o CANCEL EXPORT.

Restricción: debe especificar el parámetro TOSERVER si va a especificar el parámetro EXPORTIDENTIFIER. EXPORTIDENTIFIER se pasa por alto si FILEDATA=NONE.

## Ejemplo: exportar información de nodo cliente y todos los archivos de cliente

Para exportar información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB, emita el comando siguiente:

```
export node nodel filedata=all toserver=serverb
```

## Ejemplo: exportar información de nodo cliente y todos los archivos de un rango de fechas específico

---

Para exportar información de nodo cliente y todos los archivos para NODE1 directamente a SERVERB entre el 1 de febrero de 2009 y la fecha de hoy.

```
export node nodel filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

## Ejemplo: exportar información de nodo cliente y todos los archivos de cliente de un rango de fechas y horas específico

---

Para exportar la información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB entre las 8:00 horas del 1 de febrero de 2009 y las 08:00 de hoy, emita el comando siguiente:

```
export node nodel filedata=all toserver=serverb
fromdate=02/01/2009
fromtime=08:00:00
todate=today totime=08:00:00
```

## Ejemplo: exportar información de nodo cliente y todos los archivos de cliente de los tres últimos días

---

Para exportar la información de nodo cliente y todos los archivos de cliente para NODE1 directamente a SERVERB de los tres últimos días, emita el comando siguiente:

```
export node nodel filedata=all toserver=serverb
fromdate=today -3
```

## EXPORT POLICY (Exportar información de políticas)

---

Utilice este mandato para exportar la información de la política desde un servidor de IBM Spectrum Protect a un medio secuencial o directamente a otro servidor para su importación inmediata. Cuando se exporta una política utilizando el mandato EXPORT POLICY, la información de la agrupación de datos activos del dominio no se exporta.

El servidor exporta información de políticas, como por ejemplo:

- Definiciones del dominio de políticas
- Definiciones del juego de políticas, incluido el juego de políticas activo
- Definiciones de la clase de gestión, incluida la clase de gestión predeterminada
- Definiciones de grupo de copia de seguridad y de grupo de copia archivada
- Definiciones de planificación de cada dominio de políticas
- Asociaciones de nodos cliente, si el nodo cliente existe en el servidor destino

Puede utilizar el comando QUERY ACTLOG para ver el estado de la operación de exportación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si exporta información de políticas a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados está incompleto y no debe utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen fixpack distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos
















Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el comando emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

## Ejemplo: exportar información de política a volúmenes de cinta específicos

Desde el servidor, exportar la información de políticas a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
export policy devclass=menu1  
volumenames=tape01,tape02,tape03
```

## Ejemplo: exportar información de política a los volúmenes de cinta que se indican en un archivo

Desde el servidor, exporte la información de política a volúmenes de cinta que figuren en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA

Este archivo contiene las líneas siguientes:

```
TAPE01  
TAPE02  
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export policy devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export policy devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT POLICY (Exportar una política directamente a otro servidor)

Utilice este comando para exportar información de políticas directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

Para supervisar el progreso de la operación de importación, puede emitir un comando QUERY PROCESS desde el servidor de destino. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.



## EXPORT SERVER (Exportar información del servidor)

---

Utilice este comando para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente (si está especificado) del servidor a un medio secuencial.

Si exporta información del servidor a un medio secuencial, luego puede utilizar el medio para importar la información a otro servidor con un tipo de dispositivo compatible.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato `IMPORT`, establezca la contraseña emitiendo el mandato `UPDATE ADMIN` o `UPDATE NODE`.

También tiene la opción de procesar una operación de exportación directamente a otro servidor de la red. Esto da como resultado un proceso de importación inmediato sin que sean necesarios tipos de dispositivos secuenciales compatibles entre los dos servidores.

Puede exportar los siguientes tipos de información del servidor emitiendo el comando `EXPORT SERVER`:

- Definiciones del dominio de políticas
- Definiciones del juego de políticas
- Definiciones de clase de gestión y grupo de copia
- Planificaciones definidas para cada dominio de políticas
- Definiciones de administrador
- Definiciones de los nodos cliente

De forma opcional, puede exportar los siguientes tipos de datos:

- Definiciones de espacio de archivos
- Información de autorización de acceso relativa a los espacios de archivos exportados
- Copias de seguridad, copias archivadas y archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management

Este mandato genera un proceso subordinado que puede cancelarse con el mandato `CANCEL PROCESS`. Si exporta información del servidor a un medio secuencial y se cancela el proceso subordinado, el medio secuencial que contiene los datos exportados estará incompleto y no deberá utilizarse para importar datos. Si se cancela un proceso subordinado de exportación de servidor a servidor, la importación puede ser parcial. Evalúe los datos importados en el servidor de destino para determinar si desea conservar o suprimir los datos importados. Revise los detalles en los mensajes de importación.

Emita el comando `QUERY PROCESS` desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el mandato `QUERY EXPORT` para obtener una lista de todas las operaciones de exportación de servidor a servidor (que tienen un valor `FILEDATA` distinto de `NONE`) que están en ejecución o que se han suspendido.

Puede utilizar el mandato `QUERY ACTLOG` para ver la información de estado real que indica el tamaño y si la operación de exportación ha sido satisfactoria o no.

Se aplican las restricciones siguientes a la función de exportación:

- No se da soporte a la exportación de operaciones de una versión anterior y liberarlas a una versión y release anteriores.
- Pueden fallar las operaciones de exportación entre servidores que se hallan en la misma versión y release pero que tienen `fixpack` distintos. Por ejemplo, no puede exportar un servidor de la versión 7.1.3 a un servidor de la versión 7.1.1 o anterior.
- Los datos exportados de un servidor que tiene habilitada la protección de retención no están protegidos por la retención cuando se importan a otro servidor.
- El proceso de exportación excluye los nodos de almacenamiento adjunto de red (NAS).
- No se admite la exportación de datos a una clase de dispositivo Centera o la importación de datos desde una clase de dispositivo Centera. Sin embargo, pueden exportarse los archivos almacenados en agrupaciones de almacenamiento Centera y los archivos que deben importarse deben almacenarse en un dispositivo de almacenamiento Centera.
- Los mandatos `EXPORT NODE` y `EXPORT SERVER` no exportan datos de una agrupación de fragmentación a menos que lo permita de forma explícita estableciendo el parámetro `ALLOWSHREDDABLE` en el valor `YES`. Si se especifica este valor y los datos exportados incluyen datos de agrupaciones de destrucción, esos datos no se podrán destruir. No se emite ningún aviso si la operación de exportación incluye datos de agrupaciones de fragmentación.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
  - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.

- Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
- Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESPPACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

El mandato EXPORT SERVER ofrece dos posibilidades: exportación directa a otro servidor de la red o bien exportación a un medio secuencial. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con EXPORT SERVER

Comando	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

- EXPORT SERVER (Exportar un servidor a medios secuenciales)  
Puede exportar toda la información de control del servidor o parte de ella y los datos de archivos de cliente de un servidor a un medio secuencial, de modo que esta información se puede importar a otro servidor.
- EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)  
Utilice este comando para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

## EXPORT SERVER (Exportar un servidor a medios secuenciales)

Puede exportar toda la información de control del servidor o parte de ella y los datos de archivos de cliente de un servidor a un medio secuencial, de modo que esta información se puede importar a otro servidor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

```

.-FILEData---None-----
>>-EXPort Server-----+----->
    '-FILEData---+All-----+'
                        +-None-----+
                        +-ARChive-----+
                        +-Backup-----+
                        +-BACKUPActive-+
                        +-ALLActive----+
                        '-SPacemanged-'

.-Preview ---No-----
>-----+----->
|          (1) (2) |
'-Preview-----+No--+-'
                  '-Yes-'

>-----+----->
|          (1) |
'-DEVclass-----nombre_clase_dispositivo-'

.-Scratch---Yes-----
>-----+----->
|          (2) |
'-Scratch-----+Yes--+-'
                  '-No--'

>-----+----->
|          (2)  V |
'-VOLumenames-----+---nombre_volumen+---+-'
                  '-FILE:---nombre_archivo-'

>-----+----->
'-USEDVolumelist---nombre_archivo-'

>-----+----->
|          .-FROMTime---00:00:00-. |
'-FROMDate---fecha--+-----+-'
                  '-FROMTime---hora----'

>-----+----->
|          .-TOTime---23:59:59-. |
'-TODate---fecha--+-----+-'
                  '-TOTime---hora----'

.-ENCryptionstrength---AES-----
>-----+----->
'-ENCryptionstrength---+AES--+-'
                  '-DES-'

.-ALLOWSHREDDable---No-----
>-----+----->
'-ALLOWSHREDDable---+No--+-'
                  '-Yes-'

```

### Notas:

1. Si PREVIEW=NO, debe especificarse una clase de dispositivo.
2. Si PREVIEW=NO y SCRATCH=NO, debe especificarse uno o más volúmenes.

## Parámetros

### FILEData

Especifica el tipo de archivo que se exportan para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Si está exportando a un medio secuencial, la clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este mandato, se necesitan dos unidades para exportar la información del servidor. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad *activas* e *inactivas*. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Los valores siguientes están disponibles:

ALL

IBM Spectrum Protect exporta todas las versiones de copia de seguridad de archivos, todas las copias archivadas y todos los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no exporta archivos, sólo las definiciones.

ARchive

IBM Spectrum Protect sólo exporta las copias archivadas.

Backup

IBM Spectrum Protect sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo exporta las versiones de copia de seguridad activas.

ALLActive

IBM Spectrum Protect exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se migraron mediante el cliente IBM Spectrum Protect for Space Management.

SPacemanaged

IBM Spectrum Protect exporta solo los archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si desea previsualizar el resultado de la operación de exportación, sin exportar la información. Puede utilizar este parámetro para obtener la previsualización del número de bytes de datos que se transferirán y, por lo tanto, podrá determinar cuántos volúmenes serán necesarios. Este parámetro admite los valores siguientes:

No

Especifica que se ha de exportar la información del servidor. Si especifica este valor, también debe especificar una clase de dispositivo.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades. Si especifica este valor, no es necesario especificar una clase de dispositivo.

Este parámetro es opcional. El valor predeterminado es NO.

DEVclass

Especifica la clase de dispositivo donde se han de grabar los datos de exportación. Este parámetro es necesario si especifica PREVIEW=NO.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la exportación, IBM Spectrum Protect cancela las operaciones con prioridad más baja para que haya una unidad disponible.

Consejo: Se pueden exportar los datos a una agrupación de almacenamiento de otro servidor especificando una clase de dispositivo que tenga el tipo de dispositivo SERVER.

Scratch

Especifica si se pueden utilizar volúmenes reutilizables. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que se pueden utilizar volúmenes reutilizables para la operación de exportación. Si especifica también una lista de volúmenes, los volúmenes reutilizables sólo se utilizan si no hay suficiente espacio en los volúmenes especificados.

No

Especifica que no pueden utilizarse volúmenes reutilizables para la exportación. Para determinar el número de volúmenes que puede necesitar, puede ejecutar el comando especificando PREVIEW=YES.

VOLumenames

Especifica los volúmenes que se utilizarán para contener los datos exportados. Este parámetro es opcional, a no ser que especifique SCRATCH=NO y PREVIEW=NO. Si no especifica ningún nombre de volumen, se utilizan los volúmenes reutilizables.

Puede especificar uno de los siguientes valores:










nombre\_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se ignoran las líneas en blanco y de comentarios que empiezan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

USEDVolumelist

Especifica el archivo donde se almacena la lista de volúmenes utilizados en la operación de exportación. Este parámetro es opcional.

Este archivo se puede utilizar en la operación de importación. Este archivo contiene líneas de comentario con la fecha y hora en que se realizó la exportación y el comando emitido para crear la exportación.

Atención: Si especifica un archivo existente, el archivo se sobrescribirá.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE.  
Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.  
Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según



lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

#### FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00.  Si emite este comando a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME+=02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00.  Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

#### TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME.

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

#### ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

#### ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que los datos no se exportarán desde una agrupación de almacenamiento que aplica la destrucción.

Yes

Especifica que los datos pueden exportarse desde una agrupación de almacenamiento que aplica la destrucción. Los datos del medio de exportación no se destruyen.

## Ejemplo: exportar un servidor a volúmenes de cinta específicos

---

Desde el servidor, exportar la información del servidor a los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
export server devclass=menu1
volumenames=tape01,tape02,tape03
```

## Ejemplo: exportar un servidor desde los volúmenes de cinta que se indican en un archivo

---

Desde el servidor, exporte la información de servidor a volúmenes de cinta que figuren en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux TAPEVOL
-  Sistemas operativos Windows TAPEVOL.DATA

El archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los use un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux

```
export server devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
export server devclass=menu1 volumenames=file:tapevol.data
```

## EXPORT SERVER (Exportar información de control de servidor y datos de archivo de cliente a otro servidor)

---

Utilice este comando para exportar toda la información de control del servidor (o parte de ella) y los datos de archivo de cliente directamente a otro servidor de la red. El resultado es una importación inmediata en el servidor destino.

Las operaciones de exportación de servidor a servidor que tienen un valor para FILEDATA distinto de NONE se pueden reiniciar después de haberlas suspendido. El servidor guarda el estado de la operación de exportación para que se pueda reiniciar a partir del punto en que se encontraba cuando falló o se suspendió. La operación de exportación puede reiniciarse posteriormente mediante la emisión del comando RESTART EXPORT. Estas operaciones de exportación se pueden suspender y reiniciar manualmente. Por consiguiente, si se produce un error en una exportación, ésta se suspende automáticamente si ha completado la fase de definiciones de transmisión.

Una operación de exportación se suspende cuando se detecta una de estas condiciones:

- Se emite un comando SUSPEND EXPORT para la operación de exportación que está en ejecución.
- Operación realizada por adelantado: otro proceso ha suprimido el archivo que se va a leer para la exportación.
- Errores de comunicaciones en una exportación de servidor a servidor.
- No hay puntos de montaje disponibles.
- Los volúmenes necesarios no están disponibles.
- Se han encontrado errores de E/S.

La operación de exportación no se puede reiniciar si falla antes de transmitir al servidor de destino las definiciones de nodos y espacios de archivos seleccionables. Debe volver a especificar el comando para empezar una nueva operación de exportación.

Emita el comando QUERY PROCESS desde el servidor de destino para supervisar el progreso de la operación de importación. Emita el comando QUERY EXPORT para obtener una lista de todas las operaciones de exportación de servidor a servidor (que tienen un valor FILEDATA distinto de NONE) que están en ejecución o que se han suspendido. Consulte EXPORT ADMIN (Exportar información del administrador) si desea una lista de restricciones que se aplican a la función de exportación.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```

.-FILEData---None-----
>>-EXPort Server-----+----->
    '-FILEData---+All-----+'
                    +-None-----+
                    +-ARChive-----+
                    +-Backup-----+
                    +-BACKUPActive-+
                    +-ALLActive----+
                    '-SPacemanged-'

>+-----+----->
|               .-FROMTime---00:00:00-. |
'-FROMDate---fecha-----+'
               '-FROMTime---hora-----'

>+-----+----->
|               .-TOTime---23:59:59-. |
'-TODate---fecha-----+'
               '-TOTime---hora-----'

>+-----+----->
'-EXPORTIDentifier---identificador_exportación-'

>+-----+----->
'-TOServer---nombre_servidor-'

.-PREVIEWImport---No-----
>+-----+----->
'-PREVIEWImport---+No--+-'
                    '-Yes-'

.-MERGEfilespace---No-----
>+-----+----->
'-MERGEfilespace---+No--+-'
                    '-Yes-'

.-Replacedefs---No-----
>+-----+----->
'-Replacedefs---+No--+-'
                    '-Yes-'

.-PROXynodeassoc---No-----
>+-----+----->
'-PROXynodeassoc---+No--+-'
                    '-Yes-'

.-ENCRyptionstrength---AES-----
>+-----+----->
'-ENCRyptionstrength---+AES--+-'
                    '-DES-'

.-ALLOWSHREDDable---No-----
>+-----+----->
'-ALLOWSHREDDable---+No--+-'
                    '-Yes-'

```

## Parámetros

### FILEData

Especifica el tipo de los archivos que deben exportarse para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

Si está exportando a un medio secuencial: la clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este comando, IBM Spectrum Protect necesita dos unidades para exportar la información del servidor. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las versiones de archivos de copia de seguridad activas e inactivas. Una versión de archivo de copia de seguridad activa es la versión de copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás versiones de archivo de copia de seguridad se denominan copias inactivas. Los valores son:

ALL

IBM Spectrum Protect exporta todas las versiones de copia de seguridad de archivos, todas las copias archivadas y todos los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no exporta archivos, sólo las definiciones.

ARchive

IBM Spectrum Protect sólo exporta las copias archivadas.

Backup

IBM Spectrum Protect sólo exporta versiones de copia de seguridad, ya sean activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo exporta las versiones de copia de seguridad activas.

ALLActive

IBM Spectrum Protect exporta todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se migraron mediante el cliente IBM Spectrum Protect for Space Management.

SPacemanaged

IBM Spectrum Protect exporta solo los archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management.

FROMDate

Especifica la fecha más antigua de almacenamiento en el servidor de los archivos que se deben exportar. Los archivos almacenados en el servidor con anterioridad a la fecha especificada no se exportan. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. IBM Spectrum Protect ignora el parámetro FROMDATE cuando el parámetro FILEDATA está establecido en NONE. Proceso de directorios: El parámetro FROMDATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado. Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Los datos del grupo del nodo son, por ejemplo, los datos de la máquina virtual o los datos de la copia de seguridad de estado del sistema. Esta exportación es un resultado del proceso de copia de seguridad incremental para los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si no se especifica este parámetro, IBM Spectrum Protect exporta todos los objetos almacenados antes del parámetro TODATE y según lo calificado por el parámetro FILEDATA. Si no se especifica ningún parámetro TODATE, se exportan todos los datos según lo calificado por el parámetro FILEDATA.

Si una operación de exportación de servidor a servidor utiliza una FROMDATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó FROMDATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

## TODate

Especifica la fecha más reciente de los archivos que se exportarán del servidor. Los archivos almacenados en el servidor en una fecha posterior al valor de TODATE no se exportan. TODATE sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política.

- IBM Spectrum Protect ignora el parámetro TODATE cuando el parámetro FILEDATA está establecido en NONE.
- Si se especifica un parámetro TODATE sin un parámetro TOTIME, el servidor exporta todos los objetos insertados el día especificado en el parámetro TODATE o el día anterior a éste.
- Si ha especificado el parámetro FROMDATE, el valor de TODATE debe ser posterior o igual que el de FROMDATE. Si TODATE y FROMDATE son iguales, el parámetro TOTIME debe ser posterior a FROMTIME.
- El parámetro TODATE no se aplica a los directorios. Se procesan todos los directorios de un espacio de archivos aunque no se haya hecho una copia de seguridad de los directorios en el rango de fechas especificado.

Utilice uno de los siguientes valores para especificar la fecha:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	15/10/2006
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

Si una operación de exportación de servidor a servidor utiliza una TODATE relativa, como por ejemplo TODAY-1, y la operación se reinicia en una fecha posterior, el proceso reiniciado seguirá utilizando la fecha que se utilizó durante la operación original. Por ejemplo, si la operación de exportación de servidor a servidor se inició el 04/07/2009 y se especificó TODATE como "TODAY-1", la fecha utilizada para seleccionar archivos es 03/07/2009. Si esta misma operación de exportación se suspende y se reinicia diez días después (14/07/2009), la fecha utilizada para seleccionar archivos seguirá siendo el 03/07/2009. Este comportamiento garantiza que toda la operación de exportación utiliza la misma fecha límite para seleccionar archivos para exportar.

## FROMTime

Especifica la hora más antigua de almacenamiento en el servidor de los objetos que se deben exportar. Cuando especifica FROMTIME, también debe utilizar el parámetro FROMDATE. Este parámetro sólo se aplica a datos de archivos de cliente. Este parámetro no afecta a otra información que se pueda exportar, como por ejemplo, políticas. Los objetos almacenados en el servidor con anterioridad a la hora y la fecha especificada no se exportan. IBM Spectrum Protect ignora el parámetro FROMTIME cuando el parámetro FILEDATA está establecido en NONE.

Importante: Si tiene datos de grupo en el nodo que está exportando, los datos de los que se han hecho copia de seguridad antes de que la fecha designada con FROMDATE y FROMTIME, también se pueden exportar. Un ejemplo de datos en grupo en el nodo son los datos de la máquina virtual o los datos de copia de seguridad del estado del sistema. Esta exportación es el resultado del proceso de copia de seguridad incremental de los datos. La copia de seguridad incremental puede provocar que los archivos adicionales que no cumplen con los criterios de filtrado se exporten, por lo que hay una imagen consistente de los datos de copia de seguridad.

El valor predeterminado de este parámetro cuando se utiliza con el parámetro FROMDATE, es medianoche (00:00:00).

Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW

Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados. FROMTIME+ sólo puede utilizarse con un valor de FROMDATE anterior a hoy.	NOW+02:00 o +02:00.  Si emite este comando a las 5:00 con los valores FROMTIME=NOW+02:00 o FROMTIME=+02:00, la operación de exportación sólo contendrá los archivos que se colocaron en el servidor después de las 7:00 de la fecha especificada en FROMDATE.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW -02:00 o -02:00.  Si emite este mandato a las 5:00 con el valor FROMTIME=NOW-02:00 o FROMTIME=-2:00, la exportación incluirá los archivos que se colocaron en el servidor después de las 3:00.

#### TOTime

Especifica la hora más reciente de almacenamiento en el servidor de los objetos que se deben exportar. Debe especificar el parámetro TODATE para utilizar el parámetro TOTIME. TOTIME sólo se aplica a los datos de los archivos de cliente y no afecta al resto de información que se exporta, como la política. IBM Spectrum Protect ignora el parámetro TOTIME si el parámetro FILEDATA está establecido en NONE.

El valor predeterminado de este parámetro, cuando se utiliza con el parámetro TODATE, es medianoche menos un segundo (23:59:59).

Importante: El valor de los parámetros TOTIME y TODATE debe ser posterior a los valores de FROMDATE y FROMTIME. Utilice uno de los siguientes valores para especificar la hora:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW+02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 07:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00.  Si ejecuta este comando a las 05:00 con FROMTIME=01:00 y TOTIME=NOW-02:00, la exportación incluirá los archivos almacenados desde la 01:00 hasta las 03:00.

#### TOServer

Especifica el nombre de un servidor donde se envían directamente los datos exportados por la red para su importación inmediata.

Importante: El servidor de destino debe definirse en el servidor de origen mediante el comando DEFINE SERVER. El administrador que emita el comando de exportación debe estar definido con el mismo nombre y contraseña de administrador y debe tener autorización de sistema en el servidor de destino.

Cuando se especifica TOSERVER, no se pueden especificar los parámetros DEVCLASS, VOLUMENAMES, SCRATCH, USEDVOLUMELIST y PREVIEW.

#### PREVIEWImport

Especifica si se debe mostrar la cantidad de datos que se transfieren, sin traspasar los datos realmente. Esta información puede resultar de utilidad para determinar la cantidad de espacio de agrupación de almacenamiento que se necesita en el servidor destino. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que desea previsualizar el resultado de la operación de importación en el servidor de destino, sin importar los datos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

No

Especifica que desea importar los datos en el servidor de destino sin previsualizar los resultados.

#### MERGEfilespace

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

Replacedefs

Especifica si se deben sustituir las definiciones (no los datos de archivos) en el servidor. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que se reemplazan las definiciones en el servidor si las definiciones que tienen el mismo nombre que las que se importan existen en el servidor de destino.

No

Especifica que las definiciones importadas se omiten si sus nombres entran en conflicto con las definiciones que ya están definidas en el servidor de destino.

PROXynodeassoc

Especifica si se exportan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

ENCryptionstrength

Indica el algoritmo que se debe utilizar para cifrar contraseñas al exportar registros administrativos y de nodos. Este parámetro es opcional. El valor predeterminado es AES. Si se está exportando a un servidor que no admite AES, se debe especificar DES. Puede especificar uno de los siguientes valores:

AES

Especifica el estándar AES (Advanced Encryption Standard).

DES

Especifica el estándar DES (Data Encryption Standard).

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que aplica la destrucción se exportan. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no admite la exportación de datos desde una agrupación que aplica la destrucción.

Yes

Especifica que el servidor admite la exportación de datos desde una agrupación que aplica la destrucción. Los datos del medio de exportación no se destruirán.

Importante: Después de que una operación de exportación ha finalizado la identificación de los archivos que han de exportarse, los cambios que se realicen en el valor ALLOWSHREDABLE de la agrupación de almacenamiento se pasarán por alto. Una operación de exportación que se ha suspendido retiene el valor de ALLOWSHREDABLE original durante toda la operación. Puede optar por cancelar la operación de exportación si considera que el valor ALLOWSHREDABLE de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el comando de exportación después de realizar la operación de limpieza necesaria.

EXPORTIdentifier

Este parámetro opcional especifica el nombre que ha seleccionado para identificar esta operación de exportación. Si no especifica un nombre de comando, el servidor generará uno automáticamente. El nombre del identificador de exportación no puede tener más de 64 caracteres, no puede contener caracteres comodín y no es sensible a las mayúsculas y minúsculas. Puede utilizar el nombre del identificador para hacer referencia a las operaciones de exportación en los comandos QUERY EXPORT, SUSPEND EXPORT, RESTART EXPORT o CANCEL EXPORT. EXPORTIDENTIFIER se pasa por alto si FILEDATA=NONE o si PREVIEWIMPORT=YES.

Si especifica el parámetro EXPORTIDENTIFIER, debe especificar el parámetro TOSERVER.

## Ejemplo: exportar información de servidor directamente a otro servidor

---

Para exportar información de servidor directamente a SERVERB, emita el comando siguiente.

```
export server filedata=all toserver=serverb
```



## Ejemplo: exportar información de servidor directamente a otro servidor utilizando un rango de fechas

---

Para exportar directamente a SERVERB entre el 1 de febrero de 2009 y la fecha actual, emita el comando siguiente.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 todate=today
```

## Ejemplo: exportar información de servidor y datos de archivo de cliente directamente a otro servidor utilizando un rango de fechas y de horas

---

Para exportar directamente a SERVERB desde las 8:00 horas del 1 de febrero de 2009 hasta la fecha actual, a las 8:00 horas, emita el comando siguiente.

```
export server filedata=all toserver=serverb
fromdate=02/01/2009 fromtime=08:00:00
todate=today totime=08:00:00
```

## EXTEND DBSPACE (Incrementar el espacio para la base de datos)

---

Utilice este comando para aumentar el espacio para la base de datos añadiendo directorios para que los utilice la base de datos.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

Cuando se emite el mandato EXTEND DBSPACE, los directorios se añaden a la base de datos. Con los valores de parámetro predeterminados, los datos se redistribuyen entre todos los directorios de bases de datos y se reclama espacio de almacenamiento. Esta acción mejora el rendimiento de E/S paralela y hace que el espacio de nuevo directorio esté disponible para su uso inmediato.

Si no desea redistribuir los datos al añadir nuevos directorios, puede especificar RECLAIMSTORAGE=NO. Si especifica NO para este parámetro, se llenará todo el espacio en los directorios existentes antes de utilizar los nuevos directorios. Puede redistribuir los datos y solicitar espacio más adelante, pero debe completar el procedimiento manual que requiere esta tarea utilizando mandatos de DB2.

Restricción: La redistribución de datos y la reclamación de espacio como parte de una operación para ampliar el espacio de base de datos solo funciona con espacios de tabla de DB2 versión 9.7 o posterior. Los espacios de tablas se crean al formatear un nuevo servidor IBM Spectrum Protect Versión 6.2 o posterior. Si actualizó o restauró el servidor de IBM Spectrum Protect desde V6.1, no puede redistribuir datos ni reclamar espacio. Debe emitir el mandato EXTEND DBSPACE con RECLAIMSTORAGE=NO.

Importante: El proceso de redistribución utiliza un número considerable de recursos del sistema, por lo tanto, asegúrese de planificarlo con antelación cuando desee añadir espacio a la base de datos. Revise las indicaciones siguientes:

- Complete el proceso cuando el servidor no esté gestionando mucha carga de trabajo.
- El tiempo que se necesita para redistribuir datos y reclamar espacio puede variar. Se ve afectado por factores tales como el diseño del sistema de archivos, la proporción de rutas nuevas a rutas de almacenamiento existentes y operaciones simultáneas. Para obtener una estimación aproximada, puede intentar la operación con una pequeña base de datos de IBM Spectrum Protect en un sistema de laboratorio. Utilice los resultados como referencia para estimar el tiempo necesario para el procedimiento.
- No interrumpa el proceso de redistribución. Si intenta detener, por ejemplo, el proceso que está completando el trabajo, debe detener y reiniciar el servidor de DB2. Cuando se reinicia el servidor, éste se colocará en la modalidad de recuperación del accidente, la cual tarda varios minutos, y después se reanuda el proceso de redistribución.

Después de que se haya completado una operación para ampliar el espacio de base de datos, detenga y reinicie el servidor para poder utilizar completamente los directorios nuevos. Si los directorios de bases de datos existentes están casi llenos cuando se añade un nuevo directorio, el servidor puede recibir una condición de falta de espacio (que se notifica en db2diag.log). Puede corregir la condición de falta de espacio deteniendo y reiniciando el servidor.

### Sintaxis

---


```
      .-,-----|
      v          |
>>-EXTend DBSpace----directorio_bd+----->

.-REclaimstorage----Yes----.  .-Wait----No-----
>+-----+-----+-----+-----<
'-REclaimstorage----+No--+-'  '-Wait----+No--+-'
      '-Yes-'                '-Yes-'
```

## Parámetros

### directorio\_bd (Necesario)

Especifica los directorios para el almacenamiento de la base de datos. Los directorios deben estar vacíos y ser accesibles con el ID de usuario del gestor de bases de datos. Un nombre de directorio debe ser un nombre totalmente calificado y no puede superar los 175 caracteres de longitud. Especifique el nombre entre comillas si éste contiene espacios en blanco intercalados, un signo igual u otros caracteres especiales. Si está especificando una lista de directorios para el almacenamiento de datos, la longitud máxima de la lista puede ser de 1400 caracteres.

 Sistemas operativos Windows Restricción: No se pueden especificar rutas UNC (convenio universal de nomenclatura).

Consejo: Especifique directorios con el mismo tamaño que los directorios existentes para garantizar un grado coherente de paralelismo para las operaciones de base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de pre carga y distribución en paralelo optimizada de la base de datos.

### REclaimstorage

Especifica si los datos se redistribuyen entre los directorios de base de datos recién creados y si se reclama espacio desde las vías de acceso de almacenamiento antiguas. Este parámetro es opcional. El valor predeterminado es Yes (sí).

A menos que especifique `WAIT=YES`, la operación se ha completado como un proceso en segundo plano.

#### Yes

Especifica que los datos se redistribuyen de modo que los directorios nuevos quedan disponibles para su uso inmediato. Importante: El proceso de redistribución utiliza un número considerable de recursos del sistema, por lo que debe asegurarse de planificarlo con antelación.

Una vez que el proceso se inicia, se emiten mensajes que le informarán acerca del progreso. Puede utilizar el mandato `QUERY PROCESS` para supervisar la operación. Para cancelar el proceso, puede utilizar el mandato `CANCEL PROCESS`, pero si una operación de redistribución de datos está en curso, se completará antes de que el proceso se haya detenido.

#### No

Especifica que los datos no se redistribuyen entre los directorios de base de datos y no se reclama espacio de almacenamiento cuando se añade espacio para la base de datos.

### Wait



Especifica si el comando se procesa de forma subordinada o en primer plano.

#### No

Especifica el proceso subordinado. El valor predeterminado es NO.

#### Yes

Especifica el proceso en primer plano.

 Sistemas operativos AIX  Sistemas operativos Linux No se puede especificar YES desde la consola del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: agregar directorios al espacio de almacenamiento para la base de datos, redistribuir datos y solicitar espacio.

Añadir dos directorios (`/tsm_db/stg1` y `/tsm_db/stg2`) debajo del directorio `/tsm_db` al espacio de almacenamiento para la base de datos. Emita el comando:

```
extend dbspace /tsm_db/stg1,/tsm_db/stg2
```

 Sistemas operativos Windows

## Ejemplo: agregar controladores al espacio de almacenamiento para la base de datos, redistribuir datos y solicitar espacio.

Agregar las unidades D y E al espacio de almacenamiento para la base de datos. Emita el comando:

```
extend dbspace D:,E:
```

## Comandos relacionados

Tabla 1. Comandos relacionados con EXTEND DBSPACE

Comando	Descripción
---------	-------------




Comando	Descripción
DSMSERV EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

**Tareas relacionadas:**

Gestión de la capacidad de inventario

## Comandos GENERATE

Utilice los comandos GENERATE para los conjuntos de copia de seguridad para un espacio de archivos o un nodo cliente seleccionado.

- GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)
- GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)

## GENERATE BACKUPSET (generar un juego de copias de seguridad de los datos de cliente de archivado y copia de seguridad)

Utilice este comando para generar un juego de copias de seguridad para un nodo de cliente de archivado y copia de seguridad. Un *juego de copias de seguridad* es una recopilación de los datos activos con copia de seguridad de un cliente de archivado y copia de seguridad, almacenados y gestionados como un solo objeto, en medios específicos, en el almacenamiento del servidor. Aunque puede crear un juego de copias de seguridad para cualquier nodo de cliente, sólo puede utilizarlo un cliente de archivado y copia de seguridad.

Restricción: Un juego de copias de seguridad con el "formato de eliminación de duplicados" tiene esta designación como resultado de un comando GENERATE BACKUPSET con al menos una de las especificaciones siguientes:

- Incluye un nodo en el cliente de archivado y copia de seguridad Versión 6.1.x (como mínimo 6.1.0 pero inferior a V6.2.0).
- Incluye un nodo que tiene uno o más nodos autorizados para actuar como un proxy. Como mínimo uno de estos nodos proxy está en el cliente de archivado y copia de seguridad V6.1.x.

Los conjuntos de copias de seguridad en el formato de eliminación de duplicados sólo se pueden restaurar mediante el cliente de archivado y copia de seguridad V6.1.2 o posterior. Los clientes de archivado y copia de seguridad anteriores a V6.1.2 no se pueden restaurar del conjunto de copias de seguridad en el formato de eliminación de duplicados.

Un juego de copias de seguridad con el "formato de eliminación de duplicados distribuido" tiene esta designación como resultado de un comando GENERATE BACKUPSET con al menos una de las especificaciones siguientes:

- Incluye un nodo en el nivel de cliente de archivado y copia de seguridad V6.2.0 o posterior.
- Incluye un nodo que tiene uno o más nodos autorizados para actuar como un proxy. Como mínimo uno de estos nodos proxy está en el cliente de archivado y copia de seguridad V6.2.0.

Los conjuntos de copias de seguridad con el formato de eliminación de duplicados distribuido sólo se pueden restaurar mediante el cliente de archivado y copia de seguridad V6.2.0 o posterior.

Restricción: No puede generar un juego de copias de seguridad con archivos de los que se haya realizado copia de seguridad en IBM Spectrum Protect utilizando NDMP. Sin embargo, puede crear un juego de copias de seguridad con archivos de los que se ha realizado copia de seguridad utilizando la diferencia de instantánea NetApp.

El servidor crea las copias de las versiones activas de los objetos con copia de seguridad de un cliente que están dentro de uno o más espacios de archivos con este mandato. A continuación, el servidor las consolida en medios secuenciales. Actualmente, los tipos de objeto de copia de seguridad que están admitidos para los juegos de copias de seguridad sólo incluyen directorios y archivos.

El nodo de cliente de archivado y copia de seguridad puede restaurar el juego de copias de seguridad desde el servidor y desde el medio en el que se ha grabado el juego de copias de seguridad.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela el proceso subordinado que ha creado este mandato, es posible que el medio no contenga un juego de copias de seguridad completo. Puede utilizar el mandato QUERY PROCESS para mostrar información acerca del proceso subordinado que crea este mandato.

Consejo: Cuando IBM Spectrum Protect genera un juego de copias de seguridad, puede mejorar el rendimiento si las agrupaciones de almacenamiento primarias que contienen los datos de cliente están próximas. Si está próxima una agrupación de almacenamiento primaria, es muy probable que los datos del nodo cliente ocupen menos volúmenes de cinta que los que ocuparían si la agrupación de

almacenamiento no estuviera próxima. Con la proximidad, se emplea menos tiempo en buscar entradas de base de datos, y se necesitan menos operaciones de montaje.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

## Sintaxis

```
      .-,------.
      V           |
>>-GENerate BACKUPSET-----+---nombre_nodo-----+----->
      '-nombre_grupo_nodos-'

>--prefijo_nombre_juego_copias_seguridad----->

      .-*------.
>+-----+-----+----->
      | .-,------. |
      | V           | |
      |'---nombre_espacio_archivos-+-'|

>--DEVclass-----nombre_clase_dispositivo----->

      .-SCRatch-----Yes-----.
>+-----+-----+----->
      '-SCRatch-----+Yes-+-'
      '-No--'

>+-----+-----+----->
      | .-,------. |
      | V           | |
      |'-VOLumes-----nombres_volúmenes-+-'|

      .-RETention-----365-----.
>+-----+-----+----->
      '-RETention-----+días-+-'
      '-NOLimit-'

      .-Wait-----No-----.
>+-----+-----+----->
      '-DESCription-----descripción-' '-Wait-----+No-+-'
      '-Yes-'

      .-NAMEType-----SERVER-----.
>+-----+-----+----->
      '-NAMEType-----+SERVER-+-'
      '+UNICODE+'
      '-FSID-----'

      .-CODEType-----BOTH-----.
>+-----+-----+----->
      '-CODEType-----+UNICODE-+-'
      '+NONUNICODE+'
      '-BOTH-----'

      .-PITDate-----current_date-. .-PITTime-----current_time-.
>+-----+-----+----->
      '-PITDate-----date-----' '-PITTime-----time-----'

      .-DATAType-----FILE----- .-TOC-----Preferred-----.
>+-----+-----+----->
      | .-,------. | '-TOC-----+No-----+-'
      | V           | | '+Preferred+'
      |'-DATAType-----+FILE-+-' '-Yes-----'
      '+IMAGE+'
      '-ALL-----'

>+-----+-----+----->
      '-TOCMgmtclass-----nombre_clase-'

      .-ALLOWSHREDDable-----No-----.
>+-----+-----+----->
      '-ALLOWSHREDDable-----+No-+-'
      '<
```

## Parámetros

---

### nombre\_nodo o nombre\_grupo\_nodos (Necesario)

Especifica el nombre del nodo cliente y grupos de nodos cuyos datos se incluyen en el juego de copias de seguridad. Para especificar varios nombres de nodo y nombres de grupos de nodos, sepárelos con comas y sin espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos. Cuando se especifican varios nombres de nodo, el servidor genera un juego de copias de seguridad para cada nodo y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida.

### prefijo\_nombre\_juego\_copias\_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad del nodo cliente. La longitud máxima del nombre es de 30 caracteres.

Cuando selecciona un nombre, IBM Spectrum Protect agrega un sufijo para crear el nombre de juego de copias de seguridad. Por ejemplo, si especifica el nombre del juego de copias de seguridad *mybackupset*, IBM Spectrum Protect agrega un número exclusivo como, por ejemplo, 3099, al nombre. El nombre de juego de copias de seguridad se identifica en IBM Spectrum Protect como *mybackupset.3099*. Para mostrar posteriormente información acerca de este juego de copias de seguridad, puede incluir un comodín en el nombre, como *mybackupset.\** o puede especificar el nombre calificado al completo, como *mybackupset.3099*.

Cuando se especifican varios nombres de nodo, el servidor genera un juego de copias de seguridad para cada nodo y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida. A cada juego de copias de seguridad se otorga el mismo nombre completo que consta del *prefijo\_nombre\_juegos\_copias\_seguridad* y un sufijo determinado por el servidor.

### nombre\_espacio\_archivos

Especifica el nombre de uno o varios espacios de archivos que contienen los datos que se van a incluir en el juego de copias de seguridad. Este parámetro es opcional. El nombre de espacio de archivos que se especifique puede contener caracteres comodín. Puede especificar varios nombres separándolos con comas y sin espacios intercalados. Si no especifica un espacio de archivos, en el juego de copias de seguridad se incluirán todos los espacios de archivos activos de los que se ha realizado copia de seguridad de los nodos de cliente.

Para un servidor que tenga clientes con soporte para espacios de archivos habilitados para Unicode, puede especificar un nombre de espacio de archivos o bien un ID de espacio de archivos (FSID). Si especifica un nombre de espacio de archivos, puede que el servidor tenga que convertir el nombre del espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para conocer los detalles. Si no especifica ningún nombre de espacio de archivos o especifica sólo un carácter comodín para dicho nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

### DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo de los volúmenes donde se grabará el juego de copias de seguridad. La longitud máxima del nombre es de 30 caracteres.

Restricción: No es posible especificar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA .

### SCRatch

Especifica si se utilizarán volúmenes reutilizables para el juego de copias de seguridad. Si incluye una lista de volúmenes mediante el parámetro VOLUMES, el servidor sólo utiliza los volúmenes reutilizables si los volúmenes especificados no pueden contener los datos. El valor predeterminado es SCRATCH=YES. Los valores son:

YES

Especifica que se utilizarán volúmenes reutilizables para el juego de copias de seguridad.

NO

Especifica que no se utilizarán volúmenes reutilizables para el juego de copias de seguridad.

### VOLumes

Especifica el nombre de uno o varios volúmenes que contendrán el juego de copias de seguridad. Este parámetro es opcional. Puede especificar más de un volumen separando cada volumen con una coma y sin espacios intercalados.

Si no especifica este parámetro, se utilizan los volúmenes reutilizables para el juego de copias de seguridad.

### RETention

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor. Puede especificar un entero entre el 0 y el 30000. El valor predeterminado es 365 días. Los valores son:

días

Especifica el número de días que se retiene el juego de copias de seguridad en el servidor.

NOLimit

Especifica que el juego de copias de seguridad debe retenerse indefinidamente en el servidor.

Si especifica NOLIMIT, el servidor retendrá los volúmenes que contienen el juego de copias de seguridad sin límite de tiempo, a menos que un usuario o un administrador suprima los volúmenes del almacenamiento del servidor.

#### DESCRiption

Especifica la descripción que se asociará al juego de copias de seguridad. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Los valores son:

##### Yes

Especifica que el comando se procesa en primer plano. Los mensajes que se crean no se visualizan hasta que el mandato haya finalizado el proceso. No se puede especificar WAIT=YES desde la consola del servidor.

##### No

Especifica que el comando se procesa de forma subordinada. Utilice el comando QUERY PROCESS para supervisar el proceso subordinado de este comando.

#### NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten espacios de archivos activados para Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que utilizan sistemas operativos Windows, NetWare o Macintosh OS X.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Los valores posibles son:

##### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

##### UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

##### FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID). Importante: Preste atención al especificar este parámetro si también se han especificado varios nombres de nodo. Es posible que nodos diferentes utilicen el mismo ID de espacio de archivos para diferentes espacios de archivos, o diferentes ID de espacio de archivos para el mismo nombre de espacio de archivos. Por esta razón, especificar un ID de espacio de archivos como los nombres de espacio de archivos podría hacer que para algunos nodos se graben los datos incorrectos en el juego de copias de seguridad.

#### CODEType

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre del espacio de archivos o cuando no especifique ningún nombre de espacio de archivos. Los valores posibles son:

##### UNICODE

Incluir sólo los espacios de archivos que están en Unicode.

##### NONUNICODE

Incluir sólo los espacios de archivos que no están en Unicode.

##### BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

#### PITDate

Especifica que los archivos que estaban activos en la fecha especificada y que aún se almacenan en el servidor de IBM Spectrum Protect deben incluirse en el juego de copias de seguridad, aunque estén inactivos en el momento de emitir el comando. Este parámetro es opcional. El valor predeterminado es la fecha en la que se ejecuta el comando GENERATE BACKUPSET. Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7. Para incluir archivos que estaban activos hace una semana, especifique PITDATE=TODAY-7 o PITDATE=-7

Valor	Descripción	Ejemplo
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### PITTime

Especifica que los archivos que estaban activos a la hora especificada y que aún se almacenan en el servidor de IBM Spectrum Protect deben incluirse en el juego de copias de seguridad, aunque estén inactivos en el momento de emitir el comando. Este parámetro es opcional. Si se ha especificado una fecha PITDate, el valor predeterminado es medianoche (00:00:00); en caso contrario, el valor predeterminado es la hora a la que se ha iniciado el comando GENERATE BACKUPSET. Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha PIT especificada	12:33:28
NOW	La fecha actual en la fecha PIT especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha PIT especificada	NOW+03:00 o +03:00  Si emite este comando a las 9:00 con PITTIME=NOW+03:00 o PITTIME=+03:00. IBM Spectrum Protect incluirá archivos que estaban activos a las 12:00 en la fecha PIT.

#### DATATYPE

Especifica que se van a generar los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que se deben generar juegos de copias de seguridad de nivel de archivo. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados.

El servidor genera un juego de copias de seguridad para cada tipo de datos y coloca todos los juegos de copias de seguridad en un único juego de volúmenes de salida. A cada juego de copias de seguridad se otorga el mismo nombre completo que consta del *prefijo\_nombre\_juegos\_copias\_seguridad* y un sufijo determinado por el servidor. Sin embargo, cada juego de copias de seguridad tiene un tipo de datos diferente, tal como muestra el mandato QUERY BACKUPSET. Los valores posibles son:

#### ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) de los que se ha hecho una copia de seguridad en el servidor se deben generar.

#### FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a generar. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad. Si el cliente de copia de seguridad no ha realizado copia de seguridad de ningún archivo o directorio, no se generará un juego de copias de seguridad de nivel de archivo. Este es el valor predeterminado.

#### IMAGE

Especifica que se va a generar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el mandato BACKUP IMAGE del cliente de copia de seguridad. Los juegos de copias de seguridad de imagen se generan sólo si un cliente de copia de seguridad ha realizado copia de seguridad de una imagen.

#### TOC

Especifica si debe guardarse una tabla de contenido (TOC) para cada juego de copias de seguridad de nivel de archivo. Las tablas de contenido siempre se guardan para conjuntos de copias de seguridad que contienen datos de imagen o aplicación. Se ignorará el parámetro TOC al generar juegos de copias de seguridad de imagen y aplicación. Siempre se generará una tabla de contenido para los juegos de copias de seguridad de imagen y aplicación.

Cuando determine si desea guardar una tabla de contenido, debe tener en cuenta los puntos siguientes:

- Si se guarda una tabla de contenido para un juego de copias de seguridad, podrá utilizar el cliente web de copia de seguridad/archivado de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y seleccionar los

archivos y directorios que han de restaurarse. Para crear una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión que especifica el parámetro TOCMGMTCLASS. Para la creación de una tabla de contenido se necesitan de forma adicional procesos, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación del juego de copias de seguridad.

- Si no se guarda una tabla de contenido para un juego de copias de seguridad, todavía podrá restaurar archivos individuales o árboles de directorios mediante el comando RESTORE BACKUPSET del cliente de copia de seguridad/archivado, siempre que conozca el nombre cualificado completo de cada archivo o directorio que se desea restaurar.

Para que se visualice el contenido de los juegos de copias de seguridad, también puede utilizar el comando QUERY BACKUPSETCONTENTS.

Este parámetro es opcional. Los valores posibles son:

No

Especifica que la información de la tabla de contenido no se guardará para los juegos de copias de seguridad de nivel de archivo.

Preferred

Especifica que la información de la tabla de contenido deberá guardarse para los juegos de copias de seguridad de nivel de archivo. Este es el valor predeterminado. Sin embargo, un juego de copias de seguridad no fallará sólo porque se produzca un error durante la creación de la tabla de contenido.

Yes

Especifica que debe guardarse la información de la tabla de contenido para cada juego de copias de seguridad de nivel de archivo. Un juego de copias de seguridad fallará si se produce un error durante la creación de la tabla de contenido.

TOCMgmtclass

Especifica el nombre de la clase de gestión a la que debe estar vinculada la tabla de contenido. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado el nodo. En este caso, la creación de una tabla de contenido requiere la definición del atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

ALLOWSHREDdable

Especifica si los datos de una agrupación de almacenamiento que implementa la destrucción de datos se incluyen en el juego de copias de seguridad. Este parámetro es opcional. Los valores posibles son:

No

Especifica que los datos de una agrupación de almacenamiento que implementa la destrucción de datos no se incluyen en el juego de copias de seguridad. Este es el valor predeterminado.

Yes

Especifica que los datos de una agrupación de almacenamiento que implementa la destrucción de datos pueden incluirse en el juego de copias de seguridad. Los datos del medio del juego de copias de seguridad no se destruirán.

## Ejemplo: generar un juego de copias de seguridad de un espacio de archivos

---

Generar un juego de copias de seguridad de un espacio de archivos denominado /srvr que pertenece al nodo de cliente JANE. Denominar el juego de copias de seguridad PERS\_DATA y retenerlo durante 75 días. Especifique que los volúmenes VOL1 y VOL2 contienen los datos del juego de copias de seguridad. Los volúmenes los ha de leer un dispositivo asignado a la clase de dispositivo AGADM. Incluya una descripción.

```
generate backupset jane pers_data /srvr devclass=agadm
retention=75 volumes=vol1,vol2
description="area 51 base image"
```

## Ejemplo: generar un juego de copias de seguridad de un espacio de archivos habilitado para Unicode

---

Generar un juego de copias de seguridad de un espacio de archivos habilitado para Unicode, \\joe\c\$, que pertenece al nodo cliente JOE. Dé al conjunto de copia de seguridad el nombre JOES\_DATA. Especificar que el volumen VOL1 contiene los datos del conjunto de copia de seguridad. El volumen debe ser leído por un dispositivo asignado a la clase de dispositivo AGADM. Utilice el servidor para que éste convierta el nombre del espacio de archivos \\joe\c\$ de la página de códigos del servidor en la página de códigos UTF-8.

```
generate backupset joe joes_data \\joe\c$ devclass=agadm
volumes=vol1 nametype=unicode
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con GENERATE BACKUPSET



Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## GENERATE BACKUPSETTOC (generar una tabla de contenido para un juego de copias de seguridad)

Utilice este comando para generar una tabla de contenido para un juego de copias de seguridad que todavía no disponga de una. El cliente de copia de seguridad/archivado utiliza la tabla de contenido para visualizar el juego de copias de seguridad, lo cual permite a los usuarios seleccionar los archivos individuales que desea restaurar del mismo.

La creación de una tabla de contenido para un juego de copias de seguridad necesita espacio de agrupación de almacenamiento y, posiblemente, uno o más puntos de montaje durante la operación de creación.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

### Sintaxis

```
>>-Generate BACKUPSETTOC--nombre_nodo--nombre_juego_copias_seguridad-->
  .-DATAType-----ALL-----
>+-----+-----+-----+-----+-----+-----+-----+-----+
  |               .-,-----|
  |               V         |
  |'-DATAType-----+FILE--+-'
  |               '-IMAGE-'
>+-----+-----+-----+-----+-----+-----+-----+-----+<
  '-TOCMgmtclass-----nombre_clase-'
```

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo cliente cuyos datos están contenidos en el juego de copias de seguridad. No se pueden utilizar caracteres comodín para especificar un nombre ni se puede especificar una lista de nombres de nodos cliente.

nombre\_juego\_copias\_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad del nodo cliente. No se pueden utilizar caracteres comodín para especificar un nombre ni se puede especificar una lista de nombres de juegos de copias de seguridad.

DATAType

Especifica el tipo de datos que se va a incluir en la tabla de contenido. Este parámetro es opcional. De manera predeterminada se incluyen todos los datos. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que la tabla de contenido incluye todos los tipos de datos (nivel de archivo, imagen y aplicación) almacenados en el juego de copias de seguridad. Este es el valor predeterminado.

FILE

Especifica que la tabla de contenido sólo incluye los datos de nivel de archivo. Los datos de nivel de archivo comprenden los archivos y directorios de los que se ha hecho copia de seguridad mediante el cliente de copia de seguridad/archivado. Si el juego de copias de seguridad no contiene ningún archivo ni directorio, no se generará la tabla de contenido.

IMAGE

Especifica que la tabla de contenido incluirá únicamente las copias de seguridad de imágenes. Las copias de seguridad de imágenes comprenden las imágenes del sistema de archivos creadas mediante el comando BACKUP IMAGE del cliente de copias de seguridad. Si el juego de copias de seguridad no contiene ninguna copia de seguridad de imagen, no se generará la tabla de contenido.

TOCMgmtclass

Especifica el nombre de la clase de gestión a la que debe estar vinculada la tabla de contenido. Si no se especifica una clase de gestión, la tabla de contenido se vincula a la clase de gestión predeterminada para el dominio de políticas al que está asignado el nodo. Si crea una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copia de seguridad para la clase de gestión especificada.

## Ejemplo: generar una tabla de contenido

Genere una tabla de contenido para un juego de copias de seguridad denominado PROJX\_DATA que contiene los datos para el nodo cliente GARY. La tabla de contenido se encontrará en la clase de gestión predeterminada.




```
generate backupsettoc gary projx_data
```

## Comandos relacionados

Tabla 1. Comandos relacionados con GENERATE BACKUPSETTOC

Comando	Descripción
COPY ACTIVE DATA	Copia los datos de copia de seguridad activos.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.

Comando	Descripción
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## GENERATE DEDUPSTATS (Generar estadísticas de eliminación de duplicados de datos)

Utilice este mandato para generar estadísticas de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o una agrupación de almacenamiento de contenedores en la nube, a fin de determinar el rendimiento de la deduplicación de datos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento.

### Sintaxis

```
>>-GENerate DEDUPStats--nombre_agrupación----->
      .-,-----
      v |
>-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'

      .*-----
>-----+----->
      | .-,-----
      | v |
      +---nombre_espacio_de_archivos---+
      | .-,-----
      | v |
      |-----FSID-----|

      .-CODEType----BOTH----- .-MAXPRocess----4-----
>-----+-----+----->
      '-CODEType----+UNICODE----+' '-MAXPRocess----número-'
          +-NONUNICODE-+
          '-BOTH-----'

      .-NAMEType----SERVER----- .-Wait----No-----
>-----+-----+-----<
      '-NAMEType----+SERVER---+' '-Wait----+No---+'
          +-UNICODE-+           '-Yes-'
          '-FSID----'
```

### Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se notifica en las estadísticas de eliminación de duplicados de datos. Puede especificar hasta 30 caracteres para el nombre de agrupación de almacenamiento. Si especifica más de 30 caracteres, el mandato falla.

Restricción: Puede especificar únicamente agrupaciones de almacenamiento de contenedores de directorios o agrupaciones de almacenamiento en la nube.

nombre\_nodo o nombre\_grupo\_nodos (Necesario)

Especifica el nombre del nodo de cliente o el grupo definido de nodos de cliente que se notifican en las estadísticas de deduplicación de datos. También puede especificar una combinación de nombres de nodos de cliente y nombres de grupos de nodos de cliente. Para especificar varios nombres de nodos de cliente o nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede utilizar caracteres comodín con los nombres de nodos de cliente pero no con los nombres de grupos de nodos de cliente.

nombre\_espacio\_de\_archivos o FSID

Especifica el nombre de uno o varios espacios de archivos en las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. El asterisco es el valor predeterminado.

Especifique uno de los siguientes valores:

\*

Especifique un asterisco (\*) para mostrar todos los espacios de archivos o ID.

nombre\_espacio\_de\_archivos

Especifica el nombre del espacio de archivos. Especifique varios nombres separándolos con comas y sin espacios intercalados. FSID especifica un identificador de espacio de archivo. Este parámetro es válido para los clientes con espacios de archivos que están en formato Unicode. Especifique varios nombres separándolos con comas y sin espacios intercalados.

Para los clientes con espacios de archivos en formato Unicode, puede especificar un nombre de espacio de archivos o un FSID. Si especifica un nombre de espacio de archivos, es posible que el servidor deba convertir el nombre de espacio de archivos que especifique. Por ejemplo, puede que el servidor deba convertir el nombre que especifique de la página de códigos del servidor a Unicode.

Restricciones: Se aplican las restricciones siguientes a los nombres de espacio de archivos y FSID:

- Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.
- No especifique FSID y nombres de espacio de archivos en el mismo comando.

#### CODEType

Especifica qué tipo de espacios de archivos se van a incluir en el registro. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un asterisco para visualizar información sobre todos los espacios de archivos. Este parámetro es opcional. Especifique uno de los siguientes valores:

UNICODE

Incluir los espacios de archivos que están en formato Unicode.

NONUNICODE

Incluir los espacios de archivos que no están en formato Unicode.

BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos. Este es el valor predeterminado.

#### MAXProcess

Especifica el número máximo de procesos paralelos que se utilizarán para generar estadísticas para un contenedor en una agrupación de almacenamiento de contenedores de directorio o de contenedores en la nube. Este parámetro es opcional. Especifique un valor en el rango de 1 a 99. El valor predeterminado es 4.

#### NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro cuando los clientes de IBM Spectrum Protect tengan espacios de archivos en formato Unicode y estén en sistemas operativos Windows, NetWare o Macintosh OS X. Este parámetro es opcional.

Este parámetro es necesario si especifica un nombre de nodo y un nombre de espacio de archivos o un FSID.

Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un asterisco.

Especifique uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

UNICODE

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor.

Consejo: La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacios de archivo como sus FSID.

#### Wait

Especifica si las estadísticas de deduplicación de datos se generan en primer o en segundo plano. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que la operación se ha completado en segundo plano. Puede continuar con otras tareas mientras se está procesando el mandato. Los mensajes relacionados con el proceso en segundo plano se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Éste es el valor predeterminado.

Yes

Especifica que la operación se ha completado en primer plano. La operación puede tardar bastante tiempo en completarse. La operación debe finalizar para poder continuar con otras tareas. Los mensajes se muestran en el archivo de registro de actividades o la consola de servidor, o en ambos, en función de la ubicación en la que se registren los mensajes.

Restricción: No puede especificar el parámetro WAIT=YES desde la consola de servidor.

## Ejemplo: generar estadísticas de eliminación de duplicados de datos para un espacio de archivos

Generar estadísticas de deduplicación de datos para un espacio de archivos llamado /srvr que pertenece a una agrupación de almacenamiento de contenedores de directorio, POOL1, que está almacenada en el nodo de cliente NODE1.

```
generate dedupstats pool1 node1 /srvr
```







## Ejemplo: generar estadísticas de deduplicación de datos para un espacio de archivos habilitado para Unicode

Genere las estadísticas de deduplicación de datos para un espacio de archivos habilitado para Unicode denominado \\abc\c\$ que pertenece al nodo de cliente NODE2. Convierta el nombre de espacio de archivo \\abc\c\$ de la página de códigos del servidor a la página de códigos UTF-8.

```
generate dedupstats node2 \\abc\c$ nametype=unicode
```

## Comandos relacionados

Tabla 1. Comandos relacionados con GENERATE DEDUPSTATS

Comando	Descripción
   DELETE DEDUPSTATS	Suprime las estadísticas de eliminación de duplicados de datos.
   QUERY DEDUPSTATS	Muestra las estadísticas de eliminación de duplicados de datos.

## Comandos GRANT

Utilice el comando GRANT para otorgar el acceso o los privilegios apropiados.

- GRANT AUTHORITY (agregar autorización de administrador)
- GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)

## GRANT AUTHORITY (agregar autorización de administrador)

Utilice este comando para otorgar a un administrador una o varias clases de privilegios de administración y autorización para acceder a nodos cliente.

No puede otorgar privilegios restringidos a un administrador con privilegio de almacenamiento sin restricciones o de política sin restricciones. Debe utilizar el comando REVOKE AUTHORITY para eliminar el privilegio sin restricciones del administrador; a continuación, utilice este comando para otorgar privilegios restringidos al administrador.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>>GRant AUTHority--nombre_admin----->
      .-|-----|
      (1) V      |
>>>Classes-----+SYstem-----+----->
                +-Policy-----+
                +-Storage-----+
                +-Operator-----+
                '-Node--| A |-'
```



Atención: Al especificar la clase de privilegio de nodo, también debe especificar el parámetro DOMAIN o el parámetro NODE, pero no los dos.

#### AUTHority

Especifica el nivel de autorización de un usuario con privilegio de nodo. Este parámetro es opcional.

Si un administrador ya tiene privilegio de sistema o de políticas para el dominio de políticas al que pertenece el nodo, este comando no modificará el privilegio del administrador.

Los niveles de autorización posibles son:

#### Access

Especifica que desea otorgar autorización de acceso a cliente a un usuario con la clase de privilegio de nodo. Es el valor predeterminado si se ha especificado CLASSES=NODE. Un usuario con autorización de acceso a cliente puede acceder a un cliente de copia de seguridad/archivado de Web y ejecutar acciones de copia de seguridad y restauración para ese cliente.

Atención: Un usuario con autorización de acceso a cliente no puede acceder a ese cliente desde otro sistema utilizando el parámetro -VIRTUALNODENAME.

Un nodo cliente puede establecer la opción REVOKEREMOTEACCESS para restringir el acceso de un usuario que tiene privilegio de nodo con autorización de acceso a cliente a una estación de trabajo cliente que está ejecutando un cliente de Web. Esta opción no afecta a los administradores con autorización de propietario de cliente, privilegio de sistema o privilegio de políticas para el dominio de políticas al que pertenece el nodo.

#### Owner

Especifica que desea otorgar autorización de propietario de cliente a un usuario con la clase de privilegio de nodo. Un usuario con autorización de propietario de cliente puede acceder a un cliente de copia de seguridad/archivado de Web mediante la interfaz de cliente de Web y también acceder a los datos desde otro cliente utilizando el parámetro -VIRTUALNODENAME.

#### DOmains

Especifica que desea otorgar al administrador autorización de acceso a cliente o de propietario de cliente para todos los clientes del dominio de políticas especificado. Este parámetro no se puede utilizar junto con el parámetro NODE.

#### NOde

Especifica que desea otorgar al administrador autorización de acceso a cliente o de propietario de cliente para el nodo. Este parámetro no se puede utilizar junto con el parámetro DOMAIN.

#### DOmains

Cuando se utiliza con CLASSES=POLICY, especifica que desea otorgar a un administrador el privilegio de política con restricciones.

El privilegio de políticas con restricciones permite a un administrador emitir un subconjunto de mandatos de políticas para los dominios sobre los que el administrador tiene autorización. Puede utilizar este parámetro para otorgar autorización de dominio de políticas a un administrador de políticas con restricciones. Este parámetro es opcional. Puede especificar más de un dominio de políticas delimitando cada uno con una coma.

Puede utilizar caracteres comodín para especificar un nombre. Se otorgará autorización para todos los dominios de políticas coincidentes.

#### STGpools

Especifica que desea otorgar a un administrador privilegios de almacenamiento con restricciones. Si se especifica el parámetro STGPOOLS, entonces CLASSES=STORAGE es opcional.

El privilegio de almacenamiento con restricciones permite emitir un subconjunto de comandos de almacenamiento para las agrupaciones de almacenamiento sobre las que el administrador tiene autorización. Puede utilizar este parámetro para otorgar autorización de agrupación de almacenamiento a un administrador de almacenamiento con restricciones. Este parámetro es opcional. Puede especificar más de una agrupación de almacenamiento delimitando cada una con una coma.

Puede utilizar caracteres comodín para especificar un nombre. Se otorgará autorización para todas las agrupaciones de almacenamiento que coincidan.

## Ejemplo: otorgar privilegio de sistema a un administrador

---

Otorgar privilegio de sistema al administrador Larry.

```
grant authority larry classes=system
```

## Ejemplo: otorgar acceso a dominios de políticas adicionales

Especificar dominios de políticas adicionales que pueda gestionar el administrador CLAUDIA con privilegio de políticas restringido.

```
grant authority claudia domains=employee_records,progl
```

## Ejemplo: proporcionar a un administrador privilegio de almacenamiento sin restricciones y privilegio de políticas restringido

Proporcionar al administrador TOM privilegio de almacenamiento sin restricciones y privilegio de políticas sin restricciones para los dominios cuyos nombres comiencen por EMP.

```
grant authority tom classes=storage  
domains=emp*
```

## Ejemplo: otorgar a un administrador autorización restringida a un nodo específico

Otorgar privilegio de nodo al usuario HELP para que el personal del departamento de soporte pueda ayudar al nodo de cliente LABCLIENT a hacer copia de seguridad o a restaurar datos sin tener otros privilegios de IBM Spectrum Protect de nivel superior.

```
grant authority help classes=node node=labclient
```

## Comandos relacionados

Tabla 1. Comandos relacionados con GRANT AUTHORITY

Comando	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
REVOKE AUTHORITY	Revoca una o más clases de privilegio o limita el acceso a los dominios de políticas y agrupaciones de almacenamiento.

## GRANT PROXYNODE (otorgar la autoridad proxy a un nodo cliente)

Utilice este comando para otorgar una autoridad proxy a un nodo cliente del servidor de IBM Spectrum Protect.

Los nodos cliente de destino poseen los datos y los nodos agente actúan en nombre de los nodos de destino. Cuando se otorga autorización de proxy a un nodo cliente de destino, un nodo agente puede realizar operaciones de copia de seguridad y de restauración para el nodo de destino. Los datos que almacena el nodo agente en nombre del nodo de destino se almacena bajo el nombre del nodo de destino en el almacenamiento del servidor.

## Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones

## Sintaxis

```
>>-GRant PROXynode TArget---nombre_nodo_destino----->
```

```
>--AGent---nombre_nodo_agente-----<
```

## Parámetros

TArget (Obligatorio)

Especifica el nombre del nodo propietario de los datos. No se pueden utilizar nombres comodín para especificar el nombre de nodo de destino.

AGent (Obligatorio)

Especifica el nombre del nodo que realiza operaciones para el nodo de destino. El nodo agente no tiene que estar en el mismo dominio que el nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.



## Ejemplo: otorgar autorización de proxy a un nodo cliente

Imaginemos que MOE y JOE son nodos agente de un clúster NAS y que éstos se utilizan para realizar la copia de seguridad y restauración de datos NAS compartidos. Para crear una relación de autorización de proxy para el nodo de destino NASCLUSTER, emita el comando siguiente:

```
grant proxynode target=nascluster agent=moe,joe
```

Emita el siguiente comando en el nodo de destino MOE para realizar la copia de seguridad de los datos del clúster NAS que se almacenan en la unidad E: El nombre del nodo de destino es NASCLUSTER.

```
dsmc -asnode=nascluster incremental e:
```

## Comandos relacionados

Tabla 1. Comandos relacionados con GRANT PROXYNODE

Comando	Descripción
QUERY PROXYNODE	Visualiza los nodos con autoridad para actuar como nodos proxy.
REVOKE PROXYNODE	Revocar la autoridad de proxy a un nodo de agente.

## HALT (Concluir el servidor)

Utilice este comando para concluir el servidor. El comando HALT fuerza una conclusión precipitada, que cancela todas las sesiones de nodo cliente y de administración, aunque no se hayan completado.

Cualquier transacción en proceso que haya interrumpido el comando HALT se retrotraerá cuando vuelva a arrancar el servidor. Utilice el comando HALT sólo después de que se hayan completado o cancelado las sesiones de nodo cliente y de administración. Para concluir el servidor sin que las sesiones de nodo cliente o de administración sufran un impacto grave, realice los pasos siguientes:

1. Utilice el comando DISABLE SESSIONS para impedir que se inicien nuevas sesiones de nodo cliente.
2. Utilice el comando QUERY SESSIONS para identificar las sesiones de nodo cliente y de administración existentes.
3. Notifique a cualquier sesión de nodo cliente o de administración que piensa concluir el servidor (debe realizarlo fuera de IBM Spectrum Protect).
4. Utilice el comando CANCEL SESSIONS para cancelar las sesiones de nodo cliente o de administración existentes.
5. Emita el comando HALT para concluir el servidor y detener las sesiones de nodo cliente y de administración existentes.

Consejo:

La acción del comando HALT puede obtenerse con la opción de servidor ALIASHALT. Utilice la opción del servidor para definir un término distinto de HALT que realice la misma función. El comando HALT conserva su función normal; sin embargo, la opción del servidor proporciona un método adicional para emitir el comando HALT. Consulte el apartado ALIASHALT para obtener más información.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de operador.

## Sintaxis

```
>>-HALT-----><
```

## Parámetros

Ninguno.

## Ejemplo: concluir el servidor

Concluir el servidor, desde la consola del servidor o desde un cliente de administración. Toda la actividad de usuario se parará inmediatamente y no se podrá iniciar ninguna nueva actividad.

```
halt
```

## Comandos relacionados

Tabla 1. Comandos relacionados con HALT

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.

## HELP (Obtener ayuda sobre comandos y mensajes de error)

Utilice este comando para visualizar los comandos de administración y los mensajes de error. Puede emitir el mandato desde un cliente de línea de mandatos de administración.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Help-----><
+-numero_tema_ayuda-----+
|                           |
|           .-,----- . |
|           v               |
+-nombre_comando-----+++
|           '-nombre_subcomando-' |
+-numero_mensaje-----+
+-nombre_opción_servidor-----+
+'-nombre_programa_utilidad-----'
```

### Parámetros

numero\_tema\_ayuda

Especifica el número de su selección de los temas de ayuda. Este parámetro es opcional.

Los números de tema se muestran en la tabla de contenidos, por ejemplo:

```
3.0 Administrative commands
...
3.13.10 DEFINE DEVCLASS (Definir una clase de dispositivo)
  3.13.10.1 DEFINE DEVCLASS (Definir una clase de dispositivo 3590)
  3.13.10.2 DEFINE DEVCLASS (Definir una clase de dispositivo 3592)
...
```

El número de tema para el mandato DEFINE DEVCLASS para una clase de dispositivo 3592 es 3.13.10.2.

nombre\_comando

Especifica el nombre del comando de administración que desea visualizar. Este parámetro es opcional.

nombre\_subcomando

Especifica un máximo de dos nombres de subcomando asociados al nombre del comando de administración que desea visualizar. Este parámetro es opcional.

numero\_mensaje

Especifica el número del mensaje para el que desea visualizar información. Este parámetro es opcional. Puede obtener información de ayuda sobre mensajes del servidor (con el prefijo ANR) y mensajes del cliente (con el prefijo ANE o ANS). No incluya el prefijo ni el código de gravedad cuando especifique un número de mensaje de error.

nombre\_opción\_servidor

Especifica el nombre de un servidor sobre el que desea visualizar información. Este parámetro es opcional.  
nombre\_programa\_utilidad  
Especifica el nombre del programa de utilidad de servidor sobre el que desea visualizar información. Este parámetro es opcional.

## Ejemplo: visualizar los temas de la ayuda

---

Visualizar los temas de ayuda para la interfaz de la línea de comandos.

```
ayuda
```

Salida parcial:

```
1.0 Administración del servidor desde la línea de comandos
  1.1 Emisión de comandos desde el cliente de administración
    1.1.1 Inicio y detención del cliente de administración
    1.1.2 Supervisión de actividades del servidor desde el cliente de
        administración
```

## Ejemplo: visualizar un tema de la ayuda con el número del tema de la ayuda

---

Visualizar información de ayuda con el número del tema de la ayuda. El número de tema para el mandato DEFINE DEVCLASS para una clase de dispositivo 3592 es 3.13.10.2.

```
help 3.13.10.2
```

## Ejemplo: visualizar ayuda para un comando

---

Visualizar información de ayuda acerca de los mandatos REMOVE.

```
help remove
```

```
Mandatos 3.44 REMOVE
Utilice los comandos REMOVE para eliminar un objeto.
A continuación se muestra una lista de los comandos REMOVE:
* 3.44.1, "REMOVE ADMIN (Eliminar un administrador)"
* 3.44.2, "REMOVE NODE (Eliminar un nodo o un nodo asociado
    a una máquina)"
```

## Ejemplo: visualizar ayuda para un mensaje de error específico

---

Visualizar información de ayuda sobre el mensaje de error ANR2535E.

```
help 2535
```

```
Mandato
ANR2535E: no es posible eliminar el nombre del nodo ni cambiarle el nombre
porque tiene un transportador de datos
asociado.
Explicación: ha intentado eliminar o cambiar el nombre de un nodo
que tiene un
transportador de datos asociado.
Acción del sistema: el servidor no elimina ni cambia el nombre
del nodo.
Respuesta del usuario: para eliminar o cambiar el nombre del nodo,
elimine el transportador de datos
asociado y vuelva a emitir
el comando.
```

## Ejemplo: visualizar ayuda para una opción específica

---

Visualizar la descripción, la sintaxis y un ejemplo de la opción de servidor COMMMETHOD.

```
help commmethod
```

## Ejemplo: visualizar ayuda para un programa de utilidad específico

---

Visualizar la descripción, la sintaxis y un ejemplo del programa de utilidad DSMSERV.

```
help dsmserv
```

# IDENTIFY DUPLICATES (Identificar datos duplicados en una agrupación de almacenamiento)

---

Utilice este comando para iniciar o detener procesos que identifiquen datos duplicados en una agrupación de almacenamiento. Puede especificar el número de proceso de identificación de duplicados y su duración.

Cuando cree una nueva agrupación de almacenamiento para la eliminación de datos duplicados, puede especificar entre 0 y 50 procesos de identificación de duplicados. IBM Spectrum Protect inicia el número especificado de procesos de identificación de duplicados automáticamente, cuando se inicia el servidor. Si no los detiene, éstos se ejecutarán indefinidamente.

Este mandato solo afecta al proceso de eliminación de duplicados del lado del servidor. En el proceso de eliminación de datos duplicados del lado del cliente, los duplicados se identifican en el cliente de copia de seguridad y archivado.

Con el mandato IDENTIFY DUPLICATES puede iniciar procesos adicionales, detener algunos o todos los procesos y especificar la cantidad de tiempo que el cambio ha de permanecer en vigor. Si ha aumentado o disminuido el número de procesos de identificación de duplicados, puede utilizar el mandato IDENTIFY DUPLICATES para restablecer el número de procesos en el número especificado en la definición de agrupación de almacenamiento.

Si no ha especificado ningún proceso de identificación de duplicados en la definición de la agrupación de almacenamiento, puede utilizar el comando IDENTIFY DUPLICATES para iniciar y detener todos los procesos manualmente.

Este comando inicia y detiene un proceso o procesos subordinados que puede cancelar con el comando CANCEL PROCESS. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

Importante:

- También puede cambiar el número de procesos de identificación de duplicados mediante la actualización de la definición de agrupación de almacenamiento ejecutando el mandato UPDATE STGPOOL. No obstante, cuando actualice una definición de agrupación de almacenamiento, no puede especificar una duración. Los procesos que especifica en la definición de agrupación de almacenamiento se ejecutan indefinidamente, o hasta que emite el mandato IDENTIFY DUPLICATES, vuelve a actualizar la definición de agrupación de almacenamiento o cancela un proceso.

La emisión de IDENTIFY DUPLICATES no cambia el valor del número de procesos de identificación de duplicados en la definición de la agrupación de almacenamiento.

- Los procesos de identificación de duplicados pueden estar activos o inactivos. Los procesos que eliminan los duplicados de archivos están activos. Los procesos que esperan a que se eliminen los archivos duplicados están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. Los procesos sólo finalizan cuando se cancelan o cuando se cambia el número de procesos de identificación de duplicados para la agrupación de almacenado a un valor inferior al valor especificado. Antes de que se detenga un proceso de identificación de duplicados, éste debe finalizar el archivo cuyos duplicados está eliminando.

La salida del comando QUERY PROCESS para un proceso de identificación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de identificación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es nueve.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-IDentify DUPLicates--nombre_agrupación_almacenamiento----->
>--+-----+--+-----+-----><
  '-NUMPRocess----number-' '-DURation----minutos-'
```

## Parámetros

---

nombre\_agrupación\_almacenamiento (Necesario)

Especifica el nombre de la agrupación de almacenamiento en la que han de identificarse los datos de duplicados. Puede utilizar comodines.

NUMPRocess

Especifica el número de procesos de identificación de duplicados que deben ejecutarse después de que termine de ejecutarse el mandato. Puede especificar entre 0 y 50 procesos. El valor que especifique para este parámetro alterará temporalmente el valor que se ha especificado en la definición de la agrupación de almacenamiento o el valor más reciente que se ha especificado al emitir este mandato por última vez. Si especifica cero, todos los procesos de identificación de duplicados finalizarán.

Este parámetro es opcional. Si no especifica ningún valor, el servidor iniciará o detendrá los procesos de identificación de duplicados para que el número de procesos sea igual al número especificado en la definición de la agrupación de almacenamiento.

Por ejemplo, imaginemos que define una nueva agrupación de almacenamiento y que especifica dos procesos de identificación de duplicados. Posteriormente, emite el mandato IDENTIFY DUPLICATES para incrementar el número de procesos a cuatro. Cuando vuelva a emitir el mandato IDENTIFY DUPLICATES sin especificar ningún valor para el parámetro NUMPROCESS, el servidor detendrá dos procesos de identificación de duplicados.

Si ha especificado cero procesos al definir la agrupación de almacenamiento y emite IDENTIFY DUPLICATES sin especificar un valor para NUMPROCESS, todos los procesos de identificación de duplicados que están en ejecución se detendrán y el servidor no empezará ningún proceso nuevo.

Recuerde: Si especifica IDENTIFY DUPLICATES sin indicar un valor para NUMPROCESS, el parámetro DURATION no estará disponible. Los procesos de identificación de duplicados especificados en la definición de agrupación de almacenamiento se ejecutan indefinidamente, o hasta que vuelve a emitir el mandato IDENTIFY DUPLICATES, actualiza la definición de la agrupación de almacenamiento o cancela un proceso.

Cuando el servidor detiene un proceso de identificación de duplicados, el proceso completa el archivo físico actual y, a continuación, finaliza. Como consecuencia, puede tardar varios minutos en alcanzar el número de procesos de identificación de duplicados que especificó como valor para este parámetro.

#### DURation

Especifica el número máximo de minutos (1 - 9999) que este mandato deberá permanecer en vigor. Al final del tiempo especificado, el servidor iniciará o finalizará los procesos de identificación de duplicados para que el número de procesos sea el mismo que el número especificado en la definición de la agrupación de almacenamiento.

Este parámetro es opcional. Si no especifica un valor, los procesos que se ejecutan después de emitir el mandato, lo harán indefinidamente. Sólo finalizarán si vuelve a emitir el mandato IDENTIFY DUPLICATES, actualiza la definición de la agrupación de almacenamiento o cancela un proceso.

Por ejemplo, si define una agrupación de almacenamiento con dos procesos de identificación de duplicados y emite el mandato IDENTIFY DUPLICATES con DURATION=60 y NUMPROCESS=4, el servidor iniciará dos procesos de identificación de duplicados adicionales que se ejecutarán durante sesenta minutos. Una vez transcurrido este tiempo, dos procesos finalizarán los archivos en los que están trabajando y se detendrán. Los dos procesos que se detienen podrían no ser los dos mismos procesos que se han iniciado como resultado de la emisión de este mandato.

El servidor finalizará primero los procesos inactivos. Si, después de finalizar todos los procesos inactivos, es preciso finalizar más procesos, el servidor lo notificará a los procesos activos que deben finalizar.

Cuando el servidor detiene un proceso de identificación de duplicados, el proceso completa el archivo físico actual y, a continuación, finaliza. Como consecuencia, puede tardar varios minutos en llegar a la cantidad de tiempo especificada como valor para este parámetro.

## Ejemplo: controlar el número y la duración de los procesos de identificación de duplicados

En este ejemplo, ha especificado tres procesos de identificación de duplicados en la definición de la agrupación de almacenamiento. El comando IDENTIFY DUPLICATES se usa para cambiar el número de procesos y especificar la cantidad de tiempo que permanecerá en vigor el cambio.

Tabla 1. Control manual de los procesos de identificación de duplicados

<b>La definición de la agrupación de almacenamiento especifica tres procesos de identificación de duplicados. Con el comando IDENTIFY DUPLICATES, especifica...</b>	<b>...y una duración de...</b>	<b>El resultado es...</b>
---	--------------------------------	---------------------------

La definición de la agrupación de almacenamiento especifica tres procesos de identificación de duplicados. Con el comando IDENTIFY DUPLICATES, especifica...	...y una duración de...	El resultado es...
2 procesos de identificación de duplicados	No se especifica	Un proceso de identificación de duplicados finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. Dos procesos se ejecutan indefinidamente, o hasta que vuelva a emitir el mandato IDENTIFY DUPLICATES, actualice la definición de la agrupación de almacenamiento o cancele un proceso.
	60 minutos	Un proceso de identificación de duplicados finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. Transcurridos 60 minutos, el servidor inicia un proceso para que existan tres procesos en ejecución.
4 procesos de identificación de duplicados	No se especifica	El servidor inicia un proceso de identificación de duplicados. Cuatro procesos se ejecutan indefinidamente, o hasta que vuelva a emitir el comando IDENTIFY DUPLICATES, actualice la definición de la agrupación de almacenamiento o cancele un proceso.
	60 minutos	El servidor inicia un proceso de identificación de duplicados. Transcurridos los 60 minutos, un proceso finaliza el archivo en el que está trabajando, si lo hay, y, a continuación, se detiene. El proceso adicional que ha iniciado este comando podría no ser uno de los que han de detenerse cuando haya transcurrido la duración indicada.
0 procesos de identificación de duplicados	No se especifica	Todos los procesos de identificación de duplicados finalizan los archivos en los que están trabajando, si los hay, y se detienen. Este cambio dura indefinidamente o hasta que pueda volver a emitir el comando IDENTIFY DUPLICATES, actualizar la definición de la agrupación de almacenamiento o cancelar un proceso.
	60 minutos	Todos los procesos de identificación de duplicados finalizan los archivos en los que están trabajando, si los hay, y se detienen. Transcurridos los sesenta minutos, el servidor inicia tres procesos.
No se especifica	No disponible	El número de procesos de identificación de duplicados se restablece en el número de procesos especificado en la definición de la agrupación de almacenamiento. Este cambio dura indefinidamente o hasta que pueda volver a emitir el mandato IDENTIFY DUPLICATES, actualizar la definición de la agrupación de almacenamiento o cancelar un proceso.

## Ejemplo: identificar duplicados en una agrupación de almacenamiento

Identifique duplicados en una agrupación de almacenamiento, STGPOOLA, utilizando tres procesos de identificación de duplicados. Especificar que este cambio permanezca en vigor durante 60 minutos.

```
identify duplicates stgpoola duration=60 numprocess=3
```

## Comandos relacionados

Tabla 2. Comandos relacionados con IDENTIFY DUPLICATES

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.

Comando	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## Comandos IMPORT

Utilice los mandatos IMPORT para importar información desde los medios de exportación a un servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

- IMPORT ADMIN (Importar información del administrador)
- IMPORT NODE (Importar información de nodos clientes)
- IMPORT POLICY (Importar información de políticas)
- IMPORT SERVER (Importar información del servidor)

## IMPORT ADMIN (Importar información del administrador)

Utilice este comando para importar definiciones de administrador y de autorización para uno o varios administradores del medio de exportación al servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Puede utilizar el mandato QUERY ACTLOG para ver el estado de la operación de importación.

También puede ver esta información desde la consola del servidor.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

Este comando genera un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Si se cancela el proceso subordinado IMPORT ADMIN, ya están importados algunos datos. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Restricción:

- Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
- Si la definición del administrador que se importa incluye autorización de analista, se importa la definición del administrador pero no así la autorización de analista. La autorización de analista no es válida para servidores con la versión 6.1 o superior.
- No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

      .-*-----*.
>>-Import Admin-----+----->
      | .-,-----|. |
      | V           | |
      |---nombre_admin-+-'

.-Preview ----No-----
>+-----+----->
  '-Preview-----+No-+-'
    '-Yes-'

>--DEVclass-----nombre_clase_dispositivo----->

      .-,-----|.
      | V           |
>--VOLumentname-----+---nombre_volumen+-----+----->
      '-FILE:--nombre_archivo-'

.-Replacedefs-----No-----
>+-----+-----><
  '-Replacedefs-----+No-+-'
    '-Yes-'

```

## Parámetros

### nombre\_admin

Especifica los administradores para los que desea importar la información. Este parámetro es opcional. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

### Preview

Especifica si desea previsualizar el resultado de la operación de importación, sin importar la información de administrador. Este parámetro es opcional. Los siguientes valores de parámetro están soportados:

#### No

Especifica que se ha de importar la información.

#### Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información sobre el número y tipos de objetos importados, junto con el número de bytes transferidos se pasa a la consola del servidor y a los registros de actividades.

El valor predeterminado es NO. Si especifica YES en el valor, deberá montar los volúmenes de exportación.

### DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación.

No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

### VOLumentname (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Los siguientes valores de parámetro están soportados:

#### nombre\_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.










#### FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.



Para este dispositivo	Especifique
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux/imdata/mt1.  Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsREMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

#### Replacedefs

Especifica si se sustituirán las definiciones de administrador ya existentes en el servidor de destino. Los siguientes valores de parámetro están soportados:

No

Especifica que no se sustituirán las definiciones.

Yes

Especifica que se sustituirán las definiciones.

El valor predeterminado es NO.

## Ejemplo: importar información de administrador de volúmenes de cinta específicos

Desde el servidor, importar la información de todos los administradores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando:

```
import admin devclass=menu1
volumenames=tape01,tape02,tape03
```

## Ejemplo: importar información del administrador desde los volúmenes de cinta que se indican en un archivo

Desde el servidor, importe la información para todos los administradores definidos a los volúmenes de cintas que figuran en el archivo siguiente:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
-  Sistemas operativos WindowsTAPEVOL.DATA

Este archivo contiene estas líneas:

```
TAPE01
TAPE02
TAPE03
```

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. Emita el comando:

 Sistemas operativos AIX  Sistemas operativos Linux

```
import admin devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import admin devclass=menu1 volumenames=file:tapevol.data
```

## Comandos relacionados

Tabla 1. Comandos relacionados con IMPORT ADMIN

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT ADMIN	Copia información administrativa en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.

Comando	Descripción
IMPORT POLICY	Restaura información de políticas desde medio externo.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## IMPORT NODE (Importar información de nodos clientes)


Utilice este comando para importar definiciones de nodos clientes desde un servidor o un medio secuencial a un servidor de IBM Spectrum Protect de destino.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Si especifica un dominio en el servidor de origen y si ese dominio de políticas también existe en el servidor de destino, los nodos importados se asocian con ese mismo dominio de políticas en el servidor de destino. De lo contrario, los nodos importados se asocian al dominio de políticas STANDARD en el servidor de destino.

Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Restricciones:

1. Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
2. No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.
3. Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores de destino deben estar configurados para las contraseñas de LDAP. Los datos que se importan desde un nodo que se autentica con un servidor de directorios LDAP no son accesibles si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos importados desde un nodo de LDAP todavía pueden seguir allí. Sin embargo, el servidor de destino debe estar configurado para que utilice LDAP con el fin de acceder a los datos importados.
4. Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
5. No se puede utilizar una clase de dispositivo CENTERA como el soporte de destino para un mandato de exportación, o como el medio de origen para un mandato de importación.
6. No se admite la importación o exportación incrementales de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
  - Copias de seguridad de VMware donde deben transferirse periódica e incrementalmente copias de seguridad completas e incrementales a otro servidor.
  - Grupos de copias de seguridad donde deben transferirse periódica e incrementalmente copias de seguridad completas y diferenciales a otro servidor.
  -  Sistemas operativos Windows Datos de Windows System State que se transfieren periódica e incrementalmente a otro servidor.

La exportación/importación completa de estos datos a un nuevo sistema de archivos en el destino está soportada si se exporta el espacio de archivos completo que contiene los datos. Es decir, la exportación no debe utilizar las opciones *FILEDATA=ALLACTIVE*, *FROMDATE*, *TODATE* o *MERGEFILESPPACES*.

La práctica recomendada para transferir incrementalmente este tipo de datos entre dos servidores es utilizar la réplica de nodo.

Puede utilizar el comando QUERY ACTLOG para ver el estado de la operación de importación. También puede ver esta información desde la consola del servidor.

Este comando genera un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Si se cancela un proceso subordinado IMPORT NODE, puede que algunos de los datos ya se hayan importado. Para que se visualice información acerca de los procesos subordinados, utilice el comando QUERY PROCESS.

Para un servidor que tenga clientes que admitan Unicode, puede conseguir que el servidor convierta el nombre de espacio de archivos que especifique, o bien utilizar los parámetros siguientes:

- HEXFILESPPACE
- UNIFILESPPACE

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

.<!--*----->
>>-IMport Node----->
| .-,-----|
| v          ||
|'---nombre_nodo+-'
>+----->
| .-,-----|
| v          ||
|'-FILESpace-----nombre_espacio_archivos+-'
>+----->
| .-,-----|
| v          ||
|'-HEXFILESpace-----nombre_espacio_archivos+-'
>+----->
| .-,-----|
| v          ||
|'-UNIFILESpace-----nombre_espacio_archivos+-'
>+----->
| .-,-----|
| v          ||
|'-DOfains-----nombre_dominio+-'
.<!--FILEData-----None-----> .<!--Preview -----No----->
>+----->
|'-FILEData-----+ALL-----+| '-Preview-----+No--+|
| +None-----+ | -Yes-|
| +ARChive-----+
| +Backup-----+
| +BACKUPActive+
| +ALLActive----+
|'-SPacemanaged-'
>>-DEVclass-----nombre_clase_dispositivo----->
.<!--Dates-----Absolute----->
>+----->
|'-Dates-----+Absolute+-'
|'-Relative-'
.<!--,----->
| v          |
>>-VOLumenames-----+---nombre_volumen+-----+----->
|'-FILE:--nombre_archivo-'
.<!--Replacedefs-----No----->
>+----->
|'-Replacedefs-----+No--+|
|'-Yes-|
.<!--MERGEfilespace-----No----->
>+----->
|'-MERGEfilespace-----+No--+|
|'-Yes-|

```

```

.-PROXynodeassoc-----No-----
>-----+-----+-----><
'-PROXynodeassoc-----+No--+-'
      '-Yes-'

```

## Parámetros

### nombre\_nodo

Especifica los nodos cliente para los que desea importar la información. Este parámetro es opcional.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Se incluirán en la lista todos los nodos que coincidan.

### FILESpace

Especifica los nombres de espacios de archivos para los que desea importar la información. Este parámetro es opcional. El valor predeterminado es especificar todos los espacios de archivos.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

Importante:

1. No se sustituirán los espacios de archivos existentes. Se crearán espacios de archivos nuevos cuando se encuentren nombres idénticos. Sin embargo, es posible que este nuevo nombre coincida con un nombre existente en el nodo de cliente que puede disponer de espacios de archivos de los que aún no se ha hecho una copia de seguridad en el servidor.
2. Sólo puede especificarse este parámetro para espacios de archivos que no son Unicode. Para importar todos los espacios de archivos Unicode y no Unicode, utilice el parámetro FILEDATA=ALL sin los parámetros FILESPACE y UNIFILESPACE.

### DOMains

Especifica los dominios de políticas desde donde debe importarse información de nodos. Estos dominios deben estar incluidos en los datos exportados. Este parámetro es opcional. El valor predeterminado es especificar todos los dominios exportados.

Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre.

### FILEData

Especifica el tipo de los archivos que deben importarse para todos los nodos encontrados en el medio de exportación. Este parámetro es opcional. El valor predeterminado es NONE.

Si está importando desde un medio secuencial, la clase de dispositivo que utilizan los datos de archivos determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este comando, se necesitan dos unidades para importar la información del nodo. El límite de montaje para la clase de dispositivo debe ser como mínimo 2.

Las descripciones siguientes mencionan las copias de archivos de copia de seguridad *activas* e *inactivas*. Una copia de archivo de copia de seguridad activa es la copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás copias de archivo de copia de seguridad se denominan copias inactivas. Los valores que puede tener el parámetro son:

#### ALL

El servidor importa todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management. Los espacios de archivos que están incluidos son Unicode y no Unicode.

#### None

Sólo se importan las definiciones de nodos. El servidor no importa archivos.

#### ARchive

El servidor sólo importa las copias archivadas.

#### Backup

El servidor sólo importa las versiones de copia de seguridad, ya sean activas o inactivas.

#### BACKUPActive

El servidor sólo importa las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando IMPORT.

#### ALLActive

El servidor importa todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando IMPORT.

#### SPacemanaged

El servidor solo importa los archivos que ha migrado un cliente de IBM Spectrum Protect for Space Management.

#### Preview

Especifica si se previsualiza el resultado de la operación de importación, sin importar la información. La opción PREVIEW=YES exige que se monten los volúmenes de exportación. Los valores siguientes están soportados:

No

Especifica que se ha de importar la información de nodos.

Yes

Especifica que desea previsualizar el resultado de la operación de importación, sin importar los archivos. La información se notifica a la consola del servidor y a las anotaciones de actividades.

Este parámetro es opcional. El valor predeterminado es NO.

#### DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si al ejecutarse la importación todas las unidades para esta clase de dispositivo están ocupadas, el servidor cancela las operaciones de prioridad inferior, como por ejemplo, identificar duplicados, para que haya una unidad disponible.

#### Dates

Especifica si las fechas para las copias de archivos se establecen como la misma fecha cuando se exportaron los archivos, o se ajustan a la fecha de importación.

Este parámetro admite los valores siguientes:

Absolute

Las fechas de las copias de archivos se establecen en los valores especificados al exportarse los archivos.

Relative

Las fechas de las copias de archivos se ajustan a la fecha de importación.

El valor predeterminado es ABSOLUTE.

Si el medio de exportación está desocupado durante algún tiempo después de la exportación, por ejemplo, si permanece sobre una estantería durante seis meses, la copia original o las fechas de archivado pueden ser lo suficientemente antiguas como para desencadenar que las copias de archivo caduquen inmediatamente cuando los datos se importen a un servidor. La especificación RELATIVE de este valor se ajustará al tiempo transcurrido desde la exportación, de modo que las copias de los archivos no caduquen de forma inmediata.

Por ejemplo, supongamos que una cinta de exportación contiene una copia archivada realizada cinco días antes de la operación de exportación. Si el medio se ha guardado durante seis meses y luego se importa, el archivo de archivado aparecerá de forma predeterminada como insertada hace seis meses y cinco días (DATES=ABSOLUTE) y puede caducar inmediatamente dependiendo del valor de retención que se especifica en la clase de gestión del archivo. Especificando DATES=RELATIVE da como resultado el restablecimiento de la fecha de archivado para el archivo a hace cinco días durante la importación. De este modo, el parámetro DATES=RELATIVE ajusta las fechas de las copias archivadas y copias de seguridad en el tiempo transcurrido desde que se ha producido la operación de exportación.

#### VOLumenames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Los valores que puede tener el parámetro son:

nombre\_volumen

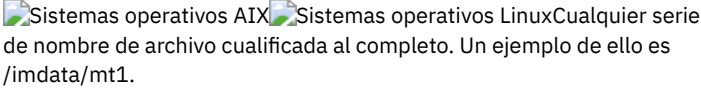





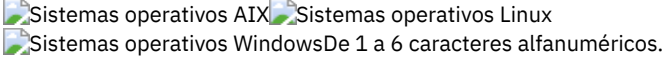


Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.

Para este dispositivo	Especifique
FILE	 Sistemas operativos AIX,  Sistemas operativos Linux Cualquier serie de nombre de archivo cualificada al completo. Un ejemplo de ello es /imdata/mt1.   Sistemas operativos Windows Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo, d:\Archivos de programa\tivoli\tsm\data1.dsm.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVABLEFILE	 Sistemas operativos AIX,  Sistemas operativos Linux  Sistemas operativos Windows De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

#### Replacedefs

Especifica si se sustituirán las definiciones del servidor destino. El valor predeterminado es NO. Los valores que puede tener el parámetro son:

No

Los objetos no se sustituyen.

Yes

Los objetos se sustituyen.

#### HEXFILESpace

Especifica la representación hexadecimal de los nombres de espacio de archivos en formato UTF-8. Puede separar varios nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Para visualizar la representación hexadecimal de un nombre de espacio de archivos, puede utilizar el comando QUERY FILESPACE con FORMAT=DETAILED.

#### UNIFILESpace

Especifica que los espacios de archivos que son conocidos por el servidor están activados para Unicode. El servidor convierte los nombres que se especifican de la página de códigos del servidor a la página de códigos UTF-8 para encontrar los espacios de archivos que deben importarse. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizarse un carácter comodín para especificar un nombre. Este parámetro es opcional.

#### MERGEfilespaces

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. El valor predeterminado es NO.

Los valores válidos son:

Yes

Especifica que los datos importados en el servidor de destino se añaden al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino, si existen espacios de archivos con el mismo nombre.

#### PROXynodeassoc



Especifica si se importan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.


## Ejemplo: importar información de nodo cliente desde cintas

Desde el servidor, importar la información de nodo cliente de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import node devclass=menu1 volumenames=tape01,tape02,tape03
```



## Ejemplo: importar información de nodo cliente desde las cintas que se indican en un archivo

 Sistemas operativos AIX,  Sistemas operativos Linux  
Desde el servidor, importar la información de nodo cliente desde los volúmenes de cinta listados en un archivo denominado TAPEVOL.

 Sistemas operativos Windows  
Desde el servidor, importar la información de nodo cliente desde los volúmenes de cinta listados en un archivo denominado TAPEVOL.DATA.

Este archivo contiene estas líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.  Sistemas operativos AIX  
 Sistemas operativos Linux

```
import node devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import node devclass=menu1 volumenames=file:tapevol.data
```

## Ejemplo: importar la copia de seguridad activa para un nodo cliente

Desde el servidor, importe las versiones de copia de seguridad activas de los datos de archivos para el nodo cliente JOE desde el volumen de cinta TAPE01. El espacio de archivos es Unicode.

```
import node joe unificspace=\\joe\c$ filedata=backupactive  
devclass=menu1  
volumenames=tape01
```

## Comandos relacionados

Tabla 1. Comandos relacionados con IMPORT NODE

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT POLICY	Restaura información de políticas desde medio externo.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## IMPORT POLICY (Importar información de políticas)

Utilice este comando para importar información de dominio de políticas del medio de exportación secuencial al servidor de IBM Spectrum Protect. Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Los datos de cliente de IBM Spectrum Protect se pueden traspasar entre servidores de mediante el proceso de exportación e importación, si ambas plataformas admiten el mismo tipo de medio extraíble.

Restricción:

1. Si los niveles del servidor de destino y origen no son compatibles, es posible que la operación de importación no funcione.
2. No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.

Puede utilizar el comando QUERY ACTLOG para ver el estado de la operación de importación. También puede ver esta información desde la consola del servidor.

Este mandato genera un proceso subordinado que puede cancelarse con el mandato CANCEL PROCESS. Si se cancela el proceso subordinado IMPORT POLICY, ya están importados algunos datos. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las

bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

>>-IMport Policy-----
| .-,-----
| V                       |
|'---nombre_dominio--+'
|
.-Preview ---No-----
>+-----
|'-Preview---+No--+'
|'-Yes-'
|
>--DEVclass-----nombre_clase_dispositivo----->
|
.-,-----
| V                       |
>--VOLumentnames-----+---+---+---nombre_volumen+---+----->
|'-FILE:--nombre_archivo-'
|
.-Replacedefs-----No-----
>+-----
|'-Replacedefs-----+No--+'
|'-Yes-'

```

## Parámetros

### nombre\_dominio

Especifica los dominios de políticas para los que se va a importar la información. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. El valor predeterminado (\*) son todas las políticas.

### Preview

Especifica si desea previsualizar el resultado de la operación de importación sin importar la información. Este parámetro admite los valores siguientes:

No

Especifica que se ha de importar la información.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se notifica a la consola del servidor y a las anotaciones de actividades.

La opción PREVIEW=YES exige que se monten los volúmenes de exportación. Este parámetro es opcional. El valor predeterminado es NO.

### DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No es posible especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

### VOLumentnames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Este parámetro admite los valores siguientes:

nombre\_volumen












Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	Cualquier serie de nombre de archivo cualificada al completo. Por ejemplo: <ul style="list-style-type: none"> <li> Sistemas operativos AIX  Sistemas operativos Linux /imdata/mt1</li> <li> Sistemas operativos Windowsd:\archivos de programa\tivoli\tsm\data1.dsm.</li> </ul>
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsREMOVABLEFILE	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsDe 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

Replacedefs

Especifica si se sustituirán las definiciones de política del servidor destino. Este parámetro admite los valores siguientes:

Yes

Especifica que se han de sustituir los objetos por objetos importados.

No

Especifica que no se han de sustituir los objetos por objetos importados.

El valor predeterminado es NO.

## Ejemplo: importar información de política desde volúmenes de cinta específicos

Desde el servidor, importar la información de todas las políticas definidas de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import policy devclass=menu1
volumenames=tape01,tape02,tape03
```

## Ejemplo: importar información de política desde los volúmenes de cinta que se indican en un archivo

Desde el servidor, importe la información de todas las políticas definidas desde los volúmenes de cinta que se indican en un archivo denominado de la siguiente manera:

-  Sistemas operativos AIX  Sistemas operativos LinuxTAPEVOL
- TAPEVOL.DATA

Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo contiene las líneas siguientes:

```
TAPE01
TAPE02
TAPE03
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
import policy devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

```
import policy devclass=menu1 volumenames=file:tapevol.data
```

Tabla 1. Comandos relacionados con IMPORT POLICY

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
EXPORT POLICY	Copia información de políticas en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## IMPORT SERVER (Importar información del servidor)

Utilice este mandato para copiar toda o parte de la información de control del servidor y datos de archivo del cliente especificado del medio de exportación al servidor de IBM Spectrum Protect.

Importante: Para los mandatos que importan administradores o nodos, se debe tener en cuenta el método de autenticación. El servidor de IBM Spectrum Protect no puede exportar o importar las contraseñas de los nodos o administradores que se autentican con los servidores de directorios LDAP. Si el método de autenticación actual utiliza un servidor de directorio LDAP y la contraseña no está sincronizada por ese servidor, debe actualizar la contraseña. Después de emitir el mandato IMPORT, establezca la contraseña emitiendo el mandato UPDATE ADMIN o UPDATE NODE.

Los servidores de IBM Spectrum Protect que tienen la protección de retención activada no permiten las operaciones de importación.

Restricciones:

- Si los niveles del servidor destino y origen no son compatibles, es posible que la operación no funcione.
- No se admite importar datos desde una clase de dispositivo CENTERA. Sin embargo, los archivos que se importan se pueden almacenar en un dispositivo de almacenamiento CENTERA.
- Si utiliza un servidor de directorios LDAP para autenticar las contraseñas, los servidores de destino deben estar configurados para las contraseñas de LDAP. Los datos del servidor que se exportan desde un nodo que se autentica con un servidor de directorios LDAP no son accesible si el servidor de destino no está configurado correctamente. Si su servidor de destino no está configurado, los datos exportados desde un nodo de LDAP todavía pueden seguir allí. Sin embargo, el servidor de destino debe estar configurado para que utilice LDAP con el fin de acceder a los datos.
- No se admite la exportación o importación incremental de los siguientes tipos de datos de cliente a otro servidor de IBM Spectrum Protect:
  - Las copias de seguridad de VMware en las que las copias de seguridad completas más las incrementales deben realizarse periódicamente y transferirse de forma incremental a otro servidor.
  - Los grupos de copias de seguridad en los que las copias de seguridad completas más las diferenciales deben realizarse periódicamente y transferirse de forma diferencial a otro servidor.
  - Los datos de estado del sistema de Windows que se transfieren de forma periódica e incremental a otro servidor

Se da soporte a la exportación o importación de estos datos a un nuevo sistema de archivos en el destino mediante la exportación del espacio de archivos completo que contiene los datos. La exportación no debe utilizar los parámetros FILEDATA=ALLACTIVE, FROMDATE, TODATE o MERGEFILESACES.

La utilización de la réplica de nodo en la transferencia incremental de este tipo de datos de cliente entre dos servidores es opcional.

También puede iniciar un proceso de importación de la información del servidor y los datos de archivo de cliente directamente desde el servidor de origen. Para obtener más información, consulte los comandos EXPORT.

Este comando genera un proceso subordinado que puede cancelarse con el comando CANCEL PROCESS. Si se cancela un proceso subordinado IMPORT SERVER, parte de los datos ya se habrán importado. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Limitación: El servidor de IBM Spectrum Protect no convierte páginas de código durante la exportación, importación ni durante las operaciones de réplica de nodos. Si los servidores se ejecutan en entornos locales diferentes, puede que parte de la información de las

bases de datos o de salida del sistema sea ilegible. Es posible que se muestren caracteres no válidos, por ejemplo, en la información de contacto para los nodos de cliente y administrador y en descripciones de dominios de política. Se puede ver afectado cualquier campo que esté almacenado en el juego de caracteres del servidor y que incluya caracteres ASCII extendidos. Para resolver el problema, después de la operación de réplica de nodo o la importación, actualice los campos con los comandos UPDATE adecuados. La limitación del servidor no afecta a los datos del cliente. Todos los datos de cliente que se exportaron, importaron o duplicaron se pueden restaurar, recuperar.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

>>-Import Server .-FILEData----None-----+----->
                '-FILEData----+ALL-----+'
                    +-None-----+
                    +-ARchive-----+
                    +-Backup-----+
                    +-BACKUPActive-+
                    +-ALLActive----+
                    '-SPacemanaged-'

.-Preview ----No-----+----->
>--+-----+-----+-----+----->
  '-Preview----+No--+-'
                    '-Yes-'

>--DEVclass----nombre_clase_dispositivo----->

.-Dates----Absolute-----+----->
>--+-----+-----+-----+----->
  '-Dates----+Absolute--+-'
                    '-Relative-'

                .-,-----+-----+----->
                v          |
>--VOLumenames----+-----nombre_volumen-+-----+----->
                '-FILE:--nombre_archivo-'

.-Replacedefs----No-----+----->
>--+-----+-----+-----+----->
  '-Replacedefs----+No--+-'
                    '-Yes-'

.-MERGEfilespace----No-----+----->
>--+-----+-----+-----+----->
  '-MERGEfilespace----+No--+-'
                    '-Yes-'

.-PROXynodeassoc----No-----+----->
>--+-----+-----+-----+-----><
  '-PROXynodeassoc----+No--+-'
                    '-Yes-'

```

## Parámetros

### FILEData

Especifica el tipo de archivos que deben importarse para todos los nodos definidos en el servidor. Este parámetro es opcional. El valor predeterminado es NONE.

La clase de dispositivo utilizada para acceder a los datos de archivos la determina la clase de dispositivo de la agrupación de almacenamiento. Si es la misma clase de dispositivo especificada en este comando, se necesitan dos unidades para importar la información. El límite de montaje para la clase de dispositivo debe establecerse como mínimo en 2.

Las descripciones siguientes mencionan las copias de archivos de copia de seguridad activas e inactivas. Una copia de archivo de copia de seguridad activa es la copia de seguridad más reciente de un archivo que todavía existe en la estación de trabajo cliente. Todas las demás copias de archivo de copia de archivo se denominan copias inactivas. Este parámetro admite los valores siguientes:

ALL

IBM Spectrum Protect importa todas las versiones de copia de seguridad de los archivos, todas las copias archivadas y todos los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management.

None

IBM Spectrum Protect no importa archivos, sólo las definiciones de los nodos.

ARchive

IBM Spectrum Protect sólo importa las copias archivadas.

Backup

IBM Spectrum Protect sólo importa las versiones de copia de seguridad, ya sean versiones activas o inactivas.

BACKUPActive

IBM Spectrum Protect sólo importa las versiones de copia de seguridad activas. Estas versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando IMPORT.

ALLActive

IBM Spectrum Protect importa todas las versiones de copia de seguridad activa de los archivos, todas las copias archivadas y todos los archivos que se han migrado con el cliente de IBM Spectrum Protect for Space Management. Las versiones de copia de seguridad activas son las versiones activas de la base de datos de IBM Spectrum Protect en el momento en que se emite el comando IMPORT.

SPacemanaged

IBM Spectrum Protect importa solo los archivos que se han migrado con un cliente de IBM Spectrum Protect for Space Management.

Preview

Especifica si se previsualiza el resultado de la operación de importación, sin importar la información. Este parámetro admite los valores siguientes:

No

Especifica que se ha de importar la información del servidor.

Yes

Especifica que se previsualizará la operación pero no se ejecutará. La información se transfiere a la consola del servidor y a las anotaciones de actividades.

Este parámetro es opcional. El valor predeterminado es NO. Si se especifica la opción PREVIEW=YES, deberá montar los volúmenes de exportación.

DEVclass (Necesario)

Especifica la clase de dispositivo donde se han de leer los datos de importación. No se pueden especificar las clases de dispositivo DISK, NAS o CENTERA.

Si todas las unidades para esta clase de dispositivo están ocupadas al ejecutarse la importación, IBM Spectrum Protect cancela las operaciones con prioridad más baja, como por ejemplo, de reclamación, para que haya una unidad disponible.

Dates

Especifica si las fechas para las copias de archivos se establecen como la misma fecha cuando se exportaron los archivos, o se ajustan a la fecha de importación.

Si el medio de importación está desocupado durante algún tiempo después de la exportación, por ejemplo, si permanece sobre una estantería durante seis meses, la copia original o las fechas de archivado pueden ser lo suficientemente antiguas como para desencadenar que las copias de archivo caduquen inmediatamente cuando los datos se importen a un servidor. La especificación RELATIVE de este valor se ajustará al tiempo transcurrido desde la exportación, de modo que las copias de los archivos no caduquen de forma inmediata.

Por ejemplo, supongamos que una cinta de importación contiene una copia archivada realizada cinco días antes de la operación de exportación. Si el medio de exportación se ha guardado durante seis meses y luego se importa, el archivo de archivado aparecerá de forma predeterminada como insertada hace seis meses y cinco días (DATES=ABSOLUTE) y puede caducar inmediatamente dependiendo del valor de retención que se especifica en la clase de gestión del archivo. Especificando DATES=RELATIVE da como resultado el restablecimiento de la fecha de archivado para el archivo a hace cinco días durante la importación. De este modo, el parámetro DATES=RELATIVE ajusta las fechas de las copias archivadas y copias de seguridad en el tiempo transcurrido desde que se ha producido la operación de exportación.

Este parámetro admite los valores siguientes:

Absolute

Las fechas de las copias de archivos se establecen en los valores especificados al exportarse los archivos.

Relative

La fecha de las copias de archivos se ajustan a la fecha de importación.

El valor predeterminado es ABSOLUTE.

## VOLumenames (Obligatorio)

Especifica los volúmenes que se utilizarán para la operación de importación. Los volúmenes se deben importar en el mismo orden en el que se han exportado. Este parámetro admite los valores siguientes:

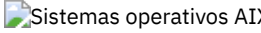
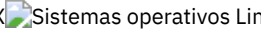
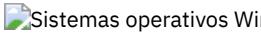
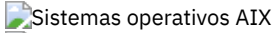
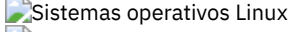
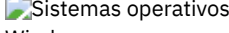
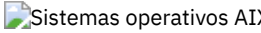
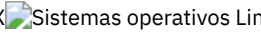
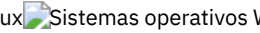
### nombre\_volumen

Especifica el nombre del volumen. Para especificar varios volúmenes, debe separar los nombres con comas y sin espacios intercalados.

### FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de volúmenes que se utiliza para los datos importados. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y las líneas de comentarios que comienzan por un asterisco.

Utilice estos convenios de denominación para especificar los volúmenes que están asociados con los tipos de dispositivo siguientes:

Para este dispositivo	Especifique
Cinta	De 1 a 6 caracteres alfanuméricos.
FILE	  Cualquier serie de nombre de archivo o volumen cualificada al completo. Un ejemplo de ello es /imdata/mt1.  Cualquier serie de nombre de archivo o volumen cualificada al completo. Por ejemplo, d:\Archivos de programa\tivoli\tsm\data1.dsm.
   REMOVABLEFILE	   De 1 a 6 caracteres alfanuméricos.
SERVER	De 1 a 250 caracteres alfanuméricos.

## Replacedefs

Especifica si se sustituirán los objetos del servidor. No se sustituirán los espacios de archivos existentes. Se crearán espacios de archivos nuevos cuando se encuentren nombres idénticos. Este parámetro admite los valores siguientes:

### No

Especifica que no se han de sustituir los objetos por objetos importados.

### Yes

Especifica que se han de sustituir los objetos por objetos importados.

El valor predeterminado es NO.

## MERGEfilespaces

Especifica si IBM Spectrum Protect añade los archivos de cliente a los espacios de archivos existentes en el servidor de destino (si existen), o bien si IBM Spectrum Protect genera nombres nuevos de espacios de archivos. No puede fusionar espacios de archivo no Unicode y Unicode de forma conjunta. Este parámetro admite los valores siguientes:

### No

Especifica que IBM Spectrum Protect genera un nombre nuevo de espacio de archivos para los datos importados en el servidor de destino si existen espacios de archivos con el mismo nombre.

### Yes

Especifica que los datos importados en el servidor de destino se agregan al espacio de archivos existente, si un espacio de archivos con el mismo nombre existe en el servidor de destino.

El valor predeterminado es NO.

## PROXynodeassoc

Especifica si se importan asociaciones de nodos proxy. Este parámetro es opcional. El valor predeterminado es NO.

## Ejemplo: importar información de todos los servidores definidos desde cintas específicas

Desde el servidor, importar la información de todos los servidores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1.

```
import server devclass=menu1 volumenames=tape01,tape02,tape03
```

## Ejemplo: importar información de todos los servidores definidos desde cintas específicas y especificar que los archivos han de fusionarse en los espacios de archivos existentes

Desde el servidor, importar la información de todos los servidores definidos de los volúmenes de cinta TAPE01, TAPE02 y TAPE03. Especifique que un dispositivo asignado a la clase de dispositivo MENU1 pueda leer estos volúmenes de cinta y que los archivos de cliente se combinen en espacios de archivo del servidor destino si existen espacios de archivos de los mismos nombres.


```
import server devclass=menu1 volumenames=tape01,tape02,tape03
mergefilespace=yes
```

## Ejemplo: importar información de todos los servidores definidos desde las cintas que se indican en un archivo

Desde el servidor, importar la información de todos los servidores definidos desde los volúmenes de cinta que se indican en el archivo denominado TAPEVOL. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo de entrada contiene estas líneas:

```
TAPE01
TAPE02
TAPE03
```

```
import server devclass=menu1 volumenames=file:tapevol
```

 Sistemas operativos Windows

## Ejemplo: importar información de todos los servidores definidos desde las cintas que se indican en un archivo

Desde el servidor, importar la información de todos los servidores definidos desde los volúmenes de cinta que se indican en el archivo denominado TAPEVOL.DATA. Especifique que estos volúmenes de cinta los lea un dispositivo asignado a la clase de dispositivo MENU1. El archivo de entrada contiene estas líneas:

```
TAPE01
TAPE02
TAPE03
```

```
import server devclass=menu1 volumenames=file:tapevol.data
```

## Comandos relacionados

Tabla 1. Comandos relacionados con IMPORT SERVER

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT ADMIN	Restaura la información de administración desde medio externo.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT POLICY	Restaura información de políticas desde medio externo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## INSERT MACHINE (Insertar información de características o instrucciones de recuperación)

Utilice este comando para agregar características de máquina cliente o instrucciones de recuperación a la información de la máquina existente en la base de datos.

Puede escribir un programa que lea los archivos que contienen la información y que genere los comandos INSERT MACHINE adecuados.

Puede utilizar los comandos QUERY para recuperar la información en caso de producirse un siniestro.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

---

```
>>-INsert MACHine--machine_name--número_secuencia----->
>--+CHaracteristics---+texto-----+-----><
  '-RECOVERYInstructions---+texto-'
```

### Parámetros

---

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina cliente.

número\_secuencia (Necesario)

Especifica el número de secuencia de la línea de texto de la base de datos.

CHaracteristics

Especifica la información de las características de la máquina. Debe especificar las características o las instrucciones de recuperación, pero no las dos. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. El texto puede tener hasta 1024 caracteres.

RECOVERYInstructions

Especifica las instrucciones de recuperación. Debe especificar las características o las instrucciones de recuperación, pero no las dos. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. El texto puede tener hasta 1024 caracteres.

### Ejemplo: actualizar la información de una máquina

---

Para la máquina DISTRICT5, insertar el texto de las características en la línea 1: "Machine owner is Mary Smith".

```
insert machine district5 1
characteristics="Machine owner is Mary Smith"
```

### Comandos relacionados

---

Tabla 1. Comandos relacionados con INSERT MACHINE

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
QUERY MACHINE	Muestra información sobre máquinas.

#### Información relacionada:

[🔗](#) Especificación de información sobre las máquinas de nodos de cliente y de servidor

## ISSUE MESSAGE (Emitir un mensaje desde un script del servidor)

---

Utilice este comando con el proceso de código de retorno en un script para emitir un mensaje desde un script del servidor para determinar dónde se encuentra el problema con un comando del script.

### Clase de privilegio

---

Cualquier administrador puede emitir este comando.

### Sintaxis

---

```
>>-ISSUE MESSAGE--gravedad_mensaje--texto_mensaje-----><
```

### Parámetros

---

gravedad\_mensaje (Obligatorio)

Especifica la gravedad del mensaje. Los indicadores de gravedad de mensajes son los siguientes:

- I Información. Se visualiza ANR1496I en el texto del mensaje.
- W Avisor. Se visualiza ANR1497W en el texto del mensaje.
- E Error. Se visualiza ANR1498E en el texto del mensaje.
- S Grave. Se visualiza ANR1499S en el texto del mensaje.

texto\_mensaje (Obligatorio)

Especifica la descripción del mensaje.

## Ejemplo: emitir un mensaje desde un script de servidor

Supongamos que tiene un script llamado backupscript que paraliza la base de datos de un cliente, toma una copia de seguridad de dicha base de datos y, a continuación reinicia la base de datos del cliente. A modo de ilustración, el script da como resultado un código de retorno distinto de cero. Utilice el comando ISSUE MESSAGE con la gravedad del mensaje y el texto del mensaje. A continuación se muestra un ejemplo de un script de servidor que llama a backupscript en la máquina cliente y emite mensajes en función del código de retorno de backupscript.

```
issue message i "Starting backup"
define clientaction nodename action=command
objects="c:\backupscript" wait=yes
if (101) goto qfail
if (102) goto qwarn
if(103) goto backupf
if (104) goto restartf
issue message i "Backup of database complete"
exit
qfail: issue message e "Quiesce of database failed"
exit
qwarn: issue message w "Quiesce of database failed, taking fuzzy backup"

exit
backupf: issue message e "Backup of database failed"
exit
restartf: issue message s "Database restart failed"
exit
```

Comando

```
issue message e "quiesce of database failed"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con ISSUE MESSAGE

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

## LABEL LIBVOLUME (Etiquetar un volumen de biblioteca)




Utilice este comando para etiquetar volúmenes de cinta o, en una biblioteca automatizada, para etiquetar automáticamente los volúmenes a medida que se dan de alta. Con este comando, servidor utiliza la etiqueta larga que, con frecuencia, los volúmenes llevan previamente etiquetada.

Restricción: Utilice este comando sólo para las bibliotecas MANUAL, SCSI, ACSLS y 349X. El proceso del comando no espera a que haya disponible una unidad, aunque la unidad está únicamente en estado IDLE. Si es necesario, puede hacer que una unidad de biblioteca



esté disponible emitiendo el comando DISMOUNT VOLUME para desmontar el volumen de esa unidad en particular. Cuando la unidad de biblioteca esté disponible, podrá volver a emitir el comando LABEL LIBVOLUME.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas y de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

 Sistemas operativos AIX  Sistemas operativos Linux

Para utilizar el comando LABEL LIBVOLUME, al menos debe existir una unidad que no se esté utilizando en ningún otro proceso de IBM Spectrum Protect. Esto incluye también los volúmenes que están montados. Si es necesario, utilice el comando DISMOUNT VOLUME para desmontar el volumen desocupado, para que la unidad quede disponible.

De forma predeterminada, el comando LABEL LIBVOLUME no graba encima de la etiqueta existente. Sin embargo, si desea grabar encima de una etiqueta existente, puede especificar la opción `OVERWRITE=YES`.

Atención:

- Cuando sobrescribe una etiqueta de volumen, destruye todos los datos en el volumen. Tenga cuidado al sobrescribir etiquetas de volumen para evitar la supresión de datos válidos.
- Las etiquetas en volúmenes VolSafe sólo pueden sobrescribirse una vez. Por lo tanto, utilice el comando LABEL LIBVOLUME sólo una vez para los volúmenes VolSafe. Puede proteger la etiqueta contra la sobrescritura con la opción `OVERWRITE=NO` del comando LABEL LIBVOLUME.

Si utiliza el comando LABEL LIBVOLUME, puede identificar los volúmenes que deben etiquetarse de la siguiente manera:

- Nombre explícitamente un volumen.
- Especifique un intervalo de volúmenes utilizando el parámetro `VOLRANGE`.
- Utilice el parámetro `VOLLIST` para especificar un archivo que contenga una lista de nombres de volumen o para nombrar explícitamente uno o varios volúmenes.

En el caso de las bibliotecas automatizadas, se le pedirá que inserte el volumen en la ranura de entrada/salida de la biblioteca. Si no hay ninguna estación de conveniencia de E/S disponible, inserte el volumen en una ranura vacía. En el caso de las bibliotecas manuales, se le pedirá que cargue el volumen directamente en una unidad.

Consejo: Para etiquetar automáticamente volúmenes de cinta, puede utilizar el parámetro `AUTOLABEL` en los comandos `DEFINE LIBRARY` y `UPDATE LIBRARY`. Utilizando el parámetro `AUTOLABEL`, se evita tener que etiquetar previamente un conjunto de cintas. Este método es más eficaz que utilizar el comando LABEL LIBVOLUME, que requiere montar los volúmenes por separado. Si utiliza el parámetro `AUTOLABEL` con una biblioteca SCSI, debe dar de alta las cintas especificando `CHECKLABEL=BARCODE` en el comando `CHECKIN LIBVOLUME`. El parámetro `AUTOLABEL` toma de forma predeterminada el valor `YES` para todas las bibliotecas no SCSI y `NO` para bibliotecas SCSI.

 Sistemas operativos Windows

Para etiquetar los volúmenes con el comando LABEL LIBVOLUME, especifique el parámetro `CHECKIN`.

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro `AUTOLABEL` en los comandos `DEFINE LIBRARY` y `UPDATE LIBRARY`. Utilizando este parámetro, se evita tener que etiquetar previamente un conjunto de cintas. Este método también es más eficaz que utilizar el comando LABEL LIBVOLUME, que requiere montar los volúmenes por separado. Si utiliza el parámetro `AUTOLABEL`, debe dar de alta las cintas especificando `CHECKLABEL=BARCODE` en el comando `CHECKIN LIBVOLUME`.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows. IBM Spectrum Protect no proporciona programas de utilidad para dar formato o etiquetar estos tipos de soportes. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el mandato `label`.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis correspondiente a las bibliotecas manuales

---

```
>>-LABEL LIBVolume--nombre_biblioteca-----nombre_volumen----->
      .-OVERWRITE----No----- . -WAITTime----60----.
>--+-----+-----+-----+-----+-----><
```

```
'-OVERWRITE-----No---' '-WAITTime----valor-'
      '-Yes--'
```

## Sintaxis correspondiente a las bibliotecas SCSI

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>----+nombre_volumen-----+----->
      '-SEARCH-----Yes--| A |---LABELSource-----Barcode-----+'
            '-Bulk--| A |-'                                +-Prompt-----+
                                                    '-Vollist--| B |-'

                        .-OVERWRITE-----No-----
>+-----+-----+-----+-----+----->
      '-CHECKIN-----SCRatch-+' '-OVERWRITE-----No-+-'
            '-PRivate-'                                '-Yes-'

      .-WAITTime----60----.
>+-----+-----+-----+-----+-----<
      '-WAITTime----valor-'

A (SEARCH=Yes, SEARCH=Bulk)

|---+VOLRange-----nombre_volumen1,nombre_volumen2---+-----|
|          .-,-----|
|          v          |
|'-VOLList-----nombre_volumen-+-----+-----|
|          '-FILE:--nombre_archivo-'

B (LABELSource=Vollist)

      .-,-----
      v          |
|'-VOLList-----nombre_volumen-+-----+-----|
|          '-FILE:--nombre_archivo-'
```

## Sintaxis correspondiente a las bibliotecas 349X

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>----+nombre_volumen-----+----->
      '-SEARCH-----Yes-----| A |---'

                        .-OVERWRITE-----No-----
>+-----+-----+-----+-----+----->
      '-CHECKIN-----SCRatch-+' '-OVERWRITE-----No-+-'
            '-PRivate-'                                '-Yes-'

      .-WAITTime----60----.
>+-----+-----+-----+-----+-----<
      '-WAITTime----valor-'

A (SEARCH=Yes)

|---+VOLRange-----nombre_volumen1,nombre_volumen2---+-----|
|          .-,-----|
|          v          |
|'-VOLList-----nombre_volumen-+-----+-----|
|          '-FILE:--nombre_archivo-'
```

## Sintaxis correspondiente a las bibliotecas ACSLS

```
>>-LABEL LIBVolume--nombre_biblioteca----->
>----+nombre_volumen-----+----->
      '-SEARCH-----Yes-----| A |---'

                        .-OVERWRITE-----No-----
>+-----+-----+-----+-----+----->
```

```

'-CHECKIN-----+SCRatch+-'  '-OVERWRITE-----+No---+'
                    '-PRivate-'            '-Yes-'

.-WAITTime-----60-----
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<<
'-WAITTime-----valor-'

A (SEARCH=Yes)

|--+VOLRange-----+-----nombre_volumen1,nombre_volumen2-----+-----|
|                .,-----|                |
|                V                |
'-VOLList-----+-----nombre_volumen-----+-----|
                    '-FILE:--nombre_archivo-'

```

## Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que contiene el volumen de almacenamiento.

nombre\_volumen

Especifica el nombre del volumen que debe etiquetarse.

- En bibliotecas SCSI: el servidor solicita que el volumen se inserte en una ranura en la biblioteca o, si está disponible, en un puerto de entrada/salida. El servidor identifica una ranura por la dirección de elemento de la ranura. Si está etiquetando un volumen en una biblioteca SCSI con varios puertos de entrada/salida, se etiquetará el volumen que tenga la ranura de número más bajo.
- Aviso: Si especifica un nombre de volumen, el nombre que especifique sobrescribe la etiqueta impresa en el cartucho.
- En bibliotecas MANUAL: el servidor solicita que el volumen se inserte en una unidad.
- En bibliotecas 349X: el volumen puede encontrarse ya en la biblioteca, o se le puede solicitar que lo coloque en la estación de E/S.

Recuerde: Si el nombre de volumen especificado ya está definido en una agrupación de almacenamiento o en un archivo histórico de volúmenes, no se etiqueta el volumen y se visualiza un mensaje.

CHECKIN

Especifica si el servidor da de alta el volumen. Este parámetro es opcional. Los siguientes son los valores posibles:

SCRatch

Especifica que el servidor dará de alta los volúmenes y los agregará a la agrupación de reutilizables de la biblioteca. Si un volumen tiene una entrada en el histórico de volúmenes, no puede darlo de alta como volumen reutilizable.

PRivate

Especifica que el servidor dará de alta los volúmenes y los designará como privados. Los volúmenes privados sólo están disponibles al pedirlos por el nombre.

Si no especifica un valor para este parámetro, el comando etiqueta el volumen, pero no lo incorpora. Si no especifica un valor para este parámetro y desea dar de alta el volumen, deberá emitir el comando CHECKIN LIBVOLUME.

SEARCH

Especifica que el servidor busca en la biblioteca los volúmenes utilizables que deben etiquetarse. Este parámetro se aplica a las bibliotecas SCSI, 349X y ACSLS.

Son válidos los valores siguientes:

Yes

Especifica que el servidor sólo etiqueta volúmenes almacenados en la biblioteca, a menos que el volumen ya esté etiquetado o su código de barras no se pueda leer.

Si especifica la opción LABELSOURCE=PROMPT, el volumen se traslada a la unidad desde su ubicación en la biblioteca o en los puertos de entrada o en los de salida. El servidor le solicitará que emita el comando REPLY que contiene la serie de etiqueta, y esa etiqueta se graba en la cinta.

Bulk

Especifica que el servidor busca en los puertos de entrada/salida de la biblioteca los volúmenes utilizables que deben etiquetarse. Esta opción sólo es válida para las bibliotecas SCSI.

Si especifica LABELSOURCE=BARCODE, se lee el código de barras del volumen. A continuación, la cinta se desplaza de su ubicación en la biblioteca o en los puertos de entrada/salida a una unidad en la que se graba la etiqueta del código de barras. Una vez etiquetada la cinta, se devuelve a su ubicación en la biblioteca, a los puertos de entrada/salida o a una ranura de almacenamiento si se especifica la opción CHECKIN. Para que el soporte para código de barras funcione correctamente en las bibliotecas admitidas en IBM Spectrum Protect, el servidor de IBM Spectrum Protect y el

controlador de dispositivo deben estar en el mismo nivel. El soporte de código de barras está disponible en las bibliotecas admitidas por IBM Spectrum Protect y que utilizan el controlador de dispositivo de IBM Spectrum Protect o el controlador de dispositivo IBM® Magstar o LTO Ultrium.

Consejo: Se pueden utilizar los parámetros VOLRANGE o VOLLIST para limitar la búsqueda.

#### VOLRange

Especifica un rango de nombres de volúmenes separados con una coma. Utilice este parámetro para limitar la búsqueda de volúmenes para etiquetarlos cuando especifique SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca dentro del rango especificado, el comando finalizará sin errores.

Sólo puede especificar los nombres de volúmenes que se puedan incrementar numéricamente. Además del área incremental, un nombre de volumen puede contener un prefijo alfanumérico, un sufijo alfanumérico o ambos.

Parámetro	Descripción
volrange=bar110,bar130	Se etiquetan los 21 volúmenes: bar110, bar111, bar112,...bar129, bar130.
volrange=bar11a,bar13a	Los 3 volúmenes se etiquetan: bar11a, bar12a, bar13a.
volrange=123400,123410	Se etiquetan los 11 volúmenes: 123400, 123401, ...123409, 123410.

#### VOLList

Especifica una lista de volúmenes. Utilice este parámetro para limitar la búsqueda de volúmenes para etiquetarlos cuando especifique SEARCH=YES (bibliotecas 349X, ACSLS y SCSI) o SEARCH=BULK (sólo bibliotecas SCSI). Si no hay volúmenes en la biblioteca que se encuentren en la lista, el comando finaliza sin errores. El parámetro VOLLIST también puede ser la fuente de nombres que se pueden utilizar para indicar volúmenes si el parámetro LABELSOURCE se define como VOLLIST. Si LABELSOURCE=VOLLIST, debe especificar el parámetro VOLLIST.

Son válidos los valores siguientes:

##### nombre\_volumen

Especifica los nombres de uno o varios volúmenes que se utilizan para el comando. Por ejemplo:

```
VOLLIST=TAPE01,TAPE02.
```

##### FILE:nombre\_archivo

Especifica el nombre de un archivo que contiene una lista de los volúmenes para el comando. En el archivo, cada nombre de volumen debe estar en una línea diferente. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo, para utilizar el volumen TAPE01, TAPE02 y TAPE03, cree un archivo denominado TAPEVOL que contenga las siguientes líneas:

```
TAPE01  
TAPE02  
TAPE03
```

Puede especificar los volúmenes para el comando según se indica a continuación: VOLLIST=FILE:TAPEVOL.

Recuerde: El nombre de archivo es sensible a las mayúsculas/minúsculas.

#### LABELSource

Especifica si el servidor lee las etiquetas de medios secuenciales de los volúmenes o cómo debe hacerlo. Esta opción sólo es válida para las bibliotecas SCSI. Especifique este parámetro sólo cuando SEARCH=YES o SEARCH=BULK.

Puede especificar los valores siguientes:

##### Prompt

El servidor solicita los nombres de volumen necesarios.

##### Barcode

El servidor intenta leer la etiqueta del código de barras. Si no lo consigue, el servidor no etiqueta el volumen y muestra un mensaje.

Importante: Para que el soporte de código de barras funcione correctamente, deben instalarse los controladores de dispositivo adecuados para las bibliotecas.

##### Vollist

Esta opción sólo se aplica a las bibliotecas SCSI. El servidor intenta leer el archivo o la lista de archivos especificados. Si no lo consigue, el servidor no etiqueta los volúmenes y muestra un mensaje.

#### OVERWRITE

Especifica si el servidor intenta grabar encima de las etiquetas existentes. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar los valores siguientes:

No

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta. Para los volúmenes StorageTek VolSafe, el valor debe ser NO.

Yes

Especifica que el servidor graba encima de las etiquetas existentes sólo si no se han definido aún ni la etiqueta existente ni la etiqueta solicitada o de código de barra en una agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

WAITTime

Especifica el número de minutos que el servidor esperará su respuesta o responderá a una petición. Especifique un valor dentro del rango de 0 a 9999. Si desea que el servidor le pregunte, especifique un tiempo de espera mayor que cero. El valor predeterminado es de 60 minutos. Por ejemplo, supongamos que el servidor le solicita que inserte una cinta en el puerto de entrada/salida de una biblioteca. Si ha especificado un tiempo de espera de 60 minutos, el servidor emite una petición y espera 60 minutos a que responda a la petición. De forma alternativa, supongamos que especifica 0 como tiempo de espera. Si ha insertado una cinta, un tiempo de espera cero dará lugar a que la operación continúe sin que se formule ninguna pregunta. Si no ha insertado una cinta, un tiempo de espera igual a cero hace que la operación falle.

## Ejemplo: etiquetar automáticamente volúmenes de biblioteca

Etiquetar automáticamente las cintas de una biblioteca SCSI denominada AUTO a medida que incorpora los volúmenes.

```
label libvolume auto checkin=scratch search=yes labelsource=barcode  
overwrite=yes
```

## Ejemplo: etiquetar volúmenes de biblioteca secuenciales

Etiquetar 3 volúmenes, de bar11a a bar13a, en una biblioteca SCSI denominada ABC. Cuando emita el siguiente comando, los tres volúmenes se etiquetarán: bar11a, bar12a, bar13a.

```
label libvolume abc checkin=scratch search=yes volrange=bar11a,bar13a  
labelsource=barcode
```

## Comandos relacionados

Tabla 1. Comandos relacionados con LABEL LIBVOLUME

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.
QUERY PROCESS	Muestra información sobre procesos subordinados.
REPLY	Permite que una petición siga procesándose.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

## LOAD DEFALERTTRIGGERS (Cargar el conjunto predeterminado de desencadenantes de alertas)

Utilice este comando para cargar el conjunto predeterminado de desencadenantes de alertas en el servidor de IBM Spectrum Protect.

Para un servidor que se acaba de instalar, se define un conjunto predeterminado de mensajes para desencadenar las alertas. Puede modificar o suprimir los desencadenantes de alertas predeterminados. Utilice este comando para completar las siguientes tareas:

- Cargar el conjunto predeterminado de desencadenantes de alertas y restaurar los que se hubieran suprimido.
- Sustituir todos los desencadenantes de alertas por el conjunto predeterminado original.

De forma predeterminada, este comando no suprime los otros desencadenantes de alertas que se hayan creado, ni sustituye los desencadenantes de alertas predeterminados que se hayan modificado. Para suprimir todos los desencadenantes de alertas y restaurar el conjunto original de desencadenantes de alertas predeterminados, especifique RESET=yes.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```

>>-L0ad DEFALertriggers--+-REset---No-----<
                              '-REset---+No--+-'
                              '-Yes-'

```

## Parámetros

### REset

Especifica si desea sustituir todos los desencadenantes de alertas por el conjunto predeterminado de desencadenantes de alertas. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

### No

Especifica que sólo se añaden los desencadenantes de alertas predeterminados. Los desencadenantes de alertas predeterminados originales se añaden al servidor. Los desencadenantes existentes no se suprimen. Si ya existe un desencadenante predeterminado en el servidor, no se sustituye ni se modifica.

### Yes

Especifica que los desencadenantes de alertas se restauran a los valores predeterminados originales. Todos los desencadenantes de alertas se suprimen y, a continuación, se añaden el conjunto original de desencadenantes de alertas predeterminados.

## Ejemplo: cargar los desencadenantes de alertas predeterminados en el servidor

Cargue los desencadenantes predeterminados para restaurar los que se han suprimido. Emita el comando:

```
load defalertriggers
```

## Ejemplo: sustituir todos los desencadenantes de alertas en el servidor por los desencadenantes de alertas predeterminados

Suprima todos los desencadenantes de alertas en el servidor y sustitúyalos por los valores predeterminados originales. Emita el comando:

```
load defalertriggers reset=yes
```

## Comandos relacionados

Tabla 1. Comandos relacionados con LOAD DEFALERTTRIGGERS

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.

## Comandos LOCK

---

Utilice el comando LOCK para impedir que los usuarios accedan al servidor.

- LOCK ADMIN (bloquear un administrador)
- LOCK NODE (Bloquear un nodo cliente)
- LOCK PROFILE (bloquear un perfil)

### LOCK ADMIN (bloquear un administrador)

---

Utilice este mandato para impedir que un administrador acceda al servidor. El acceso del administrador estará bloqueado hasta que un administrador del sistema utilice el mandato UNLOCK ADMIN para volver a establecer el acceso para el administrador.

Puede utilizar el filtro de autenticación para bloquear a todos los administradores, excluidos los administradores de la consola). Después de configurar un servidor de directorios LDAP para autenticar las contraseñas, puede bloquear los administradores para forzar que creen contraseñas que se autentican con un servidor LDAP.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

---

```
>>-LOCK Admin--+-*-----+-----+-----+-----+<<
                '-nombre_admin-'   '-AUTHentication----+Local+-'
                                     '-LDap--'
```

### Parámetros

---

nombre\_admin (Necesario)

Especifica el nombre del administrador que se ha de bloquear. Puede utilizar caracteres comodín para especificar el nombre del administrador. No tiene que especificar un nombre de administrador, si desea bloquear a todos los administradores de acuerdo con su método de autenticación. Utilice el carácter comodín con un método de autenticación para bloquear múltiples administradores.

AUTHentication

Especifica el método de autenticación que utiliza el administrador para iniciar la sesión.

Local

Especifica que se han de bloquear los administradores que se autentican en el servidor de IBM Spectrum Protect.

LDap

Especifica que se han de bloquear los administradores que se autentican en el servidor de directorios LDAP.

### Ejemplo: bloquear un administrador

---

Bloquear el administrador CLAUDIA. Emita el comando:

```
lock admin claudia
```

### Ejemplo: bloquear todos los administradores que se autentican en la base de datos del servidor de IBM Spectrum Protect.

---

Utilice el carácter comodín (\*) para bloquear todos los administradores que autentican sus contraseñas localmente. Los administradores de la consola no resultan afectados por este mandato. Emita el mandato siguiente:

```
lock admin * authentication=local
```

### Comandos relacionados

---

Tabla 1. Comandos relacionados con LOCK ADMIN

Comando	Descripción
---------	-------------

Comando	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
UNLOCK ADMIN	Permite que un administrador bloqueado acceda a IBM Spectrum Protect.

## LOCK NODE (Bloquear un nodo cliente)

Utilice este mandato para impedir que un nodo de cliente acceda al servidor. Un nodo de cliente bloqueado no puede realizar ninguna operación de IBM Spectrum Protect, aunque las operaciones estén planificadas.

Después de configurar un servidor de directorios LDAP para autenticar las contraseñas, puede bloquear los nodos para forzarles a utilizar contraseñas que se autentican con un servidor LDAP.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el nodo cliente.

### Sintaxis

```
>>-LOCK Node--+-*-----+--+-----+--<
      '-nombre_nodo-'  '-AUTHentication---+--Local+-'
                          '-LDap--'
```

### Parámetros

nombre\_nodo

Especifica el nombre del nodo de cliente que se bloqueará. Puede utilizar un carácter comodín en lugar de un nombre de nodo si desea bloquear todos los nodos de acuerdo a su método de autenticación.

AUTHentication

Especifica el método de autenticación de contraseña que se necesita para iniciar la sesión en un nodo.

Local

Especifica que se han de bloquear los nodos que se autentican en el servidor de IBM Spectrum Protect.

LDap

Especifica que se han de bloquear los nodos que se autentican con un servidor de directorios LDAP.

### Ejemplo: bloquear un nodo de cliente específico

Bloquear el nodo de cliente SMITH.

```
lock node smith
```

### Ejemplo: Bloquear todos los nodos que se autentican en la base de datos de IBM Spectrum Protect local

Emita el siguiente mandato para bloquear todos los nodos que se autentican con el servidor de IBM Spectrum Protect:

```
lock node * authentication=local
```

### Comandos relacionados

Tabla 1. Comandos relacionados con LOCK NODE

Comando	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.



Comando	Descripción
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.

## LOCK PROFILE (bloquear un perfil)

Utilice este comando en un gestor de configuración para bloquear temporalmente un perfil para que la información de configuración no se distribuya a los servidores gestionados suscritos.

Puede utilizar este comando cuando esté realizando varias actualizaciones en la configuración y no desee distribuir esta información hasta que se hayan finalizado los cambios.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-LOCK PROFILE--nombre_perfil--+-60-----+----->>
                               '-minutos-'
```

### Parámetros

nombre\_perfil (Obligatorio)

Especifica el perfil que se bloquea. Puede utilizar caracteres comodín para especificar varios nombres.

minutos

Especifica el tiempo, en minutos, que debe transcurrir para que IBM Spectrum Protect desbloquee el perfil de configuración. Especifique un entero de 0 a 10000. El valor predeterminado son 60 minutos. Si especifica 0, el perfil de configuración no se desbloqueará automáticamente. Utilice el comando UNLOCK PROFILE para desbloquear el perfil antes de que transcurra el período de tiempo indicado o para desbloquearlo si ha especificado el valor 0. Este parámetro es opcional.

### Ejemplo: bloquear un perfil durante un período de tiempo específico

Bloquear un perfil denominado DELTA durante 30 minutos.

```
lock profile delta 30
```

### Comandos relacionados

Tabla 1. Comandos relacionados con LOCK PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## MACRO (Invocar una macro)

Utilice este comando para invocar un archivo desde la línea de comandos de administración que contiene uno o varios comandos de administración de IBM Spectrum Protect que deben ejecutarse.

Restricción: Utilice este comando sólo con clientes de línea de comandos de administración.

Una macro es un archivo que contiene uno o varios comandos de administración de IBM Spectrum Protect. Las macros sólo se pueden emitir desde el cliente de administración en las modalidades de proceso por lotes o interactiva. Las macros se almacenan como un archivo en la máquina (o sistema) cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

Crear una macro para entrar comandos puede resultar muy útil si desea emitir comandos que se utilizan reiteradamente, que contienen varios parámetros, o para procesar comandos relacionados en un orden específico. Después de crear una macro, puede actualizar la información que contiene y volver a utilizarla, o puede copiar el archivo de macros, realizar cambios en la copia y, a continuación, ejecutar la copia.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
>>-MACRO--nombre_macro--+-----+-----><
      | .------. |
      | v           | |
      '---substitution_value+--'
```

## Parámetros

---

nombre\_macro (Obligatorio)

Especifica el nombre de la macro.

substitution\_value

Especifica el valor de una variable de sustitución en una macro. Si utiliza una variable de sustitución, puede volver a utilizar una macro siempre que necesite realizar la misma tarea para objetos diferentes o con valores de parámetro diferentes. Si desea especificar un valor que contenga espacios en blanco, debe encerrar el valor entre comillas. Este parámetro es opcional.

## Ejemplo: crear una macro para registrar un nuevo administrador

---

Crear el archivo de macros denominado REGNG. Se utilizará la macro para inscribir y otorgar autorización a un nuevo administrador. Escriba la macro del siguiente modo:

```
/* Registrar y otorgar autorización a un nuevo administrador */
REGister Admin jones passwd -
CONTACTinfo="x1235"
GRant AUTHority jones -
CLasses=Policy
```

Emita el siguiente comando para ejecutar la macro:

```
macro regng.mac
```

## Ejemplo: escribir una macro utilizando variables de sustitución

---

Crear el archivo de macros denominado AUTHRG, que contenga variables de sustitución, para inscribir y otorgar autorización a un nuevo administrador. Escriba la macro del siguiente modo:

```
/* Registrar y otorgar autorización a un nuevo administrador */
REGister Admin %1 %2 - /* Entrar id usuario y contraseña */
CONTACT=%3 /* Entrar infor. contacto (entre comillas, si es nec.) */
GRant AUTHority %1 - /* El servidor utiliza la variable */
- /* que ya ha definido */
CLasses=%4 /* Entrar la clase de privilegio */
```

Emita un comando similar al siguiente, especificando los valores que desea pasar al servidor, para que el comando se procese cuando se ejecute la macro.

```
macro authrg.mac jones passwd x1235 Policy
```

Tabla 1. Comandos relacionados con MACRO

Comando	Descripción
COMMIT	Hace que los cambios en la base de datos sean permanentes.
ROLLBACK	Descarga cualquier cambio no confirmado en la base de datos desde que se ejecutó el último COMMIT.

**Conceptos relacionados:**

Macros de cliente administrativo

## MIGRATE STGPOOL (Migrar agrupación de almacenamiento a agrupación de almacenamiento siguiente)

Utilice este comando para migrar archivos de una agrupación de almacenamiento a la agrupación de almacenamiento siguiente de la jerarquía de almacenamiento.

Este comando sólo puede utilizarse con agrupaciones de almacenamiento primarias. El formato de datos de la agrupación de almacenamiento no puede ser NETAPPDUMP, CELERRADUMP o NDMPDUMP. Los datos no se pueden migrar a o desde agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.

Sólo se permite un proceso de migración o reclamación para una agrupación de almacenamiento determinada en un momento dado. Si ya está ejecutándose un proceso de migración o reclamación para la agrupación de almacenamiento, no puede iniciar otro proceso de migración para la agrupación de almacenamiento.

Sólo debería utilizar este comando si no utilizará la migración automática para la agrupación de almacenamiento. Para impedir que se ejecute la migración automática, establezca el atributo HIGHMIG de la definición de agrupación de almacenamiento en 100.

Si utiliza este mandato para iniciar un proceso de migración, pero la agrupación de almacenamiento no tiene identificada la siguiente agrupación de almacenamiento en la jerarquía, se activa un proceso de reclamación se activa para la agrupación de almacenamiento de origen. Para evitar el proceso de regeneración, defina la siguiente agrupación de almacenamiento en la jerarquía. A continuación, inicie el proceso de migración.

El mandato MIGRATE STGPOOL utiliza los valores de los siguientes parámetros en los mandatos DEFINE STGPOOL y UPDATE STGPOOL:

- MIGPROCESS
- MIGDELAY
- MIGCONTINUE
- NEXTPOOL
- LOWMIG

Consejo: Puede sustituir el valor del parámetro LOWMIG en los mandatos DEFINE STGPOOL y UPDATE STGPOOL especificando un valor para el parámetro LOWMIG en el mandato MIGRATE STGPOOL.

El mandato MIGRATE STGPOOL pasa por alto el valor del parámetro HIGHMIG de la definición de agrupación de almacenamiento. La migración se produce independientemente del valor del parámetro HIGHMIG.

Este comando crea uno o varios procesos de migración que pueden cancelarse con el comando CANCEL PROCESS. El número de procesos está limitado por el atributo MIGPROCESS de la definición de agrupación de almacenamiento. Para que se visualice información acerca de los procesos subordinados, utilice el mandato QUERY PROCESS.

Recuerde: La migración de datos de una agrupación de almacenamiento primaria configurada para eliminación de datos duplicados a otra agrupación de almacenamiento primaria que también está configurada para eliminación de datos duplicados elimina los datos duplicados.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado tanto en la agrupación de almacenamiento cuyos archivos se migrarán como en la agrupación de almacenamiento siguiente a la que se migrarán los archivos.

## Sintaxis

```
>>-MIGrate STGpool--nombre_agrupación--+-----+----->
```

```

                                '-LOwmiG-----número-'
                                .-REClaim-----No-----'
>-----+-----+-----+-----+-----+----->
'-DUration---minutos-' '-REClaim---+No---+'
                                     '-Yes-'

    .-Wait-----No-----'
>-----+-----+-----+-----+-----+-----<
'-Wait---+No---+'
    '-Yes-'

```

## Parámetros

---

### nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento principal cuyos archivos se deben migrar.

### DUration

Especifica el número máximo de minutos que se ejecuta la migración antes de cancelarse automáticamente. Al transcurrir el número de minutos especificado, el servidor cancelará automáticamente todos los procesos de migración para esta agrupación de almacenamiento. Los procesos finalizarán en cuanto detecten la cancelación automática. Como resultado, la migración puede ejecutarse durante más tiempo que el valor que especificó para este parámetro. Puede especificar un número de 1 a 9999. Este parámetro es opcional. Si no se especifica, el servidor se detendrá únicamente después de alcanzar el umbral inferior de migración.

### LOwmiG

Para agrupaciones de almacenamiento en disco de acceso secuencial y acceso aleatorio, especifica que la migración se debe detener cuando la cantidad de datos en la agrupación es igual o inferior a la capacidad estimada de este porcentaje de la agrupación. Este parámetro es opcional.

El cálculo de las agrupaciones de almacenamiento en disco de acceso secuencial incluye la capacidad de todos los volúmenes reutilizables especificados para la agrupación. Dado que la migración se realiza por nodo o espacio de archivos, en función de la proximidad la ocupación de la agrupación de almacenamiento puede caer por debajo del valor especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0. En otros tipos de agrupaciones de almacenamiento de acceso secuencial, el servidor detiene la migración cuando el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento es igual o inferior a este porcentaje. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Puede especificar un número de 0 a 99 para este parámetro opcional. El valor predeterminado es el atributo LOWMIG de la definición de agrupación de almacenamiento.

### REClaim

Especifica si se intenta la reclamación para la agrupación de almacenamiento antes de completar la migración. Sólo puede especificarse este parámetro para una agrupación de almacenamiento de acceso secuencial. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

#### No

Especifica que el servidor no intentará una operación de reclamación antes de iniciar la migración.

#### Yes

Especifica que el servidor intentará una reclamación antes de iniciar la migración. La operación de reclamación se realizará para cualquier volumen de la agrupación de almacenamiento que satisfaga el umbral de reclamación especificado en el atributo RECLAIM de la definición de agrupación de almacenamiento antes de completar la migración. Si no hay ningún volumen que satisfaga el umbral de reclamación o si, tras la reclamación, el umbral LOWMIG no se ha alcanzado, el servidor iniciará la migración. Antes de reclamar espacio para las agrupaciones de almacenamiento definidas por RECLAMATIONTYPE=SNAPLOCK, el servidor suprime todos los volúmenes WORM FILE vacíos durante el proceso de reclamación que han excedido su periodo de reclamación.

### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

#### No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el comando. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, pueden haberse migrado ya algunos archivos antes de la cancelación.

#### Yes

Especifica que el servidor procesa este comando en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando la operación finaliza. Los mensajes también se visualizan en las anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Nota: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: migrar una agrupación de almacenamiento a la siguiente agrupación de almacenamiento

Migrar datos de la agrupación de almacenamiento denominada BACKUPPOOL hasta la siguiente agrupación de almacenamiento. Especificar que el servidor debe finalizar la migración lo antes posible después de 90 minutos.


```
migrate stgpool backuppool duration=90
```

## Comandos relacionados

Tabla 1. Comandos relacionados con MIGRATE STGPOOL

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Visualiza información acerca de un proceso subordinado.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RECLAIM STGPOOL	Realiza una operación de reclamación para la agrupación de almacenamiento.




### Información relacionada:

 Migración de archivos en una jerarquía de agrupaciones de almacenamiento

## Comandos MOVE

Utilice los comandos MOVE para transferir datos de copia de seguridad o datos archivados entre agrupaciones de almacenamiento o bien para trasladar medios de recuperación ante siniestro al local o fuera del local.

- MOVE CONTAINER (Mover un contenedor)
- MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)
- MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)
- MOVE GRPMEMBER (Mover un miembro de grupo de servidores)
- MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)
- MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## MOVE CONTAINER (Mover un contenedor)

Utilice este comando para mover el contenido de un contenedor de agrupación de almacenamiento a otro contenedor si se elimina un directorio de agrupación de almacenamiento o se daña un contenedor.

También puede utilizar este comando para mover el contenido de un contenedor de agrupación de almacenamiento en estas condiciones:

- Cuando actualiza hardware
- Si se producen errores de E/S en un disco

## Clase de privilegio

Para emitir este comando, debe tener privilegio de almacenamiento restringido.

## Sintaxis

```
>>-MOVE CONTainer--nombre_contenedor----->
>>+-----+-----+----->
' -STGPOOLDIRectory---nombre_directorio-'
```

```

.-Wait---Yes-----
>--+-----+-----><
'-Wait---+-Yes-+-'
      '-No--'

```

## Parámetros

nombre\_contenedor (Obligatorio)

Especifica el nombre del contenedor que se va a mover. Debe especificar el nombre completo de la vía de acceso del contenedor.

STGPOOLDIRectory

Especifica el nombre del directorio de agrupación de almacenamiento donde se mueve el contenedor. Este parámetro es opcional.

Si especifica un directorio de agrupación de almacenamiento, debe estar en la misma agrupación de almacenamiento que el contenedor original. El directorio de agrupación de almacenamiento se utiliza para el nuevo contenedor. Si no especifica un directorio de agrupación de almacenamiento, el servidor de IBM Spectrum Protect selecciona un directorio de agrupación de almacenamiento en la misma agrupación de almacenamiento.

Wait

Especifica si es necesario esperar a que el servidor de IBM Spectrum Protect termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. Especifique los siguiente valores:

No



El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes. Este es el valor predeterminado.

Yes

El servidor procesa este mandato de forma subordinada. La operación debe estar terminada para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar parámetro WAIT=YES en la consola del servidor.


## Ejemplo: mover un contenedor

  Mueva el contenedor 0000000000000001.dcf del directorio de agrupación de almacenamiento /data1/storage/dir1 al directorio de agrupación de almacenamiento /data/storage/dir2.

```

move container /data1/storage/dir1/00/0000000000000001.dcf
stgpooldir=/data/storage/dir2

```

 Mueva el contenedor 0000000000000001.dcf del directorio de agrupación de almacenamiento e:\data1\storage\dir1 al directorio de agrupación de almacenamiento e:\data\storage\dir2.

```

move container e:\data1\storage\dir1\00\0000000000000001.dcf
stgpooldir=e:\data\storage\dir2

```

Tabla 1. Comandos relacionados con MOVE CONTAINER

Comando	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
QUERY CONTAINER	Visualiza información sobre un contenedor.

## MOVE DATA (traspasar archivos de un volumen de agrupación de almacenamiento)

Utilice este comando para traspasar archivos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.

Restricción: No puede utilizar este mandato para volúmenes que están asignados a agrupaciones de almacenamiento de copias de contenedor.

Los archivos de un volumen de agrupación de almacenamiento primaria sólo se pueden traspasar a volúmenes de la misma agrupación de almacenamiento primaria o de una distinta. Los archivos de un volumen de agrupación de almacenamiento de copia sólo se pueden

traspasar a volúmenes de la misma agrupación de almacenamiento de copia. Sólo puede traspasar archivos desde un volumen de agrupación de datos activos hasta los volúmenes de la misma agrupación de datos activos.

Además de trasladar datos desde los volúmenes de las agrupaciones de almacenamiento que tienen los formatos de datos NATIVE o NONBLOCK, este mandato también le permite trasladar datos desde los volúmenes de las agrupaciones de almacenamiento que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento de destino debe tener el mismo formato de datos que la agrupación de almacenamiento de origen. Si va a sacar datos de una agrupación de almacenamiento para actualizarse a la nueva tecnología de cintas, la agrupación de almacenamiento primaria de destino deberá asociarse a una biblioteca que tenga el nuevo dispositivo para las unidades de cinta. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

No puede trasladar datos de nodo a una agrupación o desde una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Si está desplazando archivos a volúmenes de la misma agrupación de almacenamiento, debe haber espacio suficiente en los volúmenes. De lo contrario, la operación no será satisfactoria.

Al traspasar archivos de un volumen de acceso secuencial, se necesitarán varios montajes de volumen de acceso secuencial para traspasar archivos que ocupan varios volúmenes.

Al traspasar archivos de un volumen de acceso aleatorio, el servidor borra todas las copias en caché de los archivos que hay en el volumen.

Después de haber finalizado una operación de traspaso de datos, es posible que un volumen no quede vacío si hay uno o varios archivos que no se pueden reubicar en otro volumen debido a errores de entrada/salida en el dispositivo, o si se han encontrado errores en el archivo. Si es necesario, puede suprimir el volumen con la opción de descartar todos los datos. Los archivos con errores de E/S o de otro tipo se suprimirán entonces.

Puede utilizar este comando para traspasar archivos desde un volumen fuera del local de una agrupación de almacenamiento de copia o una agrupación de datos activos. Puesto que el volumen fuera del local no puede montarse, el servidor obtiene los archivos que se encuentran en el volumen fuera del local de una agrupación de almacenamiento primaria o de otra agrupación de almacenamiento de copia. A continuación, estos archivos se graban en los volúmenes de destino de la agrupación de almacenamiento de copia o la agrupación de datos activos original.

Durante el proceso de traslado de datos, las agrupaciones de datos activos no se pueden utilizar para obtener datos.

Si ejecuta el comando MOVE DATA en un volumen fuera de local que contiene datos de proximidad, puede que sea necesario emitir el mandato MOVE DATA varias veces para trasladar todos los datos fuera del volumen. Por ejemplo, si está utilizando grupos de proximidad de espacio de archivos con un volumen fuera del local que contiene espacios de archivos en un grupo de proximidad y los espacios de archivos que no están en el grupo, debe emitir dos mandatos MOVE DATA. Cada mandato MOVE DATA traslada los datos para un solo grupo de archivos de proximidad o no de proximidad.

No utilice el comando MOVE DATA si se está ejecutando un proceso de restauración (RESTORE STGPOOL o RESTORE VOLUME). Es posible que el mandato MOVE DATA cause que la restauración sea incompleta. Si emite el mandato MOVE DATA durante una operación de restauración y recibe un mensaje de error que indica que uno o más archivos están bloqueados y no se pueden trasladar, debe volver a emitir el mandato MOVE DATA después de realizarse la operación de restauración para trasladar los archivos restantes.

Recuerde:

La emisión de este comando elimina datos duplicados al:

- Mover datos de una agrupación de almacenamiento primaria configurada para eliminación de datos duplicados a otra agrupación de almacenamiento primaria que también está configurada para la eliminación de duplicados.
- Mover datos dentro de una agrupación de almacenamiento de copia configurada para la eliminación de datos duplicados.
- Mover datos dentro de una agrupación de datos activos configurada para eliminación de datos duplicados.

Un volumen en una agrupación de almacenamiento cuyos duplicados se han eliminado puede contener archivos que se han suprimido lógicamente pero continúan enlazados con archivos en otros volúmenes. Si utiliza el comando MOVE DATA para mover el contenido de un volumen de agrupación de almacenamiento cuyos duplicados se han eliminado a una agrupación de almacenamiento cuyos duplicados no se han eliminado, los archivos suprimidos de forma lógica no se graban en el nuevo volumen, ya que no existen lógicamente. Los archivos suprimidos se mantienen en los volúmenes originales para que otros archivos puedan hacer referencia a ellos. El proceso de MOVE DATA finaliza correctamente, pero ninguno de los archivos suprimidos se mueve al nuevo volumen de destino y el volumen de origen no se suprime. Puede emitir el comando QUERY CONTENT con el parámetro FOLLOWLINKS=YES o FOLLOWLINKS=JUSTLINKS para verificar si el volumen contiene archivos enlazados con archivos en otros volúmenes.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento a la que pertenece el volumen y también para la nueva agrupación de

almacenamiento, si se especifica una.

## Sintaxis

```
>>-MOVE Data--nombre_volumen----->
>+-----+----->
' -STGpool---nombre_agrupación-'
. -SHREDTONoshred---No----- .
>+-----+----->
' -SHREDTONoshred---+No--+-'
' -Yes-'

(1) (2)
. -RECONstruct---No o Yes----- . -Wait---No----- .
>+-----+-----+-----<
' -RECONstruct---+No--+-' ' -Wait---+No--+-'
' -Yes-' ' -Yes-'
```

Notas:

1. El valor predeterminado es NO si la agrupación de almacenamiento de origen o de destino es de acceso aleatorio. El valor predeterminado es YES si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial.
2. Este parámetro no está disponible o se pasa por alto en el caso de que el formato de datos sea NETAPPDUMP, CELERRADUMP o NDMPDUMP.

## Parámetros

nombre\_volumen (Necesario)

Especifica el volumen de agrupación de almacenamiento desde el que se traspasan los archivos.

STGpool

Especifica la agrupación de almacenamiento primaria a la que desea traspasar los archivos (la agrupación de almacenamiento de destino). Este parámetro es opcional y sólo se aplica a los datos que se traspasan de volúmenes de agrupaciones de almacenamiento primarias. Si no especifica un valor para este parámetro, los archivos se desplazarán a otros volúmenes en la misma agrupación de almacenamiento.

SHREDTONoshred

Especifica si los datos se trasladan de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor no permitirá que se traspasen datos de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Si la agrupación de almacenamiento de origen implementa la destrucción de datos y la agrupación de almacenamiento de destino no existe, la operación falla.

Yes

Especifica que el servidor permite que se trasladen datos de una agrupación de almacenamiento que implementa la destrucción de datos a una agrupación de almacenamiento que no implementa la destrucción de datos. Los datos de origen se destruirán cuando la operación se haya completado. Los datos de destino no se destruirán cuando se supriman.

RECONstruct

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de un conjunto. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO.

El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento.



Los valores posibles son:

No

Especifica que la reconstrucción de agregaciones de archivos no se ha completado durante el traslado de datos.

Yes

Especifica que la reconstrucción de agregaciones de archivos se ha completado durante el traslado de datos. Sólo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

No

Especifica que el servidor procesa este comando en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el mandato.

El servidor muestra mensajes que se crean desde el proceso en segundo plano en el registro de actividad o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano MOVE DATA, es posible que algunos archivos ya se hayan trasladado antes de la cancelación.

Yes

Especifica que el servidor procesa este comando en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: traspasar archivos de un volumen de agrupación de almacenamiento

Traspasar los archivos del volumen de agrupación de almacenamiento STGVOL.1 a cualquiera de los volúmenes disponibles asignados a la agrupación de almacenamiento 8MMPOOL.

```
move data stgvol.1 stgpool=8mmpool
```

## Comandos relacionados

Tabla 1. Comandos relacionados con MOVE DATA

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.

## MOVE DRMEDIA (Trasladar medios de recuperación ante siniestro fuera del local y de vuelta al local)

Utilice este mandato para hacer el seguimiento de los volúmenes que se van a trasladar fuera del local y para identificar los volúmenes caducados o vacíos que se van a trasladar al local. Puede hacer un seguimiento de los volúmenes de copia de seguridad de base de datos y de los volúmenes de agrupaciones de almacenamiento de copia de contenedor y de agrupaciones de almacenamiento de datos activos.

El proceso de volúmenes por parte de este mandato depende del uso que se les de:

#### Copias de seguridad de la base de datos del servidor

Para controlar si el mandato procesa volúmenes de copia de seguridad de base de datos, utilice el parámetro SOURCE en este mandato. El mandato puede procesar volúmenes utilizados para copias de seguridad de base de datos completas más las incrementales o de instantáneas. No se pueden especificar volúmenes virtuales (objetos de copia de seguridad almacenados en otro servidor). Puede modificar los volúmenes mediante cada estado, o bien utilizar el parámetro TOSTATE y omitir los estados para simplificar los traslados.

#### Agrupaciones de almacenamiento de copia

El mandato MOVE DRMEDIA siempre procesa volúmenes de agrupación de almacenamiento de copia.

#### Agrupaciones de almacenamiento de copia de contenedor

De forma predeterminada, los volúmenes de agrupación de almacenamiento de copia de contenedor no se pueden elegir para que las procese el mandato MOVE DRMEDIA. Para procesar volúmenes de agrupación de almacenamiento de copia de contenedor, debe emitir primero el mandato SET DRMCOPYCONTAINERSTGPOOL o especificar el parámetro COPYCONTAINERSTGPOOL en el mandato MOVE DRMEDIA.

#### Agrupaciones de almacenamiento de datos activos

De forma predeterminada, los volúmenes de agrupación de almacenamiento de datos activos no se pueden elegir para que las procese el mandato MOVE DRMEDIA. Para procesar volúmenes de agrupación de datos activos, debe emitir primero el mandato SET DRMACTIVEDATASTGPOOL o especificar el parámetro ACTIVEDATASTGPOOL en el mandato MOVE DRMEDIA.

Puede utilizar el mandato QUERY ACTLOG para comprobar si el mandato MOVE DRMEDIA se ha ejecutado correctamente. También puede ver esta información desde la consola del servidor.

Restricción: No ejecute los mandatos MOVE DRMEDIA y BACKUP STGPOOL simultáneamente. Asegúrese de que los procesos de copia de seguridad de agrupación de almacenamiento se han completado antes de emitir el mandato MOVE DRMEDIA.

## Clase de privilegio

---

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO privilegio de operador, de almacenamiento sin restricciones o de sistema.
- Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES (el valor predeterminado): privilegio de sistema.

## Sintaxis

---

```
>>-MOVE DRMedia--nombre_volumen----->
>--+-----+----->
  '-WHEREState---+Mountable-----+'
      +-NOTMountable----+
      +-COUrier-----+
      +-VAULTRetrieve---+
      '-COURIERRetrieve-'
>--+-----+-----+----->
  '-BEGINDate---fecha-' '-ENDDate---fecha-'
>--+-----+-----+----->
  '-BEGINTime---hora-' '-ENDTime---hora-'
>--+-----+----->
  '-COPYContainerstgpool---nombre_agrupación-'
>--+-----+----->
  '-COPYstgpool---nombre_agrupación-'
>--+-----+----->
  '-ACTIVEDatastgpool---nombre_agrupación-'
  .-Source---DBBackup-----
>--+-----+----->
  '-Source---+DBBackup---+'
```

```

+-DBSnapshot-+
'-DBNone-----'

.-REMove-----Bulk------.
>-----+-----+-----+-----+-----+----->
'-REMove-----+No-----+'
+-Yes-----+
+-Bulk-----+
'-Untileefull-'

>-----+-----+-----+-----+-----+----->
'-TOState-----+NOTMounTable-----+'
+-COUrier-----+
+-VAult-----+
+-COURIERRetrieve+
'-ONSITERetrieve--'

>-----+-----+-----+-----+-----+----->
'-WHERELOcation--location-'

>-----+-----+-----+-----+-----+----->
'-TOLoCation--location-' '-CMd--"comando"-'

```

## Parámetros

### nombre\_volumen (Necesario)

Especifica el nombre del volumen que se ha de procesar. Puede utilizar caracteres comodín. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE. El servidor busca nombres coincidentes de entre los siguientes volúmenes seleccionables:

- Volúmenes de copia de seguridad de base de datos, según lo especificado por el parámetro SOURCE de este mandato.
- Volúmenes de la agrupación de almacenamiento de copia de las agrupaciones de almacenamiento especificadas en el parámetro COPYSTGPOOL. Si no utiliza el parámetro COPYSTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de copia que se especificaron anteriormente en el mandato SET DRMCOPYSTGPOOL.
- Volúmenes de agrupación de almacenamiento de copia de contenedor de las agrupaciones de almacenamiento nombradas en el parámetro COPYCONTAINERSTGPOOL. Si no utiliza el parámetro COPYCONTAINERSTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de copia de contenedor que se especificaron anteriormente en el mandato SET DRMCOPYCONTAINERSTGPOOL.
- Los volúmenes de agrupación de almacenamiento de datos activos de las agrupaciones de almacenamiento nombradas en el parámetro ACTIVEDASTGPOOL. Si no utiliza el parámetro ACTIVEDASTGPOOL, el servidor procesa volúmenes de agrupaciones de almacenamiento de datos activos que se especificaron anteriormente en el mandato SET DRMACTIVEDASTGPOOL.

El resto de parámetros también pueden limitar los resultados del mandato.

### WHERESTate

Especifica el estado de los volúmenes que se han de procesar. Este parámetro es necesario si no se especifica TOSTATE o bien si se utiliza un carácter comodín para el nombre del volumen. Para obtener más información, consulte la Tabla 2 y la Tabla 3.

Especifique uno de los siguientes valores:

### MOuntable

Estos volúmenes contienen datos válidos y están disponibles para procesos en local. Los valores cambian a NOTMOUNTABLE si no se especifica el parámetro TOSTATE.

En función del comportamiento del parámetro REMOVE puede que el servidor expulse los volúmenes de una biblioteca automatizada antes de cambiar el estado del destino.

En el caso de las bibliotecas externas, el servidor envía peticiones al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas.

**NOTMOUNTABLE**

Estos volúmenes están en el local, contienen datos válidos y no están disponibles para procesos en el local. Los valores cambian a COURIER si no se especifica el parámetro TOSTATE.

**COURIER**

Estos volúmenes están con el transportista y se trasladan fuera del local. Los valores solo cambian a VAULT.

**VAULTRETRIEVE**

Estos volúmenes se encuentran en la cámara de seguridad fuera del local y no contienen datos válidos. Los valores cambian a COURIERRETRIEVE si no se especifica el parámetro TOSTATE.

**COURIERRETRIEVE**

Estos volúmenes están con el transportista y se trasladan al local. Los valores solo cambian a ONSITE RETRIEVE. El servidor elimina de la base de datos los registros de los volúmenes de agrupación de almacenamiento de copia reutilizable y de copia de seguridad de base de datos.

**BEGINDATE**

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha más antigua en la que existe información del volumen. Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/1998
TODAY	La fecha actual.	TODAY
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY-7 o -7  Para identificar los volúmenes que se han cambiado al estado actual hace una semana, puede especificar TODAY-7 o -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

**ENDDATE**

Especifica la fecha final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con anterioridad a la fecha especificada. El valor predeterminado es la fecha actual.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	09/15/1998
TODAY	La fecha actual.	TODAY  Para identificar los volúmenes que se han cambiado al estado actual hoy, especifique TODAY.
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-1 o -1  Para identificar los volúmenes que se han cambiado al estado actual hace una semana, puede especificar TODAY-1 o -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.

Valor	Descripción	Ejemplo
BOTM (principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### BEGINTime

Especifica la hora inicial utilizada para seleccionar volúmenes para su proceso. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el mandato MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada con el parámetro BEGINDATE.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada.	12:33:28
NOW	La hora actual en la fecha inicial especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada.	NOW+03:00 o +03:00
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada.	NOW-03:30 o -03:30  Si emite el mandato MOVE DRMEDIA a las 9:00 con BEGINTIME=NOW-03:30 o BEGINTIME=-03:30, el servidor identifica los volúmenes que se han cambiado a su estado actual a las 05:30 en la fecha de inicio que ha especificado.

#### ENDTime

Especifica la hora final utilizada para seleccionar volúmenes para su proceso. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el comando MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado son las 23:59:59.

Puede especificar la hora utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada.	12:33:28
NOW	La hora actual en la fecha final especificada.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada.	NOW+03:00 o +03:00  Si emite el mandato MOVE DRMEDIA a las 9:00 con ENDTIME=NOW+03:30 o ENDTIME=+03:30, el servidor identifica los volúmenes que se han cambiado a su estado actual a las 12:30 en la fecha de finalización que ha especificado.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada.	NOW-03:30 o -03:30

#### COPYContainerstgpool

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de almacenamiento de copia de contenedor que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento especificadas con el mandato SET DRMCOPYCONTAINERSTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYCONTAINERSTGPOOL se ha emitido anteriormente con nombres de agrupación de almacenamiento de copia de contenedor, el servidor procesa solo esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYCONTAINERSTGPOOL o si todas las agrupaciones de almacenamiento de copia de contenedor se han eliminado mediante el mandato SET DRMCOPYCONTAINERSTGPOOL, el servidor procesa todos los volúmenes de agrupación de almacenamiento de copia de contenedor en función de la configuración del

parámetro WHERESTATE. Si el parámetro se establece en un valor NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE, los volúmenes se procesan. Si el valor es MOUNTABLE, los volúmenes no se procesan.

#### COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de almacenamiento de copia que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento de copia especificadas con el mandato SET DRMCOPYSTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYSTGPOOL, o si se han eliminado todas las agrupaciones de almacenamiento de copia utilizando el mandato SET DRMCOPYSTGPOOL, el servidor procesará todos los volúmenes de agrupación de almacenamiento de copia que se encuentren en el estado especificado. Los estados disponibles son MOUNTABLE, NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE.

#### ACTIVEDatastgpool

Especifica el nombre de la agrupación de datos activos cuyos volúmenes van a procesarse. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si utiliza caracteres comodín para especificar este nombre, también debe especificar WHERESTATE.

Las agrupaciones de datos activos que se han especificado con este parámetro alteran temporalmente las agrupaciones de almacenamiento de datos activos que se han especificado con el mandato SET DRMACTIVEDATASTGPOOL. Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si el mandato SET DRMACTIVEDATASTGPOOL se emitió anteriormente con nombres de agrupaciones de datos activos válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMACTIVEDATASTGPOOL, o se han eliminado todas las agrupaciones de almacenamiento de copia utilizando el mandato SET DRMACTIVEDATASTGPOOL, el servidor procesa todos los volúmenes de agrupación de datos activos en el estado especificado. Los estados disponibles son NOTMOUNTABLE, COURIER, VAULTRETRIEVE o COURIERRETRIEVE. Los volúmenes que se encuentran en el estado MOUNTABLE no se procesarán.

#### Source

Especifica que se han de incluir los volúmenes de copia de seguridad de base de datos para su proceso. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Especifique uno de los siguientes valores:

##### DBBackup

Especifica que el servidor incluye volúmenes de copia de seguridad de base de datos completa e incremental para su proceso.

##### DBSnapshot

Especifica que el servidor incluye volúmenes de copia de seguridad de instantánea de base de datos para su proceso.

##### DBNone

Especifica que el servidor no incluye ningún volumen de copia de seguridad de base de datos para su proceso.

#### REMove

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles son YES, NO, BULK y UNTILEEFULL. El valor predeterminado es BULK. La respuesta del servidor a cada valor y el valor predeterminado depende del tipo de biblioteca.

Restricción: Solo puede utilizar la opción REMOVE=UNTILEEFULL con el tipo de biblioteca SCSI.

#### Bibliotecas SCSI

La respuesta del servidor al mandato depende de si la biblioteca tiene puertos de entrada/salida y, si es así, de si hay un puerto disponible para su uso. Consulte la tabla siguiente.

Tabla 1. Respuesta del servidor para bibliotecas SCSI

Característica de biblioteca	Respuesta del servidor cuando se especifica REMOVE=YES	Respuesta del servidor cuando se especifica REMOVE=BULK	Respuesta del servidor cuando se especifica REMOVE=NO	Respuesta del servidor cuando se especifica REMOVE=UNTILEEFULL

<b>Característica de biblioteca</b>	<b>Respuesta del servidor cuando se especifica REMOVE=YES</b>	<b>Respuesta del servidor cuando se especifica REMOVE=BULK</b>	<b>Respuesta del servidor cuando se especifica REMOVE=NO</b>	<b>Respuesta del servidor cuando se especifica REMOVE=UNTILEE FULL</b>
La biblioteca no tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
La biblioteca tiene puertos de entrada/salida y un puerto de entrada/salida está disponible	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no solicita un comando REPLY.	El servidor especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no solicita un comando REPLY.
La biblioteca tiene puertos de entrada/salida, pero no hay puertos disponibles	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor espera que un puerto se haga disponible.	El servidor especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no solicita un mandato REPLY.	El mandato falla y los volúmenes elegibles restantes no se procesan.  Haga que el puerto esté disponible y emita el comando de nuevo.

#### Bibliotecas 349X

##### REMOVE=YES

El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.

##### REMOVE=BULK

El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.

##### REMOVE=NO

El gestor de biblioteca 3494 no expulsa el volumen. El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

#### Bibliotecas ACSLS

##### REMOVE=YES o REMOVE=BULK

El servidor expulsa el cartucho en la estación de E/S que convenga.

El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.

Mientras tiene lugar el traspaso de volúmenes del estado MOUNTABLE cuando se ha especificado REMOVE=YES, el mandato MOVE MEDIA utiliza más de una ranura del CAP para una biblioteca StorageTek que dispone de software ACSLS.

#### REMOVE=NO

El servidor no expulsa el cartucho.

El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

#### Bibliotecas externas

Puede especificar REMOVE=YES, REMOVE=BULK o REMOVE=NO. Para cualquier valor el servidor necesita que el gestor de biblioteca externo expulse el volumen de la biblioteca.

El hecho de que el volumen se expulse de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

#### TOSTate

Especifica el estado destino de los volúmenes que están procesándose. Este parámetro es necesario si el parámetro WHERESTATE no se ha especificado. Si especifica el parámetro TOSTATE, pero no el parámetro WHERESTATE, debe especificar el nombre del volumen. Los caracteres comodín no están permitidos. Consulte los apartados Tabla 2 y Tabla 3. Especifique uno de los siguientes valores:

#### NOTMOUNTABLE

Especifica que los volúmenes se cambiarán al estado NOTMOUNTABLE. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE.

Si los volúmenes están en la biblioteca automática, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado NOTMOUNTABLE, en función del comportamiento del parámetro REMOVE.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

#### COURier

Especifica que los volúmenes se cambiarán al estado COURIER. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE o NOTMOUNTABLE.

En función del comportamiento del parámetro REMOVE y de si los volúmenes se encuentran en una biblioteca automatizada, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado COURIER.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

#### VAult

Especifica que los volúmenes se cambiarán al estado VAULT. Este valor sólo es válido si los volúmenes están en el estado MOUNTABLE, NOTMOUNTABLE o COURIER.

En función del comportamiento del parámetro REMOVE y de si los volúmenes se encuentran en una biblioteca automatizada, puede que el servidor expulse los volúmenes de la biblioteca antes de cambiarlos al estado VAULT.

En el caso de las bibliotecas externas, el servidor envía solicitudes al gestor de bibliotecas externas para expulsar los volúmenes. El hecho de que los volúmenes se expulsen de la biblioteca dependerá del gestor de bibliotecas externas. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que deberá seguir al utilizar el mandato MOVE DRMEDIA para realizar el seguimiento de volúmenes.

#### COURIERRetrieve

Especifica que los volúmenes se cambiarán al estado COURIERRETRIEVE. Este valor sólo es válido si los volúmenes están en el estado VAULTRETRIEVE.

#### ONSITERetrieve

Especifica que los volúmenes se cambiarán al estado ONSITERETRIEVE. Este valor sólo es válido si los volúmenes están en el estado VAULTRETRIEVE o COURIERRETRIEVE. Para los volúmenes de agrupaciones de almacenamiento de copia



reutilizables y de copia de seguridad de la base de datos que se cambian al estado ONSITERETRIEVE, el servidor suprime de la base de datos los registros de los volúmenes.

#### WHERELOcation

Especifica la ubicación actual de los volúmenes. Este parámetro es opcional. La longitud máxima de la lista de la ubicación es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

#### TOLOcation

Especifica la ubicación destino de los volúmenes. Este parámetro es opcional. La longitud máxima de la ubicación especificada es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Si no especifica la ubicación de destino, se utilizará la ubicación que define el comando SET DRMNOTMOUNTABLE.

#### CMd

Especifica el mandato que se emitirá para cada volumen procesado con el mandato MOVE DRMEDIA. DRM graba los mandatos en un archivo que especifica el parámetro CMDFILENAME. Una vez finalizada la operación MOVE DRMEDIA, se pueden emitir los mandatos en el archivo. El mandato puede contener hasta 255 caracteres. Si el mandato contiene más de 240 caracteres, se divide en varias líneas y se añaden caracteres de continuación (+). Es posible que necesite alterar el carácter de continuación en función del sistema operativo. Este parámetro es opcional.

#### comando

La serie de los mandatos debe estar encerrada entre comillas. La serie no debe contener comillas intercaladas. Por ejemplo, el parámetro CMD siguiente es válido:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

El ejemplo siguiente no es una forma válida de especificar el parámetro CMD:

```
cmd=""checkin libvol lib8mm" &vol status=scratch""
```

El comando puede incluir variables de sustitución. Las variables no son sensibles a las mayúsculas y minúsculas, y no deben contener espacios en blanco detrás del símbolo &. Puede especificar los valores siguientes:

#### &VOL

Un nombre de volumen.

#### &LOC

Una ubicación de volumen.



#### &VOLDSN

El nombre de archivo que se debe grabar en las etiquetas de los medios de acceso secuencial. Por ejemplo, si la clase de dispositivo aplicable establece BKP como el prefijo del volumen de cinta, un nombre de archivo del volumen de cinta de la agrupación de almacenamiento de copia podría ser BKP.BFS y un nombre de archivo del volumen de cinta de copia de seguridad de la base de datos podría ser BKP.DBB.

#### &NL

El carácter de nueva línea. Cuando se utiliza un nuevo carácter de línea, el mandato se divide en la variable &NL. Si es necesario, debe especificar el carácter de continuación adecuado antes de &NL. Si no se especifica el carácter &NL y la línea de mandatos es superior a 240 caracteres, la línea se divide en varias líneas y se añaden los caracteres de continuación (+).


#### Sistemas operativos AIX Sistemas operativos LinuxCMDFilename

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados mediante el parámetro CMD. Este parámetro es opcional.

Si no especifica un nombre de archivo o si especifica una serie nula (""), DRM utilizará el nombre de archivo que especifica el mandato SET DRMCMDFILENAME. Si no especifica un nombre de archivo con el comando SET DRMCMDFILENAME, DRM generará un nombre de archivo añadiendo `exec.cmds` al nombre de ruta de directorio del directorio de trabajo actual del servidor.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

#### Sistemas operativos WindowsCMDFilename

 Sistemas operativos WindowsEspecifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados mediante el parámetro CMD. Este parámetro es opcional.

La longitud máxima del nombre de archivo son 259 caracteres. Si no especifica un nombre de archivo o si especifica una serie nula (""), DRM utilizará el nombre de archivo que especifica el mandato SET DRMCMDFILENAME. Si no se especifica un nombre de archivo con el mandato SET DRMCMDFILENAME, DRM genera un nombre de archivo uniendo `exec.cmd` al directorio que representa esta instancia del servidor (por lo general, el directorio desde el que se ha instalado el servidor). El DRM asigna el nombre de archivo especificado o generado. Si existe el nombre de archivo, DRM intenta utilizarlo; los datos existentes quedan sobregrabados. Si ocurre esto y los mandatos ejecutables del archivo no se han ejecutado, emita el mandato QUERY DRMEDIA para volver a crear los mandatos ejecutables para la transición de volumen y la fecha deseadas.

Si el mandato MOVE DRMEDIA no se ha ejecutado correctamente y no se ha grabado ninguna de las series de mandatos especificadas con el parámetro CMD para el volumen que se ha traspasado correctamente, el nombre de archivo asignado se suprime. .

#### APPend

Especifica si se graba encima del contenido existente del archivo de mandatos o se añaden los mandatos al archivo. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No  
DRM graba encima del contenido del archivo.

Yes  
DRM agrega los comandos al archivo.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No  
Especifica que el servidor procesa este comando en un proceso subordinado.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para ver si la operación se ha realizado correctamente, emita el mandato QUERY ACTLOG.

Yes  
Especifica que el servidor procesa este comando en primer plano. Espere a que el mandato finalice antes de continuar con otras tareas. El servidor muestra a continuación los mensajes de salida en el cliente de administración.  
Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

x  
El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.

y  
El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.

z  
El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

## Reglas para estados y ubicaciones de destino

La siguiente tabla muestra cómo DRM determina el estado de destino y la ubicación de un volumen.

#### Estado de destino

- El valor del parámetro TOSTATE que se ha especificado.
- El estado siguiente del parámetro WHERESTATE que se ha especificado, si no se ha especificado el parámetro TOSTATE.

#### Ubicación destino

- El valor del parámetro TOLOCATION que se ha especificado.
- La ubicación del parámetro TOSTATE que se ha especificado, si no se ha especificado el parámetro TOLOCATION.
- La ubicación del estado siguiente del parámetro WHERESTATE que se ha especificado, si no se han especificado los parámetros TOLOCATION y TOSTATE.

Tabla 2. Destino y ubicación de volumen

Parámetros especificados	Estado de destino	Ubicación destino
--------------------------	-------------------	-------------------

Parámetros especificados	Estado de destino	Ubicación destino
WHERESTATE	El estado siguiente de WHERESTATE	Ubicación del estado siguiente
WHERESTATE, TOSTATE	TOSTATE	Ubicación de TOSTATE
WHERESTATE, TOLOCATION	El estado siguiente de WHERESTATE	TOLOCATON
WHERESTATE, TOSTATE, TOLOCATION	TOSTATE	TOLOCATION
TOSTATE	TOSTATE	Ubicación de TOSTATE
TOSTATE, WHERELOCATION	TOSTATE	Ubicación de TOSTATE
TOSTATE, WHERELOCATION, TOLOCATION	TOSTATE	TOLOCATION

## Reglas para transiciones de estado

Las tablas siguientes muestran las transiciones de estado que pueden adoptar los volúmenes según su estado actual.

Tabla 3. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino		
	MOUNTABLE	NOTMOUNTABLE	COURIER
MOUNTABLE	N	S	S
NOTMOUNTABLE	N	N	S
COURIER	N	N	N
VAULT	N	N	N
VAULTRETRIEVE	N	N	N
COURIERRETRIEVE	N	N	N
ONSITERETRIEVE	N	N	N

Tabla 4. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino	
	VAULT	VAULTRETRIEVE
MOUNTABLE	S	N
NOTMOUNTABLE	S	N
COURIER	S	N
VAULT	N	N
VAULTRETRIEVE	N	N
COURIERRETRIEVE	N	N
ONSITERETRIEVE	N	N

Tabla 5. Transiciones de estado para volúmenes

El estado actual del volumen	Estado de destino	
	COURIERRETRIEVE	ONSITERETRIEVE
MOUNTABLE	N	N
NOTMOUNTABLE	N	N
COURIER	N	N
VAULT	N	N
VAULTRETRIEVE	S	S
COURIERRETRIEVE	N	S
ONSITERETRIEVE	N	N

## Ejemplo: traspasar medios de recuperación ante siniestro desde el estado NOTMOUNTABLE

Traspasar medios de recuperación ante siniestro que se encuentran en estado NOTMOUNTABLE al estado COURIER y, a continuación, consultar los resultados.

```
move drmedia * wherestate=notmountable  
tostate=courier
```

```
query actlog search="MOVE DRMEDIA"
```

```
08/11/1999 11:12:24 ANR0984I Proceso 10 para MOVE DRMEDIA  
 iniciado  
 en BACKGROUND a las 11:12:24.  
08/11/1999 11:12:24 ANR0610I MOVE DRMEDIA iniciado por  
 HSIAO como  
 proceso 10.  
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen TAPE0P ha pasado  
 del estado NOTMOUNTABLE al  
 estado COURIER.  
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen TAPE1P ha pasado  
 del estado NOTMOUNTABLE al  
 estado COURIER.  
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen DBTP02 ha pasado  
 del estado NOTMOUNTABLE al  
 estado COURIER.  
08/11/1999 11:12:25 ANR6683I MOVE DRMEDIA: El volumen DBTP01 ha  
 pasado  
 del estado NOTMOUNTABLE al  
 estado COURIER.  
08/11/1999 11:12:25 ANR6682I El comando MOVE DRMEDIA ha  
 finalizado 4 volúmenes  
 procesados.  
08/11/1999 11:12:25 ANR0611I MOVE DRMEDIA iniciado por HSIAO  
 como  
 proceso 10 ha finalizado.  
08/11/1999 11:12:25 ANR0985I Proceso 10 para MOVE DRMEDIA  
 ejecutándose  
 BACKGROUND ha procesado  
 4 elementos y ha tenido un estado  
 de  
 terminación de SUCCESS a las 11:12:25.
```

## **Ejemplo: traspasar medios de recuperación ante siniestro desde el estado MOUNTABLE**

Traspasar medios de recuperación ante siniestro desde el estado MOUNTABLE al estado COURIER. Si el medio está en una biblioteca automatizada, MOVE DRMEDIA expulsa el medio antes de cambiar el estado.

```
move drmedia * wherestate=mountable tostate=courier wait=yes
```

```
ANR0984I Proceso 12 para MOVE DRMEDIA iniciado  
 en FOREGROUND a las 09:57:17.  
ANR0609I MOVE DRMEDIA iniciado como proceso 12.  
ANR0610I MOVE DRMEDIA iniciado por HSIAO como  
 proceso 12.  
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para  
 volumen TAPE01 de biblioteca LIB8MM iniciándose.  
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el  
 volumen TAPE01 de biblioteca LIB8MM se ha completado  
 correctamente.  
ANR6683I MOVE DRMEDIA: El volumen TAPE01 ha pasado del  
 estado MOUNTABLE al estado COURIER.  
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para  
 volumen TAPE02 de biblioteca LIB8MM iniciándose.  
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el  
 volumen TAPE02 de biblioteca LIB8MM se ha completado  
 correctamente.  
ANR6683I MOVE DRMEDIA: El volumen TAPE02 ha pasado del  
 estado MOUNTABLE al estado COURIER.  
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para  
 volumen DBTP05 de biblioteca LIB8MM iniciándose.  
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el  
 volumen DBTP05 de biblioteca LIB8MM se ha completado  
 correctamente.  
ANR6683I MOVE DRMEDIA: El volumen DBTP05 ha pasado del  
 estado MOUNTABLE al estado COURIER.  
ANR6696I MOVE DRMEDIA: CHECKOUT LIBVOLUME para  
 volumen DBTP04 de biblioteca LIB8MM iniciándose.  
ANR6697I MOVE DRMEDIA: CHECKOUT LIBVOLUME para el
```

```

volumen DBTP04 de biblioteca LIB8MM se ha completado
correctamente.
ANR6683I MOVE DRMEDIA: El volumen DBTP04 ha pasado del
estado MOUNTABLE al estado COURIER.
ANR6682I Comando MOVE DRMEDIA finalizado: 4 volúmenes
procesados.
ANR0611I MOVE DRMEDIA iniciado por HSIAO como el
proceso 12 ha finalizado.
ANR0985I Proceso 12 para MOVE DRMEDIA ejecutándose
en FOREGROUND ha procesado 4 elementos con un
estado de terminación de SUCCESS a las 10:12:25.

```

## Ejemplo: traspasar medios de recuperación ante siniestro desde el estado VAULTRETRIEVE

Traspasar los medios de recuperación ante siniestro del estado VAULTRETRIEVE al estado ONSITERETRIEVE. Generar un mandato CHECKIN LIBVOLUME para cada volumen que se procesa correctamente y almacenar los mandatos en un archivo:

 Sistemas operativos AIX  Sistemas operativos Linux

```

move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=/drm/move/exec.cmds
cmd="checkin libvol lib8mm &vol status=scratch"

```

 Sistemas operativos Windows

```

move drmedia * wherestate=vaultretrieve tostate=onsiteretrieve
cmdfilename=c:\drm\move\exec.cmd
cmd="checkin libvol lib8mm &vol status=scratch"

```

Consultar los resultados:




```

query actlog search="MOVE DRMEDIA"

08/13/1999 09:12:24 ANR0984I Proceso 15 para MOVE DRMEDIA iniciado en
BACKGROUND a las 09:12:24.
08/13/1999 09:12:24 ANR0610I MOVE DRMEDIA iniciado por HSIAO como
proceso 15.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen CSTP01
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen CSTP02
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen DBTP10
se ha suprimido.
08/13/1999 09:12:24 ANR6684I MOVE DRMEDIA: El volumen DBTP11
se ha suprimido.
08/13/1999 09:12:27 ANR6682I El comando MOVE DRMEDIA ha finalizado:
4 volúmenes
procesados.
08/13/1999 09:12:42 ANR0611I MOVE DRMEDIA iniciado por HSIAO como
proceso 15 ha finalizado.
08/13/1997 09:12:42 ANR0985I Proceso 15 para MOVE DRMEDIA
ejecutándose en
BACKGROUND ha procesado
4 elementos y ha tenido un estado
de terminación de SUCCESS a las
09:12:42.

```

Los mandatos para dar de alta los volúmenes también se han creado en el archivo especificado con el parámetro CMDFILENAME:

-  Sistemas operativos AIX  Sistemas operativos Linux/drm/move/exec.cmds
-  Sistemas operativos Windowsc:\drm\move\exec.cmd

El archivo contiene estas líneas:

```







checkin libvol lib8mm CSTP01 status=scratch
checkin libvol lib8mm CSTP02 status=scratch
checkin libvol lib8mm DBTP10 status=scratch
checkin libvol lib8mm DBTP11 status=scratch

```

Consejo: Para procesar los mandatos CHECKIN LIBVOLUME, emita el mandato MACRO con el nombre de archivo como el nombre de macro.

## Comandos relacionados

Tabla 6. Comandos relacionados con MOVE DRMEDIA

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DISMOUNT VOLUME	Desmonta un volumen secuencial extraíble según el nombre de volumen.
PREPARE	Crea un archivo de plan de recuperación.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY PROCESS	Muestra información sobre procesos subordinados.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMCOURIERNAME	Especifica el nombre del transportista del medio de recuperación ante siniestro.
SET DRMDBBACKUPEXPIREDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMVaultNAME	Especifica el nombre de la cámara de seguridad donde está almacenado el medio DRM.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.
SET DRMFILEPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.
SET DRMNOTMOUNTABLENAME	Especifica el nombre de ubicación del medio DRM que se ha de enviar fuera del local.

## MOVE GRPMEMBER (Mover un miembro de grupo de servidores)

Utilice este comando para traspasar un miembro de un grupo de servidores a otro grupo de servidores. El comando no se ejecutará si el miembro que se traspasa tiene el mismo nombre que uno de los miembros actuales del grupo.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-MOVE GRPMEMBER--nombre_miembro--grupo_origen--grupo_destino-><
```

## Parámetros

- nombre\_miembro (Obligatorio)  
Especifica el miembro (un servidor o un grupo de servidores) que se traspasa.
- grupo\_origen (Obligatorio)  
Especifica el grupo de servidores al que está asociado actualmente el miembro.
- grupo\_destino (Obligatorio)  
Especifica el nuevo grupo de servidores del miembro.

## Ejemplo: traspasar un servidor a otro grupo de servidores

Traspasar el miembro PAYSON del grupo REGION1 al grupo REGION2.

```
move grpmember payson region1 region2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con MOVE GRPMEMBER

Comando	Descripción
DEFINE GRPMEMBER	Define un servidor como miembro de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE GRPMEMBER	Suprime un servidor de un grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVER	Muestra información sobre servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## MOVE MEDIA (Mover medios de agrupación de almacenamiento de acceso secuencial)

Utilice este comando para gestionar agrupaciones de almacenamiento de desbordamiento. La base de datos hace el seguimiento de los medios que se traspasan utilizando este mandato..

Este comando se aplica a los volúmenes de las agrupaciones de almacenamiento primarias y de copia gestionadas por una biblioteca automatizada (que puede ser externa). La biblioteca no tiene que estar llena. Se pueden procesar al mismo tiempo uno o más volúmenes de agrupaciones de almacenamiento de acceso secuencial.

Utilice el parámetro DAYS para identificar los volúmenes elegibles para ser trasladados. Utilice el parámetro OVERFLOW LOCATION para registrar la ubicación de almacenamiento de los medios traspasados.

Este comando genera un proceso subordinado que puede visualizar utilizando el comando QUERY PROCESS. Para cancelarlo, emita el comando CANCEL PROCESS.

Para determinar si el mandato se ha ejecutado correctamente, emita el mandato QUERY ACTLOG o bien utilice la consola del servidor.

Los volúmenes que se trasladan mediante el mandato MOVE DRMEDIA para la recuperación fuera de local no se procesan mediante el mandato MOVE MEDIA.

El mandato MOVE MEDIA no procesa volúmenes de agrupación de almacenamiento de copia cuyo valor de DRM STATUS es NOTMOUNTABLE, COURIER o VAULT.

## Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Si el parámetro CMD NO está especificado: privilegio de operador o de sistema.
- Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO: privilegio de operador, de almacenamiento sin restricciones o de sistema.





## MOUNTABLENotinlib

Especifica que los volúmenes de agrupación de almacenamiento deben volver a cambiar del estado MOUNTABLENOTINLIB al estado MOUNTABLEINLIB. Los volúmenes en estado MOUNTABLENOTINLIB pueden contener datos válidos y están en la ubicación de desbordamiento.

- Para los volúmenes reutilizables vacíos, el mandato MOVE MEDIA suprime los registros de volúmenes para que éstos puedan volver a utilizarse.
- Para los volúmenes privados, el mandato MOVE MEDIA restablece la ubicación del volumen en un valor en blanco, cambia el estado del volumen a CHECKIN y cambia la fecha de la última actualización a la fecha actual.
- Para los volúmenes reutilizables con datos, el mandato MOVE MEDIA restablece la ubicación del volumen en un valor en blanco, cambia el estado del volumen a CHECKIN y cambia la fecha de la última actualización a la fecha actual.

Atención: Los volúmenes que están en el estado CHECKIN pueden contener datos válidos y no es necesario darlos de alta en la biblioteca.

## WHERESTATUS

Especifica que el proceso de traslado debe ser restringido por el estado de volumen. Este parámetro es opcional. Puede especificar varios estados en una lista si separa cada uno con una coma sin dejar espacios intercalados. Si no especifica este parámetro, los volúmenes traspasados del estado MOUNTABLEINLIB al estado MOUNTABLENOTINLIB están restringidos a sólo los volúmenes llenos, y los volúmenes traspasados del estado MOUNTABLENOTINLIB al estado MOUNTABLEINLIB están restringidos a sólo los volúmenes vacíos.

Los valores posibles son:

### FULL

Se traspasan los volúmenes con el estado FULL.

### FILLing

Se traspasan los volúmenes con el estado FILLING.

### EMPTy

Se traspasan los volúmenes con el estado EMPTY.

## ACCess

Especifica la forma en que los usuarios y los procesos del sistema acceden a los archivos del volumen de agrupación de almacenamiento que se traslada desde una biblioteca automatizada y se almacena en una ubicación de desbordamiento mediante el comando MOVE MEDIA. Este parámetro es opcional. Si no especifica este parámetro, el traslado de los volúmenes desde el estado MOUNTABLEINLIB hasta el proceso MOUNTABLENOTINLIB actualiza la modalidad de acceso de los volúmenes a READONLY, y el traslado de los volúmenes desde el estado MOUNTABLENOTINLIB hasta el proceso MOUNTABLEINLIB actualiza la modalidad de acceso de los volúmenes a READWRITE.

Los valores posibles son:

### READWrite

Especifica que los usuarios y los procesos del sistema pueden leer y grabar en archivos almacenados en el volumen que está en la ubicación de desbordamiento. Si se especifica este valor, IBM Spectrum Protect solicita que se dé de alta el volumen en la biblioteca cuando se necesita el volumen para una operación de lectura o grabación.

### READOnly

Especifica que los usuarios y los procesos del sistema pueden leer pero no grabar en los archivos que están almacenados en el volumen que está en la ubicación de desbordamiento. El servidor sólo solicita que se dé de alta el volumen en la biblioteca cuando el volumen se necesita para una operación de lectura.

## OVFLocation

Especifica la ubicación de desbordamiento que es el destino de los volúmenes que están procesándose. La longitud máxima del nombre de ubicación son 255 caracteres. La información de nombre de ubicación debe estar delimitada con comillas si contiene caracteres en blanco. Si no especifica una ubicación de desbordamiento y la agrupación de almacenamiento tampoco tiene ninguna ubicación de desbordamiento identificada, el servidor cambia la ubicación del volumen expulsado por una serie nula ("").

## REMove

Especifica que el servidor intenta trasladar el volumen fuera de la biblioteca en la estación o los puertos de E/S que convenga. Este parámetro es opcional. Los valores posibles son YES, BULK y NO. El valor predeterminado es BULK. La respuesta del servidor a cada una de estas opciones y los valores predeterminados se describen en las siguientes tablas.

**Bibliotecas 349X:** En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas 349X.

Tabla 1. Cómo responde el servidor en las bibliotecas 349X

REMOVE=YES	REMOVE=BULK	REMOVE=NO
------------	-------------	-----------

REMOVE=YES	REMOVE=BULK	REMOVE=NO
El gestor de biblioteca 3494 expulsa el cartucho en la estación de E/S que convenga.	El gestor de biblioteca 3494 expulsa el cartucho en el recurso de salida de alta capacidad.	El gestor de biblioteca 3494 no expulsa el volumen.  El servidor deja el cartucho en la biblioteca en la categoría INSERT para que lo utilicen otras aplicaciones.

**Bibliotecas SCSI:** La tabla siguiente muestra cómo responde el servidor ante las opciones YES, BULK y NO en las bibliotecas SCSI.

Tabla 2. Cómo responde el servidor en las bibliotecas SCSI

Si una biblioteca...	Y REMOVE=YES...	Y REMOVE=BULK...	Y REMOVE=NO
No tiene puertos de entrada/salida	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Tiene puertos de entrada/salida y un puerto de entrada/salida está disponible	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor mueve el cartucho al puerto de entrada/salida disponible y especifica la dirección del puerto en un mensaje.  El servidor no le solicita que retire el cartucho y no solicita un comando REPLY.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.
Tiene puertos de entrada/salida, pero no hay puertos disponibles	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  A continuación, el servidor le solicita que retire el cartucho de la ranura y que emita un mandato REPLY.	El servidor espera que un puerto de entrada/salida se haga disponible.	El servidor deja el cartucho en su ranura actual en la biblioteca y especifica la dirección de la ranura en un mensaje.  El servidor no le solicita que retire el cartucho y no necesita un mandato REPLY.

**Bibliotecas ACSLS:** En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas ACSLS.

Tabla 3. Cómo responde el servidor en las bibliotecas ACSLS

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho en la estación de E/S que convenga.  El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.  Mientras tiene lugar el traspaso de volúmenes del estado MOUNTABLE cuando se ha especificado REMOVE=YES, el mandato MOVE MEDIA utiliza más de una ranura del CAP para una biblioteca StorageTek que dispone de software ACSLS.	El servidor no expulsa el cartucho.  El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

**Bibliotecas externas:** En la tabla siguiente se muestra cómo responde el servidor en las bibliotecas externas.



Tabla 4. Cómo responde el servidor en las bibliotecas externas


REMOVE=YES o REMOVE=BULK	REMOVE=NO
--------------------------	-----------

REMOVE=YES o REMOVE=BULK	REMOVE=NO
El servidor expulsa el cartucho en la estación de E/S que convenga. El servidor suprime del inventario de bibliotecas del servidor la entrada del volumen.	El servidor no expulsa el cartucho.  El servidor suprime del inventario de la biblioteca del servidor la entrada del volumen y deja el volumen en la biblioteca.

## CMD

Especifica la creación de comandos ejecutables. Este parámetro es opcional. La especificación de mandatos ejecutables se ha de encerrar entre comillas. La longitud máxima de la especificación del comando ejecutable es de 255 caracteres. Para cada volumen que procese correctamente el comando MOVE MEDIA, el servidor graba los comandos asociados en un archivo. Especifique el nombre de archivo con el parámetro CMDFILENAME.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica el nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie exec.cmds.media al directorio del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no especifica el nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie exec.cmd.media al directorio del servidor de IBM Spectrum Protect.

Si la longitud del mandato escrito en el archivo sobrepasa los 255 caracteres, se divide en varias líneas y se añade un carácter de continuación, +, a todas menos a la última línea del mandato. Puede que deba alterar el carácter de continuación en función de los requisitos del producto que ejecuta los mandatos.

Si no especifica CMD, el mandato MOVE MEDIA no generará ningún mandato ejecutable.

## serie

Especifica la serie para crear un comando ejecutable. Puede especificar cualquier texto de formato libre para la serie. Encierre toda la serie entre comillas. Por ejemplo, la siguiente es una especificación válida de un mandato ejecutable:

```
CMD="UPDATE VOLUME &VOL"
```

La siguiente es una especificación no válida de un mandato ejecutable:

```
CMD=" "UPDATE VOLUME" &VOL"
```

## sustitución

Especifica una variable para la que desea que el mandato sustituya un valor. Las posibles variables de sustitución son:

### &VOL

Sustituye el nombre de volumen por &VOL. Puede especificar caracteres en minúsculas, &vol. No debe especificar ni espacios ni blancos entre el signo & y VOL. Si existen espacios o blancos entre el ampersand y VOL, el mandato MOVE MEDIA los trata como series y no se establece ninguna sustitución. Si no se especifica &VOL, no se establecerá ningún nombre de volumen en el mandato ejecutable.

### &LOC

Sustituye que el volumen por &LOC. Puede especificar caracteres en minúsculas, &loc. No debe especificar ni espacios ni blancos entre el signo & y LOC. Si existen espacios o blancos entre el ampersand y LOC, el mandato MOVE MEDIA los trata como series y no se establece ninguna sustitución. Si no se especifica &LOC, no se establecerá ningún nombre de ubicación en el mandato ejecutable.

### &VOLDSN



Sustituye el nombre de archivo del volumen por &VOLDSN. Un ejemplo de un nombre de archivo de volumen de cinta de agrupación de almacenamiento que utiliza el prefijo predeterminado ADSM es ADSM.BFS. Si no se especifica &VOLDSN, no se establecerá ningún nombre de archivo de volumen en el mandato ejecutable.


### &NL

Sustituye un nuevo carácter de línea por &NL. Cuando se especifica &NL, el mandato MOVE MEDIA subdivide el mandato en la posición en la que se encuentra &NL y no añade ningún carácter de continuación. El usuario es el responsable de especificar el carácter de continuación correcto antes de &NL, si es necesario. El usuario también es el responsable de la longitud de la línea escrita. Si no se especifica &NL y la longitud de la línea de mandatos sobrepasa los 255 caracteres, la línea de mandatos se dividirá en varias líneas y se añadirá un carácter de continuación, +, a todas menos a la última línea del mandato.

## CMDfilename

Especifica el nombre completo de vía de acceso de un archivo que contiene los mandatos que se han especificado con CMD. Este parámetro es opcional. La longitud máxima del nombre de archivo es de 1279 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica un nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie exec.cmds.media al directorio del servidor de IBM Spectrum Protect. El directorio del servidor es el directorio de trabajo actual del proceso servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no especifica un nombre de archivo, el mandato MOVE MEDIA genera un nombre de archivo predeterminado agregando la serie *exec.cmd.media* al directorio del servidor de IBM Spectrum Protect. El directorio del servidor es el directorio de trabajo actual del proceso servidor de IBM Spectrum Protect.

El mandato MOVE MEDIA asigna automáticamente el nombre de archivo que se ha especificado o generado. Si existe el nombre de archivo, puede utilizar el parámetro APPEND=YES para agregarlo al archivo. De lo contrario, el archivo quedará sobregabado. Si un archivo se ha sobregabado por accidente y debe ejecutar los mandatos que contenía el archivo, emita el mandato QUERY MEDIA para volver a crear los mandatos ejecutables para los volúmenes deseados. Si el comando MOVE MEDIA no se ejecuta correctamente después de haberse asignado el archivo de comandos, el archivo no se suprimirá.

#### APPend

Especifica que se graba al principio o al final de los datos del archivo de comandos. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se han de escribir datos desde el principio del archivo de comandos. Si el archivo de mandatos ya existe, se sobregabará el contenido.

Yes

Especifica que se agrega el archivo de comandos grabando al final de los datos del archivo de comandos.

#### CHECKLabel

Especifica si el servidor lee las etiquetas de los volúmenes de los medios secuenciales. Con los dispositivos SCSI, puede suprimir la comprobación de etiquetas si establece CHECKLabel en NO. Este parámetro no es aplicable a las bibliotecas 349X. Este parámetro es opcional. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que el servidor intenta leer la etiqueta del medio. Leer la etiqueta del medio verifica que se está dando de baja el volumen correcto.

No

Especifica que el servidor no intenta leer la etiqueta del medio. De este modo aumenta el rendimiento ya que no se produce el proceso de lectura.

#### CAP

Especifica qué puerto de acceso al cartucho (CAP) se debe utilizar para expulsar volúmenes si se especifica REMOVE=YES. Este parámetro sólo se aplica a los volúmenes de las bibliotecas ACSLS. Si no existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es obligatorio. Si existe en la biblioteca un valor de prioridad CAP superior a cero, este parámetro es opcional. De forma predeterminada, todos los CAP tienen inicialmente un valor de prioridad de 0, lo que significa que ACSLS no selecciona automáticamente el CAP.

Para que se visualicen identificadores CAP válidos (x,y,z), emita el mandato QUERY CAP especificando ALL desde la consola ACSSA (Automated Cartridge System System Administrator) del host del servidor ACSLS. Los identificadores son los siguientes:

x

El identificador de ACS (Automated Cartridge System). Este identificador puede ser un número dentro del rango de 0 a 126.

y

El identificador de LSM (Library Storage Module). Este identificador puede ser un número dentro del rango de 0 a 23.

z

El identificador de CAP. Este identificador puede ser un número dentro del rango de 0 a 11.

Para obtener más información, consulte la documentación de StorageTek.

## Ejemplo: trasladar todos los volúmenes fuera de la biblioteca

---

Trasladar fuera de la biblioteca todos los volúmenes completos que estén en la agrupación de almacenamiento primaria secuencial ARCHIVE.


```
move media * stgpool=archive
```

## Ejemplo: generar los comandos para dar de alta

---

Generar los comandos CHECKIN LIBVOLUME para los volúmenes llenos y parcialmente llenos que están en la agrupación de almacenamiento primaria ONSITE.ARCHIVE y almacenados en la ubicación de desbordamiento, room2948/bldg31.

 Sistemas operativos AIX  Sistemas operativos Linux MOVE MEDIA crea los comandos ejecutables en /tsm/move/media/checkin.vols

 Sistemas operativos Windows MOVE MEDIA crea los comandos ejecutables en c:\tsm\move\media\checkin.vols




```

move media * stgpool=onsite.archive
wherestate=mountablenotinlib wherestatus=full,filling
ovflocation=room2948/bldg31
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols

checkin libvolume lib3494 TAPE04 status=private
checkin libvolume lib3494 TAPE13 status=private
checkin libvolume lib3494 TAPE14 status=private

```

Consejo: Ejecute el mandato CHECKIN LIBVOLUME emitiendo el mandato MACRO con la información siguiente como nombre de macro:

-  Sistemas operativos AIX  Sistemas operativos Linux/tsm/move/media/checkin.vols
-  Sistemas operativos Windows:c:\tsm\move\media\checkin.vols

## Comandos relacionados

Tabla 5. Comandos relacionados con MOVE MEDIA

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY MEDIA	Muestra información acerca de los volúmenes de agrupaciones de almacenamiento que se ha trasladado mediante el mandato MOVE MEDIA.
QUERY PROCESS	Muestra información sobre procesos subordinados.

## MOVE NODEDATA (trasladar datos por nodo en una agrupación de almacenamiento secuencial)

Utilice este mandato para trasladar datos que se encuentran en una agrupación de almacenamiento de acceso secuencial. Puede trasladar datos para uno o más nodos, o para un grupo de nodos asignados con espacios de archivos seleccionados. También puede trasladar espacios de archivos seleccionados para un solo nodo. Los datos se pueden encontrar en una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia o una agrupación de datos activos.

Este comando es útil para reducir el número de montajes de volúmenes durante las operaciones de restauración o de recuperación del cliente, pues consolida los datos para un nodo específico dentro de una agrupación de almacenamiento, o bien para traspasar los datos a otra agrupación de almacenamiento. Por ejemplo, puede utilizar este comando para traspasar datos a una agrupación de almacenamiento de acceso aleatorio como preparación para el proceso de restauración del cliente.

Asegúrese de que la modalidad de acceso de los volúmenes desde los que está trasladando los datos del nodo sea de lectura y grabación o de lectura y que la modalidad de acceso de los volúmenes a los que está trasladando los datos del nodo se haya establecido para lectura/grabación. Esta operación no trasladará los datos de los volúmenes cuyas modalidades de acceso sean fuera del local, no disponible o destruido.

El mandato MOVE NODEDATA adopta dos formas, en función de si traspasa datos sólo para los espacios de archivo seleccionados. La sintaxis y los parámetros de cada formato se definen por separado.

Restricción: No puede trasladar datos de nodo a o desde una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Tabla 1. Mandatos relacionados con MOVE NODEDATA

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVE DATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.

Comando	Descripción
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
UPDATE COLLOGGROUP	Actualiza la descripción de un grupo de proximidad.

- MOVE NODEDATA (Trasladar datos de los espacios de archivos para uno o varios nodos o un grupo de proximidad)  
Utilice este mandato para mover los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.
- MOVE NODEDATA (Traspasar datos desde espacios de archivos seleccionados de un único nodo)  
Utilice este comando para traspasar datos para espacios de archivos seleccionados que pertenecen al mismo nodo.

## MOVE NODEDATA (Trasladar datos de los espacios de archivos para uno o varios nodos o un grupo de proximidad)

Utilice este mandato para mover los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, un grupo de proximidad de nodo o un grupo de proximidad de espacio de archivos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento origen. Si su autorización tiene privilegio de almacenamiento con restricciones y tiene previsto traspasar datos a otra agrupación de almacenamiento, debe tener la autorización adecuada para la agrupación de almacenamiento de destino.

### Sintaxis

```

      .-|-----|
      v      |
>>-MOVE NODEdata--+-+---nombre_nodo-+-----+----->
                    '-COLLOGGroup-----nombre_grupo-'

>--FROMstgpool--+-+---nombre_agrupación_origen-----+----->

>--+-+-----+-----+-----+-----+----->
   '-TOstgpool--+-+---nombre_agrupación_destino-'

   .-Type-----ANY-----
>--+-+-----+-----+-----+-----+----->
   '-Type-----ANY-----+-'
       +-Backup-----+
       +-ARChive-----+
       '-SPacemanaged-'

   .-MAXPRocess-----1----- .-Wait-----No-----
>--+-+-----+-----+-----+-----+----->

```



Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Especifique uno de los siguientes valores:

No

Especifica que el servidor procesa este comando en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano, es posible que ya se hayan traspasado algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el mandato finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

RECONSTRUCT

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de una agregación. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO. El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento. Puede especificar uno de los siguientes valores:

No

Especifica que la reconstrucción de agregaciones de archivos no se realiza durante la operación de traspaso.

Yes

Especifica que la reconstrucción de agregaciones de archivos no se realiza durante la operación de traspaso. Solo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

## Traspasar datos de un nodo específico desde una agrupación de almacenamiento de cinta hasta una agrupación de almacenamiento de disco

---

Traspasar todos los datos que pertenecen al nodo MARY almacenado en la agrupación de almacenamiento TAPEPOOL. Los datos deben traspasarse a la agrupación de almacenamiento de disco BACKUPOOL.

```
move nodedata mary
  fromstgpool=tapepool tostgpool=backupool
```

## Traspasar datos para un grupo de proximidad de nodo desde una agrupación de almacenamiento a otra

---

Traspasar todos los datos para el grupo de proximidad de nodo NODEGROUP1 desde la agrupación de almacenamiento SOURCEPOOL a la agrupación de almacenamiento TARGETPOOL.

```
move nodedata collocgroup=nodegroup1 fromstgpool=sourcespool tostgpool=targetpool
```

## Traspasar datos para un grupo de proximidad de espacio de archivos desde una agrupación de almacenamiento a otra

---

Traspasar todos los datos para el grupo de proximidad de espacio de archivos FSGROUP1 desde la agrupación de almacenamiento SOURCEPOOL2 a la agrupación de almacenamiento TARGETPOOL2.



```
move nodedata collogroup=fsgroup1 fromstgpool=sourcespool2 tostgpool=targetpool2
```

## MOVE NODEDATA (Traspasar datos desde espacios de archivos seleccionados de un único nodo)

Utilice este comando para traspasar datos para espacios de archivos seleccionados que pertenecen al mismo nodo.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento origen. Si tiene privilegio de almacenamiento con restricciones y tiene previsto traspasar datos a otra agrupación de almacenamiento, debe tener la autorización adecuada para la agrupación de almacenamiento destino.

### Sintaxis

```
>>-MOVE NODedata--nombre_nodo----->
>--FROMstgpool--===nombre_agrupación_origen----->
>+-----+----->
  '-TOstgpool--===nombre_agrupación_destino-'
>+-----+----->
  |           .-,------. |
  |           v               | |
  '-Filespace--===nombre_espacio_archivos+-'
>+-----+----->
  |           .-,------. |
  |           v               | |
  '-UNIFILESpace--===nombre_espacio_archivos_unicode+-'
>+-----+----->
  |           .-,------. |
  |           v               | |
  '-FSID--===identificador_espacio_archivos+-'
.-Type--===ANY-----
>+-----+----->
  '-Type--===+ANY-----+'
              +-Backup-----+
              +-ARchive-----+
              '-SPacemanaged-'
.-MAXPRocess--===1-----.-Wait--===No-----
>+-----+-----+----->
  '-MAXPRocess--===núm_procesos-' '-Wait--===+No--+-'
                                   '-Yes-'
(1)
.-RECONStruct--===No o Yes-----
>+-----+----->
  '-RECONStruct--===+No--+-----+'
                                   '-Yes-'
```

#### Notas:

1. El valor predeterminado es NO si la agrupación de almacenamiento de origen o de destino es de acceso aleatorio. El valor predeterminado es YES si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial.

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre de nodo relacionado con los datos que se traspasan en este comando. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

FROMstgpool (Obligatorio)

Especifica el nombre de una agrupación de almacenamiento de acceso secuencial que contiene datos que deben traspasarse. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK.

#### TOSTgpool

Especifica el nombre de una agrupación de almacenamiento a la que se traspasarán los datos. Esta agrupación de almacenamiento debe tener un formato de datos NATIVE o NONBLOCK. Este parámetro es opcional y no se aplica si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia o una agrupación de datos activos. Es decir, si la agrupación de almacenamiento origen es una agrupación de almacenamiento de copia, el destino debe ser la misma agrupación de almacenamiento de copia. De forma parecida, si la agrupación de almacenamiento origen es una agrupación de datos activos, el destino debe ser la misma agrupación de datos activos. Si no se especifica ningún valor, se traspasan los datos a otros volúmenes de la agrupación de almacenamiento origen.

Importante: Si va a traspasar datos en la misma agrupación de almacenamiento, deberá haber volúmenes disponibles que no contengan los datos del nodo que va a traspasar. Es decir, el servidor no puede utilizar volúmenes que contengan los datos que se van a traspasar como volúmenes de destino.

#### FILEspace

Especifica el nombre del espacio de archivos no Unicode que contiene los datos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional. Si no especifica un valor para este parámetro ni valores para UNIFILESPACE, FSID o ambos, no se traspasarán los espacios de archivos que no son Unicode.

#### UNIFILESpace

Especifica el nombre del espacio de archivos Unicode que contiene los datos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional. Si no especifica un valor para este parámetro ni valores para FILESPACE, FSID o ambos, no se traspasarán los espacios de archivos que no son Unicode.

#### FSID

Especifica los identificadores de espacios de archivos (FSID) de los espacios de archivos que deben traspasarse. Puede separar varios nombres con comas y sin espacios intercalados. Este parámetro es opcional.

#### Type

Especifica el tipo de archivos que se traspasará. Este parámetro es opcional. El valor predeterminado es ANY. Si la agrupación de almacenamiento origen es una agrupación de datos activos, los únicos valores válidos son ANY y BACKUP. Sin embargo, si TYPE=ANY sólo se trasladan las versiones activas de los datos de copia de seguridad. Los valores posibles son:

##### ANY

Especifica que se traspasan todos los tipos de archivos.

##### Backup

Especifica que se traspasan archivos de copia de seguridad.

##### ARchive

Especifica que se traspasan copias archivadas. Este valor no es válido para las agrupaciones de datos activos.

##### SPacemanaged

Especifica que se trasladan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management). Este valor no es válido para las agrupaciones de datos activos.

#### MAXPProcess

Especifica el número máximo de procesos paralelos que se utilizará para traspasar datos. Este parámetro es opcional. Puede especificar un valor entre 1 y 999, ambos incluidos. El valor predeterminado es 1. Si se aumenta el número de procesos paralelos se mejorará el rendimiento.

Al determinar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo secuencial no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otra actividad del sistema de IBM Spectrum Protect y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en el traslado. Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento y, si el tipo de dispositivo no es FILE, también necesita una unidad.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

##### No

Especifica que el servidor procesa este mandato en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando.

El servidor muestra mensajes que se crean desde el proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso en segundo plano, utilice el mandato CANCEL PROCESS. Si se cancela un proceso en segundo plano, es posible que ya se hayan traspasado algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este mandato en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### RECONStruct

Especifica si deben reconstruirse las agregaciones de archivos durante el traspaso de datos. La reconstrucción elimina el espacio vacío que se ha acumulado durante la supresión de los archivos lógicos de un conjunto. Este parámetro es opcional. Si tanto la agrupación de almacenamiento de origen como la de destino son de acceso secuencial, el valor predeterminado es YES. Si la agrupación de almacenamiento de origen o la de destino son de acceso aleatorio, el valor predeterminado es NO.

El parámetro no está disponible o se ignora si se da alguna de las condiciones siguientes:

- El formato de datos es NETAPPDUMP, CELERRADUMP o NDMPDUMP.
- Los datos están en una agrupación de almacenamiento que está configurada para la eliminación de datos duplicados.
- La agrupación de almacenamiento de destino para el traspaso de datos está configurada para la eliminación de datos duplicados.

Atención: La reconstrucción elimina archivos de copia de seguridad inactivos en agrupaciones de datos activos. Si especifica RECONSTRUCT=NO al traspasar los datos de una agrupación de datos activos que no está configurada para la eliminación de datos duplicados, los archivos de copia de seguridad inactivos permanecen en la agrupación de almacenamiento.

Los valores posibles son:

No

Especifica que la reconstrucción de agregaciones de archivos no se realizará durante la operación de traspaso.

Yes

Especifica que la reconstrucción de agregaciones de archivos se realizará durante la operación de traspaso. Sólo es posible especificar esta opción cuando las agrupaciones de almacenamiento de origen y destino son de acceso secuencial.

## Ejemplo: trasladar datos no Unicode y Unicode de un nodo

---

Trasladar datos para el nodo TOM en la agrupación de almacenamiento TAPEPOOL. Limitar el traslado de datos a archivos en espacios de archivos no Unicode y en espacios de archivos Unicode, \\jane\d\$. Los datos deben traspasarse a la agrupación de almacenamiento de disco BACKUPPOOL.

```
move nodedata tom
  fromstgpool=tapepool tostgpool=backuppool
  filespace=* unifilespace=\\jane\d$
```

## Ejemplo: trasladar datos de nodo desde agrupaciones de almacenamiento de cinta hasta una agrupación de almacenamiento de disco

---

Trasladar todos los datos del nodo SARAH, desde todas las agrupaciones de almacenamiento primarias de acceso secuencial (en este ejemplo, TAPEPOOL\*) a DISKPOOL. Para obtener una lista de agrupaciones de almacenamiento que contienen datos para el nodo SARAH, emita uno de los comandos siguientes: QUERY OCCUPANCY o SELECT:

```
query occupancy sarah

SELECT * from OCCUPANCY where node_name='sarah'
```

Atención: Para este ejemplo, se da por supuesto que los resultados son TAPEPOOL1, TAPEPOOL4 y TAPEPOOL5.

```
move nodedata sarah
  fromstgpool=tapepool1 tostgpool=DISKPOOL

move nodedata sarah
  fromstgpool=tapepool4 tostgpool=DISKPOOL

move nodedata sarah
  fromstgpool=tapepool5 tostgpool=DISKPOOL
```

## Ejemplo: trasladar espacios de archivos no Unicode y Unicode de un nodo

---




El siguiente es un ejemplo de cómo trasladar a un nodo espacios de archivos de Unicode y que no sean de Unicode. Para el nodo NOAH, trasladar el espacio de archivos no Unicode \\servtuc\d\$ y el espacio de archivos Unicode \\tsmserv1\e\$ que tiene el ID de espacio de archivos 2 desde la agrupación de almacenamiento de acceso secuencial TAPEPOOL hasta la agrupación de almacenamiento de acceso aleatorio DISKPOOL.



unidades y sus rutas para la biblioteca. También puede suprimir todas las unidades y rutas de una biblioteca emitiendo el comando con ACTION=DELETE.

Este comando sólo es válido para los tipos de biblioteca SCSI y VTL. Para utilizar este mandato con ACTION=DEFINE, la opción SANDISCOVERY debe estar soportada y habilitada.

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---

```
>>-PERForm LIBAction--nombre_biblioteca----->
>---Action-----+DEFine--| A |----->
      +DElete-----+
      +RESet--| B |--+
      '-QUIesce-----'

      .-PREView-----No-----
>+-----+-----+-----><
  '-SOURCE-----nombre_origen-' '-PREView-----+Yes-+-'
                                   '-No--'

A (DEFine)

|----->
  '-DEVIce-----nombre_dispositivo_biblioteca-'

  .-PREFix-----nombre_biblioteca-----
>+-----+-----+-----|
  '-PREFix-----nombre_prefijo_unidad-'

B (RESet)

      .-DRIVEsonly-----No-----
|-----Action-----RESet-----+-----|
      '-DRIVEsonly-----+Yes-+-'
                                   '-No--'
```

## Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se va a definir o suprimir. La longitud máxima de este nombre es de 30 caracteres, a menos que emita PERFORM LIBACTION con ACTION=DEFINE y utilice el valor PREFIX predeterminado. En este caso, la longitud máxima del nombre es de 25 caracteres.

ACTION

Especifica la acción para el mandato PERFORM LIBACTION. Los valores posibles son:

DEFine

Especifica que las unidades y sus rutas están definidas para la biblioteca especificada. El descubrimiento SAN debe estar activado antes de especificar este valor de parámetro.

DElete

Especifica que las unidades y sus rutas se han suprimido para la biblioteca especificada.

RESet

Especifica que las unidades y sus rutas se han actualizado en línea para la biblioteca especificada.

DRIVEsonly

Especifica que sólo las unidades se actualizan en línea para la biblioteca especificada.

Los valores posibles son:

No

Especifica que las unidades y rutas se actualizan en línea.

Yes

Especifica que sólo las unidades se actualizan en línea.

QUIEsce

Especifica que las unidades se actualizan fuera de línea.

DEVIce

Especifica el nombre de dispositivo de biblioteca que se utiliza cuando se definen rutas si no se ha definido todavía una ruta a la biblioteca. Si se ha definido una ruta, el parámetro DEVICE se ignora. La longitud máxima de este valor es de 64 caracteres. Este parámetro es opcional.

PREFix

Especifica el prefijo que se utiliza para todas las definiciones de unidad. Por ejemplo, un valor de PREFIX *DR* crea las unidades *DRO*, *DR1*, *DR2*, para tantas unidades como se creen. Si no se especifica un valor para el parámetro PREFIX, se utiliza el nombre de biblioteca como el prefijo de las definiciones de unidad. La longitud máxima de este valor es de 25 caracteres.

SOURCE

Especifica el nombre del servidor de origen que se utilizará cuando se definan o supriman definiciones de rutas de unidad en un cliente de biblioteca o en un cliente sin LAN. Utilice este parámetro sólo si las unidades de la biblioteca están configuradas para el servidor local. Si no se especifica ningún valor para el parámetro SOURCE, se utiliza el nombre de servidor local, que es el valor predeterminado. La longitud máxima del nombre de origen es de 64 caracteres.

Si especifica el parámetro SOURCE, puede realizar RESET sólo de las rutas de los valores SOURCE especificados. El parámetro SOURCE no es compatible con opciones RESET DRIVESONLY=YES o QUIESCE.

Si se especifica un nombre de origen distinto del nombre de servidor local con ACTION=DEFINE, las definiciones de ruta de unidad se definen con el valor de señal UNDISCOVERED. A continuación, los clientes de biblioteca que dan soporte al descubrimiento SAN actualizan dinámicamente las definiciones de ruta la primera vez que se monta la unidad.

PREView

Especifica la salida de todos los comandos que se procesan para PERFORM LIBACTION antes de emitir el comando. El parámetro PREVIEW no es compatible con el parámetro DEVICE. Si está emitiendo el mandato PERFORM LIBACTION para definir una biblioteca, no puede especificar a la vez el parámetro PREVIEW y DEVICE.

Los valores posibles son:

No

Especifica que no se muestra una vista previa de los mandatos emitidos para PERFORM LIBACTION.

Yes

Especifica que se muestra una vista previa de los mandatos emitidos para PERFORM LIBACTION.

## Ejemplo: definir una biblioteca compartida

---

Supongamos que está trabajando en una SAN y que ha configurado un gestor de bibliotecas denominado LIBMGR1. Ahora, defina una biblioteca que se denomina SHAREDTSM para un servidor cliente de biblioteca denominado LIBCL1.

Emita DEFINE LIBRARY desde el servidor cliente de biblioteca, LIBCL1:

```
define library sharedtsm libtype=shared primarylibmanager=libmgr1
```

A continuación, emita PERFORM LIBACTION desde el gestor de biblioteca, LIBMGR1, para definir las vías de acceso de unidad para el cliente de biblioteca:

```
perform libaction sharedtsm action=define source=libcl1
```

Nota: La opción SANDISCOVERY debe estar soportada y habilitada en el servidor de cliente de biblioteca.


## Ejemplo: definir una biblioteca con cuatro unidades

---

Defina una biblioteca SCSI llamada KONA:

```
define library kona libtype=scsi
```

A continuación, emita el mandato PERFORM LIBACTION para definir las unidades y las rutas para la biblioteca:

 Sistemas operativos AIX

```
perform libaction kona action=define device=/dev/lb3  
prefix=dr
```

A continuación, el servidor ejecuta los siguientes comandos:

```

define path server1 kona srct=server destt=library
device=/dev/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/mt3
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/mt4

```

#### Sistemas operativos Linux

```

perform libaction kona action=define device=/dev/tmscsi/lb3
prefix=dr

```

A continuación, el servidor ejecuta los siguientes comandos:

```

define path server1 kona srct=server destt=library
device=/dev/tmscsi/lb3
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=/dev/tmscsi/mt1
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=/dev/tmscsi/mt2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=/dev/tmscsi/mt3
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=/dev/tmscsi/mt4

```

#### Sistemas operativos Windows

```

perform libaction kona action=define device=lb0.0.0.2
prefix=dr

```

A continuación, el servidor ejecuta los siguientes comandos:

```

define path server1 kona srct=server destt=library
device=lb0.0.0.2
define drive kona dr0
define path server1 dr0 srct=server destt=drive library=kona
device=mt0.1.0.2
define drive kona dr1
define path server1 dr1 srct=server destt=drive library=kona
device=mt0.2.0.2
define drive kona dr2
define path server1 dr2 srct=server destt=drive library=kona
device=mt0.3.0.2
define drive kona dr3
define path server1 dr3 srct=server destt=drive library=kona
device=mt0.4.0.2

```

## Comandos relacionados

Tabla 1. Comandos relacionados con PERFORM LIBACTION

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DRIVE	Suprime una unidad de una biblioteca.

Comando	Descripción
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## PING SERVER (Comprobar la conexión entre servidores)

Utilice este mandato para comprobar la conexión entre el servidor local y un servidor remoto.

Importante: El nombre y la contraseña del administrador que emite este comando también deben estar definidos en el servidor remoto. Si el servidor remoto está en el nivel actual, las credenciales del servidor se verifican automáticamente cuando se ejecuta el mandato PING SERVER. Si el servidor remoto no está en el nivel actual, las credenciales del servidor no se verifican.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-PING SERVER--nombre_servidor-----<<
```

### Parámetros

nombre\_servidor (Obligatorio)  
Especifica el nombre del servidor remoto.

### Ejemplo: comprobar la conexión con un servidor

Comprobar la conexión con el servidor FRED.

```
ping server fred
```

### Comandos relacionados

Tabla 1. Comandos relacionados con PING SERVER

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY SERVER	Muestra información sobre servidores.

## PREPARE (crear un archivo de plan de recuperación)

Utilice este mandato para crear un archivo de plan de recuperación, que contiene la información necesaria para recuperar un servidor de IBM Spectrum Protect. El archivo del plan de recuperación se puede almacenar en un sistema de archivos que sea accesible para el servidor de origen o en un servidor de destino.

Puede utilizar el comando QUERY ACTLOG para determinar si el comando PREPARE se ha ejecutado correctamente.

También puede ver esta información desde la consola del servidor o, si el parámetro WAIT es YES, en una sesión de cliente de administración.

### Clase de privilegio



Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
.-Source-----DBBackup-----.  
>>-Prepare-----+----->  
    '-Source-----+DBBackup---+'  
        '-DBSnapshot-'  
  
>-----+----->  
    '-DEVclass-----nombre_clase_dispositivo-'  
  
>-----+-----+----->  
    '-PLANPrefix-----prefijo-' '-INSTRPrefix-----prefijo-'  
  
>-----+-----+----->  
    | .-,------. | |  
    | v'          | | |  
    '-COPYstgpool-----nombre_agrupación+--'  
  
>-----+-----+----->  
    | .-,------. | |  
    | v'          | | |  
    '-ACTIVEDatastgpool-----nombre_agrupación+--'  
  
>-----+-----+----->  
    | .-,------. | |  
    | v'          | | |  
    '-PRIMstgpool-----nombre_agrupación+--'  
  
.-Wait-----No-----.  
>-----+-----+-----<<  
    '-Wait-----+No---+-'  
        '-Yes-'
```

## Parámetros

### Source

Especifica el tipo de serie de copias de seguridad de base de datos que IBM Spectrum Protect presupone cuando se genera el archivo del plan de recuperación. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Las opciones son:

#### DBBackup

Especifica que IBM Spectrum Protect presupone la última serie de copias de seguridad de base de datos completas.

#### DBSnapshot

Especifica que IBM Spectrum Protect presupone la última serie de copias de seguridad de instantánea de base de datos.




### DEVclass

Especifica el nombre de clase de dispositivo que se utiliza para crear un objeto de archivo del plan de recuperación en un servidor destino. La clase de dispositivo debe tener un tipo de dispositivo SERVER.

Importante: La capacidad máxima de la clase de dispositivo debe ser mayor que el tamaño del archivo del plan de recuperación.

Si el tamaño del archivo del plan de recuperación sobrepasa la capacidad máxima, el comando no se ejecuta.

El convenio de denominación del objeto de archivo que contiene el archivo del plan de recuperación en el servidor destino es:

- **Nombre de espacio de archivos:**
  - ADSM.SERVER
- **Calificador de alto nivel:**
  -  Sistemas operativos AIX  Sistemas operativos Linuxprefijoclasedisp/nombreservidor.aaaamddd.hhmmss
  -  Sistemas operativos Windowsprefijoclasedisp\nombreservidor.aaaamddd.hhmmss
- **Calificador de bajo nivel:**
  - RPF.OBJ.1

El nombre de volumen virtual del archivo del plan de recuperación grabado en la tabla de archivos históricos de volúmenes del servidor de origen tiene el formato nombreservidor.aaaamddd.hhmmss.




Si no se especifica el parámetro DEVCLASS, el archivo del plan de recuperación se grabará en un archivo según el prefijo del plan.


Si se especifica SOURCE=DBBACKUP, o se ha tomado como valor predeterminado, la entrada de la información histórica de volúmenes para el objeto de archivo del plan de recuperación especifica un tipo de volumen de RPF. Si se especifica

SOURCE=DBSNAPSHOT, la entrada de la información histórica de volúmenes especifica un tipo de volumen de RPFNSAPSHOT.


#### PLANPrefix

Especifica el prefijo de nombre de ruta que se utiliza en el nombre de archivo del plan de recuperación. Este parámetro es opcional.

-  Sistemas operativos AIX  Sistemas operativos Linux La longitud máxima es de 250 caracteres.
-  Sistemas operativos Windows La longitud máxima son 200 caracteres.

 Sistemas operativos Windows Especifica el prefijo de nombre de ruta que se utiliza en el nombre de archivo del plan de recuperación.

IBM Spectrum Protect agrega al prefijo la información de fecha y hora ordenable con el formato `aaaammdd.hhmmss`. Por ejemplo: 20081115.051421.

 Sistemas operativos AIX  Sistemas operativos Linux El prefijo puede ser uno de los siguientes:

#### Ruta del directorio

Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
PLANPREFIX=/admsrv/recplans/
```

El nombre de archivo resultante sería:

```
/admsrv/recplans/20081115.051421
```

#### Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
PLANPREFIX=/admsrv/recplans/accounting
```

El nombre de archivo resultante sería:

```
/admsrv/recplans/accounting.20081115.051421
```

Observe el punto antes de la fecha y la hora.

#### Sólo serie

IBM Spectrum Protect especifica la ruta del directorio. IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es `/opt/tivoli/tsm/server/bin` y se especifica el parámetro siguiente:

```
PLANPREFIX=shipping
```

El nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.20081115.051421
```

Observe el punto antes de la fecha y la hora.

 Sistemas operativos Windows El prefijo puede ser uno de los siguientes:

#### Ruta del directorio

Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
PLANPREFIX=c:\admsrv\recplans\
```

El nombre de archivo resultante sería:

```
c:\admsrv\recplans\20081115.051421
```

Consejo: Si emite el comando PREPARE desde el cliente de línea de comandos de administración y el último carácter de la línea de comandos es una barra inclinada invertida, se interpretará que ésta es un carácter de continuación. Para evitar esto, especifique el valor del prefijo entre comillas dobles. Por ejemplo:

```
PLANPREFIX="c:\admsrv\recplans\"
```

#### Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
PLANPREFIX=c:\admsrv\recplans\accounting
```

El nombre de archivo resultante sería:

```
c:\admsrv\recplans\accounting.20081115.051421
```

Observe el punto antes de la fecha y la hora.

#### Sólo serie


IBM Spectrum Protect agrega la fecha y la hora con el formato *.aaaammdd.hhmmss* (observe el punto antes de la fecha y la hora) al prefijo. La ruta del directorio que utiliza el mandato PREPARE es el directorio que representa esta “instancia” del servidor de IBM Spectrum Protect. Normalmente, este directorio es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, el directorio que representa a esta instancia del servidor es *c:\Archivos de programa\Tivoli\TSM;\server2*, y se emite el comando PREPARE con el parámetro siguiente:

```
PLANPREFIX=shipping
```

El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.20081115.051421
```



Si no se especifica el parámetro PLANPREFIX, IBM Spectrum Protect selecciona el prefijo de uno de estos modos:

- Si se ha emitido el comando SET DRMPREFIX, IBM Spectrum Protect utiliza el prefijo que se ha especificado en ese comando.
-  Sistemas operativos Windows Si no se ha definido el comando SET DRMPREFIX, IBM Spectrum Protect utiliza como ruta el directorio que representa a esta “instancia” del servidor de IBM Spectrum Protect que, por lo general, es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, si el directorio que representa esta instancia del servidor es el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2\20081115.051421
```




-  Sistemas operativos AIX  Sistemas operativos Linux Si no se ha emitido el mandato SET DRMPREFIX, IBM Spectrum Protect utiliza el nombre de ruta de directorio del directorio de trabajo actual. Por ejemplo, el directorio actual de trabajo es el siguiente:



```
/opt/tivoli/tsm/server/bin
```

El nombre de archivo resultante sería:

```
/opt/tivoli/txm/server/bin/20081115.051421
```

#### INSTRPrefix

Especifica el prefijo del nombre de ruta que utiliza IBM Spectrum Protect para localizar los archivos que contienen las instrucciones de recuperación. La longitud máxima son  Sistemas operativos AIX  Sistemas operativos Linux 250  Sistemas operativos Windows 200 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux El prefijo puede ser uno de los siguientes:

#### Ruta del directorio

Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
INSTRPREFIX=/admsrv/recinstr/  
  
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

#### Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
INSTRPREFIX=/admsrv/recinstr/accounts
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```


#### Sólo serie

- IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es */opt/tivoli/tsm/server/bin* y se especifica el parámetro siguiente:

```
INSTRPREFIX=shipping
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```

 Sistemas operativos Windows El prefijo puede ser uno de los siguientes:

#### Ruta del directorio

Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
INSTRPREFIX=c:\admsrv\recinstr\
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

Consejo: Si emite el comando PREPARE desde el cliente de línea de comandos de administración y el último carácter de la línea de comandos es una barra inclinada invertida, se interpretará que ésta es un carácter de continuación. Para evitar esto, especifique el valor del prefijo entre comillas dobles. Por ejemplo:

```
INSTRPREFIX="c:\admserv\recinstr\"
```

#### Ruta del directorio seguida de una serie

IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
INSTRPREFIX=c:\admsrv\recinstr\accounts
```

IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación adecuado. En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante es:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

#### Sólo serie


IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. IBM Spectrum Protect agrega el nombre de sección del archivo del plan de recuperación al prefijo. Si el prefijo sólo es una serie, la ruta del directorio que utiliza el comando PREPARE es el directorio que representa a esta instancia del servidor de IBM Spectrum Protect. Normalmente, es el directorio de instalación original del servidor de IBM Spectrum Protect. Por ejemplo, el directorio que representa a esta instancia del servidor es c:\Archivos de programa\Tivoli\TSM;\server2, y se emite el comando PREPARE con el parámetro siguiente:

```
INSTRPREFIX=dock
```

El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.20081115.051421
```



Si no especifica el parámetro INSTRPREFIX, IBM Spectrum Protect selecciona el prefijo de uno de estos modos:

- Si se ha emitido el comando SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza el prefijo que se ha especificado en ese comando.
-  Sistemas operativos Windows Si no se ha emitido el mandato SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza como ruta el directorio que representa a esta "instancia" del servidor de IBM Spectrum Protect que, por lo general, es el directorio de instalación original del servidor. Por ejemplo, si el directorio que representa esta instancia del servidor es el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\Archivos de programa\Tivoli\TSM;\server2\RECOVERY.INSTRUCTIONS.GENERAL
```

-  Sistemas operativos AIX  Sistemas operativos Linux Si no se ha emitido el mandato SET DRMINSTRPREFIX, IBM Spectrum Protect utiliza el directorio de trabajo actual. Por ejemplo, si el directorio de trabajo actual es /opt/tivoli/tsm/server/bin, para el archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/RECOVERY.INSTRUCTIONS.GENERAL
```

#### PRIMstgpool

Especifica los nombres de las agrupaciones de almacenamiento primarias que desea restaurar. Puede separar los nombres de las agrupaciones de almacenamiento con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si se ha emitido el comando SET DRMPRIMSTGPOOL, IBM Spectrum Protect incluye las agrupaciones de almacenamiento primarias que se indican en ese comando.

- Si no se ha emitido el comando SET DRMPRIMSTGPOOL, IBM Spectrum Protect incluye todas las agrupaciones de almacenamiento primarias.

#### COPYstgpool

Especifica los nombres de las agrupaciones de almacenamiento de copia utilizadas para hacer copia de seguridad de las agrupaciones de almacenamiento primarias que desea restaurar (consulte el parámetro PRIMSTGPOOL). Puede separar los nombres de las agrupaciones de almacenamiento con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si se ha emitido el comando SET DRMCOPYSTGPOOL, IBM Spectrum Protect incluye esas agrupaciones de almacenamiento de copia.
- Si no se ha emitido el comando SET DRMCOPYSTGPOOL, IBM Spectrum Protect incluye todas las agrupaciones de almacenamiento de copia.

#### ACTIVEDatastgpool

Especifica los nombres de las agrupaciones de almacenamiento de datos activos que desea que estén disponibles para el acceso fuera del local. Separe los nombres de agrupaciones de almacenamiento de datos activos con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Si no se especifica este parámetro, IBM Spectrum Protect selecciona las agrupaciones de almacenamiento del modo siguiente:

- Si el comando SET ACTIVEDATASTGPOOL se había emitido anteriormente con nombres de agrupaciones de almacenamiento de datos activos válidos, IBM Spectrum Protect procesará esas agrupaciones de almacenamiento.
- Si no se ha emitido el comando SET ACTIVEDATASTGPOOL o si todas las agrupaciones de almacenamiento de datos activos se han eliminado con el comando SET ACTIVEDATASTGPOOL, IBM Spectrum Protect procesará únicamente los volúmenes de agrupación de almacenamiento que se habían marcado en el local en el momento de ejecutarse el comando PREPARE. IBM Spectrum Protect marcará estos volúmenes como UNAVAILABLE.

#### Wait



Especifica si el comando se procesa de forma subordinada o en primer plano.

#### No

Especifica el proceso subordinado. Este es el valor predeterminado.

#### Yes

Especifica el proceso en primer plano.

 Sistemas operativos AIX  Sistemas operativos Linux No se puede especificar YES desde la consola del servidor.

## Ejemplo: crear un archivo de plan de recuperación


Emitir el comando PREPARE y consultar las anotaciones de actividades para comprobar los resultados.

```
prepare
query actlog search=prepare
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
05/03/2008 12:01:13 ANR0984I Proceso 3 para PREPARE iniciado en
BACKGROUND a las 12:01:13.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.DATABASE.
05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de
recuperación
/home/guest/drmtest/prepare/tserver/DSM1509/
RECOVERY.INSTRUCTIONS.STGPOOL.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEP.
05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos
de copia de seguridad en la agrupación de
almacenamiento de copia CSTORAGEPSM.
05/03/2008 12:01:14 ANR6920W PREPARE: El nombre de volumen de
sustitución generado, BACK4X@ no es
válido para el tipo de dispositivo
8MM. Nombre de volumen original: BACK4X. Sección:
la macro PRIMARY.VOLUMES.REPLACEMENT.
05/03/2008 12:01:14 ANR6900I PREPARE: Se ha creado el archivo de
plan de recuperación
/home/guest/drmtest/prepare/plandir/DSM1509/
r.p.20080503.120113.
```

05/03/2008 12:01:14 ANR0985I El proceso 3 para PREPARE ejecutado en BACKGROUND se ha completado con el estado de terminación SUCCESS a las 12:01:14.

 Sistemas operativos Windows

05/03/2008 12:01:13 ANR0984I Proceso 3 para PREPARE iniciado en BACKGROUND a las 12:01:13.

05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de recuperación c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.DATABASE no encontrado.

05/03/2008 12:01:13 ANR6918W PREPARE: Archivo de instrucciones de recuperación c:\drmtest\prepare\RECOVERY.INSTRUCTIONS.STGPOOL no encontrado.

05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos de copia de seguridad en la agrupación de almacenamiento de copia CSTORAGEP.

05/03/2008 12:01:13 ANR6913W PREPARE: No hay volúmenes con datos de copia de seguridad en la agrupación de almacenamiento de copia CSTORAGEPSM.

05/03/2008 12:01:14 ANR6920W PREPARE: El nombre de volumen de sustitución generado, BACK4X@ no es válido para el tipo de dispositivo ADSM Nombre de volumen original: BACK4X. Sección: la macro PRIMARY.VOLUMES.REPLACEMENT.




05/03/2008 12:01:14 ANR6900I PREPARE: Se ha creado el archivo de plan de recuperación c:\drmtest\prepare\r.p.20080503.120113  
 05/03/2008 12:01:14 ANR0985I El proceso 3 para PREPARE ejecutado en BACKGROUND se ha completado con el estado de terminación SUCCESS a las 12:01:14.

## Comandos relacionados

Tabla 1. Comandos relacionados con PREPARE

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.
QUERY RPFFILE	Muestra información sobre archivos del plan de recuperación.
QUERY SERVER	Muestra información sobre servidores.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMINSTRPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta de las instrucciones del plan de recuperación.
SET DRMPPLANVPOSTFIX	Especifica los nombres de los volúmenes de sustitución del archivo del plan de recuperación.
SET DRMPPLANPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta del plan de recuperación.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.

Comando	Descripción
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## PROTECT STGPOOL (Proteger datos que pertenecen a una agrupación de almacenamiento)

Utilice este mandato para proteger los datos de una agrupación de almacenamiento de contenedores de directorio almacenando una copia de los datos en otra agrupación de almacenamiento en un servidor de destino de duplicación o en el mismo servidor protegiendo los datos en cinta. Cuando protege la agrupación de almacenamiento de contenedores de directorio, puede intentar posteriormente reparar los daños en la agrupación de almacenamiento mediante el mandato REPAIR STGPOOL.

Cuando emite el mandato PROTECT STGPOOL para una agrupación de almacenamiento de contenedores de directorio, se realiza una copia de seguridad de los datos almacenados en esa agrupación de almacenamiento en el destino que especifique. La copia de seguridad de los datos se puede realizar en los tipos de destino siguientes:

- Una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino.  
Requisito previo: Para la agrupación de almacenamiento que se protege, debe especificar la agrupación de destino mediante el parámetro PROTECTSTGPOOL del mandato DEFINE STGPOOL o UPDATE STGPOOL.

Cuando se utiliza regularmente el mandato PROTECT STGPOOL, normalmente puede reducir el tiempo de proceso para el mandato REPLICATE NODE. Las extensiones de datos que ya se han copiado en el servidor de réplica de destino a través de las operaciones de protección de agrupación de almacenamiento se omiten cuando se inicia la réplica.

Como parte de la operación PROTECT STGPOOL, pueden ejecutarse procesos para reparar extensiones dañadas en la agrupación de almacenamiento del servidor de destino. La operación de reparación se realiza bajo las condiciones siguientes:

- Tanto el servidor de origen como el servidor de destino deben estar en la versión V7.1.5 o posterior.
- Las extensiones que ya se han marcado como dañadas en el servidor de destino se reparan. El proceso de reparación no ejecuta un proceso de auditoría para identificar el daño.
- Sólo se reparan las extensiones de destino que coinciden con las extensiones de origen. Las extensiones de destino dañadas pero que no tienen coincidencia en el servidor de origen no se reparan.

Limitaciones: La operación de reparación que se ejecuta como parte de la operación PROTECT STGPOOL tiene las limitaciones siguientes:

- Las extensiones que pertenecen a los objetos cifrados no se reparan.
- El momento de la aparición de daños en la agrupación de almacenamiento de destino y la secuencia de los mandatos REPLICATE NODE y PROTECT STGPOOL puede afectar al éxito del proceso de reparación. Es posible que algunas extensiones almacenadas en la agrupación de almacenamiento de destino por un mandato REPLICATE NODE no se reparen.
- Agrupaciones de almacenamiento de copia de contenedor en el mismo servidor, protegidas en cinta.  
Requisito previo: Para la agrupación de almacenamiento que se está protegiendo, debe especificar la agrupación de almacenamiento de destino utilizando el parámetro PROTECTLOCALSTGPools. Para conocer los detalles sobre el parámetro, consulte los mandatos para definir y actualizar las agrupaciones de almacenamiento de contenedores de directorio (mandatos DEFINE STGPOOL y UPDATE STGPOOL).

Como parte de la operación PROTECT STGPOOL, se pueden reclamar los volúmenes de la agrupación de directorios. El valor del parámetro RECLAIM de la agrupación de almacenamiento de copia de contenedor afecta a si se reclaman los volúmenes. Para obtener detalles sobre el parámetro, consulte los mandatos para definir y actualizar agrupaciones de almacenamiento de copia de contenedor (mandatos DEFINE STGPOOL y UPDATE STGPOOL).

Restricción: No puede programar distintas operaciones de PROTECT STGPOOL para ejecutarlas simultáneamente. Espere a que una operación PROTECT STGPOOL finalice antes de iniciar otra.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis cuando el destino es el servidor de réplica

```
>>-PROTECT STGPool--agrup_almac_origen----->
      .-Type---Replserver-. .-FORCEREconcile---No-----
>+-----+-----+-----+-----+-----+----->
```





No



Especifica que la copia de seguridad de los datos no compara todas las extensiones de datos de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen con las extensiones de datos en el servidor de destino. En su lugar, la copia de seguridad de los datos realiza un seguimiento de los cambios en las extensiones de datos del servidor de origen desde la última copia de seguridad, y los sincroniza en el servidor de destino.


Yes

Especifica que la copia de seguridad de los datos compara todas las extensiones de datos en el servidor de origen con las extensiones de datos en el servidor destino, y sincroniza las extensiones de datos en el servidor de destino con el servidor de origen.

#### MAXSESSions

Especifica el número máximo de sesiones de datos que pueden enviar datos a un servidor de destino. Este parámetro es opcional. El valor que se especifique puede estar en el rango de 1 a 100.

 Sistemas operativos AIX  Sistemas operativos Windows El valor predeterminado es 10.

 Sistemas operativos Linux El valor predeterminado varía:

- Si TRANSFERMETHOD=TCPIP, el valor predeterminado del parámetro MAXSESSIONS es 10.
- Si TRANSFERMETHOD=FASP, el valor predeterminado del parámetro MAXSESSIONS es 2.

Si aumenta el número de sesiones, puede mejorar el rendimiento para la agrupación de almacenamiento.

Cuando establezca un valor para el parámetro MAXSESSIONS, asegúrese de que el ancho de banda disponible y la capacidad del procesador de los servidores de origen y de destino sean suficientes.

Consejos:

- Si emite un mandato QUERY SESSION, el número total de sesiones puede superar el número de sesiones de datos. La diferencia se debe a las sesiones de control breves que se utilizan para consultar y configurar operaciones.
- El número de sesiones que se utilizan para la protección depende de la cantidad de datos que se han copiado. Si hace copia de seguridad solamente de una cantidad pequeña de datos, el aumento del número de sesiones no proporciona beneficio.

#### Preview

Especifica si se obtiene una vista previa de los datos. Este parámetro es opcional. El valor predeterminado es NO. Especifique uno de los siguientes valores:

No

Especifica que se realiza una copia de seguridad de los datos en el servidor de destino, pero no se obtiene una vista previa de los datos.

Yes

Especifica que se obtiene una vista previa de los datos, pero no se realiza una copia de seguridad.

#### PURGEdata

Especifica que las extensiones de datos se suprimen del servidor de destino. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que las extensiones de datos no se suprimen del servidor de destino.

All

Especifica que todas las extensiones de datos se suprimen del servidor de destino. Las extensiones de datos a las que se hace referencia en otros datos en la agrupación de almacenamiento de destino no se suprimen.

Deleted

Especifica que las extensiones de datos que se han suprimido en el servidor de origen se suprimen del servidor de destino. Las nuevas extensiones de datos no están protegidas.

#### RECLaim

Especifica si se ejecuta una reclamación cuando se procesa el mandato PROTECT STGPOOL. La reclamación se ejecuta en la agrupación de almacenamiento de copia de contenedor local que es el destino de la operación de protección. Este parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que la reclamación se ejecuta cuando se emite el mandato, junto con la operación de protección de la agrupación de almacenamiento. La reclamación se ejecuta hasta finalizar, sin limitaciones relativas a la cantidad de volúmenes de la agrupación de almacenamiento que se procesan para la reclamación.

No

Especifica que la reclamación no se ejecuta cuando se emite el mandato. Solo se ejecuta la protección de la agrupación de almacenamiento.

Only

Especifica que la reclamación es la única operación que se ejecuta cuando se emite el mandato. La operación de protección de la agrupación de almacenamiento no se ejecuta, de modo que los datos de la agrupación de almacenamiento de contenedores de directorio que se hayan actualizado desde la última operación de protección no se protegerán. La reclamación se ejecuta hasta finalizar, sin limitaciones relativas a la cantidad de volúmenes de la agrupación de almacenamiento que se procesan para la reclamación.

YESLIMITed

Especifica que la reclamación se ejecuta cuando se emite el mandato, junto con la operación de protección de la agrupación de almacenamiento. La reclamación se ejecuta hasta que se alcanza el límite de reclamación que se ha definido para la agrupación de almacenamiento de copia de contenedor. El límite de reclamación se define con el parámetro RECLAIMLIMIT en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

ONLYLIMITed

Especifica que la reclamación es la única operación que se ejecuta cuando se emite el mandato. La operación de protección de la agrupación de almacenamiento no se ejecuta, de modo que los datos de la agrupación de almacenamiento de contenedores de directorio que se hayan actualizado desde la última operación de protección no se protegerán. La reclamación se ejecuta hasta que se alcanza el límite de reclamación que se ha definido para la agrupación de almacenamiento de copia de contenedor. El límite de reclamación se define con el parámetro RECLAIMLIMIT en los mandatos DEFINE STGPOOL o UPDATE STGPOOL.

Wait

Especifica si se debe esperar a que el servidor procese este mandato en primer plano. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:


No


Especifica que el mandato se procesa en segundo plano. Para supervisar los procesos en segundo plano de este mandato, emita el mandato QUERY PROCESS.

Yes

Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

 Sistemas operativos Linux

 Especifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN). Si especifica TRANSFERMETHOD=FASP, altera temporalmente cualquier parámetro TRANSFERMETHOD que haya especificado en los mandatos DEFINE SERVER o UPDATE SERVER.

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si las licencias no se encuentran o han caducado, las operaciones para proteger las agrupaciones de almacenamiento fallan.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.

## Ejemplo: suprimir todas las extensiones de datos del servidor de destino

---

Suprimir todas las extensiones de datos en una agrupación de almacenamiento de contenedores de directorio en el servidor de destino. La agrupación de almacenamiento de contenedores de directorio denominada POOL1 en el servidor de origen ya no está protegida por la agrupación de almacenamiento de contenedores de directorio en el servidor de destino. Puede suprimir todas las extensiones para limpiar la agrupación de almacenamiento de contenedores de directorio en el servidor de destino que ya no protege el servidor de origen.

```
protect stgpool pool1 purgedata=all
```

## Ejemplo: proteger una agrupación de almacenamiento y especificar un número máximo de sesiones de datos

---

Proteja una agrupación de almacenamiento denominada SPOOL1 en el servidor de origen realizando una copia de seguridad de los datos en un servidor de réplica de destino, TPOOL1. Especifique un máximo de 20 sesiones de datos.

```
update stgpool spool1 protectstgpool=tpool1
protect stgpool spool1 maxsessions=20
```

## Ejemplo: copiar los datos de la agrupación de almacenamiento en cinta

Proteja una agrupación de almacenamiento de contenedores de directorio copiando los datos a una agrupación de almacenamiento de copia de contenedor en el mismo servidor. En este ejemplo, la agrupación de almacenamiento de contenedores de directorio se llama SPOOL1 y la agrupación de almacenamiento de copia de contenedor que utiliza cinta para almacenamiento se llama TAPES1.

1. Actualice la agrupación de almacenamiento de contenedores de directorio para añadir TAPES1 como la agrupación de almacenamiento local para protección. La agrupación de almacenamiento TAPES1 debe ser una agrupación de almacenamiento de copia de contenedor. Emita el mandato siguiente:

```
update stgpool spool1 protectlocalstgpools=tapes1
```

2. Proteja los datos de la agrupación de almacenamiento de contenedores de directorio con una copia local emitiendo el mandato siguiente:

```
protect stgpool type=local spool1
```

Los datos se copia en la agrupación de almacenamiento TAPES1.

## Ejemplo: reclamar espacio en volúmenes de cinta antes de proteger una agrupación de almacenamiento

Reclame espacio en los volúmenes de cinta utilizados para proteger una agrupación de almacenamiento de contenedores de directorio. A continuación, proteja los datos de la agrupación de almacenamiento de contenedores de directorio. En este ejemplo, la agrupación de almacenamiento de contenedores de directorio se denomina SPOOL1.

1. Reclamar espacio en la agrupación de almacenamiento de copia de contenedor local definida como agrupación de protección de destino para SPOOL1.

```
protect stgpool spool1 type=local reclaim=only
```

2. Proteger los datos en la agrupación de almacenamiento de contenedores de directorio denominada SPOOL1 sin ejecutar la reclamación.

```
protect stgpool spool1 type=local reclaim=no
```

Tabla 1. Comandos relacionados con PROTECT STGPOOL

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE STGPOOL (copia de contenedor)	Actualizar una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.

## Comandos QUERY

---

Utilice los comandos QUERY para solicitar o visualizar información sobre los objetos de IBM Spectrum Protect.

- QUERY ACTLOG (Consultar las anotaciones de actividades)
- QUERY ADMIN (Visualizar información de administrador)
- QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)
- QUERY ALERTSTATUS (Consultar el estado de una alerta)
- QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)
- QUERY AUDITOCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)
- QUERY BACKUPSET (Consultar un juego de copias de seguridad)
- QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)
- QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)
- QUERY COLLOGROUP (Consultar un grupo de proximidad)
- QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CONTAINER (Consulta de un contenedor)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)
- QUERY COPYGROUP (Consultar grupos de copia)
- QUERY DATAMOVER (visualizar definiciones de un transportador de datos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)
- QUERY DB (Visualizar información de base de datos)
- QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)
- QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)
- QUERY DIRSPACE (Consultar utilización de almacenamiento de directorios FILE)
- QUERY DOMAIN (Consultar un dominio de políticas)
- QUERY DRIVE (Consultar información acerca de una unidad)
- QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)
- QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)
- QUERY ENABLED (Consultar eventos activados)
- QUERY EVENT (Consultar eventos planificados y realizados)
- QUERY EVENTRULES (Consultar reglas para eventos de servidor o de cliente)
- QUERY EVENTSERVER (Consultar el servidor de eventos)
- QUERY EXPORT (Consultar las operaciones de exportación activas o suspendidas)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)
- QUERY FILESPACE (Consultar uno o más espacios de archivos)
- QUERY LIBRARY (Consultar una biblioteca)
- QUERY LIBVOLUME (Consultar un volumen de biblioteca)
- QUERY LICENSE (Visualizar información sobre licencias)
- QUERY LOG (Visualizar información sobre el registro de recuperación)
- QUERY MACHINE (Consultar información de máquina)
- QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)
- QUERY MGMTCLASS (Consultar una clase de gestión)
- QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)
- QUERY MONITORSTATUS (Consultar el estado de supervisión)
- QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)
- QUERY NODE (Consultar nodos)
- QUERY NODEDATA (Consultar datos de cliente en volúmenes)
- QUERY NODEGROUP (Consultar un grupo de nodos)
- QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)
- QUERY OPTION (Consultar opciones del servidor)
- QUERY PATH (visualizar una definición de ruta)
- QUERY POLICYSET (Consultar un juego de políticas)
- QUERY PROCESS (Consultar uno o más procesos de servidor)
- QUERY PROFILE (Consultar un perfil)





Valor	Descripción	Ejemplo
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, IBM Spectrum Protect visualizará los mensajes con la hora 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00.  Si emite el comando QUERY ACTLOG a las 9:00 con BEGINTime=NOW-3:30 o BEGINTime= -3:30, IBM Spectrum Protect visualiza los mensajes con la hora 5:30 o posterior en la fecha inicial.

#### ENDDate

Especifica la fecha final del rango de los mensajes que se han de visualizar. Se visualizarán todos los mensajes, que reúnan el criterio de rango horario, que se hayan producido antes de esta fecha. Si no especifica un valor, se utilizará la fecha actual. Este parámetro es opcional.

Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1.  Para visualizar la información creada hasta ayer, puede especificar ENDDATE=TODAY-1, o simplemente, ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final del rango de los mensajes que se han de visualizar. Se visualizan todos los mensajes que se ajusten a los criterios de rango horario que se han producido con anterioridad a esta hora. Si no especifica un valor, se visualizarán todos los mensajes hasta la hora en que se ha emitido este mandato. Este parámetro es opcional.

Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, IBM Spectrum Protect visualiza los mensajes con la hora 12:00 o anterior en la fecha final especificada.

Valor	Descripción	Ejemplo
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30.  Si emite este comando a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, IBM Spectrum Protect visualizará los mensajes con la hora 5:30 o anterior en la fecha final especificada.

#### MSGno

Especifica un entero que define el número de mensaje de las anotaciones de actividades que se ha de visualizar. Este entero es sólo la parte numérica del mensaje. Este parámetro es opcional.

#### Search

Especifica una serie de texto que desea buscar en las anotaciones de actividades. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

Nota: No escriba como una serie de texto el nombre del servidor de IBM Spectrum Protect ni texto con un carácter comodín para buscar el nombre del servidor. De hacerlo, la salida incluirá mensajes que no contendrán la serie de búsqueda.

#### NODENAME

Especifica que la consulta visualiza los mensajes que se han anotado para este nodo. Si no especifica un valor para este parámetro, se muestran los mensajes de todos los nodos.

#### ORIGINATOR

Especifica que la consulta visualiza los mensajes que ha anotado el servidor, el cliente o ambos. El valor predeterminado es ALL. Los valores posibles son:

#### ALL

Especifica que la consulta visualiza los mensajes que se han originado en el cliente y en el servidor.

#### SERVER

Especifica que la consulta visualiza los mensajes que se han originado en el servidor.

#### CLIENT

Especifica que la consulta visualiza los mensajes que se han originado en el cliente.

Puede especificar uno de los valores siguientes para minimizar el tiempo de proceso al consultar en las anotaciones de actividades los mensajes que ha anotado el cliente:

#### OWNERNAME

Especifica que la consulta visualiza los mensajes que se han anotado para un propietario concreto. Si no especifica ningún valor en este parámetro, se visualizan los mensajes de todos los propietarios.

#### SCHEDNAME

Especifica que la consulta visualiza los mensajes que una actividad de cliente planificada concreta ha anotado. Si no especifica ningún valor para este parámetro, se muestran los mensajes de todas las planificaciones.

#### DOMAINNAME

Especifica que la consulta visualiza los mensajes que se han anotado para un dominio de políticas concreto al que pertenece la planificación indicada. Este parámetro es opcional, a menos que especifique un nombre de planificación.

#### SESSNUM

Especifica que la consulta visualiza los mensajes que se han anotado a partir de un número de sesión de cliente concreto. Si no especifica ningún valor para este parámetro, se visualizan los mensajes de todas las sesiones de cliente.

## Ejemplo: buscar en las anotaciones de actividades mensajes que contengan texto específico

Buscar en el registro de actividades los mensajes que contengan la serie "suprimir". La salida incluirá únicamente los mensajes generados durante la última hora. Emita el comando:

```
query actlog search=suprimir
```

```
Fecha/Hora      Mensaje
-----
27/08/1998 15:19:43 ANR0812I La caducidad de archivos de
                    clientes del inventario se ha
                    completado: 0 archivos suprimidos.
```

## Ejemplo: buscar en las anotaciones de actividades los mensajes que se han generado dentro de un período de tiempo específico

Visualizar los mensajes que se produjeron ayer entre las 9:30 y las 12:30. Emita el comando:



```
query actlog begindate=today-1
begintime=09:30:00 endtime=12:30:00
```

Fecha/Hora	Mensaje
21/10/1998 10:52:36	ANR0407I Sesión 3921 iniciada para administrador ADMIN (WebBrowser) (HTTP 9.115.20.100(2315)).
21/10/1998 11:06:08	ANR0405I Sesión 3922 finalizada para administrador ADMIN (WebBrowser).
21/10/1998 12:16:50	ANR0405I Sesión 3934 finalizada para administrador ADMIN (WebBrowser).

## Ejemplo: buscar en las anotaciones de actividades los mensajes de un nodo de cliente específico

Buscar en las anotaciones de actividades los mensajes de IBM Spectrum Protect originados en el cliente para el nodo JEE. Emita el comando:

```
query actlog originator=client node=jee
```

Fecha/Hora	Mensaje
10/06/1998 15:46:22	ANE4007E (Núm. sesión: 3 Nodo: JEE) Error al procesar '/jee/report.out': denegado acceso al objeto
11/06/1998 15:56:56	ANE4009E (Núm. sesión: 4 Nodo: JEE) Error al procesar '/jee/work.lst': condición de disco lleno

## Ejemplo: buscar en las anotaciones de actividades los mensajes de cliente y servidor de un nodo de cliente y sesión específicos

Buscar en el registro de actividades los mensajes de IBM Spectrum Protect del cliente y el servidor para el nodo A asociado con la sesión 1. La salida incluye todos los mensajes con la cadena de texto definida, SESSION: 1". Emita el comando:

```
query actlog search="(SESSION:1) "
```

Fecha/Hora	Mensaje
02/13/2012 12:13:42	ANR0406I Sesión 1 iniciada para el nodo A (WinNT) (Tcp/Ip colind(2463)). (SESSION: 1)
02/13/2012 12:13:56	ANE4952I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Número total de objetos inspeccionados: 34 (SESSION: 1)
02/13/2012 12:13:56	ANE4954I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Número total de objetos de copia de seguridad: 34 (SESSION: 1)
02/13/2012 12:13:56	ANE4958I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Número total de objetos actualizados: 0 (SESSION: 1)
02/13/2012 12:13:56	ANE4964I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Tiempo transcurrido en el proceso: 00:00:02 (SESSION: 1)
02/13/2012 12:13:59	ANR0403I La sesión 1 finalizada para nodo A (WinNT). (SESSION: 1)

## Ejemplo: Buscar registro de actividad de los mensajes generados por el cliente de una sesión de cliente

Buscar en el registro de actividades los mensajes de IBM Spectrum Protect de una sesión de cliente específica. La salida incluirá únicamente los mensajes generados por el cliente. Emita el comando:

```
query actlog sessnum=1
```

Fecha/Hora	Mensaje
02/13/2012 12:13:56	ANE4952I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Número total de objetos inspeccionados: 34 (SESSION: 1)
02/13/2012 12:13:56	ANE4954I (ANE4985I Sesión: 1, ANE4986I Nodo: A) Número total de objetos de copia de seguridad: 34 (SESSION: 1)
02/13/2012 12:13:56	ANE4958I (ANE4985I Sesión: 1, ANE4986I Nodo: A)

Número total de objetos actualizados: 0  
 (SESSION: 1)  
 02/13/2012 12:13:56 ANE4964I (ANE4985I Sesión: 1, ANE4986I Nodo: A)  
 Tiempo transcurrido en el proceso: 00:00:02  
 (SESSION: 1)

## Descripciones de los campos

### Date/Time

Especifica la fecha y hora en la que el servidor o el cliente generó el mensaje.

### Mensaje

Especifica el mensaje que generó el servidor o el cliente.

## Comandos relacionados

Tabla 1. Comando relacionado con QUERY ACTLOG

Comando	Descripción
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.

## QUERY ADMIN (Visualizar información de administrador)

Utilice este mandato para visualizar información acerca de uno o más administradores.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-*-----
>>-Query Admin----->
      '-nombre_admin-'

>+-----+
|          .-,-----| |
|          v          | |
| '-Classes-----+System---+-'
|           +-Policy---+
|           +-Storage---+
|           +-Operator---+
|           '-Node-----'

.-Format-----Standard-----
>+-----+----->
| '-Format-----+Standard+-'
|           '-Detailed-'

>+-----+-----+-----+-----<
| '-AUTHentication---+Local+-' | '-ALerts---+Yes+-'
|           '-LDap--'           | '-No--'

```

## Parámetros

### nombre\_admin

Especifica el nombre de un administrador sobre el que desea visualizar información. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se visualizarán todos los administradores.

### Classes

Especifica que desea limitar la salida a aquellos administradores que tengan las clases de privilegio que especifique. Este parámetro es opcional. Puede especificar varias clases de privilegio en una lista separándolas con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, se visualizará la información relacionada con todos los administradores, independientemente de la clase de privilegio. Los valores posibles son:

System

- Visualiza información acerca de los administradores con privilegio de sistema.
- Policy Visualiza información acerca de los administradores con privilegio de políticas.
- STorage Visualiza información acerca de los administradores con privilegio de almacenamiento.
- Operator Visualiza información acerca de los administradores con privilegio de operador.
- Node Visualiza información sobre los usuarios con privilegio de nodo cliente.

**Format**

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

**Standard**

Especifica que se visualizará la información parcial para los administradores especificados.

**Detailed**

Especifica que se visualizará la información completa para los administradores especificados.

**Authentication**

Especifica el método de autenticación de la contraseña para el administrador.

**Local**

Mostrar los administradores que se autentican en el servidor de IBM Spectrum Protect.

**LDap**

Mostrar los administradores que se autentican en un servidor de directorios LDAP. La contraseña del administrador es sensible a las mayúsculas/minúsculas.

**Alert**

Especifica si las alertas se envían a una dirección de correo electrónico de los administradores.

**Yes**

Especifica que las alertas se envíen a la dirección de correo electrónico especificada de los administradores.

**No**

Especifica que las alertas no se envíen a la dirección de correo electrónico especificada de los administradores. Este es el valor predeterminado.

Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

## Ejemplo: visualizar información acerca de todos los administradores

Visualizar información parcial acerca de todos los administradores. Emita el comando:

```
query admin
```

Nombre administrador	Días desde último	Días desde asignación	Bloqueo acceso	Clases privilegio contraseña
ADMIN	<1	<1	No	Sistema
SERVER_CONSOLE			No	Sistema

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información completa acerca de un administrador

Desde un servidor gestionado, visualizar información completa del administrador denominado ADMIN. Emita el comando:

```
query admin admin format=detailed
```

```
Nombre administrador: ADMIN
Fecha/hora último acceso: 1998.06.04 17.10.52
Días desde último acceso: <1
Fecha/hora asignación contraseña: 1998.06.04 17.10.52
Días desde asignación contraseña: 26
Número conexiones no válidas: 0
Bloqueo: No
Contacto:
```

```

Privilegio de sistema: Sí
Privilegio de políticas: **Incluido con privilegio
de sistema**
Privilegio de almacenamiento: **Incluido con privilegio
de sistema**
Privilegio de operador: **Incluido con privilegio
de sistema**
Privilegio de acceso a cliente: **Incluido con privilegio
de sistema**
Privilegio de propietario de cliente: **Incluido con privilegio
de sistema**
Fecha/hora registro: 05/09/1998 23:54:20
Inscrito por administrador: SERVER_CONSOLE
Perfil de gestión:
Período caducidad contraseña: 90 día(s)
Dirección de correo electrónico:
Alertas de correo electrónico: Sí
Autenticación: Local
SSL necesario: No
Session Security: Strict
Transport Method: TLS 1.2

```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

### Nombre administrador

Especifica el nombre del administrador.

### Fecha/hora último acceso

Especifica la fecha y la hora en que el administrador accedió por última vez al servidor.

### Días desde último acceso

Especifica el número de días transcurridos desde que el administrador accedió por última vez al servidor.

### Fecha/hora asignación contraseña

Especifica la fecha y hora en que se ha definido la contraseña del administrador o de la actualización más reciente.

### Días desde asignación contraseña

Especifica el número de días transcurridos desde que se ha definido la contraseña del administrador o desde la actualización más reciente.

### Contador de conexiones no válidas

Especifica el número de intentos de inicio de sesión no válidos que se han realizado desde el último inicio de sesión satisfactorio. Este número únicamente no puede ser distinto a cero cuando un límite de contraseña no válida (SET INVALIDPWLIMIT) es mayor que cero. Cuando el número de intentos no válidos es igual al límite establecido mediante el mandato SET INVALIDPWLIMIT, se bloquea el acceso del administrador al sistema.

### Bloqueo

Especifica si el administrador tiene bloqueado el acceso al sistema.

### Contacto

Especifica cualquier información de contacto para el administrador.

### Privilegio sistema

Especifica si se ha otorgado al administrador el privilegio de sistema.

### Privilegio política

Especifica si se ha otorgado al administrador privilegio de política sin restricciones o los nombres de cualquier dominio de políticas que pueda gestionar el administrador con privilegio de política con restricciones.

### Privilegio almacenamiento

Especifica si se ha otorgado al administrador privilegio sin restricciones de almacenamiento o los nombres de cualquier agrupación de almacenamiento que pueda gestionar el administrador con privilegio de almacenamiento con restricciones.

### Privilegio operador

Especifica si se ha otorgado al administrador el privilegio de operador.

### Privilegio acceso cliente

Especifica que se ha otorgado autorización de acceso a cliente a un usuario con privilegio de nodo.

### Privilegio propietario cliente

Especifica que se ha otorgado autorización de propietario de cliente a un usuario con privilegio de nodo.

### Fecha/hora registro

Especifica la fecha y hora en que se ha registrado el administrador.

### Registrado por administrador

Especifica el nombre del administrador que ha registrado al administrador. Si este campo contiene \$\$CONFIG\_MANAGER\$\$, el administrador está asociado a un perfil que gestiona el gestor de configuración.

### Perfil de gestión

Especifica los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este administrador.

### Período de caducidad de contraseña

Especifica el período de caducidad de la contraseña del administrador.

Dirección de correo electrónico

Especifica la dirección de correo electrónico del administrador.

Alertas de correo electrónico

Especifica si las alertas se envían al administrador especificado por correo electrónico.

Autenticación

Especifica el método de autenticación de contraseña: LOCAL, LDAP o LDAP (pendiente).

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP
Este administrador está configurado para autenticarse con un servidor de directorio LDAP, pero el administrador aún no se autenticó a través de un nodo de cliente.	LDAP (pendiente)

SSL necesario (en desuso)

Especifica si la configuración de seguridad para el ID de usuario administrador requiere capa de sockets seguros (SSL). Los valores pueden ser SI, NO o predeterminado. Debe tener autorización de nivel de sistema para actualizar el valor de administrador SSLREQUIRED . Este parámetro está en desuso.

Seguridad de sesión

Especifica el nivel de seguridad de sesión que se impone para el ID de administrador. Los valores pueden ser STRICT o TRANSITIONAL.

Método de transporte

Especifica el método de transporte que se ha utilizado la última vez para el administrador especificado. Los valores pueden ser TLS 1.2, TLS 1.1 o NONE. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY ADMIN

Comando	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REMOVE ADMIN	Suprime un administrador de la lista de administradores registrados.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
REVOKE AUTHORITY	Revoca una o más clases de privilegio o limita el acceso a los dominios de políticas y agrupaciones de almacenamiento.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.

## QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)

Utilice este mandato para visualizar qué mensajes de servidor se han definido como alertas.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query ALERTTrigger .-*-----+-----><
                        +-----+-----><
                        '---número_mensaje---'
```

## Parámetros

### número\_mensaje

Especifica el número de mensaje que desea consultar. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres. Puede utilizar caracteres comodín para especificar números de mensajes. Si no especifica un número de mensaje, se visualizan todos los desencadenantes de alerta.

## Consultar desencadenantes de alerta para visualizar qué mensajes se designan como alertas

Visualice todos los mensajes designados como alertas, emitiendo el mandato siguiente:

```
query alerttrigger
```

Ejemplo de salida:

Desencadenante alerta	Categoría	Administrador
ANR1067E	SERVER	HARRYH
ANR1073E	SERVER	CSDADMIN, DJADMIN, HARRYH
ANR1074E	STORAGE	CSDADMIN, DJADMIN, HARRYH
ANR1096E	STORAGE	CSDADMIN, DJADMIN, HARRYH, MHAYE

## Consultar desencadenantes de alerta para un número de mensajes específico

Visualice todos los desencadenantes de alerta que tienen designado el número de mensaje ANR1067E emitiendo el mandato siguiente:

```
query alerttrigger ANR1067E
```

Ejemplo de salida:

Desencadenante alerta	Categoría	Administrador
ANR1067E	SERVER	HARRYH

## Descripciones de los campos

### Activador de alerta

Número de mensaje del activador de alerta.

### Categoría

Categoría del activador de alerta.

### Administrador

Nombre del administrador que recibe las alertas de este activador de alerta.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY ALERTTRIGGER

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.



## CATegory

Especifica el tipo de categoría de la alerta, que está determinado por los tipos de mensajes. Especifique uno de los siguientes valores:

### APplication

La alerta se clasifica como una categoría de aplicación. Por ejemplo, puede especificar esta categoría para los mensajes asociados con los clientes de aplicación (TDP).

### INventory

La alerta se clasifica como categoría de inventario. Por ejemplo, puede especificar esta categoría para mensajes que están asociados con la base de datos, el archivo de registro activo o el archivo de registro de archivado.

Nota: Se utiliza la categoría `CATalog` en lugar de `INventory` en las alertas de servidores que no se han actualizado a IBM Spectrum Protect 7.1.0 o posterior.

### CLient

La alerta se clasifica como una categoría de cliente. Por ejemplo, puede especificar esta categoría para los mensajes asociados con actividades de cliente generales.

### DEvice

La alerta se clasifica como una categoría de dispositivo. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados a las clases de dispositivos, bibliotecas, unidades o vías de acceso.

### SErver

La alerta se clasifica como una categoría de servidor general. Por ejemplo, puede especificar esta categoría para los mensajes asociados a las actividades del servidor generales o a sucesos.

### STorage

La alerta se clasifica como una categoría de almacenamiento. Por ejemplo, puede especificar esta categoría para los mensajes asociados con las agrupaciones de almacenamiento.

### SYstems

La alerta se clasifica como una categoría de clientes del sistema. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con los clientes de archivado y copia de seguridad del sistema o archivado y copia de seguridad de gestión de almacenamiento jerárquico (HSM).

### VMclient

La alerta se clasifica bajo la categoría `VMclient`. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con clientes de máquina virtual.

## SOURCEType

Especifica el tipo de origen que se está consultando. Especifique uno de los siguientes valores:

### LOcal

Visualiza alertas que se han originado en el servidor de IBM Spectrum Protect local.

### CLient

Visualiza alertas que se han originado en el cliente de IBM Spectrum Protect.

### REmote

Visualiza alertas que se han originado en otro servidor de IBM Spectrum Protect.

## SOURCENAME

Especifica el nombre del origen donde se ha originado la alerta. `SOURCENAME` puede ser el nombre de un servidor de IBM Spectrum Protect local o remoto, o un cliente de IBM Spectrum Protect.

## ID

Este parámetro opcional especifica el ID exclusivo de la alerta que desea visualizar. Especifique un valor de 1 a 9223372036854775807.

## ASSigned

Especifica el nombre del administrador que se asigna a la alerta que desea consultar.

## RESolvedby

Especifica el nombre de administrador que ha resuelto la alerta que desea consultar.

## Consultar alertas activas

---

Muestra solo las alertas que están activas en la base de datos de servidor emitiendo el siguiente mandato:

```
query alertstatus status=active
```

## Consultar alertas activas para dos mensajes emitidos por el servidor local

---

Emita el mandato siguiente para visualizar sólo las alertas activas para los números de mensaje ANE4958I y ANR4952E que han sido emitidos por el servidor local:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=local
```



## Consultar alertas activas de los mensajes ANR4958I y ANR4952E emitidos por un cliente

---

Emita el mandato siguiente para visualizar sólo las alertas activas para los números de mensaje ANE4958I y ANE4952I emitidas por un cliente:

```
query alertstatus msgnum=4958,4952 status=active sourcetype=client
```

## Consultar todas las alertas en un servidor

---

Emita el mandato siguiente para visualizar todas las alertas que hay en el servidor:

```
query alertstatus
```

Salida de ejemplo: Visualizar todas las alertas que hay en el servidor:

```
Identificador de alerta: 83
Número de mensaje de alerta: 293
Nombre origen: SEDONA
Tipo de origen: LOCAL
Primera aparición: 03/07/2013 17:08:35
Última aparición: 03/07/2013 17:08:35
Recuento: 1
Estado: ACTIVE
Último cambio de estado: 12/31/1969 17:00:00
Categoría: INVENTORY
Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla AF_BITFILES.
Asignado:
Resuelto por:
Observación:
```

```
Identificador de alerta: 85
Número de mensaje de alerta: 293
Nombre origen: SEDONA
Tipo de origen: LOCAL
Primera aparición: 03/08/2013 05:45:00
Última aparición: 03/08/2013 05:45:00
Recuento: 1
Estado: ACTIVE
Último cambio de estado: 12/31/1969 17:00:00
Categoría: INVENTORY
Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
BF_AGGREGATED_BITFILES.
Asignado:
Resuelto por:
Observación:
```

```
Identificador de alerta: 1282
Número de mensaje de alerta: 293
Nombre origen: ALPINE
Tipo de origen: LOCAL
Primera aparición: 02/13/2013 15:47:50
Última aparición: 02/13/2013 15:47:50
Recuento: 1
Estado: CLOSED
Último cambio de estado: 02/26/2013 09:46:39
Categoría: INVENTORY
Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
TSMON_ALERT.
Asignado:
Resuelto por:
Observación:
```

```
Identificador de alerta: 1792
Número de mensaje de alerta: 293
Nombre origen: ALPINE
Tipo de origen: LOCAL
Primera aparición: 02/19/2013 08:58:14
Última aparición: 02/19/2013 08:58:14
Recuento: 1
Estado: CLOSED
Último cambio de estado: 03/01/2013 12:39:21
Categoría: INVENTORY
Mensaje: ANR0293I Se ha iniciado la reorganización de la tabla
ACTIVITY_LOG.
```

Asignado:  
Resuelto por:  
Observación:

## Descripciones de los campos

---

Identificador de alerta  
Identificador exclusivo de la alerta.

Número de mensaje de alerta  
Número de mensaje de la alerta.

Nombre de origen  
Nombre del origen desde el que se originó la alerta.

Tipo de origen  
Tipo de origen inicial

Primera aparición  
Fecha y hora de la primera aparición de la alerta.

Última aparición  
Fecha y hora de la última aparición de la alerta.

Recuento  
Número total de veces que se ha desencadenado la alerta.

Estado  
Especifica el estado de la alerta.

Último cambio de estado  
Especifica la fecha y la hora a las que cambió por última vez el estado de la alerta.

Categoría  
Categoría de la alerta.

Mensaje  
Mensaje que desencadena la alerta.

Asignado  
Especifica el usuario al que incumbe esta alerta.

Resuelto por  
Especifica el usuario que ha investigado y resuelto la alerta.

Comentarios  
Observación opcional registrada por el solucionador.

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con QUERY ALERTSTATUS

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

## QUERY ASSOCIATION (Consultar asociaciones de nodos cliente con una planificación)

---

Utilice este comando para visualizar la información sobre qué nodos cliente están asociados a una o varias planificaciones. Los nodos cliente asociados a una planificación realizan operaciones como, por ejemplo, copia de seguridad o copia archivada, en función de la planificación.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query ASSOCIATION----->
.
.*-----
>--+-----+-----><
|          .*-----|
|'-nom_dominio--+-----+'
|          '-nombre_planificación-'
```

## Parámetros

### nombre\_dominio

Especifica el nombre del dominio de políticas que se visualizará. Puede utilizar un carácter comodín para especificar este nombre. Se visualizarán todos los nombres de dominios de políticas que coincidan. Si no especifica un valor para este parámetro, se visualizarán todos los dominios de políticas existentes. Si especifica un nombre de dominio, no tiene que especificar un nombre de planificación.

### nombre\_planificación

Especifica el nombre de la planificación que se visualizará. Puede utilizar un carácter comodín para especificar este nombre. Se visualizarán todos los nombres de planificación que coincidan. Si no especifica un valor para este parámetro, se consultarán todas las planificaciones existentes. Si especifica un nombre de planificación, debe especificar también un nombre de dominio de políticas.

## Ejemplo: visualizar los nodos cliente que se asocian a una planificación

Visualizar todos los nodos cliente que están asociados a cada planificación que pertenece al dominio de políticas EMPLOYEE\_RECORDS. Emita el comando:

```
query association employee_records *

Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre planificación: WEEKLY_BACKUP
Nodos asociados: JOE JOHNSON LARRY SMITH SMITHERS TOM
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

### Nombre dominio políticas

Especifica el nombre del dominio de políticas al que pertenece la planificación.

### Schedule Name

Especifica el nombre de la planificación.

### Nodos asociados

Especifica los nombres de los nodos cliente que están asociados a la planificación indicada.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY ASSOCIATION

Comando	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DELETE ASSOCIATION	Suprime la asociación entre los clientes y una planificación.

## QUERY AUDITOCUPANCY (Consultar la utilización del almacenamiento de los nodos cliente)

Utilice este mandato para visualizar información sobre la utilización del almacenamiento del servidor del nodo de cliente. Para visualizar la información de auditoría de licencias actual del servidor, utilice el mandato AUDIT LICENSE antes de emitir el mandato QUERY AUDITOCUPANCY.

Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento de gestión de espacio, de copia de seguridad/archivado que está utilizándose. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de processor y puede atascar otras actividades del servidor. Puede utilizar la opción de servidor AUDITSTORAGE para especificar que no se calcule el almacenamiento como parte de una auditoría de licencia.

Puede utilizar la información de esta consulta para determinar si se debe equilibrar la utilización de almacenamiento de nodos de cliente y dónde debe hacerse. Esta información puede ayudarle en la facturación de clientes por utilización del almacenamiento.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query AUDITOccupancy-----+----->
      | .-,----- . |
      | v          | |
      +---nombre_nodo---+
-----+----->
      | .-,----- . |
      | v          | |
      +---Dmain-----nombre_dominio---+
      .-POoltype-----ANY-----
>-----+-----<<
      '-POoltype-----+ANY-----'
              +-PRimary--+
              '-COpy----'
```

## Parámetros

### nombre\_nodo

Especifica una lista de nodos para los que se ha de visualizar la información de utilización del almacenamiento del servidor. Puede especificar varios nodos separando los nombres de nodos con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. El valor predeterminado (\*) es consultar todos los nodos clientes. Utilice el parámetro DOMAIN para que esta lista se limite a los dominios de políticas. Este parámetro es opcional.

### DOMAIN

Especifica una lista de los dominios de políticas para limitar qué nodos se han de visualizar. Se visualizan los nodos que pertenecen a los dominios de políticas especificados. Puede especificar varios dominios de políticas separando los nombres de dominios de políticas con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Este parámetro es opcional.

### POoltype

Especifica el tipo de almacenamiento de agrupación de almacenamiento que se visualizará. Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

#### ANY

Especifica las agrupaciones de almacenamiento primarias y de copia. El valor que se presenta es el total para las dos agrupaciones.

#### PRimary

Especifica sólo agrupaciones de almacenamiento primarias.

#### COpy

Especifica sólo agrupaciones de almacenamiento de copia.

## Ejemplo: visualizar la utilización del almacenamiento

Visualizar la utilización de almacenamiento combinada de las agrupaciones de almacenamiento primarias y de copia. Emita el comando:

```
query auditoccupancy
```

Información según última auditoría con fecha 22/05/1996 14:49:51.

Nombre nodo	Copia de seguridad copias seg. (MB)	Archivado copias archivadas	Espacio gestionado gestión espacio (MB)	Total total (MB)
-----	-----	-----	-----	-----



```

>----->
'-WHERERetention---+---días---+'
          '-NOLimit-'

>----->
'-WHEREDEScription----descripción-'

>----->
'-WHEREDEVclass---+---nombre_clase_dispositivo-'

>----->
'-WHERETOCexists---+---Yes---+'
          '-No---'

>----->
|           .-,-----|.
|           V           |
'-WHEREDATAType---+---FILE---+'
          '-IMAGE-'

.-Format---+---Standard---.
>----->
'-Format---+---Standard---+'
          '-Detailed-'

```

## Parámetros

nombre\_nodo o nombre\_grupo\_nodos

Especifica el nombre del nodo cliente y grupos de nodos cuyos datos contenidos en el juego de copias de seguridad se van a visualizar. Para especificar varios nombres de nodo y nombres de grupos de nodos, sepárelos con comas y sin espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos.

nombre\_juego\_copias\_seguridad

Especifica el nombre del juego de copias de seguridad cuya información se va a visualizar. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

BEGINDate

Especifica la fecha inicial del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la hora y la fecha. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

#### ENDDate

Especifica la fecha de finalización del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha finales. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final del rango en el que debe encontrarse la fecha de instante específico del juego de copias de seguridad que debe mostrarse. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDDATE para especificar una fecha y hora. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

#### WHERERetention

Especifica el valor de retención, expresado en días, que debe asociarse a los juegos de copias de seguridad que han de visualizarse. Puede especificar un entero entre el 0 y el 30000. Los valores son:

días

Especifica que los juegos de copias de seguridad que permanecen retenidos durante este número de días, se visualizarán.

NOLimit

Especifica que los juegos de copias de seguridad que permanecen retenidos indefinidamente, se visualizarán.

#### WHEREDescription

Especifica la descripción que debe estar asociada al juego de copias de seguridad que se va a visualizar. La descripción que especifique puede contener caracteres comodín. Este parámetro es opcional. La descripción debe estar delimitada por comillas

si contiene algún carácter en blanco.

#### WHEREDEVclass

Especifica el nombre de la clase de dispositivo asociada al juego de copias de seguridad se va a visualizar. Puede utilizar caracteres comodín para especificar un nombre de clase de dispositivo. Este parámetro es opcional.

#### WHERETOCexists

Especifica si un juego de copias de seguridad debe incluir una tabla de contenido para poder visualizarse. Este parámetro es opcional. El valor predeterminado es mostrar todos los juegos de copias de seguridad independientemente de si tienen o no una tabla de contenido.

#### WHEREDATATYPE

Especifica el tipo de datos del juego de copias de seguridad que se visualizará. Este parámetro es opcional. El valor predeterminado es visualizar todos los tipos de juegos de copias de seguridad. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados.

#### FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a visualizar. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad/archivado.

#### IMAGE

Especifica que se va a visualizar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el comando BACKUP IMAGE del cliente de copia de seguridad/archivado.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial sobre los juegos de copias de seguridad especificados.

##### Detailed

Especifica que se visualizará información completa sobre los juegos de copias de seguridad especificados.

## Ejemplo: consultar un juego de copias de seguridad

---

Visualizar información para los juegos de copias de seguridad cuyos nombres empiecen por PERS\_DATA. Los juegos de copias de seguridad pertenecen al nodo JANE y están asignados a la clase de dispositivo DVLMENT.

```
query backupset jane pers_data*
```

```
Nombre nodo: JANE
Juego copias seguridad: PERS_DATA.3089
Tipo de datos: Archivo
Fecha/hora: 03/17/2007 16:17:47
Período de retención: 60
Nombre clase dispositivo: DVLMENT
Descripción: juego de copias de seguridad
                creado desde /srvr
```

```
¿Tiene tabla de contenido (TOC)? : Sí
```

## Descripciones de los campos

---

#### Nombre del nodo

Especifica el nombre del nodo de cliente cuyos datos están contenidos en el juego de copias de seguridad.

#### Nombre del conjunto de copias de seguridad

Especifica el nombre del juego de copias de seguridad.

#### Tipo de datos

Visualiza el tipo de datos de los juegos de copias de seguridad. Los tipos posibles son archivo, imagen y aplicación.

#### Date/Time

Especifica la fecha y la hora (PITDate y PITTime) del comando GENERATE BACKUPSET. Los valores PITDate y PITTime especifican que los archivos que estaban activos en la fecha y hora especificadas y que todavía están almacenados en el servidor de IBM Spectrum Protect deben incluirse en el juego de copias de seguridad, aunque estén inactivos en el momento en el que emite el comando GENERATE BACKUPSET. El valor predeterminado es la fecha en la que se ejecuta el comando GENERATE BACKUPSET.

#### Período de retención

Especifica el número de días que se retiene en el servidor el juego de copias de seguridad.

#### Nombre clase dispositivo

Especifica el nombre de la clase de dispositivo para el que se asignan los volúmenes que contienen el juego de copias de seguridad.

#### Descripción



Especifica la descripción asociada al juego de copias de seguridad.  
 ¿Tiene tabla de contenido (TOC)?  
 Especifica si el juego de copias de seguridad tiene una tabla de contenido.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY BACKUPSET

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## QUERY BACKUPSETCONTENTS (Consultar el contenido de un juego de copias de seguridad)

Utilice este comando para visualizar información acerca de los archivos y directorios que contiene un juego de copias de seguridad para un nodo cliente.

Recuerde: Al procesar este comando es posible que se utilice una cantidad considerable de recursos de red y de puntos de montaje.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

### Sintaxis

```
>>-Query BACKUPSETCONTENTS----->
>--nombre_nodo--nombre_juego_copias_seguridad----->
  .-DATAType----FILE-----
>--+-----+-----<
  '-DATAType----+FILE--+'
      '-IMAGE-'
```

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo cliente cuyos datos contenidos en el juego de copias de seguridad se van a visualizar. El nombre especificado no puede contener caracteres comodín ni puede ser una lista de nombres de nodos separados por comas.

nombre\_juego\_copias\_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a visualizar. El nombre que se especifique no puede contener caracteres comodín ni puede ser una lista de nombres de nodos separados por comas.

## DATATYPE

Especifica que se va a consultar el juego de copias de seguridad que contiene los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que se va a consultar un juego de copias de seguridad de nivel de archivo. Los valores posibles son:

### FILE

Especifica que se va a consultar un juego de copias de seguridad de nivel de archivo. Los juegos de copias de seguridad de nivel de archivo contienen archivos y directorios cuya copia de seguridad ha sido realizada por el cliente de copia de seguridad/archivado.

### IMAGE

Especifica que se va a consultar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el comando BACKUP IMAGE del cliente de copia de seguridad/archivado.

## Ejemplo: consultar el contenido de un juego de copias de seguridad para un nodo específico

Visualizar el contenido del juego de copias de seguridad denominado PERS\_DATA.3099 que pertenece al nodo cliente JANE. Emita el comando:

```
query backupsetcontents jane pers_data.3099
```

Nombre nodo	Espacio archivos	Nombre de archivo del cliente
JANE	/srvr	/deblock
JANE	/srvr	/deblock.c
JANE	/srvr	/dsmerror.log
JANE	/srvr	/dsmxxxxx.log
JANE	...	.....

## Descripciones de los campos

### Node Name

Especifica el nombre del nodo cliente cuyos datos están contenidos en el juego de copias de seguridad.

### Filespace Name

Especifica el nombre del espacio de archivos al que pertenece el archivo especificado.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

### Nombre del archivo en el cliente

Especifica el nombre del archivo.

Los nombres de espacios de archivos y nombres de archivo que pueden estar en una página de códigos o un entorno local diferente de los del servidor no se visualizan correctamente en el Centro de operaciones ni en la interfaz de línea de comandos de administración. Se efectúa una copia de seguridad de los propios datos que se pueden restaurar correctamente pero el nombre del espacio de archivos o del archivo puede visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está activado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El resultado de la conversión de caracteres que no soporta la página de códigos actual depende del sistema operativo. Los nombres que IBM Spectrum Protect puede convertir parcialmente pueden ir acompañados de signos de interrogación (??), espacios en blanco, caracteres que no se pueden imprimir o "...". Estos caracteres indican al administrador que existen archivos. Si la conversión no es satisfactoria, el nombre se visualiza como "...". La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.




Un nombre de archivo visualizado como "....." indica que ni la ruta del archivo ni el nombre del archivo se han convertido correctamente. Un ejemplo de ruta y nombre puede ser:

```
my\dir\...
```

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY BACKUPSETCONTENTS

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY CLEANUP (Consultar la limpieza necesaria en una agrupación de almacenamiento de origen)

Utilice este mandato para visualizar información acerca de los archivos dañados identificados durante un proceso de conversión de agrupación de almacenamiento.

Si emite el mandato CONVERT STGPOOL para convertir una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedores de directorio, es posible que algunos archivos de la agrupación de almacenamiento de origen no se conviertan debido a los datos dañados. Para visualizar los datos dañados identificados durante el proceso de conversión, emita el mandato QUERY CLEANUP en una agrupación de almacenamiento de origen.

Para recuperar una versión sin daños de los datos de una agrupación de almacenamiento de copia o de datos activos, emita el mandato RESTORE STGPOOL. Para recuperar una versión sin daños de los datos de un servidor de réplica de destino, emita el mandato REPLICATE NODE y especifique el parámetro RECOVERDAMAGED=YES.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

### Sintaxis

```
>>-Query CLeanup--nombre_agrupación-----<<
```

### Parámetros

nombre\_agrupación (Obligatorio)  
Especifica la agrupación de almacenamiento que se consulta.

## Ejemplo: Visualizar los archivos dañados identificados por un proceso de conversión de agrupación de almacenamiento

Visualice los archivos dañados de una agrupación de almacenamiento denominada POOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query cleanup pool1
```

```
Nombre de archivo: \RTC\BDAT\GIGFILES\BF1.GB
Estado: Activo
Tamaño almacenado: 1 GB
```

Nombre de espacio de archivos: \\ibm838-r90gf0gx\c\$\nTipo: Backup\nNombre de cliente: CAKINProtection\nFecha de protección: 03/25/2016 16:47:57

## Descripciones de los campos

### Nombre de archivo

El nombre del archivo dañado.

### Estado

El estado de los datos en el inventario. Son posibles los siguientes estados:

#### Activo

La versión del archivo en el inventario está activa. Solo puede haber una versión activa del archivo en el inventario.

#### Inactivo

La versión del archivo en el inventario está inactiva. Pueden haber varias versiones inactivas del archivo en el inventario.

### Tamaño almacenado

El tamaño de los datos, en megabytes (MB) o gigabytes (GB), que se almacenan en la agrupación de almacenamiento.

### Nombre de espacio de archivos

El nombre del espacio de archivos donde está asignado el archivo.

### Tipo

El tipo de operación utilizado para almacenar el archivo. Son posibles los valores siguientes:

#### Copia de seguridad

Archivos de los que se ha realizado una copia de seguridad.

#### Archivado

Archivos que se han archivado.

#### Gestión espacio

Archivos que se migran desde un cliente IBM Spectrum Protect for Space Management.

### Nombre cliente

El nombre del cliente que es propietario del archivo.

### Fecha de protección

Fecha y hora de la copia de seguridad, el archivado o la migración del archivo por parte del cliente de IBM Spectrum Protect for Space Management.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY CLEANUP

Comando	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY CONVERSION	Consultar estado de conversión de una agrupación de almacenamiento.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.

## QUERY CLOPTSET (Consultar un conjunto de opciones de cliente)

Utilice este comando para consultar un conjunto de opciones de cliente.



Valor de opción  
Especifica el valor de la opción.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY CLOPTSET

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.
UPDATE CLOPTSET	Actualiza la descripción de un conjunto de opciones de cliente.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.

## QUERY COLLOGROUP (Consultar un grupo de proximidad)

Utilice este mandato para visualizar los grupos de proximidad definidos en el servidor.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
.-*-----.  
>>-Query COLLOGGroup--+-----+----->  
      '-nombre_grupo-'  
  
.-Format----Standard----.  
>--+-----+-----><  
      '-Format----+Standard-+ '  
      '-Detailed-'
```

### Parámetros

#### nombre\_grupo

Especifica el nombre del grupo de proximidad que se visualizará. Para especificar varios nombres, utilice un carácter comodín. Este parámetro es opcional. El valor predeterminado es visualizar todos los grupos de proximidad.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información. Para visualizar los miembros del grupo de proximidad, debe especificar FORMAT=DETAILED.

## Visualizar grupos de proximidad definidos

Mostrar los grupos de proximidad definidos en el servidor. Emita el mandato siguiente:

```
query collogroup
```

```
Nombre del grupo de      Descripción del grupo de  
proximidad                proximidad
```

-----  
DEPT\_ED  
GROUP1

-----  
Departamento de formación  
Nodos cliente de baja capacidad.

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Mostrar información detallada para grupos de proximidad

Mostrar información completa sobre todos los grupos de proximidad y determinar qué nodos cliente pertenecen a qué grupos de proximidad. Emita el mandato siguiente:

```
query colloggroup format=detailed
```

```
Nombre del grupo de proximidad: DEPT_ED
Descripción del grupo de proximidad: Departamento de formación
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:03
Miembro(s) del grupo de proximidad: EDU_1 EDU_7
Miembros(s) de espacio de archivos:
```

```
Nombre del grupo de proximidad: GROUP1_ED
Descripción del grupo de proximidad: nodos cliente de baja
capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:16
Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: alpha
```

```
Nombre del grupo de proximidad: GROUP1_ED
Descripción del grupo de proximidad: nodos cliente de baja
capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:16
Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: beta
```

```
Nombre del grupo de proximidad: GROUP1_ED
Descripción del grupo de proximidad: nodos cliente de baja
capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora de la última actualización: 21/04/2013 10:59:16
Miembro(s) de grupo de proximidad: CHESTER
Miembro(s) de espacio de archivos: gamma
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

Nombre de grupo de proximidad

El nombre del grupo de proximidad.

Descripción de grupo de proximidad

La descripción del grupo de proximidad.

Última actualización por (administrador)

El nombre del administrador que ha definido o ha actualizado más recientemente el grupo de proximidad.

Fecha/hora última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente el grupo de proximidad.

Miembro(s) de grupo de proximidad

Los miembros del grupo de proximidad.

Miembro(s) de espacio de archivos




El espacio o espacios de archivos miembros del grupo de proximidad. Si hay más de un espacio de archivos, aparecen cada uno en una entrada distinta.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY COLLOGGROUP

Comando	Descripción
DEFINE COLLOGGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY CONTAINER (Consulta de un contenedor)

Utilice este mandato para visualizar información sobre uno o más contenedores.

### Clase de privilegio

Cualquier administrador puede emitir este mandato.

### Sintaxis

```

.-*-----
>>-Query CONTAINER--+-+-----+----->
                        '-nombre_contenedor-'

>+-----+----->
  '-STGpool----nombre_agrupación-'

.-Format----Standard----.  .-State----ANY-----
>+-----+-----+-----+----->
  '-Format-----Standard-+-'  '-State-----AVAILABLE---+'
                        '-Detailed-'                        +-UNAvailable-+
                                                                +-ANY-----+
                                                                +-REAdonly----+
                                                                '-PENding----'

.-TYPE----ANY-----
>+-----+-----+-----+-----><
  '-TYPE-----NONdedup-+-'
                        +-DEDup-----+
                        +-CLOud-----+
                        '-ANY-----'

```

### Parámetros

nombre\_contenedor

Especifica el nombre del contenedor. Especifique uno de los siguientes valores:

\*

Especifica que un asterisco (\*) representa un carácter comodín. Utilice los caracteres comodín como, por ejemplo, un asterisco para que coincida con cualquier carácter. De forma alternativa, puede utilizar un signo de interrogación (?) o un



signo de porcentaje (%) para hacer coincidir con exactitud un carácter. Si especifica un asterisco, se visualizarán todos los nombres de contenedor. Este es el valor predeterminado.

nombre\_contenedor

Especifica el nombre del contenedor. La longitud máxima del nombre de archivo es de 1024.

#### STGpool

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. La longitud máxima del nombre de la agrupación de almacenamiento es de 30.

#### Format

Especifica el nivel de detalla de los resultados de la consulta. Este parámetro es opcional. Especifique uno de los siguientes valores:

Standard

Especifica que se visualiza un resumen de la información. Este es el valor predeterminado.

Detailed

Especifica que se visualizará información detallada.

#### STate

Especifica el estado del contenedor que se está consultando. Este parámetro es opcional. Especifique uno de los siguientes valores:

AVAIable

Especifica que sólo se muestran los contenedores que están disponibles.

UNAVailable

Especifica que sólo se muestran los contenedores que no están disponibles. Por ejemplo, un contenedor puede no estar disponible si la cabecera está dañada o si el contenedor no puede abrirse.

ANY

Especifica que se visualizan contenedores que se hallan en cualquier estado. Este es el valor predeterminado.

READonly

Especifica que sólo se visualizan contenedores cuyo estado es de sólo lectura. Los datos se pueden leer pero no se pueden grabar en el contenedor.

PENding

Especifica que sólo se visualizan contenedores cuyo estado es pendiente.

#### TYPE

Especifica el tipo de contenedor que se consulta. Este parámetro es opcional. Especifique uno de los valores siguientes:

NONdedup

Visualiza contenedores que contienen datos de los que no se eliminan duplicados. Este tipo de datos incluye metadatos, datos cifrados y datos que son demasiado pequeños para eliminar duplicados de datos.

DEDup

Visualiza contenedores que contienen datos con duplicados eliminados.

CLOud

Muestra los contenedores que están almacenados en una agrupación de almacenamiento en la nube.

ANY

Visualiza cualquier tipo de contenedor. Este es el valor predeterminado.

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: visualizar información sobre un contenedor

---

Consulte Descripciones de los campos para ver una descripción de los campos.

```
query container /Containers/09/0000000000000943.ncf
```

Container	Storage Pool Name	Container Type	State
/Containers/09/0000000000000943.ncf	STGPOOL1	Non Dedup	Available

 Sistemas operativos Windows

## Ejemplo: visualizar información sobre un contenedor

---

Consulte Descripciones de los campos para ver una descripción de los campos.

```
query container C:\abc\00\0000000000000005.ncf
```

Container	Storage	Container	State
		Pool Name	Type
C:\abc\00\0000000000000005.ncf		STGPOOL1	Non Dedup Available

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: visualizar información detallada sobre un contenedor

---

Visualice información detallada sobre contenedores que contienen datos con duplicados eliminados en la agrupación de almacenamiento STGPOOL1:

```
query container stgpool=STGPOOL1 type=dedup format=detail

Container: /abc/00/0000000000000001.dcf
Nombre de la agrupación de almacenamiento: STGPOOL1
Tipo de contenedor: Dedup
Estado: Disponible
Tamaño máximo (MB): 40.960
Espacio libre (MB): 39.700
Fecha aprox. última grabación: 11/10/2014 15:17:09
Fecha aprox. de última auditoría:
Tipo de nube:
URL de nube:
Espacio utilizado (MB):
Recuento de objetos:
```

 Sistemas operativos Windows

## Ejemplo: visualizar información detallada sobre un contenedor

---

Visualice información detallada sobre contenedores que contienen datos con duplicados eliminados en la agrupación de almacenamiento STGPOOL1:

```
query container stgpool=STGPOOL1 type=dedup format=detail

Container: C:\abc\00\0000000000000001.dcf
Nombre de la agrupación de almacenamiento: STGPOOL1
Tipo de contenedor: Dedup
Estado: Disponible
Tamaño máximo (MB): 40.960
Espacio libre (MB): 39.700
Fecha aprox. última grabación: 11/10/2014 15:17:09
Fecha aprox. de última auditoría:
Tipo de nube:
URL de nube:
Espacio utilizado (MB):
Recuento de objetos:
```

## Ejemplo: visualizar información detallada sobre los contenedores que están almacenados en una agrupación de almacenamiento en la nube

---

Visualice información detallada sobre los contenedores que están almacenados en la agrupación de almacenamiento en la nube CLOUDPOOL:

```
query container stgpool=CLOUDPOOL format=detail

Container: 7-64a1261000c811e58e8f005056c00008
Nombre agrupación almacenamiento: CLOUDPOOL
Container Type: Cloud
Estado:
Espacio libre (MB):
Tamaño máximo (MB):
Fecha aprox. última grabación: 05/22/2015 14:36:57
Fecha aprox. de última auditoría:
Tipo de nube: SWIFT
URL de nube: http://cloudurl:5000/v2.0
Espacio utilizado (MB): 7104
Recuento de objetos: 2472
```

## Descripciones de los campos

---

Contenedor

El nombre del contenedor.

Nombre de la agrupación de almacenamiento  
El nombre de la agrupación de almacenamiento.

Tipo de contenedor  
Tipo del contenedor.

Estado  
El estado de los datos en el contenedor. El campo puede contener uno de los siguientes valores:

- Disponible  
El contenedor está disponible para su uso.
- Unavailable  
El contenedor no se puede abrir o validar.  
Consejo: Emita el comando AUDIT CONTAINER para validar el contenido del contenedor.
- Sólo lectura  
El contenedor puede leerse pero no se pueden escribir datos en el contenedor.
- Pendiente  
El contenedor está pendiente de supresión. Cuando caduca el valor especificado para el parámetro REUSEDELAY en el mandato DEFINE STGPOOL o UPDATE STGPOOL, el contenedor se suprime.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Tamaño máximo (MB)  
El tamaño máximo del contenedor, en megabytes.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Espacio libre (MB)  
La cantidad total de espacio libre que está disponible en el contenedor, en megabytes.

Este campo no es aplicable a los contenedores que están almacenados en agrupaciones de almacenamiento de nube.

Fecha aprox. última grabación  
La fecha y hora aproximadas en que se grabaron los datos en el contenedor.

Fecha aprox. de última auditoría  
La fecha y hora aproximadas en que los datos se auditaron en el contenedor.

Tipo de nube  
Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es el tipo de plataforma de la nube.

URL de nube  
Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es el URL para acceder a la nube privada en las instalaciones o a la nube pública fuera de las instalaciones.

Espacio utilizado (MB)  
Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es la cantidad de espacio que utiliza el contenedor en la nube privada en las instalaciones o en la nube pública fuera de las instalaciones.

Recuento de objetos  
Si el contenedor se almacena en una agrupación de almacenamiento en la nube, es el número de objetos gestionados por la nube privada en las instalaciones o la nube pública fuera de las instalaciones del contenedor.

Tabla 1. Comandos relacionados con QUERY CONTAINER

Comando	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
MOVE CONTAINER	Mueve el contenido de un contenedor de agrupación de almacenamiento a otro contenedor.
QUERY DAMAGED	Muestra información sobre los archivos dañados.

## QUERY CONTENT (Consultar el contenido de un volumen de agrupación de almacenamiento)

Utilice este mandato para visualizar la información sobre los archivos de un volumen de agrupación de almacenamiento y los nombres de archivos de cliente que se enlazan a un grupo con duplicados eliminados.

Puede utilizar este mandato para identificar los archivos que el servidor ha encontrado dañados y los archivos de los que se ha realizado una copia de seguridad en una agrupación de almacenamiento de copias o se han copiado en una agrupación de datos activos. Este

mandato es útil cuando se daña un volumen o antes de que el usuario:

- Solicite al servidor que solucione las incoherencias entre un volumen y la base de datos
- Mueva archivos de un volumen a otro
- Suprima un volumen de una agrupación de almacenamiento

Puesto que este mandato puede tardar mucho tiempo en ejecutarse y los resultados pueden ser voluminosos, considere la posibilidad de utilizar el parámetro COUNT para limitar el número de archivos visualizados.

Nota: Los archivos que se almacenan en caché de un volumen de disco y que están marcados como dañados no se incluyen en el resultado.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query Content--nombre_volumen--+-----+----->
                                     '-NODE---nombre_nodo-'
>--+-----+----->
   '-Filespace---nombre_espacio_archivos-'
                                     .-Type---ANY-.
>--+-----+-----+----->
   '-COUnt---número-' '-Type---+ANY-+'
                                     +-Backup-----+
                                     +-Archive-----+
                                     '-SPacemanaged-'
                                     .-Format---Standard-. .-DAmaged---ANY-.
>--+-----+-----+----->
   '-Format---+Standard-+' '-DAmaged---+ANY-+'
                                     '-Detailed-'           +-Yes-+
                                     '-No--'                 '-No--'
                                     (1)
                                     .-COPIed---ANY-. .-NAMEType---SERVER-.
>--+-----+-----+----->
   '-COPIed---+ANY-+' '-NAMEType---+SERVER-+'
                                     +-Yes-+           +-UNICode-+
                                     '-No--'           '-FSID---'
                                     .-CODEType---BOTH-.
>--+-----+----->
   '-CODEType---+UNICode-+'
                                     +-NONUNICode-+
                                     '-BOTH-----'
                                     .-FOLLOWLinks---No-.
>--+-----+-----+-----><
   '-FOLLOWLinks---+No-+'
                                     +-Yes-----+
                                     '-JUSTLinks-'
```

Notas:

1. Utilice este parámetro únicamente para los volúmenes de las agrupaciones de almacenamiento primarias.

## Parámetros

nombre\_volumen (Necesario)

Especifica el volumen que se ha de consultar.

NODE

Especifica el cliente de copia de seguridad/archivado o de IBM Spectrum Protect for Space Management asociado al espacio de archivos que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica ningún nombre, se incluyen todos los clientes de copia de seguridad/archivado y IBM Spectrum Protect for Space Management.

Filespace

Especifica el espacio de archivos que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Si no especifica un nombre de espacio de archivos, se incluirán todos los espacios de archivos.

Para un servidor que tenga clientes con soporte de Unicode, es posible que necesite hacer que el servidor convierta el nombre de espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para obtener información detallada. Si no especifica ningún nombre de espacio de archivos o especifica sólo un carácter comodín para dicho nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

#### COUnT

Especifica el número de archivos que se han de visualizar. Este parámetro es opcional. Puede especificar un número entero negativo o un número entero positivo. Si especifica un número entero positivo, *n*, se visualizarán los *n* primeros archivos. Si especifica un número entero negativo, *-n*, se visualizarán los *n* últimos archivos en orden *inverso*. No es posible especificar COUNT=0. Si no especifica un valor para este parámetro, se visualizarán todos los archivos.

#### Type

Especifica los tipos de archivos que se consultan. Este parámetro es opcional. El valor predeterminado es ANY. Si el volumen que se consulta está asignado a una agrupación de datos activos, los únicos valores válidos son ANY y BACKUP. Los valores posibles son:

##### ANY

Especifica que se consultan todos los tipos de archivos del volumen de agrupación de almacenamiento; versiones de copia de seguridad de archivos, copias archivadas de archivos y archivos que clientes de IBM Spectrum Protect for Space Management migran desde los nodos cliente.

##### Backup

Especifica que sólo se consultarán los archivos de copia de seguridad.

##### Archive

Especifica que sólo se consultarán las copias archivadas. Este valor no es válido para las agrupaciones de datos activos.

##### SPacemanaged

Especifica que solo se consultan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management). Este valor no es válido para las agrupaciones de datos activos.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial. Los nombres Unicode se convierten a la página de códigos del servidor.

##### Detailed

Especifica que se visualizará toda la información. Los nombres Unicode se visualizan en formato hexadecimal.

#### DAMaged

Especifica criterios para restringir la salida de la consulta en función de si los archivos están marcados como dañados. A los efectos de estos criterios, el servidor sólo examina los archivos físicos (un archivo que puede ser un único archivo lógico o un añadido que consta de archivos lógicos). Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

##### ANY

Especifica que los archivos se visualizarán independientemente de si el servidor detectó que los archivos están dañados.

##### Yes

Especifica que sólo se visualizarán los archivos que están marcados como dañados. Son los archivos en los que el servidor ha detectado errores, cuando un usuario intentaba restaurar o recuperar el archivo o cuando se ejecutaba un mandato AUDIT VOLUME.

##### No

Especifica que sólo se visualizan los archivos que no se sabe si están dañados.

#### COPIed

Especifica los criterios para restringir la salida de la consulta en función de si la copia de seguridad de los archivos se ha hecho en una agrupación de almacenamiento de copia. El hecho que los archivos estén o no estén almacenados en una agrupación de datos activos no influye sobre el resultado. Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

##### ANY

Especifica que los archivos se visualizarán independientemente de si se ha realizado o no una copia de seguridad en una agrupación de almacenamiento de copia. Se visualizarán las copias de los archivos primarios y en caché.

##### Yes

Especifica que sólo se visualizarán los archivos de los que exista como mínimo una copia de seguridad utilizable en una agrupación de almacenamiento de copia. No se visualizará un archivo si se sabe que la copia que existe en la agrupación

de almacenamiento de copia contiene errores. No se visualizarán las copias de archivos en caché ya que estos archivos no se restauran nunca.

Utilice COPIED=YES para identificar los archivos primarios que pueden restaurarse utilizando el mandato RESTORE VOLUME o RESTORE STGPPOOL.

No

Especifica que sólo se visualizarán los archivos de los que no existan copias de seguridad utilizables en una agrupación de almacenamiento de copia. No se visualizarán las copias de archivos en caché ya que estos archivos no se restauran nunca.

Utilice COPIED=NO para identificar los archivos primarios que no pueden restaurarse utilizando el mandato RESTORE VOLUME o RESTORE STGPPOOL.

#### NAMEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Actualmente, un cliente de copia de seguridad/archivado con soporte Unicode sólo está disponible para Windows, Macintosh OS 9, Macintosh OS X y NetWare. Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado.

El valor predeterminado es SERVER. Los valores posibles son:

##### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

##### UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen los nombres y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

##### FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

#### CODEType

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos.

El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Los valores posibles son:

##### UNICODE

Incluir los espacios de archivos que solo están en Unicode.

##### NONUNICODE

Incluir espacios de archivos que no están sólo en Unicode.

##### BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

#### FOLLOWLinks

Especifica si se mostrarán solo los archivos que están almacenados en el volumen o solo los archivos que están enlazados al volumen. También puede mostrar los archivos almacenados y los archivos enlazados. El valor predeterminado es NO. Los valores posibles son:

No

Se muestran solo los archivos que se encuentran almacenados en el volumen. No se muestran los archivos que tienen enlaces al volumen.

Yes

Se muestran todos los archivos, incluidos aquellos que están almacenados en el volumen y los que tienen enlaces al volumen.

JUSTLinks


Se muestran solo los archivos que tienen enlaces al volumen. No se muestran los archivos que están almacenados en el volumen.

## Ejemplo: mostrar el contenido de un volumen para un nodo cliente específico

Consultar el contenido de un volumen y limitar el resultado a los archivos cuya copia de seguridad se hizo desde el nodo cliente PEGASUS.

 Sistemas operativos AIX  Sistemas operativos Linux Para el volumen /tsmstg/diskvol1.dsm, emita el comando:

```
query content /tsmstg/diskvol1.dsm node=pegasus  
type=backup
```

 Sistemas operativos Windows Para el volumen f:\tsmstg\diskvol1.dsm, emita el comando:

```
query content f:\tsmstg\diskvol1.dsm node=pegasus
type=backup
```

El resultado del comando incluye todos los archivos lógicos que forman cualquier agregación de archivos que hay en el volumen, incluso aunque la agregación de archivos esté almacenada en varios volúmenes además de éste. Con las agregaciones de archivos, la consulta no determina cuáles son los archivos lógicos que realmente están almacenados en el volumen cuya consulta se realiza.

zNombre nodo	Tipo	Espacio	FSID	Nombre de archivo
		archivos		del cliente
PEGASUS	Bkup	\\pegasus\e\$	1	\UNI_TEST\ SM01.DAT
PEGASUS	Bkup	\\pegasus\e\$	1	\UNI_TEST\ SM02.DAT

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: mostrar información detallada para un volumen de cinta

Consultar el contenido del volumen de cinta denominado WPD001. Mostrar solo los archivos de los que ha realizado una copia de seguridad el nodo MARK y los archivos que están almacenados en el volumen o enlazados a él. Mostrar solo los cuatro primeros archivos del volumen.

```
query content wpd001 node=mark count=4 type=backup followlinks=yes
format=detailed
```

```

        Nombre nodo: MARK
        Tipo: C.S.
        Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
        FSID: 1
        Nombre del archivo en el cliente: \UNI_TEST\ SM01.DAT
Nombre hexadecimal del archivo en el cliente:
        ¿Agregación?: 1/3
        Tamaño almacenado: 2.746
        Número de segmento:
        ¿Copia en caché?: No
        Enlazado: No
        Número de fragmento:

        Nombre nodo: MARK
        Tipo: C.S.
        Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
        FSID: 1
        Nombre del archivo en el cliente: \UNI_TEST\ SM02.DAT
Nombre hexadecimal del archivo en el cliente:
        ¿Agregación?: 2/3
        Tamaño almacenado: 2.746
        Número de segmento:
        ¿Copia en caché?: No
        Enlazado: No
        Número de fragmento: 2

        Nombre nodo: MARK
        Tipo: C.S.
        Nombre de espacio de archivos: \\mark\e$
Nombre espacio archivos hexadecimal:
        FSID: 1
        Nombre del archivo en el cliente: \UNI_TEST\ SM03.DAT
Nombre hexadecimal del archivo en el cliente:
        ¿Agregación?: 3/3
        Tamaño almacenado: 2.746
        Número de segmento:
        ¿Copia en caché?: No
        Enlazado: No
        Número de fragmento: 3
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

Node Name

El nodo al que pertenece el archivo.

Type

Tipo de archivo: copia archivada (Arch), copia de seguridad (Bkup) o bajo gestión de espacio (SpMg) mediante un cliente IBM Spectrum Protect for Space Management.

Filespace Name

El espacio de archivos al que pertenece el archivo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre espacio archivos hexadecimal

El espacio de archivos al que pertenece el archivo. Si el nombre del espacio de archivos está en Unicode, el nombre se visualiza en formato hexadecimal.

FSID

El identificador del espacio de archivos (FSID). El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

Nombre del archivo en el cliente

El nombre del archivo en el cliente.

Los nombres de espacios de archivos y nombres de archivo que pueden estar en una página de códigos o un entorno local diferente de los del servidor no se visualizan correctamente en el Centro de operaciones ni en la interfaz de línea de comandos de administración. Se efectúa una copia de seguridad de los propios datos que se pueden restaurar correctamente pero el nombre del espacio de archivos o del archivo puede visualizarse con una combinación de caracteres no válidos o espacios en blanco. El resultado de la conversión de caracteres que no soporta la página de códigos actual depende del sistema operativo. Los nombres que IBM Spectrum Protect puede convertir parcialmente pueden ir acompañados de signos de interrogación (??), espacios en blanco, caracteres que no se pueden imprimir o "...". Estos caracteres indican al administrador que existen archivos.

Nombre de cliente hexadecimal para archivo

El nombre del cliente del archivo que se visualiza en formato hexadecimal.

Aggregated?

Si el archivo es un archivo lógico que está almacenado como componente de una agregación de archivos. Si el archivo forma parte de una agregación de archivos, se visualizan la secuencia de este archivo en la agregación de archivos y el número total de archivos lógicos que hay en la agregación de archivos. El resultado del comando incluye todos los archivos lógicos que forman cualquier agregación de archivos que hay en el volumen, incluso aunque la agregación de archivos esté almacenada en varios volúmenes además de éste. La consulta no determina cuáles son los archivos lógicos que realmente están almacenados en el volumen cuya consulta se realiza.

Si el archivo no forma parte de un agregado, el campo muestra "no".

Tamaño almacenado

El tamaño del archivo físico, en bytes. Si el archivo es un archivo lógico que está almacenado como componente de una agregación de archivos, este valor indica el tamaño de toda la agregación de archivos.

Número de segmento

En volúmenes de agrupaciones de almacenamiento de acceso secuencial, especifica si el archivo físico (tanto si es un único archivo lógico como si es una agregación de archivos lógicos) se almacena en varios volúmenes. Por ejemplo, si el archivo lógico se almacena en una agregación de archivos que abarca dos volúmenes, el número de segmento indica 1/2 (la primera parte del archivo físico se almacena en el volumen) o 2/2 (la segunda parte del archivo físico se almacena en el volumen). Si el número de segmento es 1/1, el archivo físico se almacena entero en el volumen. Para los volúmenes de las agrupaciones de almacenamiento de acceso aleatorio, no se visualiza ningún valor.

¿Copia en caché?

Si el archivo físico es una copia en caché de un archivo migrado a la siguiente agrupación de almacenamiento. Si el archivo forma parte de una agregación de archivos, este valor pertenece a la agregación de archivos.

Enlazado

Indica si el archivo se almacena en el volumen o si se encuentra enlazado al volumen.

Número de fragmento




Especifica el número de fragmento. Si el número de fragmento está en blanco, es el primer fragmento o no es un fragmento.



## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY CONTENT

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY CONVERSION (Consultar estado de conversión de una agrupación de almacenamiento)

Utilice este mandato para visualizar información acerca de una operación de conversión. Puede convertir una agrupación de almacenamiento primario que utiliza una clase de dispositivo de tipo FILE o una biblioteca virtual de cintas (VTL) en una agrupación de almacenamiento de contenedor de directorios.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

### Sintaxis

```
>>-Query CONVERSION--+-+-----+----->
                        '-nombre_agrupación-'
.-Format----Standard----.
>--+-+-----+-----<<
  '-Format----+Standard-+-'
                        '-Detailed-'
```

### Parámetros

#### nombre\_agrupación

Especifica la agrupación de almacenamiento que se consulta. Este parámetro es opcional. Si no especifica un valor para este parámetro, la información se visualiza para todas las agrupaciones de almacenamiento.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

### Ejemplo: visualizar información de conversión para todas las agrupaciones de almacenamiento

Visualizar información de conversión para todas las agrupaciones de almacenamiento. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query conversion
```

Source Storage Pool	Target Storage Pool	Starting Amount	Total Converted	Last Converted
FILEPOOL	CTR	3 GB	3 GB	3 GB
FPOOL	CTR	333 MB	333 MB	267 MB

## Ejemplo: visualizar información detallada sobre la conversión de agrupación de almacenamiento

Visualizar información detallada sobre la conversión de agrupación de almacenamiento. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query conversion format=detailed
```

```
Agrupación de almacenamiento de origen: FILEPOOL
Agrupación de almacenamiento de destino: CTR
Número máximo de procesos: 4
Duración: 60 minutos
Cantidad inicial: 333 MB
Total convertido: 333 MB
Último convertido: 333 MB
Fecha/hora inicio: 03/24/2016 13:22:32
```

## Descripciones de los campos

**Agrupación de almacenamiento de origen**

El nombre de la agrupación de almacenamiento que se está convirtiendo.

**Agrupación de almacenamiento de destino**

El nombre de la agrupación de almacenamiento de destino donde se almacenarán los datos convertidos.

**Número máximo de procesos**

Especifica el número máximo de procesos de conversión.

**Duración**

Especifica el tiempo, en minutos, para la conversión.

**Cantidad inicial**

La cantidad inicial de datos a convertir, en megabytes (MB), gigabytes (GB) o terabytes (TB).

**Total convertido**

La cantidad total de datos convertidos, en megabytes (MB), gigabytes (GB) o terabytes (TB).

**Último convertido**

La cantidad de datos, en megabytes (MB), gigabytes (GB) o terabytes (TB), convertidos durante este proceso de conversión.

**Fecha/hora inicio**

La fecha y la hora en que se emitió el mandato CONVERT STGPOOL por primera vez para la agrupación de almacenamiento.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY CONVERSION

Comando	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.

## QUERY COPYGROUP (Consultar grupos de copia)

Utilice este mandato para visualizar información sobre uno o varios grupos de copia.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis



ENGPOLDOM	STANDARD	MCENG	STANDARD	5	4	90	600
ENGPOLDOM	STANDARD	STANDARD	STANDARD	2	1	30	60
ENGPOLDOM	TEST	STANDARD	STANDARD	2	1	30	60

## Ejemplo: mostrar información detallada acerca de un grupo de copias de seguridad

Mostrar información completa sobre grupo de copia de seguridad asignado a la clase de gestión ACTIVEFILES del juego de políticas VACATION, del dominio de políticas EMPLOYEE\_RECORDS. Emita el mandato:

```
query copygroup employee_records vacation
activefiles format=detailed
```

## Ejemplo: mostrar información acerca del grupo de copias de seguridad asignado en la clase de gestión y juego de políticas STANDARD

Desde un servidor gestionado, visualizar información completa sobre el grupo de copia de seguridad asignado a la clase de gestión STANDARD del juego de políticas STANDARD del dominio de políticas ADMIN\_RECORDS. Emita el comando:

```
query copygroup admin_records
standard standard format=detailed

Nombre dominio políticas: ADMIN_RECORDS
Nombre juego políticas: STANDARD
Nombre clase gestión: STANDARD
Nombre grupo copia: STANDARD
Tipo grupo de copia: Copia seguridad
Versiones si datos existen: 2
Versiones si datos suprimidos: 1
Retener versión adicional: 30
Retener única versión: 60
    Modalidad copia: Modificado
Serialización copia: Estático compartido
Frecuencia copias: 0
Destino copias: BACKUPOOL
Destino de Tabla de contenido (TOC):
    Última actualización por (administrador): $$CONFIG_MANAGER$$
    Fecha/Hora última actualización: 2002.10.02 17.51.49
Perfil de gestión: ADMIN_INFO
Cambios pendientes: Si
```

## Ejemplo: mostrar información acerca del grupo de copias archivadas

Desde un servidor gestionado, visualizar información completa sobre el grupo de copia archivada STANDARD que está asignado a la clase de gestión MCLASS1 del juego de políticas SUMMER del dominio de políticas PROG1. Emita el comando:

```
query copygroup progl summer mclass1
type=archive format=detailed

Nombre dominio políticas: PROG1_RECORDS
Nombre juego políticas: SUMMER
Nombre clase gestión: MCLASS1
Nombre grupo copia: STANDARD
Tipo grupo copia: Archivado
Retener versión: 730
Iniciación de retención: Creación
Retención mínima:
Serialización copia: Estático compartido
Frecuencia copia: Cmd
    Modalidad copia: Absoluto
Destino copia: ARCHPOOL
    Última actualización por (administrador): $$CONFIG_MANAGER$$
    Fecha/Hora última actualización: 2002.10.02 17.42.49
Perfil de gestión: ADMIN_INFO
```

## Ejemplo: mostrar información acerca del grupo de copias para una copia de seguridad NAS

Consultar al grupo de copias acerca de la copia de seguridad NAS. Emita el comando:

```
query copygroup nasdomain
type=backup

Nombre dominio políticas: NASDOMAIN
Nombre juego políticas: ACTIVE
```

```

Nombre clase gestión: STANDARD
Nombre grupo copia: STANDARD
Tipo grupo de copia: Copia seguridad
Versiones si datos existen: 2
Versiones si datos suprimidos: 1
Retener versión adicional: 30
Retener única versión: 60
  Modalidad copia: Modificado
Serialización copia: Estático compartido
Frecuencia copias: 0
Destino copias: NASPOOL
Destino de tabla de contenido (TOC): BACKUPPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/Hora última actualización: 10/02/2002 12:16:52
Perfil de gestión:
Cambios pendientes: Sí

```

## Descripciones de los campos

---




- Nombre de dominio de políticas  
El nombre del dominio de políticas.
- Nombre de juego de políticas  
El nombre del juego de políticas.
- Nombre clase gestión  
El nombre de la clase de gestión.
- Nombre grupo copia  
El nombre del grupo de copia. Este nombre siempre es STANDARD.
- Tipo grupo copia  
El tipo del grupo de copia.
- Versiones si datos existen  
Número máximo de versiones de copia de seguridad que han de retenerse para los archivos que actualmente se encuentran en el sistema de archivos del cliente.
- Versiones si datos suprimidos  
Número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad utilizando IBM Spectrum Protect.
- Retener versión adicional  
Número de días que ha de retenerse una versión de copia de seguridad cuando la versión pasa a ser inactiva.
- Retener única versión  
Número de días que ha de retenerse la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente.
- Serialización copias  
Si puede utilizarse un archivo durante una operación de archivado.
- Frecuencia copia  
La frecuencia de copias del grupo de copia. En los grupos de copia archivada, este valor siempre es CMD.
- Modalidad copia  
Especifica que los archivos del grupo de copia se archivan independientemente de si se han modificado. En los grupos de copia archivada, este valor siempre es ABSOLUTE.
- Destino de copia  
El nombre de la agrupación de almacenamiento donde el servidor almacena inicialmente los archivos asociados a este grupo de copia archivada.
- Destino de tabla de contenido (TOC)  
Nombre de la agrupación de almacenamiento primaria en la que inicialmente se almacenan las TOC para las operaciones de copia de seguridad de imagen en las que se solicita la generación de la TOC.
- Última actualización por (administrador)  
El nombre del administrador o del servidor que ha actualizado por última vez el grupo de copia. Si este campo contiene \$\$CONFIG\_MANAGER\$\$, el grupo de copias está asociado a un dominio que gestiona el gestor de configuración.
- Fecha/hora última actualización  
La fecha y la hora en que se ha definido o actualizado por última vez el grupo de copia.
- Perfil de gestión  
El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este grupo de copias de políticas.
- Cambios pendientes  
Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

## Comandos relacionados

---

Tabla 1. Comandos relacionados con QUERY COPYGROUP

Comando	Descripción
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY DAMAGED (Consultar los datos dañados de una agrupación de almacenamiento de contenedores de directorios o de contenedores en la nube)

Utilice este mandato para visualizar información sobre las extensiones de datos dañadas de una agrupación de almacenamiento de contenedores de directorios o de nubes. Utilice este comando junto con el comando AUDIT CONTAINER para determinar un método de recuperación para los datos dañados.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query DAMaged--nombre_agrupación----->
  .-Type----Status-----
>-----+-----<
'-Type----+-INventory-----+'
      +-Node--| A |-----+
      '-CONTAINER--| A |-'
```

A (filtro adicional por nombre de nodo)

```
|-----+-----|
  '-Nodename----nombre_nodo-'
```

### Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio o de nube.

Type

Especifica el tipo de información que desea visualizar. Este parámetro es opcional. Especifique uno de los siguientes valores:

Status

Especifica que se visualiza información sobre extensiones de datos dañadas. Para las agrupaciones de almacenamiento de nube, también se visualizan las extensiones huérfanas. Este es el valor predeterminado.

Nodo

Especifica que se visualiza información sobre el número de archivos dañados por nodo.

INventory

Especifica que se visualiza información de inventario para cada archivo dañado.

CONTAINER

Especifica que se visualizan los contenedores que contienen extensiones de datos dañadas o extensiones huérfanas en la nube. Para las agrupaciones de almacenamiento de contenedores de directorio, también se visualizan los directorios de agrupación de almacenamiento.

Nodename

Especifica que se visualiza la información del archivo dañado para un único nodo.

Restricción: No puede especificar este parámetro si se ha especificado el parámetro TYPE=CONTAINER o TYPE=STATUS.

### Ejemplo: Visualizar información de estado sobre extensiones de datos dañadas o huérfanas

Visualizar información sobre el estado de las extensiones de datos dañadas que están almacenadas en un contenedor.

```
query damaged pool1 type=status
```

Agrup. de almac. Name	Datos de no dedup. Extent Count	Datos de dedup. Extent Count	Huérfano de nube Extent Count
POOL1	58	145	

Para las agrupaciones de almacenamiento en la nube, también se visualiza el número de extensiones huérfanas.

Agrup. de almac. almacenamiento	Datos de no dedup. sin duplic. eliminados	Datos de dedup. con duplic. eliminados	Huérfano de nube de nube huérfanas
POOL1	65	238	18

## Ejemplo: visualizar información sobre un archivo dañado para un tipo de nodo

Visualice información sobre los archivos dañados que están almacenados en un nodo.

```
query damaged pool1 type=node
```

Node Name	Number of Damaged Files
POOL1	37

## Ejemplo: visualizar información sobre un archivo dañado para un tipo de inventario

Visualice la información acerca de los archivos dañados almacenados en un inventario.

```
query damaged pool2 type=inventory
```

```
Nombre del archivo en el cliente: /data/files/10.out
Tipo: C.S.
Nombre nodo: NODE1
Nombre de espacio de archivos: /data/space
Estado: Disponible
Hora de inserción: 01/19/2015 16:01:35
ID de objeto: 2073
```

## Ejemplo: visualizar información sobre un archivo dañado para un tipo de contenedor

Visualice información sobre los archivos dañados que están almacenados en un contenedor.

```
query damaged pool3 type=container
```

```
ID de directorio: 1
Directorio: /abc/space/container1
Contenedor: /abc/space/container1/00/000000000000022.dcf
Estado: No disponible
```

Para los contenedores en la nube, sólo se visualiza el nombre del contenedor.

```
ID de directorio:
Directorio:
Contenedor: ibmsp.12520ae05b4011e613320a0027000000/
001-10006a3278bc34f0e4118a850090fa3dcb48/
000000000000001.ncf
Estado:
```

Para el almacenamiento local, se muestra la información siguiente acerca de un contenedor dañado.

```
ID de directorio: 1
Directorio: localdirectory
Contenedor: localdirectory/00/00000000000011.ncf
Estado: No disponible
```

## Descripciones de los campos

Nombre del archivo en el cliente (solo TYPE=INVENTORY)

El nombre del archivo.

Recuento de extensiones huérfanas en la nube (solo TYPE=STATUS)

El número de extensiones huérfanas en una agrupación de almacenamiento en la nube. Las extensiones son consideradas huérfanas si no tienen una entrada de base de datos correspondiente.

Contenedor (solo TYPE=CONTAINER)

El nombre del contenedor.

Recuento de extensiones con duplicados eliminados (solo TYPE=STATUS)

El número de extensiones dañadas en la agrupación de almacenamiento para datos duplicados eliminados.

Directorio (solo TYPE=CONTAINER)

El nombre del directorio de la agrupación de almacenamiento.

ID de directorio (solo TYPE=CONTAINER)

El número de identificación del directorio de agrupación de almacenamiento.

Nombre del espacio de archivos (solo TYPE=INVENTORY)

El nombre del espacio de archivos.

Hora de la inserción (solo TYPE=INVENTORY)

La fecha y la hora en las que el objeto se ha almacenado en el servidor.

Nombre de nodo (solo TYPE=INVENTORY o TYPE=NODE)

El nombre del nodo.

Recuento de extensiones sin duplicados eliminados (solo TYPE=STATUS)

El número de extensiones dañadas en la agrupación de almacenamiento para datos que no son duplicados eliminados, como metadatos y datos cifrados de cliente.

Número de archivos dañados (solo TYPE=NODE)

El número de archivos dañados por nodo.

ID de objeto (solo TYPE=INVENTORY)

El número de identificación del objeto.

Estado (solo TYPE=INVENTORY o TYPE=CONTAINER)

El estado de los datos en el inventario o el contenedor, en función del tipo de datos que esté consultando. El campo puede contener uno de los siguientes valores:

Activo

La versión del archivo en el inventario está activa. Sólo puede haber una versión activa del archivo en el inventario.

Inactivo

La versión del archivo en el inventario está inactiva. Puede haber varias versiones inactivas del archivo en el inventario.

Disponible

El estado del contenedor es disponible.

No disponible

El estado del contenedor es no disponible. Por ejemplo, un contenedor puede no estar disponible si la cabecera está dañada o si el contenedor no puede abrirse.

Sólo lectura

El contenedor está en estado de solo lectura. Los datos del contenedor se pueden leer pero no se pueden grabar en el contenedor.

Pendiente

El contenedor está pendiente de supresión. El contenido del contenedor se ha trasladado a un contenedor diferente y el contenedor está listo para ser suprimido.

Tipo (solo TYPE=INVENTORY)

El tipo de datos del archivo.

Tabla 1. Comandos relacionados con QUERY DAMAGED

Comando	Descripción
AUDIT CONTAINER	Auditar una agrupación de almacenamiento de contenedores de directorio.
QUERY CLEANUP	Consultar el estado de limpieza de una agrupación de almacenamiento de origen.
QUERY CONTAINER	Visualiza información sobre un contenedor.
REMOVE DAMAGED	Elimina datos dañados de una agrupación de almacenamiento de origen.



# QUERY DATAMOVER (visualizar definiciones de un transportador de datos)

Utilice este comando para visualizar definiciones de transportadores de datos.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```

>>-Query DATAMover-+-----+----->
                        .-*-----+-----+
                        '-nombre_transportador_datos-'

.-Format----Standard----.
>+-----+-----+-----+----->
'-Format----+Standard-+-'
      '-Detailed-'

.-Type----=*-----+-----+
>+-----+-----+-----+-----><
|                                     (1) (2) |
'-Type----+NAS-----+-----+'
      +-NASCLUSTER-+
      '-NASVSERVER-'

```

Notas:

1. Debe especificar el parámetro TYPE si FORMAT=DETAILED.
2. Puede especificar TYPE=NASCLUSTER y TYPE=NASVSERVER solo en un sistema operativo AIX, Linux o Windows.

## Parámetros

nombre\_transportador\_datos

Especifica el nombre del transportador de datos que se visualizará. Puede especificar varios nombres con un carácter comodín. De forma predeterminada, se visualizarán todos los transportadores de datos.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD.

Standard

Especifica que se visualizará la información de nombre y dirección.

Detailed

Especifica que se visualizará toda la información.

Type

Especifica el tipo de transportador de datos que se visualizará. Si especifica FORMAT=DETAILED, debe especificar un valor para el parámetro TYPE.




NAS

Especifica un servidor de archivos de NAS.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NASCLUSTER

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsEspecifica un servidor de archivos NAS en clúster.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NASVSERVER

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsEspecifica un dispositivo de almacenamiento virtual dentro de un clúster.

## Ejemplo: visualizar información acerca de todos los transportadores de datos

Visualizar los transportadores de datos en el servidor. Emita el comando:

```
query datamover
```

```
Nombre de
transportador de datos  Tipo de transportador de datos  En línea
-----
```

NASMOVER1	NAS	Sí
NASMOVER2	NAS	No

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información acerca de un transportador de datos

Visualice información parcial sobre el transportador de datos DATAMOVER6. Emita el comando:

```
query datamover datamover6 type=nas
```

Nombre origen	Tipo	Activado
-----	-----	-----
DATAMOVER6	NAS	Sí

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información detallada acerca de un transportador de datos

Visualice información detallada sobre el transportador de datos DATAMOVER6. El parámetro TYPE es necesario si FORMAT = DETAILED. Emita el comando:




```
query datamover datamover6 format=detailed type=nas
```

```

Nombre de transportador de datos: DataMover6
Tipo de transportador de datos:   NAS
Dirección IP: 198.51.100.0
Número de puerto TCP/IP: 10000
Nombre de usuario: NDMPadmin
Formato datos agrupación almacenamiento: NDMPDUMP
Activado: Yes
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 05/23/2015 09:26:33

```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Ejemplo: visualizar información detallada acerca de un transportador de datos NAS en clúster

Visualice información detallada acerca de un transportador de datos NAS en clúster de nombre CLUSTERA Emita el comando siguiente:

```
query datamover clustera format=detailed type=nascluster
```

```

Nombre de transportador de datos: CLUSTERA
Tipo de transportador de datos:  NASCLUSTER
Dirección IP: 192.0.2.255
Número de puerto TCP/IP: 10000
Nombre de usuario: ndmp
Formato de datos de agrupación de almacenamiento: NETAPPDUMP
Activado: Yes
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 04/28/2015 09:26:33

```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

Nombre de transportador de datos

Especifica el nombre del transportador de datos.

Tipo de transportador de datos

Especifica el tipo de transportador de datos.

Dirección IP

Especifica la dirección IP del transportador de datos.

Número de puerto TCP/IP

Especifica el número de puerto TCP del transportador de datos.

Nombre usuario

Especifica el ID de usuario que utiliza el servidor para obtener acceso al transportador de datos.

Formato de datos de agrupación de almacenamiento

Especifica el formato de datos utilizado por el transportador de datos.

Activado

Especifica si el transportador de datos está en línea y disponible para utilizarlo.

Última actualización por (administrador)

Especifica el ID del administrador que ha realizado la última actualización.

Fecha/hora última actualización

Especifica la fecha y hora de la última actualización.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DATAMOVER

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DELETE DATAMOVER	Suprimir un transportador de datos.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

## QUERY DB (Visualizar información de base de datos)

Utilice este comando para visualizar información sobre la base de datos.

### Clase de privilegio

Cualquier administrador puede emitir este mandato.

### Sintaxis

```
.-Format-----Standard-----.  
>>-Query DB-----+----->>  
'-Format-----+Standard-+-'  
'-Detailed-'
```

### Parámetros

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

### Ejemplo: visualizar estadísticas de resumen acerca de la base de datos

Visualiza información de estadísticas acerca de la base de datos. Emita el comando:

```
query db
```

```
Base datos  Total pág.  Pág. utilizables  Pág. utiliz.  Pág. libres  
-----  
TSMDB1      32.776      32.504      24.220      8.284
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

### Ejemplo: visualizar información detallada de la base de datos

Visualizar información estadística detallada acerca de la base de datos. Emita el comando:

```
query db format=detailed
```

```
Nombre de la base de datos: TSM_DB2  
Espacio total del sistema de archivos (MB): 1.748.800  
Espacio utilizado del sistema de archivos (MB): 2,304,355  
Espacio utilizado por la base de datos (MB): 448  
Espacio libre disponible (MB): 235.609
```

Páginas en total: 32.776  
Páginas utilizables: 32.504  
Páginas utilizadas: 24.220  
Páginas libres: 8.284  
Proporción aciertos agrupación búferes: 99,3  
Total peticiones búferes: 204.121  
Clasificar desbordamientos: 0  
Proporción aciertos caché paquete: 89,8  
Última reorganización base datos: 05/25/2009 16:44:06  
Nombre completo clase dispositivo: FILE  
Número de corrientes de copia de seguridad de base de datos: 4  
Incrementales desde última completa: 0  
Fecha/hora última copia seguridad completa: 05/18/2009 22:55:19  
Comprimir copias de seguridad de base de datos: Si  
Proteger clave de cifrado maestra: No



Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.



## Descripciones de los campos


---


### Nombre de la base de datos

Nombre de la base de datos que se ha definido y configurado para que la utilice el servidor IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux Espacio total del sistema de archivos (MB)

 Sistemas operativos AIX  Sistemas operativos Linux El espacio total, en megabytes, del sistema de archivos en el que se encuentra la base de datos.

 Sistemas operativos Windows Espacio total del sistema de archivos (MB)

 Sistemas operativos Windows El espacio total, en megabytes, de las unidades en las que se encuentra la base de datos.

### Espacio utilizado en el sistema de archivos (MB)

Cantidad de espacio de base de datos, en megabytes, que se utiliza.

### Espacio utilizado por la base de datos (MB)

Especifica el tamaño de la base de datos en megabytes. El valor no incluye ningún espacio de tabla temporal. El tamaño de la base de datos se calcula a partir de la cantidad de espacio utilizado en el sistema de archivos que contiene la base de datos.

### Espacio libre disponible (MB)

Cantidad de espacio de base de datos, en megabytes, que no se utiliza.

### Páginas en total

El número total de páginas en el espacio de tabla.

### Páginas utilizables

El número de páginas utilizables en el espacio de tabla.

### Páginas utilizadas

El número de páginas utilizadas en el espacio de tabla.

### Páginas libres

El número total de páginas libres en todos los espacios de tabla. La base de datos de IBM Spectrum Protect tiene un máximo de 10 espacios de tabla.

### Proporción aciertos agrupación búferes

Porcentaje total de proporción de aciertos.

### Total peticiones búferes

Número total de lecturas lógicas de datos de agrupación de búferes y de lecturas lógicas de índice desde la última vez que se inició la base de datos o desde que se restableció el supervisor de base de datos.

### Clasificar desbordamientos

Número total de clasificaciones que se han quedado sin almacenamiento dinámico de clasificación y que pueden necesitar espacio de disco para almacenamiento temporal.

### Proporción de aciertos de caché de paquete

Porcentaje que indica la capacidad de ayuda de la caché de paquete para evitar la recarga de paquetes y secciones para SQL estático desde los catálogos del sistema. También indica la capacidad de ayuda de la caché de paquete para evitar la recompilación de las sentencias SQL dinámicas. Una proporción alta indica el éxito en evitar estas actividades.

### Última reorganización base datos

Última vez que el gestor de bases de datos ha completado una actividad de reorganización automática.

### Nombre completo clase dispositivo

Nombre de la clase de dispositivo que se utiliza para las copias de seguridad completas de la base de datos.

### Número de corrientes de copia de seguridad de base de datos

El número de corrientes de movimiento de datos simultáneas que se han utilizado durante la copia de seguridad de la base de datos.

### Incrementales desde última completa

Número de copias de seguridad incrementales que se han completado desde la última copia de seguridad completa.

### Fecha/hora última copia seguridad completa

La fecha y hora de la última copia de seguridad completa.

### Comprimir copias de seguridad de base de datos

Especifica si las copias de seguridad de base de datos se comprimen.  
 Proteger clave de cifrado maestra  
 Especifica si las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DB

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

## QUERY DBSPACE (Visualizar espacio de almacenamiento de base de datos)

Utilice este mandato para mostrar la información sobre los directorios que utiliza la base de datos para almacenar los datos.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-QUERY DBSpace-----<<
```

### Parámetros

Ninguno.

### Ejemplo: visualizar información de espacio de almacenamiento de base de datos

Visualizar información acerca del espacio de almacenamiento de la base de datos. Emita el comando:

```
query dbspace
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ubicación	Espacio total del sistema de archivos (MB)	Espacio utilizado en el sistema de archivos (MB)	Espacio libre disponible (MB)
/tsmdb001	1.748.800	1.513.191,125	117.804,422
/tsmdb002	1.748.800	1.513.191,125	117.804,422

 Sistemas operativos Windows


Ubicación	Espacio total de sistema de archivos (MB)	Espacio utilizado sistema de archivos (MB)	Espacio libre disponible (MB)
d:\tsm\db001	1.748.800	1.513.191,125	117.804,422
e:\tsm\db002	1.748.800	1.513.191,125	117.804,422


Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.


### Descripciones de los campos


Ubicación

Especifica las ubicaciones de los directorios de base de datos.

 Sistemas operativos AIX Espacio total del sistema de archivos (MB)



 Sistemas operativos AIX La cantidad total de espacio, en megabytes, del sistema de archivos en el cual se encuentra la base de datos.


 Sistemas operativos Windows Espacio total del sistema de archivos (MB)

 Sistemas operativos Windows La cantidad total de espacio, en megabytes, de las unidades en las cuales se encuentra la base de datos.

Espacio utilizado en sistema de archivos (MB)


La cantidad de espacio de almacenamiento, en megabytes, que se utiliza.


 Sistemas operativos AIX  Sistemas operativos Linux Cuando ejecuta el mandato QUERY DBSPACE, el valor en la salida podría ser mayor que el valor que se obtiene al ejecutar el mandato df system. La salida para el mandato df system no incluye la cantidad de espacio reservada para el usuario root.

 Sistemas operativos Linux Si ejecuta el mandato df system, el porcentaje predeterminado de espacio reservado para el usuario root es 5%. Puede cambiar este valor predeterminado.

Espacio libre disponible (MB)

Cantidad de espacio, en megabytes, que no se utiliza.




 Sistemas operativos Windows Espacio libre disponible (MB)

 Sistemas operativos Windows Cantidad de espacio que queda en la unidad en la que se encuentra el directorio.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DBSPACE

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
EXTEND DBSPACE	Agrega directorios para incrementar el espacio que utiliza la base de datos.
QUERY DB	Visualiza información de asignación acerca de la base de datos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY DEDUPSTATS (Consultar las estadísticas de eliminación de duplicados de datos)

Utilice este mandato para visualizar información sobre estadísticas de deduplicación de datos para una agrupación de almacenamiento de contenedores de directorio o una agrupación de almacenamiento de nube.

Debe emitir el mandato GENERATE DEDUPSTATS para poder emitir el mandato QUERY DEDUPSTATS.

## Clase de privilegio

Cualquier administrador puede emitir este mandato.

## Sintaxis

```
>>-Query DEDUPStats--+-+-----+-----+-----+----->
                        '-nombre_agrupación-' '-nombre_nodo-'

.-*-----
>-+-----+-----+-----+----->
| .-,------. |
| V              | |
+---nombre_espacio_de_archivos---+
| .-,------. |
| V              | |
'-----FSID---+-----'

.-Format-----Standard-----
>-+-----+-----+-----+----->
'-Format-----+Standard-+-'
      '-Detailed-'

.-CODEType-----BOTH-----
>-+-----+-----+-----+----->
```



Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes con soporte para los espacios de archivos que están en formato Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que utilizan sistemas operativos Windows, NetWare o Macintosh OS X. Utilice este parámetro sólo cuando especifique un nombre de nodo y un nombre de espacio de archivos o un FSID. Restricción: Cuando especifica este parámetro, el nombre del espacio de archivos no puede contener un comodín.

Especifique uno de los siguientes valores:

**SERVER**

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos. Este es el valor predeterminado.

**UNICODE**

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

**FSID**

El servidor interpreta los nombres de espacios de archivos como sus FSID.

**BEGINDate**

Especifica la fecha de inicio para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora es a las 12:00 de la noche de la fecha que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha específica.	15/09/2015
TODAY	La fecha actual.	TODAY
TODAY -días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los registros que estaban activos el día 10 del mes actual.

**BEGINTime**

Especifica la hora de inicio para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha es la fecha actual a la hora que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	10:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados.	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados.	NOW-02:00 o -02:00.

**ENDDate**

Especifica la fecha de finalización para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha. Si especifica una fecha de finalización sin una hora final, la hora es a las 11:59:59 de la noche de la fecha de finalización especificada.



Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.  
Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY -días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los registros que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los registros que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora de finalización del rango para consultar las estadísticas de eliminación de duplicados de datos. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha. Si especifica una hora final sin una fecha final, la fecha es la fecha actual a la hora que especifique.

Restricción: Sólo puede especificar este parámetro cuando especifique el parámetro ALLSTATS=YES.

Especifique uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora específica.	10:30:08
NOW	La hora actual.	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha de finalización especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha de finalización especificada	NOW-02:00 o -02:00.

#### ALLStats

Especifica si se deben mostrar todas las estadísticas de eliminación de duplicados de datos o sólo las estadísticas de eliminación de duplicados de datos generadas más recientemente. Este parámetro es opcional. Especifique uno de los siguientes valores:

No

Muestra sólo las estadísticas de eliminación de duplicados de datos que se han generado más recientemente para cada nodo y espacio de archivos.

Yes

Muestra todas las estadísticas de eliminación de duplicados de datos.

### Ejemplo: ver estadísticas de eliminación de duplicados de datos en formato estándar

Vea las estadísticas de eliminación de duplicados de datos para una agrupación de almacenamiento denominada POOL1. Las estadísticas de eliminación de duplicados de datos son para el nodo NODE1 y se muestran las estadísticas del 8 de mayo de 2015. Consulte Descripciones de los campos para ver una descripción de los campos.

```
query dedupstats pool1 node1 begindate=05/08/2015
```

```

Date/Time: 05/05/2015 15:15:23
Nombre agrupación almacenamiento: POOL1
Nombre nodo: NODE1
Nombre espacio archivos: \\fs1\al
FSID: 41
Tipo: C.S.
Porcentaje total de ahorro: 86,62
Total de datos protegidos (MB): 311

```

### Ejemplo: ver estadísticas de eliminación de duplicados de datos detalladas

Vea información detallada para la eliminación de duplicados de datos de una agrupación de almacenamiento denominada POOL1.

```
query dedupstats pool1 format=detailed
```

```
          Date/Time: 05/05/2015 15:15:23
Nombre agrupación almacenamiento: POOL1
Nombre nodo: NODE1
Nombre espacio archivos: \\fs1\al
          FSID: 41
          Tipo: C.S.
Total de datos protegidos (MB): 47.646
Espacio total utilizado (MB): 10.139
Espacio total ahorrado (MB): 37.507
Porcentaje total de ahorro: 78,72
Ahorro de deduplicación: 21.278.892.501
Porcentaje de deduplicación: 42,59
Recuento de extensiones sin duplicados eliminados: 1.658
Espacio de extensión no deduplicado utilizado: 732.626
Recuento de extensiones exclusivas: 189.791
Espacio de extensión exclusivo utilizado: 23.385.014.635
Recuento de extensiones compartidas: 178.712
Datos de extensiones compartidas protegidos: 26.575.010.669
Espacio de extensiones compartidas utilizado: 5.267.815.421
Ahorro de compresión: 5.267.815.421
Porcentaje de compresión: 62,93
Recuento de extensiones comprimidas: 352.498
Recuento de extensiones no comprimidas: 17.663
Espacio de extensión cifrada utilizado: 52.901.672
Encryption Percentage: 100.00
Encrypted Extent Count: 188
Unencrypted Extent Count: 0
```

## Descripciones de los campos

---

### Fecha/hora

Muestra la fecha y la hora en las que se han generado las estadísticas de eliminación de duplicados de datos.

### Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

### Nombre del nodo

El nombre del nodo de cliente cuyos datos se incluyen en las estadísticas de eliminación de duplicados de datos.

### Nombre de espacio de archivos

El nombre del espacio de archivos.

### FSID

El nombre del identificador del espacio de archivos.

### Tipo

El tipo de datos. Son posibles los siguientes valores:

#### Arch

Datos que se han archivado.

#### C.S.

Datos de los que se ha realizado una copia de seguridad.

#### G.E.

Datos que se han migrado desde un cliente IBM Spectrum Protect for Space Management.

### Total de datos protegidos (MB)

La cantidad lógica de datos, en megabytes, protegidos en la agrupación de almacenamiento antes de la deduplicación y la compresión de datos. Este valor representa la suma de los valores de Espacio total utilizado (MB) y Espacio total ahorrado (MB).

### Espacio total utilizado (MB)

La cantidad total de espacio utilizado en la agrupación de almacenamiento, en megabytes. Este valor es la cantidad física de datos de los que realizan copias de seguridad tras la deduplicación de datos y la compresión.

### Espacio total ahorrado (MB)

La cantidad total de espacio, en megabytes, de datos que se han eliminado de la agrupación de almacenamiento debido a la deduplicación de datos y la compresión. Este valor representa la suma de los valores de Ahorro de deduplicación y Ahorro de compresión.

### Porcentaje total de ahorro

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la compresión y la deduplicación de datos.

### Ahorro de deduplicación

La cantidad de espacio utilizado que se ha ahorrado en la agrupación de almacenamiento debido a la deduplicación de datos.

Porcentaje de eliminación de duplicados

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la deduplicación de datos.

Recuento de extensiones no deduplicadas

El número de extensiones de datos donde no se han eliminado los duplicados en la agrupación de almacenamiento.

Espacio de extensión no deduplicado utilizado

La cantidad de espacio utilizado por extensiones de datos que no se han deduplicado en la agrupación de almacenamiento. Este valor se aplica a los contenedores con un tipo de archivo .ncf que no tienen datos duplicados eliminados.

Consejo: Las extensiones de datos cuyos duplicados no se han eliminado constan de los siguientes tipos de archivos o datos:

- Metadatos de archivo.
- Archivos de menos de 2 KB.
- Archivos que utilizan el cifrado del cliente.

Recuento de extensiones exclusivas

El número de extensiones de datos que no están compartidas por un nodo.

Espacio de extensión exclusiva utilizado

La cantidad de espacio en la agrupación de almacenamiento que no comparte un nodo. Este valor se aplica a los contenedores con un tipo de archivo .dcf que no tienen datos duplicados eliminados.

Recuento de extensiones compartidas

El número de extensiones de datos que se utilizan varias veces en el mismo nodo o en nodos distintos debido a la deduplicación de datos.

Datos de extensiones compartidas protegidas

La cantidad de espacio de la agrupación de almacenamiento que está protegido por extensiones de datos compartidas antes de la deduplicación de datos.

Espacio de extensión compartida utilizado

La cantidad de espacio de la agrupación de almacenamiento que utilizan las extensiones de datos compartidas tras la deduplicación de datos.

Ahorro de compresión

Cantidad de espacio utilizado que se ha ahorrado en la agrupación de almacenamiento debido a la compresión tras la deduplicación de datos.

Porcentaje de compresión

El porcentaje de datos que se han eliminado de la agrupación de almacenamiento debido a la compresión.

Recuento de extensiones comprimidas

El número de extensiones de datos que se han comprimido.

Recuento de extensiones descomprimidas

El número de extensiones de datos que se han descomprimido.

Espacio de extensión cifrada utilizado

La cantidad de espacio en la agrupación de almacenamiento utilizado por extensiones de datos cifradas.

Porcentaje de cifrado

Porcentaje de datos cifrados en la agrupación de almacenamiento.

Recuento de extensiones cifradas

El número de extensiones de datos que se han cifrado.

Recuento de extensiones sin cifrar

El número de extensiones de datos que no se han cifrado.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DEDUPSTATS

Comando	Descripción
DELETE DEDUPSTATS	Suprime las estadísticas de eliminación de duplicados de datos.
GENERATE DEDUPSTATS	Genera las estadísticas de eliminación de duplicados de datos.

## QUERY DEVCLASS (visualizar información en una o más clases de dispositivo)

Utilice este comando para visualizar información sobre una o varias clases de dispositivo.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

```

.*-----
>>-Query DEVclass----->
      '-nombre_clase_dispositivo-'

.-Format----Standard----.
>-----><
      '-Format----Standard--'
          '-Detailed-'

```

## Parámetros

### nombre\_clase\_dispositivo

Especifica el nombre de la clase de dispositivo que se ha de consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Se visualizarán todas las clases de dispositivos coincidentes. Si no especifica un valor para este parámetro, se visualizarán todas las clases de dispositivos.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial para la clase de dispositivo especificada.


#### Detailed

Especifica que se visualizará información completa para la clase de dispositivo especificada.

## Ejemplo: obtener una lista de todas las clases de dispositivos

Visualizar información sobre todas las clases de dispositivos.

```
query devclass
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

Nombre clase disp.	Estrategia acceso disp.	Número agrupac. almacen.	Tipo dispos.	Formato	Capacidad est/máx (MB)	Límite montajes
8MMTAPE	Secuencial	1	8MM	DRIVE	6.144,0	2
DISK	Aleatorio	4				
PLAINFILES	Secuencial	1		FILE	50,0	1
8MMSP2	Secuencial	2	8MM	DRIVE	44,4	DRIVES

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información detallada para una clase de dispositivo FILE específica

Visualizar información completa sobre la clase de dispositivo PLAINFILES.

```
query devclass plainfiles format=detailed
```

```

Nombre clase dispositivo: PLAINFILES
Estrategia acceso dispositivo: Secuencial
Número agrupaciones almacenamiento: 1
Tipo dispositivo: FILE
Formato:
Capacidad est/máx (MB): 50.0
Límite montajes: 1
Espera montaje (min):
Retención montaje (min):
Prefijo etiqueta:

```

 Sistemas operativos Windows Letra unidad:

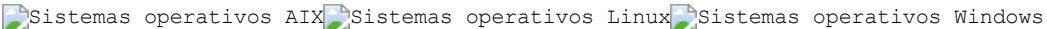
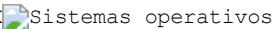
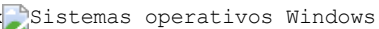
Biblioteca:


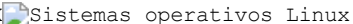
Directorio:

Nombre servidor:

Período de reintento:

Intervalo entre reintentos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows  
Compartido:

 Sistemas operativos AIX  Sistemas operativos Linux Asignación primaria (MB):

Asignación secundaria (MB):  
Compresión:  
Retención:  
Protección:  
Fecha caducidad:  
Unidad:  
Protección de bloques lógicos:  
Última actualización por (administrador): ADMIN  
Fecha/hora última actualización: 05/31/2000 13:15:36

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información detallada para una clase de dispositivo 3592 específica

---

Visualizar detalles completos sobre la clase de dispositivo 3592.

```
query devclass 3592 format=detailed
```

```
Nombre clase dispositivo: 3592
Estrategia acceso dispositivo: Secuencial
Número agrupaciones almacenamiento: 1
Tipo dispositivo: 3592
Formato: 3592
Capacidad est/máx (MB):
Límite montaje: DRIVES
Espera montaje (min): 60
Espera montaje (min): 60
Prefijo etiqueta: ADSM
Letra unidad:
Biblioteca: MANLIB
Directorio:
Nombre servidor:
Período de reintento:
Intervalo entre reintentos:
Compartido:
Dirección de alto nivel:
WORM: No
Capacidad de escala: 90
Cifrado de unidad: Activado
Asignación secundaria (MB):
Compresión:
Retención:
Protección:
Fecha caducidad:
Unidad:
Protección de bloques lógicos: Lectura/Grabación
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 08/04/03 14:28:31
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

Nombre clase dispositivo

El nombre de la clase de dispositivo.

Estrategia acceso a dispositivo

Especifica cómo se graban los datos en la clase de dispositivo.

Número agrupaciones almacenamiento

El número de agrupaciones de almacenamiento asignadas a la clase de dispositivo.

Tipo dispositivo

El tipo de dispositivo de la clase de dispositivo.

Format

El formato de grabación.

Capacidad est/máx (MB)

La capacidad máxima o estimada de un volumen asociado con la clase de dispositivo.

Límite montajes

El número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente o especifica que DRIVES es el límite de montaje.

Espera montaje (min)

El número máximo de minutos que debe esperarse a que se monte un volumen de acceso secuencial.


#### Retención montaje (min)

El número de minutos que debe retenerse un volumen de acceso secuencial desocupado antes de desmontarlo.

#### Prefijo de etiquetas

El calificador de alto nivel del nombre del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial.

 Sistemas operativos Windows Letra unidad

 Sistemas operativos Windows La letra de unidad de un archivo extraíble.

#### Biblioteca

El nombre del objeto de biblioteca definido que contiene las unidades que utiliza la clase de dispositivo.

#### Directorio

Directorio o directorios de una clase de dispositivo FILE compartida.

#### Nombre servidor

El nombre de un servidor definido.

#### Período de reintento

El intervalo durante el cual el servidor intenta ponerse en contacto con un servidor de destino en caso de que se sospeche de que existe un problema de comunicaciones.

#### Intervalo entre reintentos

La frecuencia con la que se llevan a cabo los reintentos en un período de reintento.

#### Compartido

Si esta clase de dispositivo FILE se comparte entre el servidor y uno o más agentes de almacenamiento.

#### Dirección alto nivel

Dirección IP del dispositivo en formato decimal con puntos.

#### Capacidad mínima

La capacidad mínima de un volumen asociado con la clase de dispositivo.

#### WORM



Especifica si esta unidad es un dispositivo WORM (una sola grabación, varias lecturas).



#### Cifrado de unidad



Si se permite el cifrado de unidad. Este campo se aplica sólo a volúmenes de una agrupación de almacenamiento que está asociada a un tipo de dispositivo de 3592, LTO o ECARTRIDGE.



#### Capacidad de escala



Porcentaje de la capacidad del medio que puede utilizarse para almacenar datos.



 Sistemas operativos AIX  Sistemas operativos Linux Asignación principal (MB)



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo FILE que representan el almacenamiento que gestiona un servidor de medios de z/OS. Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen.



 Sistemas operativos AIX  Sistemas operativos Linux Asignación secundaria (MB)



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo FILE que representan el almacenamiento que gestiona un servidor de medios de z/OS. Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado.



 Sistemas operativos AIX  Sistemas operativos Linux Compresión



 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica si los datos están comprimidos.



 Sistemas operativos AIX  Sistemas operativos Linux Retención

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica el número de días que se retiene la cinta, si se utiliza la retención.



 Sistemas operativos AIX  Sistemas operativos Linux Protección

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica si los volúmenes están protegidos por el programa RACF.

 Sistemas operativos AIX  Sistemas operativos Linux Fecha caducidad

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo, si se utiliza la caducidad.

 Sistemas operativos AIX  Sistemas operativos Linux Unidad

 Sistemas operativos AIX  Sistemas operativos Linux Para clases de dispositivo de cinta que representan el almacenamiento que gestiona el servidor de medios de z/OS. Especifica el nombre de unidad esotérico para el grupo de dispositivos de cinta.

#### Protección de bloques lógicos

Especifica si la protección de bloques lógicos está habilitada y, si lo está, la modalidad. Los valores posibles son Lectura/Grabación, Sólo lectura y No. Puede utilizar la protección de bloques lógicos solamente con los siguientes tipos de unidades y medios:

- IBM® LTO5 y posterior
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior
- Unidades Oracle StorageTek T10000C y T10000D

#### Última actualización por (administrador)

El administrador que ha realizado la última actualización de la clase de dispositivo.



Clase de dispositivo	Directorio	Capacidad estimada	Disponibilidad estimada
DBBKUP	G:\This\is\a\large\directory	13,000 M	5,543 M
DBBKUP	G:\This\is\directory2	13,000 M	7,123 M
DBBKUP2	G:\This\is\a\huge\directory	2,256 G	2,200 G

## Descripciones de los campos

### Nombre clase dispositivo

El nombre de la clase de dispositivo.

### Directorio

Vía de acceso del directorio ubicado en el servidor.

### Capacidad estimada

Capacidad estimada total del directorio.

### Disponibilidad estimada

Espacio disponible restante estimado para el directorio.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DIRSPACE

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.

## QUERY DOMAIN (Consultar un dominio de políticas)

Utilice este comando para visualizar información sobre uno o varios dominios de políticas.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query D0main-+-----+----->
      .-*-----+
      '-nombre_dominio-'
      .-Format----Standard----.
>-+-----+-----<
      '-Format----+Standard-+'
      '-Detailed-'
  
```

### Parámetros

#### nombre\_dominio

Especifica el dominio de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se visualizarán todos los dominios de políticas.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial.

##### Detailed

Especifica que se visualizará toda la información.



## Ejemplo: visualizar un resumen de dominios de política

---

Visualizar información parcial de todos los dominios de políticas del servidor. Emita el comando:

```
query domain
```

Nombre dominio políticas	Juego políticas activado	Clase gestión predeterm. activada	Número de nodos registrad.	Descripción
-----	-----	-----	-----	-----
EMPLOYEE- _RECORDS PROG1	VACATION	ACTIVEFI- LES	6	Dominio de registros de empleados
PROG2			0	Dominio de prueba de grupo de programación
STANDARD	STANDARD	STANDARD	1	Dominio de políticas instalado de forma dominio de políticas

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar la lista de agrupaciones de datos activos

---

Visualizar la lista de agrupaciones de datos activos. Emita el comando:

```
query domain format=detailed
```

```
Nombre dominio políticas: STANDARD
Juego de políticas activado: STANDARD
Fecha/hora activación: 05/16/2006 16:18:05
Días desde activación: 15
Clase gestión predeterminada activada: STANDARD
Número de nodos registrados: 1
Descripción: Dominio de
políticas
predeterminado
instalado.

Retención copias seguridad (período gracia): 30
Retención copias archivadas (período gracia): 365
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 05/31/2006 15:17:48
Perfil de gestión:
Cambios pendientes: Sí
Lista de agrupaciones de datos activos: ADPPPOOL
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

Nombre de dominio de políticas

El nombre del dominio de políticas.

Juego de políticas activado

El nombre del último juego de políticas que se ha activado en el dominio.

Las definiciones del último juego de políticas activado y del el juego de políticas ACTIVE no son necesariamente idénticas. Al activar un juego de políticas, el servidor copia el contenido del juego de políticas en el juego de políticas con el nombre especial ACTIVE. Las definiciones copiadas que hay en el juego de políticas ACTIVE sólo se pueden modificar activando otro juego de políticas. Puede modificar el juego de políticas original sin que afecte al juego de políticas ACTIVE. Por lo tanto, las definiciones que hay en el último juego de políticas que se ha activado pueden ser distintas de las que hay en el juego de políticas ACTIVE.

Fecha/hora activación

La fecha y hora en que se ha activado el juego de políticas.

Días desde activación

El número de días transcurridos desde que se ha activado el juego de políticas.

Clase gestión predeterminada activada

La clase de gestión predeterminada asignada al juego de políticas.

Número de nodos inscritos

El número de nodos cliente registrados en el dominio de políticas.

Descripción

La descripción del dominio de políticas.

Retención copias seguridad (período gracia)

El número de días que se retienen las versiones de copia de seguridad inactivas de los archivos cuando existen algunas de las condiciones siguientes:

- Un archivo se vuelve a vincular a una nueva clase de gestión, pero ni la nueva clase de gestión ni la clase de gestión predeterminada contienen un grupo de copia de seguridad.
- La clase de gestión a la que está asociado un archivo no existe ya y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.
- El grupo de copia de seguridad se ha suprimido de la clase de gestión a la que está asociado un archivo y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

Retención copias archivadas (período gracia)

El número de días que se retiene una copia archivada que cumple una de las condiciones siguientes:

- La clase de gestión a la que está asociado un archivo no existe ya y la clase de gestión predeterminada no contiene un grupo de copia de archivada.
- El grupo de copia de archivada se ha suprimido de la clase de gestión a la que está asociado un archivo y la clase de gestión predeterminada no contiene un grupo de copia archivada.

Última actualización por (administrador)

El administrador que ha definido o que ha actualizado más recientemente el dominio de políticas. Si este campo contiene \$\$CONFIG\_MANAGER\$\$, el dominio de políticas está asociado a un perfil que gestiona el gestor de configuración.

Fecha/hora última actualización

Especifica cuándo ha definido o ha actualizado más recientemente el administrador el dominio de políticas.

Perfil de gestión

El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de este dominio de políticas.

Cambios pendientes

Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

Lista de agrupaciones de datos activos

La lista de las agrupaciones de datos activos del dominio.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DOMAIN

Comando	Descripción
COPY DOMAIN	Crea una copia de un dominio de políticas.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
UPDATE DOMAIN	Cambia los atributos de un dominio de políticas.

## QUERY DRIVE (Consultar información acerca de una unidad)

Utilice este mandato para visualizar la información sobre las unidades asociadas a una biblioteca.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
.-***-----
>>-Query DRive-----+-----
|                       .-*****. |
|'-nombre_biblioteca-+-+-----+-'|
|                       '-nombre_unidad-'
.-Format----Standard----.
>-+-----+-----+-----><
|'-Format----+Standard+-'|
|'-Detailed-'
```

## Parámetros

---

### library\_name

Especifica el nombre de la biblioteca donde está situada la unidad consultada. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar este nombre.

Debe especificar un valor para este parámetro si especifica un nombre de unidad.

### nombre\_unidad

Especifica el nombre asignado a la unidad. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar este nombre. Si especifica un nombre de unidad, debe especificar también un valor para *nombre\_biblioteca*.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial sobre la unidad.

#### Detailed

Especifica que se visualizará información completa sobre la unidad.

## Ejemplo: obtener una lista de las unidades que se asocian al servidor

---

Visualizar información acerca de todas las unidades asociadas con el servidor. Emita el comando:

```
query drive
```

Nombre bib.	Nombre unidad	Tipo dispos.	Activado
LIB1	DRIVE01	3590	Sí
LIB2	DRIVE02	3590	Sí

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información detallada acerca de una unidad y biblioteca específicas

---

Visualizar información detallada sobre la unidad denominada DRIVE02 asociada a la biblioteca LIB2. Emita el mandato:

```
query drive lib2 drive02 format=detailed
```

```
Nombre biblioteca: LIB2
Nombre unidad: DRIVE02
Tipo dispositivo: 3590
Activado: Yes
Estado de unidad: Empty
Asignado a:
Última actualización por (administrador): ADMIN
Fecha/hora última actualización: 29/02/2002 09:26:23
Frec. limpieza (Gigabytes/ASNEEDED/NONE): NONE
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

### Nombre de biblioteca

Nombre de la biblioteca a la que se ha asignado la unidad.

### Nombre de unidad

El nombre asignado a la unidad.

### Tipo de dispositivo

El tipo de dispositivo especificado en la clase de dispositivo asociada. El servidor debe tener una ruta definida del servidor a la unidad para poder determinar el tipo de dispositivo verdadero. Siempre que haya una ruta definida del servidor a la unidad, el servidor mostrará el tipo de dispositivo verdadero de la unidad aunque haya otras rutas definidas en esta unidad. La excepción a esto se da cuando el tipo de dispositivo es remoto o desconocido.

### REMOTE

El servidor no tiene una ruta al dispositivo. Las únicas rutas definidas al dispositivo proceden de los transportadores de datos.

### UNKNOWN

No existe ninguna ruta.

Consejo: Revise la salida del mandato QUERY PATH para determinar si están definidas las rutas deseadas. Si no están definidas, defina las rutas deseadas mediante el mandato DEFINE PATH. Asimismo, si utiliza un dispositivo transportador de datos, revise la salida del mandato QUERY DATAMOVER para determinar el tipo del dispositivo transportador de datos. Si utiliza una ruta del servidor a una unidad, el tipo de dispositivo de la clase de dispositivo y la unidad deberán coincidir. Si utiliza una ruta de un dispositivo transportador de datos a una unidad, revise la documentación de su tipo de transportador de datos para asegurarse de que el tipo de dispositivo de la clase de dispositivo sea compatible con el tipo de dispositivo transportador de datos.

En línea

Especifica el estado de la unidad:

Sí

La unidad está activada y disponible para las operaciones de servidor.

No

La unidad está desactivada y un administrador la ha situado en este estado al actualizar el estado.

No disponible desde

Especifica que la unidad no está disponible desde *mm/dd/aa hh:mm:ss*. La salida muestra la hora en que el servidor marcó la unidad como no disponible.

Sondeando desde

Especifica que el servidor está sondeando la unidad ya que ésta ha dejado de responder. La salida muestra la hora en que el servidor detectó un problema y empezó a sondear. El servidor sondeará una unidad antes de indicar que no está disponible. La salida de la hora tiene el siguiente formato: *mm/dd/aa hh:mm:ss*.

Formatos de lectura

Los formatos de lectura de la unidad.

Formatos de grabación

Los formatos de grabación de la unidad.

Elemento

El número de elemento de la unidad.

Estado de la unidad

Especifica el estado actual de esta unidad basándose en el resultado del último mandato SCSI en la unidad o biblioteca. El servidor realiza el seguimiento del estado de la unidad para mejorar la selección de una unidad para una operación y para las operaciones de recuperación de la unidad. Los valores son:

Unavailable

La unidad no está disponible en la biblioteca para operaciones.

Empty

La unidad está vacía y lista para operaciones.

Loaded

La unidad está cargada actualmente y el servidor realiza operaciones en la unidad.

Unloaded

Se han expulsado los medios de la unidad.

Reserved

La unidad está reservada para una petición de montaje.

Desconocido

La unidad empieza en el estado de unidad desconocido como resultado de su definición, de la inicialización del servidor o porque se ha actualizado su estado a Activado.

Nombre de volumen

El nombre de volumen de la unidad.

Asignado a

El nombre del cliente de bibliotecas que actualmente utiliza la unidad. Esto sólo se aplica a las bibliotecas SCSI compartidas; el campo se deja en blanco para las demás bibliotecas.

WWN

El nombre de ámbito mundial de la unidad.

Última actualización por (administrador)

Especifica quién ha realizado la última actualización de la unidad.

Fecha/hora última actualización

Fecha y hora en las que tuvo lugar la última actualización.

Frec. limpieza (Gigabytes/ASNEEDED/NONE)

La frecuencia con que el servidor activa la limpieza de la unidad. Este valor puede ser el número de gigabytes, ASNEEDED o NONE.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DRIVE

Comando	Descripción
---------	-------------

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE DRIVE	Cambia los atributos de una unidad.

## QUERY DRMEDIA (Consultar medio de recuperación ante siniestro)

Utilice este mandato para visualizar información sobre volúmenes de copia de seguridad de base de datos y volúmenes en agrupaciones de almacenamiento, agrupaciones de almacenamiento de copia de contenedor y agrupaciones de almacenamiento de datos activos. También puede utilizar el mandato para crear un archivo de mandatos ejecutables para procesar los volúmenes.

El proceso de volúmenes por parte de este mandato depende del uso que se les de:

Copias de seguridad de la base de datos del servidor

Para controlar si el mandato procesa volúmenes de copia de seguridad de base de datos, utilice el parámetro SOURCE. El mandato puede procesar volúmenes utilizados para copias de seguridad de base de datos completas más las incrementales o de instantáneas. No se pueden especificar volúmenes virtuales (objetos de copia de seguridad almacenados en otro servidor).

Puede modificar los volúmenes mediante cada estado, o bien utilizar el parámetro TOSTATE y omitir los estados para simplificar los traslados.

Agrupaciones de almacenamiento de copia

El comando QUERY DRMEDIA siempre procesa volúmenes de agrupación de almacenamiento de copia que pueden seleccionarse.

Agrupaciones de almacenamiento de copia de contenedor

De forma predeterminada, los volúmenes de agrupación de almacenamiento de copia de contenedor no se pueden elegir para que las procese el mandato QUERY DRMEDIA. Para procesar volúmenes de agrupación de almacenamiento de copia de contenedor, debe emitir primero el mandato SET DRMCOPYCONTAINERSTGPOOL o especificar el parámetro COPYCONTAINERSTGPOOL en el mandato QUERY DRMEDIA.

Agrupaciones de almacenamiento de datos activos

De forma predeterminada, los volúmenes en agrupaciones de almacenamiento de datos activos no se pueden elegir para que las procese el mandato QUERY DRMEDIA. Para procesar volúmenes de agrupación de datos activos, debe emitir primero el mandato SET DRMACTIVEDATASTGPOOL o especificar el parámetro ACTIVATEDATASTGPOOL en el mandato QUERY DRMEDIA.

Si utiliza una biblioteca externa y ha traspasado un volumen al estado NOTMOUNTBLE con el mandato MOVE DRMEDIA, puede que el mandato QUERY DRMEDIA todavía informe de que el estado del volumen es MOUNTABLE si detecta que el volumen se encuentra en la biblioteca. Consulte la documentación de la biblioteca externa para obtener información acerca de los procedimientos que debería seguir al utilizar los mandatos MOVE DRMEDIA y QUERY DRMEDIA.

## Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Si el parámetro *CMD* NO está especificado: privilegio de operador o de sistema.
- Si el parámetro *CMD* está especificado y la opción del servidor *REQSYSAUTHOUTFILE* está establecida en *NO*: privilegio de operador, de almacenamiento sin restricciones o de sistema.
- Si el parámetro *CMD* está especificado y la opción del servidor *REQSYSAUTHOUTFILE* está establecida en *YES* (el valor predeterminado): privilegio de sistema.

## Sintaxis

```

.*-----
>>-Query DRMedia-----+----->
      '-nombre_volumen-'
.-WHEREState-----All-----

```



**NOTMOUNTable**

Los volúmenes con este estado están en el local, contienen datos válidos y no son accesibles para procesos en el local.

**COURier**

Los volúmenes con este estado se están trasladando a una ubicación fuera del local.

**VAULT**

Los volúmenes con este estado están fuera del local, contienen datos válidos y no son accesibles para procesos en el local.

**VAULTRetrieve**

Los volúmenes con este estado se encuentran en la cámara de seguridad fuera del local y no contienen datos válidos.

- Se considera que un volumen de agrupación de almacenamiento de copia se encuentra en estado VAULTRETRIEVE si éste ha estado vacío durante, como mínimo, el número de días que se ha especificado con el parámetro REUSEDELAY del mandato DEFINE STGPOOL.
- Se considera que un volumen de copia de seguridad de base de datos se encuentra en estado VAULTRETRIEVE si éste se ha asociado a una serie de copias de seguridad de base de datos que ha caducado en función del valor que se ha especificado con el mandato SET DRMDBBACKUPEXPIREDDAYS.

Importante: Al emitir QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE, el servidor determina de forma dinámica qué volúmenes se pueden devolver al local para volver a utilizarlos o eliminarlos. Por tanto, para asegurarse de que identifica todos los volúmenes que se encuentran en estado VAULTRETRIEVE, emita QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE sin los parámetros BEGINDATE, ENDDATE, BEGINTIME ni ENDTIME. En el campo Fecha/hora última actualización de la salida de QUERY DRMEDIA WHERESTATE=VAULTRETRIEVE se visualizan la fecha y la hora en las que un volumen se ha traspasado al estado VAULT, no al estado VAULTRETRIEVE.

**COURIERRetrieve**

Los volúmenes con este estado se devuelven a la ubicación en el local.

**REmote**

Los volúmenes con este estado contienen datos válidos y están ubicados en el servidor remoto fuera del local.

**BEGINDate**

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el comando MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha más antigua en la que existe información del volumen. Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-7 o -7. Para consultar los volúmenes empezando por los registros cambiados al estado actual hace una semana, puede especificar BEGINDATE=TODAY-7 o BEGINDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

**ENDDate**

Especifica la fecha final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el comando MOVE DRMEDIA ha cambiado el volumen a su estado actual en la fecha especificada o con posterioridad a la fecha especificada. El valor predeterminado es la fecha actual. Puede especificar la fecha empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998

Valor	Descripción	Ejemplo
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-7 o -7. Para consultar los volúmenes empezando por los registros cambiados al estado actual hace una semana, puede especificar <code>BEGINDATE=TODAY-7</code> o <code>BEGINDATE=-7</code> .
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### BEGINTime

Especifica la hora inicial utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el comando `MOVE DRMEDIA` ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con posterioridad a la fecha y hora especificadas. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada con el parámetro `BEGINDATE`.

Puede especificar la hora empleando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	12:33:28
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00. Si emite el mandato <code>QUERY DRMEDIA</code> a las 09:00 con <code>BEGINTIME=NOW+03:00</code> o con <code>BEGINTIME=+03:00</code> , El servidor visualiza los volúmenes que se han modificado al estado actual a las 12:00 en la fecha inicial especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30. Si emite el mandato <code>QUERY DRMEDIA</code> a las 09:00 con <code>BEGINTIME=NOW-03:30</code> o con <code>BEGINTIME=-03:30</code> , El servidor visualiza los volúmenes que se han modificado al estado actual a las 5:30 en la fecha inicial especificada.

#### ENDTime

Especifica la hora final utilizada para seleccionar los volúmenes. Este parámetro es opcional. Los volúmenes podrán seleccionarse si el comando `MOVE DRMEDIA` ha cambiado el volumen a su estado actual en la fecha y hora especificadas o con anterioridad respecto a la fecha y hora especificadas. El valor predeterminado son las 23:59:59.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW



Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite el comando QUERY DRMEDIA a las 09:00 con ENDTIME=NOW+03:00 o con ENDTIME=+03:00, IBM Spectrum Protect procesará los volúmenes que han cambiado a su estado actual a las 12:00 de la fecha de finalización que ha especificado.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30  Si emite el comando QUERY DRMEDIA a las 09:00 con ENDTIME=NOW-03:00 o con ENDTIME=-03:00, IBM Spectrum Protect procesará los volúmenes que han cambiado a su estado actual a las 06:00 de la fecha de finalización que ha especificado.

#### COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de copia que se especifican con este parámetro alteran temporalmente las agrupaciones de almacenamiento de copia especificadas con el mandato SET DRMCOPYSTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYSTGPOOL o si se han eliminado todas las agrupaciones de almacenamiento de copia con el mandato SET DRMCOPYSTGPOOL, el servidor procesará todos los volúmenes de agrupación de almacenamiento de copia que se encuentren en el estado especificado (ALL, MOUNTABLE, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE).

#### Source

Especifica si se selecciona algún volumen de copia de seguridad de base de datos. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Los valores posibles son:

##### DBBackup

Se seleccionan los volúmenes de copia de seguridad de base de datos completa e incremental.

##### DBSnapshot

Se seleccionan los volúmenes de copia de seguridad de instantánea de base de datos.

##### DBNone

No se selecciona ningún volumen de copia de seguridad de base de datos.

#### ACTIVEDatastgpool

Especifica el nombre de la agrupación de almacenamiento de datos activos cuyos volúmenes van a procesarse. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de datos activos que se han especificado con este parámetro alteran temporalmente las agrupaciones de almacenamiento de datos activos que se han especificado con el mandato SET DRMACTIVEDATASTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMACTIVEDATASTGPOOL se emitió anteriormente con nombres de agrupaciones de almacenamiento de datos activos válidos, el servidor sólo procesa esas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMACTIVEDATASTGPOOL o todas las agrupaciones de almacenamiento de datos activos se han eliminado mediante el mandato SET DRMACTIVEDATASTGPOOL, el servidor procesa todos los volúmenes de agrupaciones de almacenamiento de datos activos cuyo estado sea el especificado (ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE). Los volúmenes que se encuentran en el estado MOUNTABLE no se procesarán.

#### COPYCONTAINERstgpool

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor cuyos volúmenes se van a procesar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Las agrupaciones de almacenamiento de copia de contenedor especificadas usando este parámetro alteran temporalmente a aquellas especificadas usando el mandato SET DRMCOPYCONTAINERSTGPOOL.

Si no se especifica este parámetro, el servidor selecciona las agrupaciones de almacenamiento de la manera siguiente:

- Si el mandato SET DRMCOPYCONTAINERSTGPOOL se ha emitido anteriormente con nombres de agrupaciones de almacenamiento de copia de contenedor válidos, el servidor solo procesará dichas agrupaciones de almacenamiento.
- Si no se ha emitido el mandato SET DRMCOPYCONTAINERSTGPOOL, o si todas las agrupaciones de almacenamiento de copia de contenedor se han eliminado usando el mandato SET DRMCOPYCONTAINERSTGPOOL, el servidor procesará todos los volúmenes de agrupación de copia de contenedor basados en el valor especificado por el parámetro WHERESTATE. Si el parámetro está establecido en un valor ALL, NOTMOUNTABLE, COURIER, VAULT, VAULTRETRIEVE, COURIERRETRIEVE o REMOTE, los volúmenes se procesan. Si el valor está establecido en MOUNTABLE, los volúmenes no se procesan.

#### Format

Especifica la información que se visualizará. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial.

##### Detailed

Especifica que se visualizará información detallada.

##### Cmd

Especifica que se han creado comandos ejecutables para los volúmenes seleccionados. Si especifica FORMAT=CMD, también debe especificar el parámetro CMD.

#### WHERELocation

Especifica la ubicación de los volúmenes que se han de consultar. Este parámetro es opcional. La longitud máxima de la lista de la ubicación es de 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Si especifica un nombre de servidor destino, el gestor de recuperación ante siniestro visualiza todos los volúmenes de copia de seguridad de base de datos y todos los volúmenes de agrupaciones de almacenamiento de copia ubicados en el servidor destino.

#### CMd

Especifica la creación de comandos ejecutables para procesar el nombre de volumen y la ubicación que obtiene este comando. Este parámetro es opcional. La especificación de comandos ejecutables se ha de delimitar con comillas. La longitud máxima de este parámetro son 255 caracteres. El gestor de recuperación ante siniestro graba los comandos en un archivo que se ha especificado mediante el parámetro CMDFILENAME o el comando SET DRMCMDFILENAME o que ha generado el comando QUERY DRMEDIA. Si la longitud del comando es superior a 240 caracteres, se divide en varias líneas y se agregan caracteres de continuación (+). Tal vez necesite modificar el carácter de continuación según los requisitos del producto que ejecuta los comandos.

Si no especifica el parámetro FORMAT=CMD, este mandato no creará líneas de mandatos.

#### serie

La serie de los comandos. La serie no debe contener comillas intercaladas. Por ejemplo, éste es un parámetro CMD válido:

```
cmd="checkin libvol lib8mm &vol status=scratch"
```

Éste es un ejemplo de un parámetro CMD *no* válido:

```
cmd=""checkin libvolume lib8mm" &vol status=scratch""
```

#### sustitución

Especifica una variable de sustitución para indicar a QUERY DRMEDIA que sustituya un valor por la variable. Las variables no son sensibles a las mayúsculas y minúsculas, y no deben contener espacios en blanco detrás del símbolo &. Las variables posibles son:

##### &VOL

Una variable de nombre de volumen.

##### &LOC



Una ubicación de volumen.

##### &VOLDSN

El nombre del archivo donde el servidor graba las etiquetas de los medios de acceso secuencial. Un ejemplo de un nombre de archivo de volumen de cinta de agrupación de almacenamiento de copia que utilice el prefijo TSM predeterminado es TSM.BFS. Un ejemplo de un nombre de archivo de volumen de cinta de copia de seguridad de base de datos que utilice el prefijo TSM310 definido con la clase de dispositivo es TSM310.DBB.

##### &NL


El carácter de nueva línea. Cuando se especifica &NL, el comando QUERY DRMEDIA subdivide el comando donde se encuentra la variable &NL y no añade un carácter de continuación. Debe especificar el carácter de continuación adecuado antes de &NL si es necesario. Si no se especifica &NL y la línea de comandos es superior a 240 caracteres, la línea se divide en varias líneas y se agregan los caracteres de continuación (+).

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados con el parámetro CMD. Este parámetro es opcional.

Si no especifica un nombre con el comando SET DRMCMDFILENAME, el servidor creará un nombre de archivo añadiendo `exec.cmds` al nombre de ruta absoluto del directorio de la instancia de IBM Spectrum Protect. Si especifica una serie nula (""), los mandatos sólo se visualizan en la consola. Puede redirigir los mandatos a un archivo mediante el carácter de redirección del sistema operativo.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

 Sistemas operativos Windows CMDFilename

 Sistemas operativos Windows Especifica el nombre de archivo totalmente calificado que contendrá los mandatos especificados con el parámetro CMD. Este parámetro es opcional.

Si no se especifica un nombre de archivo con el mandato SET DRMCMDFILENAME, el servidor crea un nombre de archivo añadiendo `exec.cmd` al directorio que representa esta instancia del servidor (normalmente el directorio en el que se instaló originalmente IBM Spectrum Protect). Si especifica una serie nula (""), los mandatos sólo se visualizan en la consola. Puede redirigir los mandatos a un archivo usando `> o >>`, que el sistema proporciona. El gestor de recuperación ante siniestro asigna el nombre de archivo especificado o generado. Si el archivo existe, el gestor de recuperación ante siniestro intenta utilizarlo, y se graba encima de los datos existentes.

Si la operación no se puede ejecutar después de haberse creado el archivo de mandatos, el archivo no se suprime.

#### APPend

Especifica si se graba encima del contenido existente del archivo de comandos o se agregan los comandos al archivo. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

El gestor de recuperación ante siniestro sobregaba el contenido del archivo.

Yes

El gestor de recuperación ante siniestro añade los comandos al archivo.

## Ejemplo: obtener una lista de los volúmenes que se van a enviar al almacenamiento fuera del local

Visualizar todos los volúmenes que han de entregarse a un transportista para su almacenamiento fuera del local.

```
query drmedia wherestate=notmountable
format=standard
```

Nombre	Estado	Fecha/hora última actualización	Biblioteca automatizada
TAPE01	No montable	20/01/1998 14:25:22	
DBTP01	No montable	20/01/1998 14:25:22	
DBTP03	No montable	20/01/1998 14:31:53	

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información acerca de los volúmenes de la cámara de seguridad

Visualizar información detallada sobre todos los volúmenes que están en la cámara de seguridad.

```
query drmedia wherestate=vault format=detailed
```

```
Nombre volumen: DBTP02
Estado: Cámara seguridad
Fecha/hora última actualización: 20/01/1998 13:29:02
Ubicación: Ironmnt
Tipo volumen: DBBackup
Nombre agrupación almacenamiento copia:
Nombre agrupación almacenamiento datos activos: TSMACTIVEPOOL
Nombre biblioteca automatizada:
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

Nombre de volumen

El nombre del volumen de copia de seguridad de base de datos o de agrupación de almacenamiento de copia.

Estado

El estado del volumen.

Fecha/hora última actualización

La fecha y la hora de la última actualización del estado del volumen. Para los volúmenes en estado de VAULTRETRIEVE, este campo muestra la fecha y la hora en las cuales se ha modificado un volumen al estado de VAULT, no VAULTRETRIEVE. El servidor no "actualiza" volúmenes a VAULTRETRIEVE. En el momento de emitirse el comando QUERY DRMEDIA, el servidor determina dinámicamente si los datos de los volúmenes de agrupación de almacenamiento de copia y los volúmenes de copia de seguridad de base de datos ya no son válidos y si éstos pueden devolverse al local para su reutilización o desecho.

Ubicación

El campo Ubicación aparece cuando el volumen no puede montarse o no está la biblioteca. El campo Ubicación está vacío si el volumen puede montarse y está en la biblioteca.

Tipo volumen

El tipo del volumen. Los valores posibles son:

DBBackup

Volumen de copia de seguridad de base de datos completa o incremental.

DBSnapshot

Volumen de copia de seguridad de instantánea de base de datos.

CopyStgPool

Volumen de agrupación de almacenamiento de copia.

ContcopyStgPool

Un volumen de agrupación de almacenamiento de copia de contenedor.

Nombre agrupación almacenamiento copia

Para un volumen de agrupación de almacenamiento de copia, el nombre de la agrupación de almacenamiento de copia.

Nombre de la agrupación de almacenamiento de datos activos

Para un volumen de agrupación de almacenamiento de datos activos, el nombre de la agrupación de almacenamiento de datos activos.

Nombre agrupación almacenamiento copia contenedor




Para un volumen de agrupación de almacenamiento de copia de contenedor, el nombre de la agrupación de almacenamiento de copia de contenedor.

Biblioteca automatizada

El nombre de la biblioteca automatizada si el volumen está en una biblioteca.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DRMEDIA

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL	Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.
SET DRMFILPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.

# QUERY DRMSTATUS (Consultar parámetros del sistema del gestor de recuperación ante siniestro)

---

Utilice este comando para visualizar la información sobre los parámetros del sistema que se han definido para el gestor de recuperación ante siniestro (DRM).

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
>>-Query DRMStatus-----<<
```

## Parámetros

---

Ninguno.

## Ejemplo: visualizar información acerca de los parámetros del sistema de DRM

---

Visualizar información acerca de los parámetros del sistema de DRM:

```
query drmstatus

    Prefijo plan recuperación:
    Prefijo instrucciones plan:
    Sufijo volumen sustitución: @
    Agrupaciones almacenamiento primarias: PRIM1 PRIM2
    Agrupaciones almacenamiento de copia: COPY*
    Agrupaciones almacenamiento datos activos: TSMACTIVEPOOL
    Agrupaciones de almacenamiento de copia de contenedor: COPYCNRPOOL
    Nombre ubicación no montable: Local
    Nombre transportista: Fedex
    Nombre ubicación cámara seguridad: Ironmnt
    Días caducidad serie copia seguridad BD: 30 Día(s)
    Días de caducidad del archivo del plan de recuperación: 30 día(s)
    ¿Comprobar etiqueta?: No
    ¿Procesar tipo dispositivo FILE?: No
    Nombre archivo comandos:
```

## Descripciones de los campos

---

### Prefijo plan recuperación

Parte de prefijo especificada por el usuario del nombre del archivo del plan de recuperación.

### Prefijo de instrucciones del plan

Parte de prefijo especificada por el usuario de los nombres de los archivos de instrucciones de recuperación del servidor.

### Sufijo volumen sustitución

El carácter agregado al final de los nombres de volúmenes de sustitución del archivo del plan de recuperación.

### Agrupaciones de almacenamiento primarias

Las agrupaciones de almacenamiento primarias que pueden seleccionarse para que las procese el comando PREPARE. Si este campo está en blanco, se podrán seleccionar todas las agrupaciones de almacenamiento primarias.

### Agrupaciones de almacenamiento de copia

Las agrupaciones de almacenamiento de copia que pueden seleccionarse para que las procesen los comandos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, se podrán seleccionar todas las agrupaciones de almacenamiento de copia.

### Agrupaciones de almacenamiento de datos activos

Las agrupaciones de datos activos que pueden seleccionarse para que las procesen los comandos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, no se podrán seleccionar agrupaciones de datos activos.

### Agrupaciones de almacenamiento de copia de contenedor

Las agrupaciones de almacenamiento de copia de contenedor que pueden seleccionarse para que las procesen los mandatos MOVE DRMEDIA, PREPARE y QUERY DRMEDIA. Si este campo está en blanco, no se podrán seleccionar agrupaciones de almacenamiento de copia de contenedor.

### Nombre ubicación no montable

El nombre de la ubicación fuera del local donde se almacenará el medio que se envía.

Nombre del transportista

El nombre del transportista que se utiliza para transportar el medio a la cámara de seguridad.

Nombre de ubicación de la cámara seguridad

El nombre de la cámara de seguridad donde se almacena el medio.

Días de caducidad de la serie de copia de seguridad de la base de datos

El número mínimo de días que deben transcurrir desde la creación de una serie de base de datos antes de que pueda darse caducidad a ésta. Consulte el comando SET DRMDBBACKUPEXPIREDDAYS para obtener información acerca de los criterios que deben satisfacerse para que tenga lugar la caducidad de una serie de copia de seguridad de base de datos.

Días de caducidad del archivo del plan de recuperación

El número mínimo de días que deben transcurrir desde la creación de un archivo de plan de recuperación, almacenado en un servidor de destino, antes de que pueda darse caducidad a éste. Consulte el comando SET DRMRPFEXPIREDDAYS para obtener información acerca de los criterios que deben satisfacerse para que tenga lugar la caducidad de un archivo de plan de recuperación.

¿Comprobar etiqueta?

Si han de leerse las etiquetas de medios de los volúmenes de medios secuenciales a los que se han dado de baja mediante el comando MOVE DRMEDIA. Los valores posibles son Yes o No.

¿Procesar tipo dispositivo FILE?

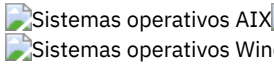
Si los comandos MOVE DRMEDIA o QUERY DRMEDIA han de procesar los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo que tiene un tipo de dispositivo FILE. Los valores posibles son Yes o No.

Nombre de archivo de comandos

El nombre del archivo con la ruta completa que contiene los comandos ejecutables que ha generado el comando MOVE DRMEDIA o el comando QUERY DRMEDIA.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY DRMSTATUS

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
SET DRMCHECKLABEL	Especifica si IBM Spectrum Protect debe leer las etiquetas de volúmenes durante el proceso del mandato MOVE DRMEDIA.
SET DRMACTIVEDATASTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento de datos activos.
 Sistemas operativos AIX, Linux y Windows SET DRMCOPYCONTAINERSTGPOOL	Especifica las agrupaciones de almacenamiento de copia de contenedor utilizadas en mandatos de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.
SET DRMCMDFILENAME	Especifica un nombre de archivo que contendrá los mandatos DRM ejecutables.
SET DRMCOURIERNAME	Especifica el nombre del transportista del medio de recuperación ante siniestro.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SET DRMFILEPROCESS	Especifica si el mandato MOVE DRMEDIA o QUERY DRMEDIA procesa los archivos asociados con un tipo de dispositivo.
SET DRMINSTRPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta de las instrucciones del plan de recuperación.
SET DRMPPLANVPOSTFIX	Especifica los nombres de los volúmenes de sustitución del archivo del plan de recuperación.
SET DRMPPLANPREFIX	Especifica la parte del prefijo correspondiente al nombre de ruta del plan de recuperación.

Comando	Descripción
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.
SET DRMRPFEXPIREDAYS	Establece los criterios de caducidad del plan de recuperación.
SET DRMVaultNAME	Especifica el nombre de la cámara de seguridad donde está almacenado el medio DRM.
SET DRMNOTMOUNTABLENAME	Especifica el nombre de ubicación del medio DRM que se ha de enviar fuera del local.

## QUERY ENABLED (Consultar eventos activados)

Utilice este comando para visualizar una lista de eventos activados o una lista de eventos desactivados, la que sea más corta de las dos.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query--ENabled--+-CONSOLE-----+----->
      +-ACTLOG-----+
      +-EVENTSERVER---+
      +-FILE-----+
      +-FILETEXT-----+
      |                |
      |                (1) |
      +-NTEVENTLOG-----+
      |                |
      |                (2) |
      +-SYSLOG-----+
      +-TIVOLI-----+
      '-USEREXIT-----'

>--+-----+-----><
  +-NODEname---+---nombre_nodo-----+
  '-SERVername---+---nombre_servidor-'
```

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro sólo está disponible para el sistema operativo Linux.

### Parámetros

receptor

Especifica un tipo de receptor para los eventos activados. Este parámetro es necesario. Los valores válidos son:

**ACTLOG**

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor.

**CONSOLE**

Especifica la consola estándar del servidor como receptor.

**EVENTSERVER**


Especifica el servidor de eventos como receptor.

**FILE**


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


**FILETEXT**

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos Windows**NTEVENTLOG**

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos Linux**SYSLOG**

 Sistemas operativos LinuxEspecifica el registro de sistema de Linux como receptor.

**TIVOLI**

Especifica Tivoli Management Environment (TME) como receptor.  
USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

NODENAME

Especifica un nombre de nodo a consultar. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para los eventos activados para el servidor donde se ejecuta este comando.

SERVERNAME

Especifica el nombre de servidor que se va a consultar. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para los eventos activados para el servidor donde se ejecuta este comando.

## Ejemplo: consultar al servidor acerca de eventos de consola

Consultar al servidor los eventos de servidor que se han activado para la consola. Existen 10000 eventos de servidor posibles. Se muestra una lista de los eventos activados o de los eventos desactivados (la lista que sea más corta).

```
query enabled console
```

Se han activado 9998 eventos para el receptor CONSOLE. Los eventos siguientes para el receptor CONSOLE:

```
ANR8409, ANR8410
```

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY ENABLED

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY EVENTRULES	Visualiza información acerca de las reglas del servidor y los eventos del cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## QUERY EVENT (Consultar eventos planificados y realizados)

Utilice este comando para visualizar el estado de los eventos planificados. Los parámetros de fecha y hora le permiten limitar la consulta a los eventos que se planificaron para que ocurrieran en las fechas y horas especificadas. Puede minimizar el tiempo necesario para procesar esta consulta limitando la salida a los eventos cuyos tiempos de inicio planificados pertenezcan a un rango de fecha y hora.

La sintaxis del comando es diferente para consultas que se aplican a operaciones planificadas de cliente y para comandos planificados de administración.

Tabla 1. Comandos relacionados con QUERY EVENT

Comando	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.
DELETE EVENT	Elimina los registros de eventos antes de una fecha y hora especificadas.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.
SET RANDOMIZE	Especifica la aleatorización de las horas de inicio de un margen de las planificaciones en modalidad por sondeo de cliente.





Valor	Descripción	Ejemplo
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7.  Para consultar los eventos que estaban planificados para iniciarse durante los últimos siete días, especifique BEGINDATE=TODAY-7 ENDDATE=TODAY o BEGINDATE=-7 ENDDATE=TODAY.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### BEGINTime

Especifica la hora inicial del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es 00:00.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW+03:00 o BEGINTIME=+03:00. IBM Spectrum Protect visualizará los eventos a las 12:00 en la fecha de inicio especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00.  Si emite este a las 9:00 para consultar los eventos que estaban planificados para iniciarse durante las últimas 4 horas, puede especificar BEGINTIME=NOW-04:00 ENDTIME=NOW o BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect visualizará los eventos a las 5:00 en la fecha de inicio especificada.

#### ENDDate

Especifica la fecha final del rango horario para los eventos que se han de visualizar. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. Para el parámetro BEGINDATE, se utiliza el valor predeterminado.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.

Valor	Descripción	Ejemplo
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-8 o -8.  Para consultar los eventos planificados para iniciarse durante una semana que terminaba ayer, puede especificar BEGINDATE=TODAY-8 ENDDATE=TODAY-1 o BEGINDATE=-8 ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. El valor predeterminado es 23:59.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW ENDTIME=NOW+03:00 o BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-04:00 o -04:00

#### EXceptiononly

Especifica el tipo de información que desea sobre los eventos planificados o completados. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que se visualizará información sobre eventos pasados y proyectados.

Yes

Especifica que se visualizan los eventos que no se han podido ejecutar según estaba planificado.

#### Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

Standard

Especifica que se visualiza información parcial acerca de los eventos.

Detailed

Especifica que se visualiza información completa acerca de los eventos.

## Visualizar información parcial para los eventos no satisfactorios

Visualizar información parcial acerca de todos los eventos planificados para DOMAIN1 que no se han ejecutado correctamente. Limitar la búsqueda al cliente denominado JOE. Limitar los eventos visualizados a los eventos planificados entre el 11 de febrero de 2001 (02/11/2001) y el 12 de febrero de 2001 (02/12/2001).

```
query event domain1 * nodes=joe begindate=02/11/2001
enddate=02/12/2001 exceptionsonly=yes
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
02/11/1999 01:00:00	02/11/1999 01:13:55	BACK1	JOE	No ejecutado
02/12/1999 01:00:00		DAILYBKP	JOE	No hecho

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Visualizar información parcial para eventos planificados de un cliente

Visualizar información completa para todos los eventos planificados para procesarse. Utilizar la fecha de inicio como la correspondiente a 10 días antes de la fecha de hoy y la finalización incluye la fecha de hoy.

```
query event * * begindate=today-10 enddate=today
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
02/04/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/04/2013 14:00:00	02/04/2013 14:12:49	VDATAMVR1-IN1	VDATAMVR1-T1	Completado
02/04/2013 14:30:00	02/04/2013 14:33:10	VDATAMVR1-IN2	VDATAMVR1-T2	Completado
02/04/2013 15:00:00	02/04/2013 15:01:49	VDATAMVR1-IN3	VDATAMVR1-T3	Completado
02/04/2013 15:30:00	02/04/2013 15:42:00	VDATAMVR1-IN4	VDATAMVR1-T4	Completado
02/05/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/05/2013 14:00:00	02/05/2013 14:05:22	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/05/2013 14:30:00	02/05/2013 14:32:53	VDATAMVR1-F2	VDATAMVR1-F2	Error 12
02/05/2013 15:00:00	02/05/2013 15:00:38	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/05/2013 15:30:00	02/05/2013 15:36:41	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/06/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/06/2013 14:00:00	02/06/2013 14:06:42	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/06/2013 14:30:00	02/06/2013 14:35:41	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/06/2013 15:00:00	02/06/2013 15:08:56	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/06/2013 15:30:00	02/06/2013 15:40:49	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/07/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/07/2013 14:00:00	02/07/2013 14:03:43	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/07/2013 14:30:00	02/07/2013 14:35:10	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/07/2013 15:00:00	02/07/2013 15:09:12	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/07/2013 15:30:00	02/07/2013 15:40:21	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/08/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/08/2013 14:00:00	02/08/2013 14:10:17	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/08/2013 14:30:00	02/08/2013 14:39:16	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/08/2013 15:00:00	02/08/2013 15:08:17	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/08/2013 15:30:00	02/08/2013 15:41:16	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/09/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/09/2013 14:02:16		VDATAMVR1-F1	VDATAMVR1-F1	Error 12
02/09/2013 14:30:00	02/09/2013 14:44:26	VDATAMVR1-F2	VDATAMVR1-F2	Error 12
02/09/2013 15:00:00	02/09/2013 15:06:24	VDATAMVR1-F3	VDATAMVR1-F3	Error 12
02/09/2013 15:30:00	02/09/2013 15:32:18	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/11/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/11/2013 14:00:00	02/11/2013 14:01:05	VDATAMVR1-F1	VDATAMVR1-F1	Error 12
02/11/2013 14:30:00	02/11/2013 14:31:42	VDATAMVR1-F2	VDATAMVR1-F2	Error 12
02/11/2013 15:00:00	02/11/2013 15:06:17	VDATAMVR1-F3	VDATAMVR1-F3	Error 12
02/11/2013 15:30:00	02/11/2013 15:30:19	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/12/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/12/2013 14:00:00	02/12/2013 14:03:37	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/12/2013 14:30:00	02/12/2013 14:33:07	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/12/2013 15:00:00	02/12/2013 15:03:56	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/12/2013 15:30:00	02/12/2013 15:36:44	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/13/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Inexistente
02/13/2013 14:00:00	02/13/2013 14:06:24	VDATAMVR1-F1	VDATAMVR1-F1	Completado
02/13/2013 14:30:00	02/13/2013 14:34:50	VDATAMVR1-F2	VDATAMVR1-F2	Completado
02/13/2013 15:00:00	02/13/2013 15:15:01	VDATAMVR1-F3	VDATAMVR1-F3	Completado
02/13/2013 15:30:00	02/13/2013 15:30:18	VDATAMVR1-F4	VDATAMVR1-F4	Completado
02/14/2013 14:00:00		SCHD_INCR-DM1	TSM_CET_DM1	Futuro
02/14/2013 14:00:00		VDATAMVR1-F1	VDATAMVR1-F1	Futuro
02/14/2013 14:30:00		VDATAMVR1-F2	VDATAMVR1-F2	Futuro
02/14/2013 15:00:00		VDATAMVR1-F3	VDATAMVR1-F3	Futuro

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Visualizar información detallada para eventos planificados de un cliente

Visualizar información detallada acerca de los eventos planificados para que los procese el cliente DOC entre las 10:00 y las 11:00 horas el 1 de noviembre de 2005 (11/01/2005). Observe que cuando el estado es Error, se visualiza el código de resultado.

```
query event domain1 * nodes=doc begindate=11/01/2005
begintime=10:00 endtime=11:00 enddate=11/01/2005
exceptiononly=yes format=detailed
```

Inicio planificado	Inicio real	Nombre planif.	Nombre nodo	Estado
11/01/2005 10:01:01	11/01/2005 10:03:46	T1	DOC	Error 8
11/01/2005 10:16:01	11/01/2005 10:16:10	T1	DOC	Error 4
11/01/2005 10:31:01	11/01/2005 10:33:08	T1	DOC	Hecho
11/01/2005 10:46:01		T1	DOC	Inexist.
11/01/2005 10:57:49	11/01/2005 10:58:07	T0	DOC	Error 12

## Descripciones de los campos

### Nombre de dominio de políticas

Especifica el nombre del dominio de políticas al que está asignada la planificación.

### Nombre de la planificación

Especifica el nombre de la planificación que ha iniciado este evento.

### Nombre del nodo

Especifica el cliente que está planificado para realizar la operación.

### Inicio planificado

Especifica la fecha y hora de inicio planificadas para el evento.

### Inicio real

Especifica la fecha y hora en las que el cliente ha iniciado el proceso de la operación planificada. No se visualizará ninguna información si la operación planificada no se ha iniciado.

### Hecho

Especifica la fecha y hora en que se ha completado el evento planificado.

### Estado

Especifica el estado del evento en el momento de emitirse el comando QUERY EVENT. Son posibles los siguientes valores:

#### Hecho

Especifica que el evento planificado se ha completado.

#### No válido

Especifica que el cliente informa de un error al ejecutar la operación planificada y los reintentos sucesivos han fallado.

#### Error; no se ha reiniciado

Especifica un estado intermedio, cuando se interrumpe una sesión de cliente a causa de un error de comunicaciones o de haber excedido el tiempo de espera en el servidor. Cuando el evento se completa, este estado se puede modificar a un estado final de "Completado" o "Error".

#### Futuro

Especifica que el inicio del margen de puesta en marcha de los eventos es en el futuro. Este estado también indica que todavía no se ha creado un registro para este evento.

#### En curso

Especifica que el evento planificado se está ejecutando y que aún no ha informado del estado de finalización al servidor.

Compruebe periódicamente el estado de finalización del evento planificado. Si el estado no se actualiza en un período de tiempo razonable, consulte los archivos dsmsched.log y dsmererror.log del cliente para determinar porqué el cliente no ha informado del resultado de este evento al servidor. Si la copia de seguridad planificada es anómala, vuelva a ejecutar el evento planificado o realice una copia de seguridad incremental manual para asegurar la copia de seguridad de los datos.

#### No hecho

Especifica que el margen de puesta en marcha planificado para este evento ha pasado y la planificación no ha comenzado.

#### Pendiente

Especifica que el mandato QUERY EVENT se ha emitido durante el margen de puesta en marcha del evento, pero que todavía no se ha iniciado el proceso de la operación planificada.

#### Reiniciado

Especifica que el cliente ha intentado procesar la operación planificada de nuevo.

#### Cortado

Especifica que las comunicaciones con el cliente se han cortado antes de que el evento pudiera realizarse.

#### Iniciado

Especifica que el evento ha empezado a procesarse.

#### Incierto

Especifica que el estado del evento no se puede determinar. El servidor especifica *Incierto* si el comando QUERY EVENT no encuentra un registro de eventos. No se encontrará un registro de eventos si el registro se ha suprimido o si el servidor

no estaba disponible durante el margen de puesta en marcha planificado (la planificación no se ha iniciado en ningún momento). Los registros con el estado `Incierto` no se almacenan en la base de datos. Si no desea que se visualicen estos registros, especifique `EXCEPTIONSONLY=YES` o suprima la planificación si ya no la necesita.

Atención: Cuando se procesa una operación planificada sin haberla reiniciado dentro de su duración especificada, el campo Estado muestra `Iniciado`. Si la operación continúa más allá de la duración especificada, no se crea ningún registro de eventos. Si se emite una consulta una vez transcurrida la duración especificada, se mostrará el estado `Error` aunque la operación se encuentre todavía en ejecución. Una vez completada la operación, se crea un registro de eventos y la consulta posterior muestra el resultado en el campo de estado.

#### Resultado

Especifica el código de retorno del cliente que indica si la planificación se ha procesado correctamente. Si el código de retorno es un valor distinto a cero, consulte el registro de actividades del servidor, el registro de errores del cliente y el registro de planificación.

Código de retorno	Explicación
0	Todas las operaciones se han completado correctamente.
4	La operación se ha completado correctamente, pero algunos archivos no se han procesado.
8	La operación se ha completado con al menos un mensaje de aviso.
12	La operación se ha completado con al menos un mensaje de error. El número de mensajes de error no incluye ninguna notificación acerca de archivos omitidos.
-99	La operación ha fallado debido a que la sesión entre el cliente y el servidor ha finalizado por un motivo desconocido. Se desconoce si el cliente puede volver a conectarse con el servidor para completar el suceso de planificación.

Si una planificación incluye el parámetro `ACTION=COMMAND`, y el mandato no es un mandato de IBM Spectrum Protect, este puede producir otros valores en el campo Resultado.

#### Motivo

Especifica el motivo del código de retorno.

## QUERY EVENT (Visualizar planificaciones de eventos de administración)

Utilice el comando `QUERY EVENT` para visualizar los eventos planificados y que se han completado para las planificaciones de comandos de administración seleccionadas.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query EVent--nombre_planificación--Type---Administrative-->
  .-BEGINDate---fecha_actual-.  .-BEGINTime---00:00-.
>+-----+-----+-----+-----+-----+-----+-----+-----+
  '-BEGINDate---fecha-----'  '-BEGINTime---hora--'

  .-ENDDate---fecha_inicial-.  .-ENDTime---23:59-.
>+-----+-----+-----+-----+-----+-----+-----+-----+
  '-ENDDate---fecha-----'  '-ENDTime---hora--'

  .-EXceptiononly---No------.
>+-----+-----+-----+-----+-----+-----+-----+-----+
  '-EXceptiononly---No---+'
                               '-Yes-'

  .-Format---Standard------.
>+-----+-----+-----+-----+-----+-----+-----+-----+
  '-Format---Standard-+'
                               '-Detailed-'
```

### Parámetros

nombre\_planificación (Obligatorio)

Especifica el nombre de la planificación para la que se visualizan eventos. Puede utilizar caracteres comodín para especificar nombres.

Type=Administrative (Necesario)

Especifica que la consulta visualiza los eventos de las planificaciones de comando de administración.

BEGINDate

Especifica la fecha inicial del rango horario de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es la fecha actual.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7.  Para consultar los eventos que estaban planificados para iniciarse durante los últimos siete días, especifique BEGINDATE=TODAY-7 ENDDATE=TODAY o BEGINDATE=-7 ENDDATE=TODAY.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio esté planificado para esta hora. Este parámetro es opcional. El valor predeterminado es 00:00.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW+03:00 o BEGINTIME=+03:00. IBM Spectrum Protect visualizará los eventos a las 12:00 en la fecha de inicio especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00.  Si emite este a las 9:00 para consultar los eventos que estaban planificados para iniciarse durante las últimas 4 horas, puede especificar BEGINTIME=NOW-04:00 ENDTIME=NOW o BEGINTIME=-04:00 ENDTIME=NOW. IBM Spectrum Protect visualizará los eventos a las 5:00 en la fecha de inicio especificada.

ENDDate

Especifica la fecha final del rango horario para los eventos que se han de visualizar. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. Para el parámetro BEGINDATE, se utiliza el valor predeterminado.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-8 o -8.  Para consultar los eventos planificados para iniciarse durante una semana que terminaba ayer, puede especificar BEGINDATE=TODAY-8 ENDDATE=TODAY-1 o BEGINDATE=-8 ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final del rango de los eventos que se visualizan. Se visualizarán todos los eventos cuyo inicio está planificado a dicha hora. Este parámetro es opcional. El valor predeterminado es 23:59.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 para consultar los eventos que estaban planificados para iniciarse dentro de 3 horas, puede especificar BEGINTIME=NOW ENDTIME=NOW+03:00 o BEGINTIME=NOW ENDTIME=+03:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-04:00 o -04:00

#### EXceptiononly

Especifica el tipo de información que desea sobre los eventos planificados o completados. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que se visualizará información sobre eventos pasados y proyectados.

Yes

Especifica que se visualizan los eventos que no se han podido ejecutar según estaba planificado.

#### Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualiza información parcial acerca de los eventos.



## Detailed

Especifica que se visualiza información completa acerca de los eventos.

## Ejemplo: obtener una lista de los eventos de una planificación de administración específica

Visualizar información parcial para todos los eventos planificados para la planificación de administración denominada DOSADMIN. La consulta se limitará a los eventos planificados para el 30 de marzo de 1999 (03/30/1999). Emita el comando:

```
query event dosadmin type=administrative
begindate=03/30/1999
enddate=03/30/1999
```

Inicio planificado	Inicio real	Nombre archivos	Estado del cliente
03/30/1999 00:00:00	03/30/1999 00:00:01	DOSADMIN	Hecho
03/30/1999 04:00:00	03/30/1999 04:00:01	DOSADMIN	Hecho
03/30/1999 12:00:00		DOSADMIN	Futuro
03/30/1999 16:00:00		DOSADMIN	Futuro

## Descripciones de los campos

### Inicio planificado

Especifica la fecha y hora de inicio planificadas para el evento.

### Inicio real

Especifica la fecha y hora en las que el cliente ha iniciado el proceso de la operación planificada. No se visualizará información si no se ha comenzado la ejecución de la planificación.

### Nombre de la planificación

Especifica el nombre de la planificación que ha iniciado este evento.

### Estado

Para los comandos de administración o scripts donde se especifique WAIT=YES, el estado de un evento planificado es STARTED hasta que la operación especificada mediante el comando o el script finalice. El estado final del evento planificado depende del código de retorno de la operación. Sin embargo, si WAIT=YES y la planificación ejecuta un script donde se especifica PREVIEW=YES, el estado final es COMPLETED, a menos que el script contenga un error de sintaxis.

Para los comandos de administración o scripts donde se especifique WAIT=NO, el estado de un evento planificado es COMPLETED si el comando o el script se ha iniciado. El éxito de la planificación dependerá del éxito de la operación realizada con el comando o con el script.

## QUERY EVENTRULES (Consultar reglas para eventos de servidor o de cliente)

Utilice este mandato para visualizar el archivo histórico de los eventos que un receptor especificado ha activado o desactivado para el servidor o para un nodo de cliente.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query--EVENTRULES-----*-----><
| .,-----|
| v |-----|
| +--CONSOLE-----+-----+
| +-ACTLOG-----+
| +-EVENTSERVER----+
| +-FILE-----+
| +-FILETEXT-----+
| | (1) |
| +-NTEVENTLOG-----+
| | (2) |
| +-SYSLOG-----+
| +-TIVOLI-----+
| '-USEREXIT-----'
+--NODEname-----nombre_nodo-----+
```

'-SERVername---nombre\_servidor-'

Notas:

1. Este parámetro sólo está disponible para el sistema operativo Windows.
2. Este parámetro solo está disponible para el sistema operativo Linux.

## Parámetros

---

receptores

Especifica el nombre de uno o varios receptores para eventos activados. Este parámetro es opcional.

Puede utilizar un carácter comodín para especificar todos los receptores.

Los valores válidos son:

CONSOLE

Especifica la consola estándar del servidor como receptor.

ACTLOG

Especifica las anotaciones de actividades de IBM Spectrum Protect como receptor.

EVENTSERVER

Especifica el servidor de eventos como receptor.


FILE


Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es un registro del archivo y no le resultará fácil a cualquier persona el leerlo.


FILETEXT

Especifica un archivo de usuario como receptor. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

 Sistemas operativos WindowsNTEVENTLOG

 Sistemas operativos WindowsEspecifica las anotaciones de aplicaciones de Windows como receptor.

 Sistemas operativos LinuxSYSLOG

 Sistemas operativos LinuxEspecifica el registro del sistema Linux como receptor.

TIVOLI

Especifica Tivoli Management Environment (TME) como receptor.

USEREXIT

Especifica como receptor una rutina escrita por el usuario donde IBM Spectrum Protect graba la información.

NODENAME

Especifica un nombre de nodo a consultar. Puede utilizar un carácter comodín para especificar un nombre. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para las reglas de eventos para el servidor donde se ejecuta este comando.

SERVER

Especifica el nombre de servidor que se va a consultar. Puede utilizar un carácter comodín para especificar un nombre. Puede especificar NODENAME o SERVERNAME. Si no se especifica ninguno de los parámetros, la consulta es para las reglas de eventos para el servidor donde se ejecuta este comando.

## Ejemplo: visualizar el historial de los eventos de cliente para la consola del servidor

---

Visualizar la información histórica de eventos de clientes activados o desactivados para la consola del servidor y los receptores de anotaciones de actividades.

```
query eventrules console,actlog nodename=*
```

Fecha/hora	Reglas eventos cliente
29/05/97 13:39:58	ENABLE EVENTS CONSOLE ANE4001 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4962 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4963 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4965 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4966 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4967 NODENAMES=JEE
30/05/97 13:46:25	DISABLE EVENTS ACTLOG ANE4968 NODENAMES=JEE
30/05/97 14:24:20	ENABLE EVENTS CONSOLE ANE4015 NODENAMES=RON
30/05/97 14:24:50	ENABLE EVENTS CONSOLE ANE4026 NODENAMES=DONNA
30/05/97 14:25:59	ENABLE EVENTS CONSOLE ANE4015 NODENAMES=DONNA

## Ejemplo: visualizar el historial de los eventos de cliente para todos los receptores

---

Visualizar la información histórica de los eventos del servidor activados o desactivados para todos los receptores.

```
query eventrules
```

```
Fecha/hora          Reglas eventos servidor
-----
22/05/97 14:35:13  ENABLE EVENTS CONSOLE ANR2578
30/05/97 14:29:31  ENABLE EVENTS CONSOLE ANR0272
30/05/97 14:31:46  ENABLE EVENTS USEREXIT ANR0130
30/05/97 14:31:54  ENABLE EVENTS USEREXIT ANR0131
30/05/97 14:50:28  ENABLE EVENTS USEREXIT ANR0266
```

## Descripciones de los campos

### Date/Time

Especifica la fecha y hora en que se ha habilitado o inhabilitado el evento.

### Reglas de eventos de cliente

Especifica los eventos de cliente que se habilitaron o inhabilitaron para los receptores especificados.

### Reglas de eventos de servidor

Especifica los eventos de servidor que se habilitaron o inhabilitaron para los receptores especificados.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY ENABLED

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE EVENTS	Inhabilita eventos específicos para receptores.
ENABLE EVENTS	Habilita eventos específicos para receptores.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY ENABLED	Visualiza los eventos activados o desactivados para un servidor específico.

## QUERY EVENTSERVER (Consultar el servidor de eventos)

Utilice este comando para visualizar el nombre del servidor de eventos.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query EVENTSERVER-----<<
```

### Ejemplo: visualizar el nombre del servidor de eventos

Visualizar el nombre del servidor de eventos.

```
query eventserver
```

```
ANR1669I Está definido como el servidor de eventos.
```

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY EVENTSERVER

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DEFINE EVENTSERVER	Define un servidor como un servidor de eventos.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.



ejecución correspondiente al número de proceso. Si no se especifica PROCESS, IBM Spectrum Protect mostrará información acerca de todas las operaciones de exportación de servidor a servidor. No puede especificar este parámetro si especifica un identificador de exportación o si especifica el parámetro STATE con un valor de SUSPENDED.

#### Format

Este parámetro opcional especifica cómo se ha de visualizar la información. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial sobre las operaciones de exportación especificadas.

#### Detailed

Cuando se especifica, visualiza toda la información disponible relacionada con las operaciones de exportación.

## Ejemplo: visualizar las operaciones de exportación en ejecución y suspendidas

Mostrar una lista con la información sobre todas las operaciones de exportación en ejecución y suspendidas. Emita el comando siguiente:

```
query export state=all
```

Identificador exportación	Hora inicio	Estado	ID de proceso	Comando
MYEXPORTNODE	01/24/2007 10:30:03	Suspendido	--	Export NODE me,you,them filespace=c\$ nametype=unicode filedata=all durunits=indefinite toserver=athens exportid=MYEXPORTNODE
EXPORT_HOME_DIRS	01/25/2007 09:30:03	Ejecutando	11	Export NODE n2,n3,n4 filespace=/home nametype=server filedata=all durunits=indefinite toserver=athens exportid=EXPORT_HOME_DIRS
EXPORT_NODE_0001	01/25/2007 14:30:33	Ejecutando, Suspendible	--	Export NODE n5,n6,n7 filespace=d\$ nametype=unicode filedata=archive durunits=indefinite toserver=athens

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información acerca de una operación de exportación en ejecución

Visualizar información acerca de la operación de exportación actualmente en ejecución que tiene el número de proceso "7". Emita el comando siguiente:

```
query export process=7
```

Identificador exportación	Hora inicio	Estado	ID de proceso	Comando
MYEXPORTNODE	01/24/2007 10:30:03	Ejecución	7	Export NODE me,you,them filespace=c\$ nametype=unicode filedata=all toserver=athens exportid=MYEXPORTNODE

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información detallada acerca de todas las operaciones de exportación suspendidas.

Mostrar una lista con la información sobre todas las operaciones de exportación suspendidas. Emita el comando siguiente:

```

query export state=suspended format=detailed

Identificador de exportación : MyExportNode
Hora de inicio : 24/01/2007 10:30:03
Estado : Suspending
ID de proceso : --
Mandato: Export NODE m* filespace=c$
        nametype=unicode
        filedata=all
        durunits=indefinite
        toserver=athens
Fase : Lista de archivos
        finalizada. Exportando
        archivos seleccionables
Tiempo total de ejecución : 3 días 0 horas 24 minutos
Tiempo de ejecución del proceso actual :
Número de reinicios de operación
        de exportación : 0
Fecha y hora del último reinicio : --
Fecha y hora de la última suspensión : 25/01/2007 08:30:11
Dominios de políticas exportados : 0
Juegos de políticas exportados : 0
Planificaciones exportadas : 0
Clases de gestión exportadas : 0
Grupos de copia exportados : 0
Administradores exportados : 1
Conjuntos de opciones exportados : 0
Definiciones de nodos exportadas : 3
Definiciones de espacios de archivos exportadas : 7
Copias archivadas exportadas : 50.000
Archivos de copia de seguridad exportados : 150.000
Archivos bajo gestión de espacio exportados : 0
Copias archivadas omitidas : 0
Archivos de copia de seguridad omitidos : 25
Archivos bajo gestión de espacio omitidos : 0
Número total de bytes transferidos (MB) : 7.000
Número total de archivos por transferir : 900.000
Archivos restantes : 700.000

```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información acerca de las operaciones de exportación de servidor a servidor

Mostrar una lista con la información detallada sobre todas las operaciones de exportación de servidor a servidor en ejecución. Emita el comando siguiente:

```

query export state=running format=detailed

Identificador de exportación : export_HOME_Dirs
Hora de inicio : 25/01/2007 09:30:03
Estado : Ejecutando
ID de proceso : 11
Comando: Export NODE n2,n3,n4
        filespace=/home nametype=
        server
        filedata=all
        toserver=athens
Fase : Identificando y exportando
        archivos seleccionables
Tiempo total de ejecución : 0 días 22 horas 0
        minutos
Tiempo de ejecución del proceso actual : 01:30:00
Número de reinicios de operación de exportación: 4
Fecha y hora del último reinicio : 01/02/2007 11:00:03
Fecha y hora de la última suspensión : 31/01/2007 05:01:00
Dominios de políticas exportados : 0
Juegos de políticas exportados : 0
Planificaciones exportadas : 0
Clases de gestión exportadas : 0
Grupos de copia exportados : 0
Administradores exportados : 1
Conjuntos de opciones exportados : 0
Definiciones de nodos exportadas : 3
Definiciones de espacios de archivos exportadas : 7
Copias archivadas exportadas : 0
Archivos de copia de seguridad exportados : 1000

```

Archivos bajo gestión de espacio exportados : 0  
Copias archivadas omitidas : 0  
Archivos de copia de seguridad omitidos : 0  
Archivos bajo gestión de espacio omitidos : 0  
Número total de bytes transferidos (MB) : 50  
Número total de archivos por transferir : 400.000  
Archivos restantes : 399.000

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

### Identificador de exportación

Identificador exclusivo asignado a esta operación de exportación de servidor a servidor.

### Hora inicio

Hora y fecha en que se inició esta operación de exportación.

### Estado

Estado actual de esta operación de exportación. El valor puede ser uno de los siguientes:

#### Ejecutando -- no suspendible

La operación está activa y está transmitiendo definiciones al servidor de destino. El proceso no se puede suspender y, si falla en este estado, no podrá reiniciarlo.

#### Ejecutando

La operación está activa y está buscando archivos seleccionables o bien transmitiendo definiciones al servidor de destino.

#### En ejecución - suspensión en curso

La operación está en proceso de ser suspendida como resultado de un comando SUSPEND EXPORT. La operación de exportación está completamente suspendida cuando se guardan todos los datos de la operación de exportación. Una operación de exportación en este estado no responde a los comandos siguientes:

- CANCEL PROCESS
- CANCEL EXPORT
- RESTART EXPORT
- SUSPEND EXPORT

#### Suspendido

La operación ha dejado de ejecutarse debido a un error o a que se ha suspendido con el comando SUSPEND EXPORT.

### ID de proceso

El ID de proceso para la operación de exportación cuando el estado es "Inicializando" o "Ejecutando".

### Comando

Comando completo que se ha emitido para iniciar esta exportación de servidor a servidor.

### Fase

Paso actual que está llevando a cabo la operación. Las fases posibles se muestran en el orden en el que se realizan:

#### Creando definiciones en el servidor de destino

La operación está exportando definiciones. El proceso no se puede suspender. Si el proceso falla en esta fase, no se podrá reiniciar.

#### Identificando y exportando archivos seleccionables

La operación está creando una lista de archivos seleccionables para exportarlos. Algunos archivos también se puede transmitir al destino en esta fase. Un proceso que está en esta fase se puede suspender. Si el proceso falla en esta fase, se podrá reiniciar.

#### Lista de archivos finalizada. Exportando archivos seleccionables

La operación ha acabado de crear la lista de archivos seleccionables para la exportación y está transmitiendo los archivos al destino. Un proceso que está en esta fase se puede suspender. Si el proceso falla en esta fase, se podrá reiniciar.

### Tiempo total de ejecución

Tiempo que ha tardado en ejecutarse esta operación de exportación de servidor a servidor. Por ejemplo, si esta operación se inició y luego se suspendió y se inició dos veces, este valor corresponde al tiempo de ejecución total de los tres procesos activos de la operación de exportación.

### Tiempo de ejecución de proceso actual

Tiempo que ha tardado en ejecutarse el proceso activo de una operación de exportación de servidor a servidor. No se visualizará ningún valor para una operación suspendida, pues no existe ningún proceso activo.

### Cuenta de reinicio de operación de exportación

Número de veces que la operación de exportación de servidor a servidor se ha reiniciado.

### Fecha y hora del último reinicio

Fecha y hora de la última vez que esta operación de exportación de servidor a servidor se ha reiniciado.

### Fecha y hora de la última suspensión

Fecha y hora de la última vez que esta operación de exportación de servidor a servidor se ha suspendido.

Dominios de políticas exportados  
Número de definiciones de dominios de políticas que se han exportado correctamente al servidor de destino.

Juegos de políticas exportados  
Número de definiciones de juegos de políticas que se han exportado correctamente al servidor de destino.

Planificaciones exportadas  
Número de definiciones de planificaciones que se han exportado correctamente al servidor de destino.

Clases de gestión exportadas  
Número de definiciones de clases de gestión que se han exportado correctamente al servidor de destino.

Grupos de copia exportados  
Número de definiciones de grupos de copia que se han exportado correctamente al servidor de destino.

Administradores exportados  
Número de definiciones de administradores que se han exportado correctamente al servidor de destino.

Conjuntos de opciones exportados  
Número de definiciones de conjuntos de opciones que se han exportado correctamente al servidor de destino.

Definiciones de nodos exportadas  
Número de definiciones de nodos que se han exportado correctamente al servidor de destino.

Definiciones de espacio de archivos exportadas  
Número de definiciones de espacios de archivos que se han exportado correctamente al servidor de destino.

Copias archivadas exportadas  
Número de copias archivadas que se han exportado correctamente al servidor de destino.

Archivos de copia de seguridad exportados  
Número de archivos de copia de seguridad que se han exportado correctamente al servidor de destino.

Archivos bajo gestión de espacio exportados  
Número de archivos bajo gestión de espacio que se han exportado correctamente al servidor de destino.

Copias archivadas omitidas  
Número de copias archivadas que se podían seleccionar para la exportación pero que se han omitido.

Archivos de copia de seguridad omitidos  
Número de archivos de copia de seguridad que se podían seleccionar para la exportación pero que se han omitido.

Archivos bajo gestión de espacio omitidos  
Número de archivos bajo gestión de espacio que se podían seleccionar para la exportación pero que se han omitido.

Número total de bytes transferidos (MB)  
Número total de bytes transmitidos hasta el momento al servidor de destino en esta operación de exportación.




Número total de archivos por transferir  
Número total de archivos transmitidos hasta el momento al servidor de destino en esta operación de exportación.

Archivos restantes  
Número total de archivos que quedan por transmitir al servidor de destino en esta operación de exportación.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY EXPORT

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL EXPORT	Suprime una operación de exportación suspendida.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
IMPORT NODE	Restaura información de nodo cliente desde medios externos.
IMPORT SERVER	Restaura todo o una parte del servidor desde un medio externo.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY EXTENTUPDATES (Consultar extensiones de datos actualizadas)



Utilice este mandato para visualizar información sobre las actualizaciones de las extensiones de datos en las agrupaciones de almacenamiento de contenedores de directorio y para determinar qué extensiones de datos se suprimen y cuáles son elegibles para supresión.

## Clase de privilegio

---

Cualquier administrador puede emitir este mandato.

## Sintaxis

---

```
>>-Query EXTENTUPDates--nombre_agrupación-----><
```

## Parámetros

---

nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que se consulta. No puede utilizar caracteres comodín para especificar este nombre.

## Ejemplo: visualizar información sobre las actualizaciones de las extensiones de datos

---

Visualice información sobre las actualizaciones de las extensiones de datos emitiendo el siguiente comando:

```
query extentupdates
```

```
    Número de extensiones pendientes de actualización: 0
    Número de extensiones no referenciadas: 0
    Número de extensiones elegibles para su supresión: 0
    Retardo de reutilización de extensión (días): 1
```

Consulte Descripciones de los campos para ver una descripción de los campos.

## Descripciones de los campos

---

Número de extensiones pendientes de actualización

Especifica el número de referencias de extensión de datos que están pendientes de actualización en la agrupación de almacenamiento de contenedores de directorio. Los datos que se almacenan en la agrupación de almacenamiento de contenedores de directorio aumentan el número de referencias y la supresión de datos disminuye el número de referencias.

Número de extensiones no referenciadas

Especifica el número de extensiones de datos a las que no se hace referencia en la agrupación de almacenamiento de contenedores de directorio. Puede suprimir las extensiones de datos si no se hace referencia a ellas de nuevo en el periodo de retardo de reutilización que se especifica en el comando DEFINE STGPOOL.

Número de extensiones elegibles para su supresión

Especifica el número de extensiones de datos que pueden suprimirse de la agrupación de almacenamiento. Las extensiones de datos exceden el periodo de retardo de reutilización que se ha especificado en el comando DEFINE STGPOOL.

Retardo de reutilización de extensión (días)

Especifica el periodo de retardo de reutilización, en días, de las extensiones de datos.

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con QUERY EXTENTUPDATES

Comando	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.

## QUERY FILESPACE (Consultar uno o más espacios de archivos)

---

Utilice este comando para visualizar información acerca de los espacios de archivos que pertenecen a un nodo cliente. La salida de este mandato incluye los resultados de la última copia de seguridad incremental o réplica.



Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente cualificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

**SERVER**

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

**UNICODE**

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

**FSID**

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

**CODEType**

Especifique qué tipo de espacios de archivos deben incluirse en la operación. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

**UNICODE**

Incluir sólo los espacios de archivos que están en Unicode.

**NONUNICODE**

Incluir sólo los espacios de archivos que no están en Unicode.

**BOTH**

Incluir espacios de archivos independientemente del tipo de página de códigos.

## Ejemplo: obtener una lista de todos los espacios de archivos

Consultar todos los espacios de archivos que están asociados con todos los nodos cliente.

```
query filesystem
```

Nombre	Nombre esp.	FSID	Plataforma	Tipo esp.	¿Es el	Capacidad %		
Nombre	Nombre			Tipo	Espacio de archivos	Unicode?		Util
JOE	\\joe\c\$	1	WinNT	NTFS	Si	2.502,3	75,2	
JOE	\\joe\d\$	2	WinNT	NTFS	Si	6.173,4	59,6	

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información de espacio de archivos detallada acerca de un espacio de archivos virtual

Visualizar información detallada para el espacio de archivos /HomeDir, que es una correlación de espacio de archivos virtual y que pertenece al nodo NAS NAS1.

```
query filesystem nas1 /HomeDir
```

Nombre	Nombre esp.	FSID	Plataforma	Tipo esp.	¿Es el	Capacidad %		
Nombre	Nombre			Tipo	Espacio de archivos	Unicode?		Util
NAS1	/HomeDir	1	NetApp	WAFL (VFS)	No	2.502,3	75,2	

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Importante: Es posible que no vea los resultados esperados después de solicitar un formato detallado porque la aplicación de la API debe completar varios campos. Estos campos incluyen:

- Tipo de espacio de archivos
- Plataforma
- Capacidad
- Pct. util
- Fecha/hora inicio última copia seguridad
- Fecha/hora finalización última copia de seguridad

Para obtener más información sobre los campos específicos actualizados por la API, consulte la publicación *IBM Spectrum Protect: Utilización de la interfaz de programación de aplicaciones*.

## Ejemplo: visualizar información de espacio de archivos detallada acerca de un espacio de archivos y nodo específicos

---

Visualizar información detallada acerca del espacio de archivos \\joe\c\$ que pertenece al nodo cliente JOE.

```
query filesystem joe \\joe\c$ nametype=unicode format=detailed

Nombre nodo: JOE
Nombre espacio archivos: \\joe\c$
Nombre esp. archivos hexadecimal: 5c5c6a6f655c6324
FSID: 1
Nombre del grupo de proximidad: FSGRP1
Plataforma: WinNT
Tipo espacio archivos: NTFS
¿Es el esp. de archivos Unicode?: Sí
Capacidad: 2.502,3
Pct. Util: 75,2
Fecha/hora inicio última copia seguridad:
Días desde inicio última copia de seguridad:
Fecha/hora finalización última copia seguridad:
Días desde finalización última copia seguridad:
Fecha/hora inicio última réplica: 12/02/2012, 12:42:00
Días desde inicio última réplica de nodo: 30
Fecha/hora finalización última réplica: 12/02/2012, 12:42:00
Días desde finalización última réplica: 30
Fecha/hora última copia de seguridad de cliente (UTC): 02/06/2013, 09:10:00
Fecha/hora último archivado de cliente (UTC): 02/06/2013, 09:10:00
Nombre de regla de réplica de copia de seguridad: ACTIVE_DATA
Estado de regla de réplica de copia de seguridad: ENABLED
Nombre de la regla de réplica de archivado: DEFAULT
Estado de regla de réplica de archivado: ENABLED
Nombre de regla de réplica de gestión de espacio: NONE
Estado de regla de réplica de gestión de espacio: DISABLED
En Tipo de riesgo: intervalo personalizado
Intervalo de riesgo : 2,222
Fuera de servicio: No
Fecha de fuera de servicio:
Dirección MAC:
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

Importante: Es posible que no vea los resultados esperados después de solicitar un formato detallado porque la aplicación de la API tiene que completar varios campos. Estos campos incluyen:

- Tipo espacio archivos
- Plataforma
- Capacidad
- Pct. util
- Fecha/hora inicio última copia seguridad
- Fecha/hora finalización última copia de seguridad

Para obtener más información sobre los campos específicos actualizados por la API, consulte la publicación *IBM Spectrum Protect: Utilización de la interfaz de programación de aplicaciones*.

Nombre del nodo

Especifica el nombre del nodo cliente.

Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de

códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Nombre espacio archivos hexadecimal

Especifica el nombre hexadecimal del espacio de archivos para el nodo cliente en formato UTF-8.

FSID

Especifica el identificador del espacio de archivos.

Nombre de grupo de proximidad

Nombre del grupo de proximidad, si lo hay, al que pertenece el espacio de archivos.

Plataforma

Especifica la plataforma del nodo cliente.

Tipo espacio archivos

Especifica el tipo del espacio de archivos.

El tipo de espacio de archivos con la agregación "(VFS)" denota que se trata de una asignación de espacio de archivos virtual para una ruta de directorio de un dispositivo NAS.

Espacio de archivos Unicode

Indica si el espacio de archivos es Unicode.

Capacidad

Especifica la cantidad de espacio, en megabytes, asignado a este espacio de archivos en el nodo cliente.

Para un espacio de archivos virtual que es una asignación de espacio de archivos virtual para una ruta de directorio, este campo representa la capacidad del espacio de archivos en el que se encuentra la ruta de directorio.

Pct. util

Especifica el porcentaje del espacio de archivos que está ocupado.

Para un espacio de archivos virtual que es una asignación de espacio de archivos virtual para una ruta de directorio, el porcentaje utilizado se calcula como el porcentaje de la capacidad del espacio de archivos que ocupaba el directorio en el momento de la última copia de seguridad completa.

Fecha/hora inicio última copia seguridad

Especifica la fecha y hora de inicio de la última copia de seguridad incremental del espacio de archivos.

Días desde inicio última copia seguridad

Especifica el número de días desde el inicio de la última copia de seguridad incremental del espacio de archivos.

Fecha/hora finalización última copia de seguridad

Especifica la fecha y hora de terminación de la última copia de seguridad incremental del espacio de archivos.

Días desde finalización última copia seguridad

Especifica el número de días desde que se terminó la última copia de seguridad incremental del espacio de archivos.

Fecha/hora inicio última réplica

Especifica la fecha y la hora en que se ha iniciado la última réplica de espacio de archivos.

Días desde inicio última réplica

Especifica el número de días desde que se ha iniciado la última réplica de espacio de archivos

Fecha/hora finalización última réplica

Especifica la fecha y la hora en que ha finalizado la última réplica de espacio de archivos.

Días desde finalización última réplica

Especifica el número de días desde que ha finalizado la última réplica de espacio de archivos

Fecha/hora última copia de seguridad de cliente (UTC)

La fecha y la hora, en hora UTC (Hora universal coordinada), de la última operación de copia de seguridad de este espacio de archivos.

Fecha/hora último archivado de cliente (UTC)

La fecha y la hora, en hora UTC (Hora universal coordinada), de la última operación de archivado de este espacio de archivos.

Nombre de norma de réplica de copia de seguridad

Especifica la regla de réplica que se aplica a los datos de copia de seguridad en el espacio de archivos. Son posibles los siguientes valores:

ALL\_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

ACTIVE\_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.

- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

#### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica `ACTIVE_DATA` excepto que los datos se replican con una prioridad alta.

#### DEFAULT

Replica los datos de seguridad según la regla del cliente de nodo para los datos de seguridad. Si la regla del cliente para los datos de seguridad es `DEFAULT`, los datos de seguridad se replican según la regla del servidor para los datos de seguridad.

#### NONE

Los datos de copia de seguridad en el espacio de archivos no se replican.

#### Estado de norma de réplica de copia de seguridad

Especifica si la réplica de los datos de copia de seguridad en el espacio de archivos está activada o desactivada. Si el estado es `ENABLED`, los archivos de copia de seguridad pueden replicarse. Si el estado es `DISABLED`, los archivos de copia de seguridad no pueden replicarse.

#### Nombre de norma de réplica archivada

Especifica la regla de réplica que se aplica a los datos de archivado en el espacio de archivos. Son posibles los siguientes valores:

#### ALL\_DATA

Replica los datos de archivado. Los datos se replican con una prioridad normal.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de archivado. Los datos se replican con una prioridad alta.

#### DEFAULT

Replica los datos de archivado según la regla del cliente para los datos de archivado. Si la regla del cliente para los datos de archivado es `DEFAULT`, los datos de archivado se replican según la regla del servidor para los datos de archivado.

#### NONE

Los datos de archivado en el espacio de archivos no se replican.

#### Estado de norma de réplica archivada

Especifica si la réplica de los datos de archivado en el espacio de archivos está activada o desactivada. Si el estado es `ENABLED`, los archivos de archivado pueden replicarse. Si el estado es `DISABLED`, los archivos de archivado no pueden replicarse.

#### Nombre de norma de réplica de gestión de espacio

Especifica la regla de réplica que se aplica a los datos gestionados por espacio en el espacio de archivos. Son posibles los siguientes valores:

#### ALL\_DATA

Replica los datos gestionados por espacio. Los datos se replican con una prioridad normal.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos gestionados por espacio. Los datos se replican con una prioridad alta.

#### DEFAULT

Replica los datos gestionados por espacio según la regla del cliente para los datos gestionados por espacio. Si la regla del cliente para los datos gestionados por espacio es `DEFAULT`, los datos gestionados por espacio se replican según la regla del servidor para los datos gestionados por espacio.

#### NONE

Los datos gestionados por espacio en el espacio de archivos no se replican.

#### Estado de norma de réplica de gestión de espacio

Especifica si la réplica de los datos gestionados por espacio en el espacio de archivos está activada o desactivada. Si el estado es `ENABLED`, los archivos gestionados por espacio pueden replicarse. Si el estado es `DISABLED`, los archivos gestionados por espacio no pueden replicarse.

#### Tipo de riesgo

Especifica el tipo de evaluación de riesgo. Los valores pueden ser Predeterminado, Eludido o Personalizado. Predeterminado especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el mandato `SET STATUSATRISKINTERVAL`. Eludido especifica que el nodo no se evalúa para el estado de riesgo por el supervisor de estado. Personalizado indica que el nodo se evalúa con el intervalo que se ha especificado mediante el mandato `SET VMATRISKINTERVAL`, en lugar del intervalo que se ha especificado mediante el mandato `SET STATUSATRISKINTERVAL`.

#### Intervalo de riesgo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en peligro. Este campo se aplica sólo cuando el tipo de riesgo es Personalizado.

Fuera de servicio

Especifica si la máquina virtual que representa el espacio de archivos está fuera de servicio.

Fecha de fuera de servicio

Especifica la fecha en la que la máquina virtual que representa el espacio de archivos ha quedado fuera de servicio.

Dirección MAC

Especifica la dirección de control de acceso a soportes (MAC) de los espacios de archivos de los que se ha hecho copia de seguridad para las máquinas virtuales VMWare. En el caso de que la máquina virtual tenga varias direcciones MAC, esta es la dirección con el valor más bajo.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY FILESPACE

Comando	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
RENAME FILESPACE	Redenomina un espacio de archivos de cliente en el servidor.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## QUERY LIBRARY (Consultar una biblioteca)

Utilice este comando para visualizar la información sobre las bibliotecas.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
.*-----
>>-Query LIBRARY--+-+-----+----->
                    '-nombre_biblioteca-'

.-Format----Standard----.
>--+-+-----+-----<
    '-Format----+-Standard-+-'
        '-Detailed-'
```

### Parámetros

library\_name

Especifica el nombre de la biblioteca que se ha de consultar. Puede utilizar caracteres comodín para especificar los nombres. Este parámetro es opcional.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial sobre la biblioteca.

Detailed

Especifica que se visualizará información completa sobre la biblioteca.

## Ejemplo: visualizar información de resumen acerca de una biblioteca específica

---

Visualizar información acerca de la biblioteca denominada AUTO. Emita el comando:

```
query library auto
```

```
Nombre biblioteca: AUTO
Tipo biblioteca: SCSI
ID ACS:
Categoría privada:
Categoría reutilizable:
Categoría reutilizable WORM:
Gestor externo:
Compartido: No
Fuera de LAN:
Obedecer retención de montaje:
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: visualizar información de biblioteca detallada acerca de una biblioteca específica

---

Visualizar información detallada acerca de la biblioteca denominada EZLIFE. Emita el comando:

 Sistemas operativos Linux

```
query library ezlife format=detailed
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
Nombre biblioteca: EZLIFE
Tipo biblioteca: SCSI
ID ACS:
Categoría privada:
Categoría reutilizable:
Categoría reutilizable WORM:
Gestor externo:
Compartido: Sí
Fuera de LAN:
Obedecer retención de montaje:
Gestor de bibliotecas primario: EZSERVER
WWN:
Número de serie:
Etiquetado automático: OVERWRITE
Volver a etiquetar para reutilizar: Sí
Última actualización por (administrador): DOCTOR MIKE
Fecha/hora última actualización: 2002-12-05 15:24:53
```

 Sistemas operativos Windows

```
Nombre biblioteca: EZLIFE
Tipo biblioteca: SCSI
ID ACS:
Categoría privada:
Categoría reutilizable:
Categoría reutilizable WORM:
Gestor externo:
Compartido: Sí
Fuera de LAN:
Obedecer retención de montaje:
Gestor de bibliotecas primario: EZSERVER
WWN:
Número de serie:
Etiquetado automático: OVERWRITE
Restaurar unidades: No
Volver a etiquetar para reutilizar: Sí
Última actualización por (administrador): DOCTOR MIKE
Fecha/hora última actualización: 2000-12-05 15:24:53
```





Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

---

Nombre de biblioteca



- El nombre de la biblioteca.
- Tipo de biblioteca  
El tipo de la biblioteca.
- Identificador ACS  
Especifica que la biblioteca es una biblioteca StorageTek controlada mediante StorageTek ACSLS (Automated Cartridge System Library Software).
- Categoría privada  
El número de categoría para los volúmenes privados que deben montarse por nombre.  
  
La información que aparezca visualizada en este campo únicamente se aplica a un IBM® Tape Library Dataserver, modelo 3494 ó 3495.
- Categoría reutilizable  
El número de categoría que se utilizará para los volúmenes reutilizables de la biblioteca.  
  
La información que aparezca visualizada en este campo únicamente se aplica a un IBM Tape Library Dataserver, modelo 3494 ó 3495.
- Categoría reutilizable WORM  
Indica el número de categoría utilizado por los volúmenes reutilizables WORM en la biblioteca.  
  
La información que aparezca visualizada en este campo únicamente se aplica a un IBM Tape Library Dataserver, modelo 3494 ó 3495.
- Gestor externo  
La ubicación del gestor de bibliotecas externo donde el servidor puede enviar peticiones de acceso a medios.
- Compartido  
Especifica si esta biblioteca se comparte con otros servidores de IBM Spectrum Protect en la red de área de almacenamiento (SAN).
- Fuera de LAN  
Especifica si se utiliza una biblioteca externa para operaciones fuera de LAN.
- Obedecer retención de montaje  
Especifica si el servidor utiliza el valor definido para la retención de montaje en la clase de dispositivo asociada a esta biblioteca externa.
- Gestor de bibliotecas primario  
El nombre del servidor responsable del control del acceso a los recursos de biblioteca.
- WWN  
Nombre de ámbito universal del canal de fibra de la biblioteca.
- Número de serie  
Especifica el número de serie de la biblioteca que se está consultando.
- Etiquetado automático  
Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas.
-  Sistemas operativos AIX  Sistemas operativos Windows Restaurar unidades  
 Sistemas operativos AIX  Sistemas operativos Windows Especifica si el servidor realiza un restablecimiento del destino cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.
- Volver a etiquetar para reutilizar  
Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables.
- Última actualización por (administrador)  
Especifica quién ha realizado la última actualización de la biblioteca.
- Fecha/hora última actualización  
Fecha y hora en las que tuvo lugar la última actualización.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY LIBRARY

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE LIBRARY	Suprime una biblioteca.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.

Comando	Descripción
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

## QUERY LIBVOLUME (Consultar un volumen de biblioteca)

Utilice este comando para visualizar información acerca de uno o varios volúmenes que se han dado de alta en una biblioteca automatizada para que los utilice el servidor de IBM Spectrum Protect.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-*-----*. .-*-----*
>>-Query LIBVolume--+-----+----->
      '-nombre_biblioteca-' '-nombre_volumen-'

.-Format----Standard----.
>--+-----+-----><
      '-Format----+Standard+-'
          '-Detailed-'

```

### Parámetros

#### library\_name

Especifica el nombre de la biblioteca. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todas las bibliotecas.

#### nombre\_volumen

Especifica el nombre del volumen. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todos los volúmenes.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial.

##### Detailed

Especifica que se visualizará toda la información.

### Ejemplo: obtener una lista de los volúmenes dados de alta para una biblioteca específica

Visualizar información acerca de todos los volúmenes que se dan de alta en la biblioteca denominada TAPE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query libvolume tape
```

Nombre bibl.	Nombre vol.	Estado	Propiet.	Últ. util.	Elemento inicio	Tipo disposit.
TAPE	000114	Reutilizable			1.000	LTO
TAPE	NY1602	Reutilizable			1.001	DLT

### Ejemplo: visualizar información detallada acerca de una biblioteca específica

Visualizar la información detallada sobre un volumen denominado JJY008. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query libvolume jjy008 format=detailed
```

```

Nombre biblioteca: HPW3494
Nombre volumen: JJY008
Estado: Privado
Propietario: SUNSET
Última utilización: Datos

```

Elemento inicio:  
Tipo dispositivo:  
Limpiezas restantes:  
Tipo de medio:

## Descripciones de los campos

**Nombre de biblioteca**

El nombre de la biblioteca donde se encuentra el volumen de almacenamiento.

**Nombre de volumen**

El nombre del volumen de almacenamiento.

**Estado**

El estado del volumen de almacenamiento según el inventario de biblioteca. Si el estado es Privado, el volumen lo está utilizando IBM Spectrum Protect. Si el estado es Reutilizable, el volumen está disponible para ser utilizado.

**Propietario**

El servidor propietario del volumen, si el volumen es privado.

**Última utilización**

Tipo de datos del volumen. Este campo se aplica únicamente a los volúmenes en estado Privado. Para volúmenes de agrupación de almacenamiento, este campo muestra **Data**. Para los volúmenes de copia de seguridad de la base de datos (completa, incremental, de instantánea), este campo muestra **DbBackup**.

**Elemento inicial**

La dirección de elemento de la ranura de biblioteca que contiene el volumen.

**Tipo de dispositivo**

El tipo de dispositivo en el que se utiliza el volumen. Este campo sólo visualizará un valor para los volúmenes dados de alta en una biblioteca que tenga funciones de medios mixtas.

**Limpiezas restantes**

Para cartuchos de limpieza, el número de limpiezas restantes.

**Tipo de medio**

El tipo de medio que representa el volumen (por ejemplo, cinta de 8mm).

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY LIBVOLUME

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.

## QUERY LICENSE (Visualizar información sobre licencias)

Utilice este comando para visualizar la auditoría de licencias, los plazos de licencias y la información de conformidad.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

>>-Query LICense-----><

## Parámetros

---

Ninguno.

Para visualizar la información sobre licencia, emita el mandato siguiente:

```
query license
```

Se visualiza la salida de ejemplo siguiente:

```
ANR2017I El administrador SERVER_CONSOLE ha emitido el mandato: QUERY LICENSE
      Última auditoría licencia: 10/17/2016 14:28:08
      Número de Data Protection para Oracle en uso: 0
      Número de Data Protection for
      Oracle en evaluación con opción a compra: 0
      Número de Data Protection for Microsoft SQL en uso: 0
      Número de Data Protection for
      Microsoft SQL en evaluación con opción a compra: 0
      Número de Data Protection for
      Microsoft Exchange en uso: 0
      Número de Data Protection for
      MS Exchange en evaluación con opción a compra: 0
      Número de TDP para Lotus Notes en uso: 12
      Número de TDP para Lotus Notes en evaluación con opción a compra: 0
      Número de Data Protection for Lotus Domino en uso: 0
      Número de Data Protection for
      Lotus Domino en evaluación con opción a compra: 0
      Número de TDP para Informix en uso: 1
      Número de TDP para Informix en evaluación con opción a compra: 0
      Número de TDP para SAP R/3 en uso: 0
      Número de TDP para SAP R/3 en evaluación con opción a compra: 0
      Número de TDP para ESS en uso: 0
      Número de TDP para ESS en evaluación con opción a compra: 0
      Número de TDP para ESS R/3 en uso: 0
      Número de TDP para ESS R/3 en evaluación con opción a compra: 0
      Número de TDP para EMC Symmetrix en uso: 0
      Número de TDP para EMC Symmetrix en evaluación con opción a compra: 0
      Número de TDP para EMC Symmetrix R/3 en uso: 6
      Número de TDP para EMC Symmetrix R/3 en evaluación con opción a compra: 0
      Número de TDP para WAS en uso: 0
      Número de of TDP para WAS en evaluación con opción a compra: 0
      ¿Se está utilizando IBM Spectrum Protect for Data Retention?: No
      ¿Tiene licencia IBM Spectrum Protect for Data Retention?: Sí
      ¿Se está utilizando IBM Spectrum Protect Basic Edition?: Sí
      ¿Tiene licencia IBM Spectrum Protect Basic Edition?: Sí
      ¿Se está utilizando IBM Spectrum Protect Extended Edition?: No
      ¿Tiene licencia IBM Spectrum Protect Extended Edition?: Sí
      Cumplimiento licencia servidor: Válido
```

## Descripciones de los campos

---

Última auditoría licencia

Especifica la fecha y hora en que se ha producido la última auditoría de licencia.

Número de Data Protection para Oracle en uso

Especifica el número de Data Protection para Oracle en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection para Oracle en evaluación con opción a compra

Especifica el número de Data Protection para Oracle que están en evaluación con opción a compra.

Número de Data Protection for Microsoft SQL en uso

Especifica el número de Data Protection for Microsoft SQL que se están utilizando. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection for Microsoft SQL en evaluación con opción a compra

Especifica el número de Data Protection for Microsoft SQL en evaluación con opción a compra.

Número de Data Protection for Microsoft Exchange en uso

Especifica el número de Data Protection for Microsoft Exchange que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.

Número de Data Protection for Microsoft Exchange en evaluación con opción a compra

Especifica el número de Data Protection for Microsoft Exchange en evaluación con opción a compra.

- Número de TDP para Lotus Notes en uso  
Especifica el número de TDP para Lotus Notes que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- Número de TDP para Lotus Notes en evaluación con opción a compra  
Especifica el número de TDP para Lotus Notes que están en evaluación con opción a compra.
- Número de Data Protection for Lotus Domino en uso  
Especifica el número de Data Protection for Lotus Domino que se están utilizando. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- Número de Data Protection for Lotus Domino en evaluación con opción a compra  
Especifica el número de Data Protection for Lotus Domino que están en evaluación con opción a compra.
- Número de TDP para Informix en uso  
Especifica el número de TDP para Informix que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- Número de TDP para Informix con opción a compra  
Especifica el número de TDP para Informix que están en evaluación con opción a compra.
- Número de TDP para SAP R/3 en uso  
Especifica el número de TDP para SAP R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- TDP para SAP R/3 de evaluación con opción a compra  
Especifica el número de TDP para SAP R/3 que están en evaluación con opción a compra.
- Número de TDP para ESS en uso  
Especifica el número de TDP para ESS que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- TDP para ESS de evaluación con opción a compra  
Especifica el número de TDP para ESS que están en evaluación con opción a compra.
- Número de TDP para ESS R/3 en uso  
Especifica el número de TDP para ESS R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- TDP para ESS R/3 de evaluación con opción compra  
Especifica el número de TDP para ESS R/3 que están en evaluación con opción a compra.
- Número de TDP para EMC Symmetrix en uso  
Especifica el número de TDP para EMC Symmetrix que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- TDP para EMC Symmetrix de eval. con opción compra  
Especifica el número de TDP para EMC Symmetrix que están en evaluación con opción a compra.
- Número de TDP para EMC Symmetrix R/3 en uso  
Especifica el número de TDP para EMC Symmetrix R/3 que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- TDP para EMC Symmetrix R/3 de eval. con opción compra  
Especifica el número de TDP para EMC Symmetrix R/3 que están en evaluación con opción a compra.
- Número de TDP para WAS en uso  
Especifica el número de TDP para WAS que están en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- Número de TDP de WAS de evaluación con opción a compra  
Especifica el número de TDP para WAS que están en evaluación con opción a compra.
- ¿Se está utilizando IBM Spectrum Protect for Data Retention?  
Especifica si IBM Spectrum Protect para retención de datos está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- ¿Tiene licencia IBM Spectrum Protect for Data Retention?  
Especifica si IBM Spectrum Protect para retención de datos tiene licencia.
- ¿Se está utilizando IBM Spectrum Protect Basic Edition?  
Especifica si IBM Spectrum Protect Basic Edition está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- ¿Tiene licencia IBM Spectrum Protect Basic Edition?  
Especifica si IBM Spectrum Protect Basic Edition tiene licencia.
- ¿Se está utilizando IBM Spectrum Protect Extended Edition?  
Especifica si IBM Spectrum Protect Extended Edition está en uso. Un producto está en uso si ha adquirido el producto y registrado la licencia.
- ¿Tiene licencia IBM Spectrum Protect Extended Edition?  
Especifica si IBM Spectrum Protect Extended Edition tiene licencia.
- Cumplimiento licencia servidor  
Especifica si la licencia de servidor es válida.

## Comandos relacionados

---

Tabla 1. Comandos relacionados con QUERY LICENSE

Comando	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY AUDIT OCCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra las estimaciones de las unidades de valor de procesador. Recuerde: El mandato QUERY PVUESTIMATE informa de las licencias proporcionando información de PVU para cada nodo para los dispositivos de servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## QUERY LOG (Visualizar información sobre el registro de recuperación)

Utilice este comando para visualizar la información sobre las anotaciones de recuperación.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-Format-----Standard-----
>>-Query LOG-+-----+-----><
               '-Format-----+Standard-+'
                   '-Detailed-'

```

### Parámetros

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

### Ejemplo: visualizar información de resumen acerca de las anotaciones de recuperación

Visualizar información de resumen acerca de las anotaciones de recuperación. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query log
```

```

Espacio total (MB)  Espacio utilizado (MB)  Espacio libre (MB)
-----

```

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: visualizar información detallada acerca de las anotaciones de recuperación

---

Visualizar información detallada sobre las anotaciones de recuperación. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query log format=detailed
```

```

Directorio anotaciones activas: /actlog
Espacio total(MB): 524.032
Espacio utilizado(MB): 3.517
Espacio libre (MB): 520.515

Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722

Directorio anotaciones archivado: /archlog
Tamaño total del sistema de archivos (MB): 603.751,82
Espacio utilizado en el sistema de archivos (MB): 80.642,30
Espacio libre en el sistema de archivos (MB): 523.109,52
Registro de archivado comprimido: Sí

Directorio anotaciones duplicadas: /mirrorlog
Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722

Directorio anotac. recuperación errores archivado: /archfaillog
Tamaño total del sistema de archivos (MB): 301.372,06
Espacio utilizado en el sistema de archivos (MB): 44.741,80
Espacio libre en el sistema de archivos (MB): 256.630,26

```

 Sistemas operativos Windows

## Ejemplo: visualizar información detallada acerca de las anotaciones de recuperación cuando el registro duplicado y el registro de migración tras error de archivado no están definidos.

---

La salida de este mandato en sistemas Windows es diferente. Por ejemplo, la salida contiene espacios en blanco para el registro duplicado y el registro de migración tras error de archivado.

Visualizar información acerca de las anotaciones de recuperación cuando el registro duplicado y el registro de migración tras error de archivado no están definidos.

```
query log format=detailed
```

 Sistemas operativos Windows

```

Directorio de registro activo : d:\actlog
Espacio total(MB): 524.032
Espacio utilizado(MB): 3.517
Espacio libre (MB): 520.515

Tamaño total del sistema de archivos (MB): 564.443
Espacio utilizado en el sistema de archivos (MB): 527.049
Espacio libre en el sistema de archivos (MB): 8.722

Directorio de registro activo : e:\archlog
Tamaño total del sistema de archivos (MB): 603.751,82
Espacio utilizado en el sistema de archivos (MB): 80.642,30
Espacio libre en el sistema de archivos (MB): 523.109,52
Registro de archivado comprimido: Sí

Directorio anotaciones duplicadas:
Tamaño total del sistema de archivos (MB):
Espacio utilizado en el sistema de archivos (MB):
Espacio libre en el sistema de archivos (MB):

Directorio de registro de recuperación de errores de archivado:
Tamaño total del sistema de archivos (MB):

```

Espacio utilizado en el sistema de archivos (MB):  
Espacio libre en el sistema de archivos (MB):

## Descripciones de los campos

---

- Espacio total  
Especifica el tamaño máximo de las anotaciones activas en megabytes.
- Espacio utilizado  
Especifica la cantidad de espacio de anotaciones activas utilizado en megabytes.
- Espacio libre  
Especifica la cantidad de espacio de anotaciones activas que no se utiliza para transacciones sin validar, en megabytes.
- Tamaño total del sistema de archivos  
Especifica el tamaño total del sistema de archivos, en megabytes.
- Espacio utilizado en el sistema de archivos  
Especifica la cantidad de espacio utilizado en el sistema de archivos, en megabytes.
- Espacio libre en el sistema de archivos  
Especifica la cantidad de espacio disponible en el sistema de archivos, en megabytes.
- Registro de archivado comprimido  
Especifica si los registros de archivado están comprimidos.
- Directorio de anotaciones activas  
Especifica la ubicación donde se guardan los archivos de anotaciones activas. Cuando cambie el directorio de anotaciones activas, el servidor moverá todas las anotaciones archivadas al directorio de anotaciones de archivado y todas las anotaciones activas a un nuevo directorio de anotaciones activas.
- Directorio anotaciones duplicadas  
Especifica la ubicación en la que se mantiene la duplicación de las anotaciones activas.
- Directorio de anotaciones de recuperación de errores de archivado  
Especifica la ubicación en la que el servidor guarda las anotaciones de archivado si las anotaciones no se pueden archivar en el directorio de anotaciones de archivado.
- Directorio de anotaciones de archivado  
Especifica la ubicación en la que el servidor puede archivar un archivo de anotaciones una vez finalizadas todas las transacciones representadas en dicho archivo de anotaciones.

## QUERY MACHINE (Consultar información de máquina)

---

Utilice este comando para visualizar información sobre una o varias máquinas. Puede utilizar esta información para recuperar máquinas cliente de IBM Spectrum Protect en caso de producirse un siniestro.

Atención: IBM Spectrum Protect no utiliza la información de ningún modo. Sólo está disponible para ayudar a planificar la recuperación ante siniestro de las máquinas cliente.

IBM Spectrum Protect visualiza la información de varias máquinas en el orden siguiente:

- Según la prioridad especificada.
- Dentro de una prioridad, según el nombre de ubicación y de máquina especificado.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```

      .-*-----
>>-Query MACHine--+-----+-----+-----+----->
      '-machine_name-' '-BUilding---edificio-'

>--+-----+-----+-----+----->
      '-FLoor---planta-' '-ROom---sala-'

>--+-----+-----+-----+----->
      '-PRIority---prioridad-' '-ADSMServer---+Yes-+'
                                     '-No--'

      .-Format---Standard-----
>--+-----+-----+-----+-----<
      '-Format---+Standard-----+
                +-Detailed-----+
                +-RECOVERYInstructions-+
```



## Parámetros

---

### machine\_name

Especifica el nombre de una o varias máquinas que se consultarán. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todas las máquinas que se ajustan a los criterios especificados.

### BUilding

Especifica el nombre o número del edificio donde están las máquinas. Este parámetro es opcional. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

### Floor

Especifica el nombre o número de la planta donde están las máquinas. Este parámetro es opcional. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

### ROom

Especifica el nombre o número de la sala donde están las máquinas. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

### PRiority

Especifica el número de prioridad de las máquinas. Este parámetro es opcional.

### ADSMServer

Especifica si la máquina contiene un servidor IBM Spectrum Protect. Este parámetro es opcional. El valor predeterminado es visualizar todas las máquinas que se ajustan a los demás criterios. Los valores posibles son:

#### Yes

La máquina contiene un servidor de IBM Spectrum Protect.

#### No

Las máquinas no contienen un servidor de IBM Spectrum Protect.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Visualiza información parcial sobre las máquinas.

#### Detailed

Visualiza toda la información sobre las máquinas.

#### RECOVERYInstructions

Sólo visualiza las instrucciones de recuperación de las máquinas. Esta opción sólo es válida cuando se consulta una máquina específica.

#### CHaracteristics

Sólo visualiza las características de las máquinas. Esta opción sólo es válida cuando se consulta una máquina específica.

## Ejemplo: visualizar información acerca de una máquina específica

---

Visualizar información sobre la máquina denominada MACH1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query machine MACH1
```

Nombre máquina	Prioridad máquina	Edifi- ficio	Planta	Sala	Nodo	Nombre medio recuperación
MACH1	1	21	2	2929	VIRGINIA	RECMED1

## Ejemplo: visualizar información detallada acerca de las máquinas que tienen prioridad 1

---

Visualizar información detallada para todas las máquinas con prioridad 1 situadas en la segunda planta del edificio 21. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query machine * building=21 floor=2 priority=1  
format=detailed
```

```
Nombre máquina: MACH1  
Prioridad máquina: 1  
Edificio: 21  
Planta: 2  
Sala: 2929
```

¿Servidor?: Sí  
 Descripción: Máquina del servidor de TSM  
 Nombre nodo: VIRGINIA  
 Nombre medio recuperación: RECMED1  
 ¿Características?: Sí  
 ¿Instrucciones recuperación?: Sí

## Descripciones de los campos

Nombre de máquina	El nombre de la máquina.
Prioridad máquina	La prioridad de recuperación de la máquina.
Edificio	El edificio donde está situada la máquina.
Planta	La planta donde está situada la máquina.
Sala	La sala donde está situada la máquina.
¿Servidor?	Si la máquina contiene un servidor de IBM Spectrum Protect.
Descripción	La descripción de la máquina.
Nombre del nodo	Los nodos cliente de IBM Spectrum Protect asociados a esta máquina.
Nombre del medio de recuperación	Los medios de recuperación asociados a esta máquina.
¿Características?	Si el texto de las características de la máquina está almacenado en la base de datos.
¿Instrucciones de recuperación?	Especifica si el texto de instrucciones de recuperación de una máquina se almacena en la base de datos de IBM Spectrum Protect.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY MACHINE

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
UPDATE MACHINE	Cambia la información para una máquina.

## QUERY MEDIA (Consultar medio de agrupación de almacenamiento de acceso secuencial)

Utilice este comando para que se visualice información acerca de los volúmenes de agrupación de almacenamiento primaria y de copia de acceso secuencial que se han trasladado con el comando MOVE MEDIA.

### Clase de privilegio

Todos los administradores con privilegios de sistema o de operador pueden emitir este comando, excepto si incluye el parámetro CMD. Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de almacenamiento sin restricciones o de sistema. Si el parámetro CMD está especificado y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES (el valor predeterminado), el administrador debe tener privilegio de sistema.

El mandato QUERY MEDIA solo muestra volúmenes con un valor ACCESS MODE de READONLY o READWRITE.

## Sintaxis

```
.-*-----.  
>>-Query MEDia-----+----->  
      '-nombre_volumen-'  
  
      .-Days-----0----.  
>>-STGpool-----nombre_agrupación-----+----->  
      '-Days-----días-'  
  
>+-----+----->  
|          .-,'-----| |  
|          V          | |  
'-WHERESTATUS-----+FULL-----+-'  
      +-FILLing-+  
      '-EMPTy---'  
  
>+-----+----->  
'-WHEREACcEss-----+READWrite-+-'  
      '-READOnly--'  
  
      .-Format-----Standard-----.  
>+-----+----->  
'-Format-----+Standard-+-'  
      +-Detailed-+  
      '-Cmd-----'  
  
>+-----+----->  
'-WHEREState-----+All-----+-'  
      +-MOUNTABLEInlib-----+  
      '-MOUNTABLENotinlib-'  
  
>+-----+-----+-----+----->  
'-WHEREOVFLOcation-----ubicación- ' '-CMd-----"comando"- '  
  
      .-APPend-----No-----.  
>+-----+-----+-----+-----<<  
'-CMDFilename-----nombre_archivo- ' '-APPend-----+No-+-'  
      '-Yes-'
```

## Parámetros

### nombre\_volumen

Especifica el nombre del volumen de agrupación de almacenamiento de copia o primaria de acceso secuencial que se visualizará. Este parámetro es opcional. Puede utilizar un carácter comodín para especificar el nombre. Todos los volúmenes que coincidan se considerarán para su proceso. Si no especifica este parámetro, se visualizarán todos los volúmenes definidos en la agrupación de almacenamiento especificada con el parámetro STGPOOL.

### STGpool (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de copia o primaria de acceso secuencial que se utilizará para seleccionar los volúmenes para proceso. Puede utilizar caracteres comodín para especificar el nombre. Se procesarán todas las agrupaciones de almacenamiento que coincidan. Si la agrupación de almacenamiento especificada no está gestionada por una biblioteca automatizada, no se visualizará ningún volumen.

### Days

Especifica el número de días que deben transcurrir después de que se haya leído o grabado el volumen, y antes de que el volumen se pueda seleccionar para procesarlo. Este parámetro es opcional. Puede especificar un número comprendido entre 0 y 9999. El valor predeterminado es 0. Para calcular el número de días transcurridos, se utiliza la fecha de última grabación o la fecha de última lectura del volumen, la que sea más reciente de las dos.

### WHERESTATUS

Especifica que la salida de la consulta debe restringirse en función del estado del volumen. Este parámetro es opcional. Puede especificar varios estados en una lista si separa cada uno con una coma sin dejar espacios intercalados. Si no especifica un valor para este parámetro, se visualizarán todos los volúmenes de la agrupación de almacenamiento especificada, independientemente de su estado.

Los valores posibles son:

#### FULL

Especifica que se visualizarán los volúmenes con estado FULL.

#### FILLing

Especifica que se visualizarán los volúmenes con estado FILLING.

#### EMPTy

Especifica que se visualizarán los volúmenes con estado EMPTY.

#### WHEREACcEss

Especifica que la salida debe limitarse según la modalidad de acceso a volumen. Este parámetro es opcional. Si no especifica un valor para este parámetro, la salida no estará limitada según la modalidad de acceso.

Los valores posibles son:

#### READWrite

Especifica que se visualizarán los volúmenes con la modalidad de acceso READWRITE.

#### READOnly

Especifica que se visualizarán los volúmenes con la modalidad de acceso READONLY.

#### Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial para los volúmenes de agrupaciones de almacenamiento de acceso secuencial especificados.

#### Detailed

Especifica que se visualizará información completa para los volúmenes de agrupaciones de almacenamiento de acceso secuencial especificados.

#### Cmd

Especifica que se crean mandatos ejecutables para los volúmenes de agrupación de almacenamiento que se han procesado mediante el mandato QUERY MEDIA. Estos comandos se encontrarán en el archivo que se ha especificado con el parámetro CMDFILENAME en el comando QUERY MEDIA. Si desea que los comandos sólo se visualicen en la consola, especifique una serie nula ("") para CMDFILENAME. Si se ha especificado FORMAT=CMD pero no se ha especificado ninguna serie de comandos con el parámetro CMD, el comando QUERY MEDIA no se ejecutará correctamente.

#### WHEREState

Especifica el estado de los volúmenes que se procesan. Este parámetro restringe el proceso a los volúmenes que tienen el estado especificado. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

#### All

Especifica que se consultan los volúmenes en todos los estados. Los estados válidos son: MOUNTABLEINLIB y MOUNTABLENOTINLIB.

#### MOUNTABLEInlib

Especifica que se consultan los volúmenes que actualmente están en el estado MOUNTABLEINLIB. Los volúmenes en estado MOUNTABLEINLIB están en la biblioteca, y en el local, contienen datos válidos y están disponibles para su proceso en el local.

#### MOUNTABLENotinlib

Especifica que se consultan los volúmenes que actualmente están en el estado MOUNTABLENOTINLIB. Los volúmenes en estado MOUNTABLENOTINLIB no están en la biblioteca, no contienen datos válidos y no están disponibles para el proceso en el local.



#### WHEREOVFLocation


Especifica la ubicación de desbordamiento de los volúmenes que se visualizarán. Este parámetro es opcional. Este parámetro restringe el proceso a los volúmenes que están en la ubicación especificada. La longitud máxima de la lista de la ubicación es de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco.

#### CMd

Especifica la creación de mandatos ejecutables. Encierre la especificación de comandos entre comillas. La longitud máxima de la especificación del comando ejecutable es de 255 caracteres. Este parámetro es opcional.

Para cada volumen que el comando QUERY MEDIA procesa correctamente, el servidor graba los comandos asociados en un archivo. Especifique el nombre de archivo con el parámetro CMDFILENAME.

 Sistemas operativos AIX  Sistemas operativos Linux Si no especifica un nombre de archivo, el comando generará un nombre de archivo predeterminado agregando la serie exec.cmds.media al directorio del servidor.

 Sistemas operativos Windows Si no especifica un nombre de archivo, el mandato generará un nombre de archivo predeterminado agregando la serie exec.cmd.media al directorio del servidor.

Recuerde:

1. Si el mandato escrito en el archivo sobrepasa los 255 caracteres, se divide en varias líneas y se agrega un carácter de continuación (+) a todas menos a la última línea. Puede que deba alterar el carácter de continuación en función de los

- requisitos del producto que ejecuta los comandos.
2. Si se especifica un comando ejecutable con un valor para FORMAT distinto de CMD, la serie del comando se pasará por alto y el comando QUERY MEDIA no grabará ninguna línea de comandos.

Especifique una serie de comandos y las variables de sustitución que convengan:

#### serie

Especifica la serie para crear un mandato ejecutable que procese el nombre de volumen y/o la ubicación del volumen. Puede especificar cualquier texto de formato libre para la serie. No utilice comillas intercaladas. Por ejemplo, la siguiente es una especificación válida de un comando ejecutable:

```
cmd="checkin libvolume &vol"
```

La siguiente es una especificación no válida de un comando ejecutable:

```
cmd="checkin libvolume "&vol""
```

#### sustitución

Especifica una variable para la que desea que el mandato QUERY MEDIA sustituya un valor. Las posibles variables de sustitución son:

##### &VOL

Sustituye el nombre de volumen por &VOL. Puede especificar caracteres en minúsculas, &vol. No debe especificar ni espacios ni blancos entre el signo & y VOL. Si existen espacios o blanco entre el ampersand y VOL, el mandato QUERY MEDIA los tratará como si fueran series y no se establecerá ninguna sustitución. Si no se especifica &VOL, no se establecerá ningún nombre de volumen en el comando ejecutable.

##### &LOC

Sustituye que el volumen por &LOC. Puede especificar caracteres en minúsculas, &loc. No debe especificar ni espacios ni blancos entre el signo & y LOC. Si existen espacios o blanco entre el ampersand y LOC, el comando QUERY MEDIA los tratará como si fueran series y no se establecerá ninguna sustitución. Si no se especifica &LOC, no se establecerá ningún nombre de ubicación en el comando ejecutable.

##### &VOLDSN



Sustituye el nombre de archivo del volumen por &VOLDSN. Un ejemplo de nombre de archivo de volumen de cinta de una agrupación de almacenamiento que utiliza el prefijo definido IBM Spectrum Protect310 es IBM Spectrum Protect310.BFS. Si no se especifica &VOLDSN, no se establecerá ningún nombre de archivo de volumen en el comando ejecutable.


##### &NL

Sustituye un nuevo carácter de línea por &NL. Cuando se especifica &NL, el mandato QUERY MEDIA subdividirá el mandato en la posición en la que se encuentra &NL y no agregará ningún carácter de continuación. El usuario es el responsable de especificar el carácter de continuación correcto antes de &NL, si es necesario. El usuario también es el responsable de la longitud de la línea escrita. Si no se especifica &NL y el comando sobrepasa los 255 caracteres, el comando se dividirá en varias líneas y se agregará un carácter de continuación (+) a todas las líneas menos a la última.



#### CMDFilename


Especifica el nombre de ruta totalmente calificado que contendrá los mandatos especificados con el parámetro CMD, cuando se especifica FORMAT=CMD. Este parámetro es opcional. La longitud máxima del nombre de archivo es de 1279 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux Si especifica "" con el parámetro CMDFILENAME, el mandato QUERY MEDIA generará un nombre de archivo agregando "exec.cmds.media" al directorio del servidor. El directorio del servidor es el directorio de trabajo actual del proceso de servidor.

 Sistemas operativos Windows Si especifica "" con el parámetro CMDFILENAME, el comando QUERY MEDIA generará un nombre de archivo agregando "exec.cmd.media" al directorio del servidor. El directorio del servidor es el directorio de trabajo actual del proceso de servidor.

Si especifica una serie nula ("" ) para CMDFILENAME, los mandatos creados se visualizarán únicamente en la consola. Puede redirigir los comandos visualizados a un archivo, utilizando los caracteres de redirección del sistema operativo (> o >>).

 Sistemas operativos AIX  Sistemas operativos Linux Si el nombre de archivo no está especificado, el mandato generará un nombre de archivo predeterminado agregando la serie "exec.cmds.media" al directorio del servidor.

 Sistemas operativos Windows Si el nombre de archivo no está especificado, el mandato generará un nombre de archivo predeterminado agregando la serie "exec.cmd.media" al directorio del servidor.

El mandato QUERY MEDIA asigna automáticamente el nombre de archivo especificado o generado. Si ya existe el nombre del archivo, el comando QUERY MEDIA intentará utilizar éste y los datos existentes, si los hubiera, en el archivo que va a

sobregrabarse. Puede especificar APPEND=YES para impedir que los datos existentes se sobregaben. Si el comando QUERY MEDIA no se ejecuta correctamente después de haberse asignado el archivo de comandos, el archivo no se suprimirá.

#### APPend

Especifica que se graba al principio o al final de los datos del archivo de comandos. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

#### No

Especifica que se han de escribir datos desde el principio del archivo de comandos. Si el archivo de comandos dado ya existe, se sobregabará el contenido.

#### Yes

Especifica que se agrega el archivo de comandos grabando al final de los datos del archivo de comandos.

## Ejemplo: visualizar información acerca de una agrupación de almacenamiento de acceso secuencial específica

---

Visualizar todos los volúmenes completos o parcialmente completos que se encuentren en la agrupación de almacenamiento primaria de acceso secuencial, ARCHIVE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query media * stgpool=archive wherestatus=full, filling
```

Nombre volumen	Estado	Ubicación	Nombre biblioteca automatizada
TAPE01	Montable en biblioteca		LIB3494
TAPE03	Montable no en biblioteca	Room1234/Bldg31	
TAPE07	Montable en biblioteca		LIB3494
TAPE09	Montable no en biblioteca	Room1234/Bldg31	

## Ejemplo: visualizar información acerca de una agrupación de almacenamiento de acceso secuencial con un prefijo específico

---

Visualizar detalladamente todos los volúmenes completos en estado MOUNTABLENOTINLIB para las agrupaciones de almacenamiento de acceso secuencial que tengan un nombre de prefijo de ONSITE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query media wherestate=mountablenotinlib stgpool=onsite* wherestatus=full format=detailed
```

```
Nombre volumen: TAPE21
Estado: Montable no en biblioteca
Estado volumen: Lleno
Acceso: ReadOnly
Fecha última referencia: 30/01/98
Fecha/hora última actualización: 20/08/1996 13:29:02
Ubicación: Rm569/bldg31
Nombre agrupación almacenamiento: ONSITE.ARCHIVE
Nombre biblioteca automatizada:

Nombre volumen: TAPE22
Estado: Montable no en biblioteca
Estado volumen: Lleno
Acceso: ReadOnly
Fecha última referencia: 30/01/98
Fecha/hora última actualización: 20/08/1996 15:29:02
Ubicación: Rm569/bldg31
Nombre agrupación almacenamiento: ONSITE.ARCHIVEPOOL
Nombre biblioteca automatizada:
```

## Ejemplo: generar comandos para dar de alta

---

Generar los comandos CHECKIN LIBVOLUME para los volúmenes llenos y parcialmente llenos que se encuentran en la agrupación de almacenamiento primaria ONSITE.ARCHIVE y que están almacenados en la ubicación de desbordamiento Room 2948/Bldg31.

```
query media * stgpool=onsite.archive format=cmd wherestatus=full,filling wherestate=mountablenotinlib whereovflocation=room2948/bldg31
```

```
cmd="checkin libvol lib3494 &vol status=private"
cmdfilename=/tsm/move/media/checkin.vols
```

El comando QUERY MEDIA que ha creado los comandos ejecutables CHECKIN LIBVOLUME en /tsm/move/media/checkin.vols, que puede ejecutarse emitiendo el comando MACRO con /tsm/move/media/checkin.vols como nombre de la macro.

```
checkin libvol lib3494 TAPE04 status=private
checkin libvol lib3494 TAPE13 status=private
checkin libvol lib3494 TAPE14 status=private
```

## Descripciones de los campos

Nombre de volumen

Especifica el nombre del volumen de agrupación de almacenamiento de acceso secuencial primaria.

Estado

Especifica el estado del volumen.

Estado volumen

Especifica el estado del volumen.

Acceso

Especifica la modalidad de acceso del volumen.

Fecha última referencia

Especifica la fecha de la última grabación o de la última lectura del volumen, la que sea más reciente.

Fecha/hora última actualización

Especifica la fecha y la hora en que se ha actualizado por última vez el volumen.

Ubicación

Especifica donde se almacena el volumen. Si se expulsa el volumen de la biblioteca y su ubicación no se ha especificado ni definido, se visualizará un signo de interrogación (?) para la ubicación.

Nombre de la agrupación de almacenamiento




Especifica el nombre de la agrupación de almacenamiento de acceso secuencial donde está definido el volumen.

Biblioteca automatizada

Especifica el nombre de la biblioteca automatizada si el volumen está en la biblioteca.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY MEDIA

Comando	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows MOVE MEDIA	Mueve los volúmenes de agrupaciones de almacenamiento gestionados por una biblioteca automatizada.

## QUERY MGMTCLASS (Consultar una clase de gestión)

Utilice este mandato para visualizar la información sobre las clases de gestión.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query Mgmtclass----->
.
.*-----*-----
>+-----+----->
|          .-*-----*-----|
|'-nom_dominio-----+-----'|
|          |          .-*-----*-----| |
|          |'-nom_juego_politicas-----+-----+-----'|
|          |          |'-nombre_clase-'|
.
.-Format-----Standard-----
>+-----+-----><
|'-Format-----+-----Standard-----+-----'|
|          |          |'-Detailed-'|
```

## Parámetros

### nombre\_dominio

Especifica el dominio de políticas asociado a la clase de gestión que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se consultarán las clases de gestión de todos los dominios de políticas. Debe especificar este parámetro cuando consulte una clase de gestión denominada explícitamente.

### nombre\_juego\_políticas

Especifica el juego de políticas asociado a la clase de gestión que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se consultarán las clases de gestión de todos los juegos de políticas. Debe especificar este parámetro cuando consulte una clase de gestión denominada explícitamente.

### nombre\_clase

Especifica la clase de gestión que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se consultarán todas las clases de gestión.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

## Ejemplo: visualizar información acerca de todas las clases de gestión

Consultar información parcial sobre todos los dominios de políticas. Crear la salida en formato estándar. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query mgmtclass
```

Nombre dominio políticas	Nombre juego políticas	Nombre clase gestión	¿Clase gestión predeterm.?	Descripción
EMPLOYEE_RECORDS	ACTIVE	ACTIVEFILES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE_RECORDS	HOLIDAY	ACTIVEFILES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE_RECORDS	HOLIDAY	FILEHISTORY	No	Clase de gestión de prueba modificada
EMPLOYEE_RECORDS	VACATION	ACTIVEFILES	Sí	Clase de gestión predeterminada modificada
EMPLOYEE_RECORDS	VACATION	FILEHISTORY	No	Clase de gestión de prueba modificada
PROG1	SUMMER	MCLASS1	No	Clase de gestión de soporte técnico
PROG2	SUMMER	MCLASS1	No	Clase de gestión de soporte técnico
STANDARD	ACTIVE	STANDARD	Sí	Clase gestión predeterminada instalada
STANDARD	STANDARD	STANDARD	Sí	Clase gestión clase de gestión

Para visualizar información sobre las clases de gestión de un dominio de políticas específico, por ejemplo el dominio ENGPOLDOM, emita el mandato siguiente:

```
query mgmtclass engpoldom * *
```

## Ejemplo: visualizar información detallada acerca de una clase de gestión específica

Consultar la clase de gestión ACTIVEFILES que se ha asignado al juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS. Crear la salida en formato detallado. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query mgmtclass employee_records vacation  
activefiles format=detailed
```

```
Nombre dominio políticas: EMPLOYEE_RECORDS  
Nombre juego políticas: VACATION
```



```

Nombre clase gestión: ACTIVEFILES
¿Clase de gestión predeterminada?: Sí
    Descripción: Clase de gestión
                                predeterminada
                                instalada

Técnica gestión espacio: Ninguna
¿Migrar automáticamente al no utilizar?: 0
¿Migración requiere copia de seguridad?: Sí
    Destino migración: SPACEMGPOOL
Última actualización por (administrador): $$CONFIG MANAGER$$
    Fecha/hora última actualización: 31/05/1996 13:15:45
    Perfil gestión: EMPLOYEE
    Cambios pendientes: Sí

```

## Descripciones de los campos

Nombre de dominio de políticas	El dominio de políticas.
Nombre de juego de políticas	El juego de políticas.
Nombre clase gestión	La clase de gestión.
¿Clase gestión predeterminada?	Si la clase de gestión es la clase de gestión predeterminada para el juego de políticas.
Descripción	La descripción de la clase de gestión.
Técnica gestión espacio	La técnica de gestión de espacio de la clase de gestión, para los clientes de IBM Spectrum Protect for Space Management.
Migrar automáticamente al no utilizar	El número de días que deben transcurrir desde que se accedió por última vez a un archivo hasta que pueda seleccionarse para la migración automática mediante clientes IBM Spectrum Protect for Space Management.
¿Migración requiere copia seguridad?	Si debe existir una versión de copia de seguridad de un archivo para que pueda migrarse mediante clientes IBM Spectrum Protect for Space Management.
Destino migración	La agrupación de almacenamiento que es el destino de los archivos migrados mediante clientes IBM Spectrum Protect for Space Management.
Última actualización por (administrador)	El administrador o el servidor que ha actualizado por última vez la clase de gestión. Si este campo contiene \$\$CONFIG_MANAGER\$\$, la clase de gestión se asocia a un dominio que el gestor de configuración gestiona.
Fecha/hora última actualización	La fecha y la hora en que se ha definido o actualizado por última vez la clase de gestión.
Perfil de gestión	El perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de esta clase de gestión.
Cambios pendientes	Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY MGMTCLASS

Comando	Descripción
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE MGMTCLASS	Cambia los atributos de una clase de gestión.

## QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)

Utilice este mandato para visualizar información acerca de los valores de supervisión de alertas y de estado del servidor.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
>>-Query MONITORSEttings-----<<
```

## Visualizar valores de supervisión

---

Visualizar detalles sobre los valores de supervisión. Para obtener información detallada, consulte Descripciones de los campos.

```
query monitorsettings
```

Ejemplo de salida:

```
                Estado de supervisión: Activo
Intervalo de renovación de estado (minutos): 5
                Retención de estado (horas): 48
                Alertas de mensajes del supervisor: Activo
Intervalo de actualización de alertas (min.): 10
                Alerta por correo electrónico: Activo
Enviar resumen de alertas a administradores: Activo
                Alerta desde dirección de correo electrónico: DJADMIN@MYDOMAIN.COM
                Host SMTP de alerta: DJHOST.MYDOMAIN.COM
                Puerto SMTP de alerta: 25
                Duración de alerta activa (min.): 480
                Duración de alerta inactiva (min.): 480
                Duración de alerta cerrada (min.): 60
                Admin. supervisión: ADMIN
                Grupo supervisado: MONGROUP
                Servidores supervisados: SERVER2
Intervalo en peligro para aplicaciones: 24
¿Se han omitido archivos como en peligro para aplicaciones?: Sí
Intervalo en peligro para máquinas virtuales: 24
¿Se han omitido archivos como en peligro para máquinas virtuales?: Sí
Intervalo en peligro para sistemas: 24
¿Se han omitido archivos como en peligro para sistemas?: Sí
```

## Descripciones de los campos

---

Estado de supervisor

Especifica si la supervisión de alertas en el servidor está habilitada o inhabilitada.

Intervalo de renovación de estado (minutos)

Especifica el número de minutos entre los intervalos de tiempo que el servidor de supervisión recopila datos de evento.

Retención de estado (horas)

Especifica el número de horas que se retienen los indicadores de supervisión de estado.

Alertas de mensaje del supervisor

Especifica si se envían las alertas a los administradores por correo electrónico

Intervalo de actualización de alerta (minutos)

Especifica el periodo de tiempo, en minutos, que el supervisor de alertas espera antes de que se actualice o borre la alerta en el servidor.

Alertas en correo electrónico

Especifica si se envían las alertas a los administradores por correo electrónico

Enviar resumen de alertas a los administradores

Especifica los administradores que recibirán un resumen de las alertas existentes en el servidor por correo electrónico.

Alertas desde dirección de correo electrónico

Especifica la dirección de correo electrónico del remitente.

Host SMTP de alertas

Especifica el servidor de correo del host de protocolo simple de transferencia de correo (SMTP) que se utilizará para enviar las alertas.

Puerto SMTP de alertas

Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.

Duración activa de alerta (minutos)

- Especifica el tiempo, en minutos, que una alerta permanece activa.
- Duración inactiva de alerta (minutos)
  - Especifica el tiempo, en minutos, en que la alerta estará inactiva.
- Duración cerrada de alerta (minutos)
  - Especifica el tiempo, en minutos, que una alerta permanece cerrada antes de que se suprima del servidor.
- Administración de supervisión
  - Especifica el nombre del administrador de supervisión que se utiliza para conectarse a los servidores del grupo supervisado.
- Grupo supervisado
  - Especifica el nombre del grupo de servidores supervisados.
- Servidores supervisados
  - Especifica los nombres de los servidores del grupo de servidores supervisados. Los valores de supervisión pueden ser diferente en cada servidor supervisado. Si es así, emita el mandato de consulta para cada servidor para visualizar los valores de supervisión.
- Intervalo de en riesgo para aplicaciones
  - Especifica el intervalo de tiempo, en horas, que un cliente de aplicaciones puede no registrar actividad antes de que se considere en peligro.
- ¿Archivos omitidos como en riesgo para aplicaciones?
  - Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.
- Intervalo de en riesgo para máquinas virtuales
  - Especifica el intervalo de tiempo, en horas, que un cliente virtual puede no registrar actividad antes de que se considere en peligro.
- ¿Archivos omitidos como en riesgo para máquinas virtuales?
  - Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.
- Intervalo de en riesgo para sistemas
  - Especifica el intervalo de tiempo, en horas, que un cliente de sistemas puede no registrar actividad antes de que se considere en peligro.
- ¿Archivos omitidos como en riesgo para sistemas?
  - Especifica que el servidor considera los archivos omitidos por el cliente como una anomalía y marca el cliente en peligro.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY MONITORSETTINGS

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	Suprime un servidor de un grupo de servidores.
DELETE SERVER (Suprimir una definición de servidor)	Suprime la definición de un servidor.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSSKIPFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

## QUERY MONITORSTATUS (Consultar el estado de supervisión)

Utilice este mandato para visualizar mensajes de estado que están dentro del periodo de retención de estado definido.

Puede limitar la salida a un estado especificado, por ejemplo sólo los mensajes con un estado de activo. Si no especifica ningún parámetro, se visualizan todos los mensajes.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```

      .-Format-----Standard-----.
>>-Query MONITORStatus-----+----->
      '-Format-----+Standard-+-'
                        '-Detailed-'

      .-Type-----Active-----.
>-----+----->
      '-Type-----+All-----+'
                +-Active---+
                '-Inactive-'

>-----+----->
      '-ACTivity-----nombre_actividad-'

>-----+----->
      '-Name-----nombre_elemento-'

>-----+-----><
      |           .-,-----|
      |           V         |
      '-Status-----+Normal--+--+'
                        +-Warning-+
                        '-Error---'

```

## Parámetros

---

### Format

Especifica la cantidad de información que se visualiza. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

#### Standard

Especifica que sólo se visualice información parcial para los mensajes especificados.

#### Detailed

Especifica que se visualice toda la información para los mensajes especificados.

### Type

Este parámetro restringe la salida sólo a mensajes con el valor de tipo especificado. Especifique uno de los siguientes valores:

#### ALL

Visualiza toda la información.

#### Active

Visualiza todos los mensajes activos. Este es el valor predeterminado.

#### Inactive

Visualiza todos los mensajes inactivos.

### ACTivity

Especifica la actividad que desea consultar. Consulte el mandato DEFINE STATUSTHRESHOLD para obtener detalles sobre las actividades disponibles que se deben consultar.

### NAme

Especifica el nombre que desea consultar. El valor NAME hace referencia al nombre del elemento con la actividad especificada. Por ejemplo, un indicador de estado que contiene información sobre una agrupación de almacenamiento que se denomina `backuppool` tiene NAME establecido en BACKUPPOOL.

### Status

Especifica el estado de los mensajes que se desea consultar. Puede especificar varios valores de estado en una lista separando los valores con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, se visualiza información para todos los valores de estado. Especifique uno de los siguientes valores:

**Normal**

Visualiza todos los mensajes con un estado normal.

**Warning**

Visualiza todos los mensajes con un estado de aviso.

**Error**

Visualiza todos los mensajes con un estado de error.

## Visualizar valores de supervisión

---

Visualizar detalles acerca del estado de supervisión.

```
Query MONITORStatus type=active
```

Ejemplo de salida:

```
Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY TAPE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY TAPE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
```

## Visualizar valores de supervisión

---

Visualizar detalles acerca del estado de supervisión.

```
query monitorstatus f=d type=active
```

Salida del ejemplo:

```
Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
Detalles de elemento:
Sugerencia de reparación principal:
Primera sugerencia de reparación alternativa:
Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1
Fecha de actividad: 03/05/2013 15:57:37
Nombre de actividad: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Nombre de elemento: USED CAPACITY OF PRIMARY DISK AND FILE STORAGE
Valor numérico de elemento: 0
Valor de serie de elemento:
Estado de elemento: NORMAL
```

Detalles de elemento:  
 Sugerencia de reparación principal:  
 Primera sugerencia de reparación alternativa:  
 Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1  
 Fecha de actividad: 03/05/2013 15:57:37  
 Nombre de actividad: CAPACITY OF PRIMARY TAPE STORAGE  
 Nombre de elemento: CAPACITY OF PRIMARY TAPE STORAGE  
 Valor numérico de elemento: 0  
 Valor de serie de elemento:  
 Estado de elemento: NORMAL  
 Detalles de elemento:  
 Sugerencia de reparación principal:  
 Primera sugerencia de reparación alternativa:  
 Segunda sugerencia de reparación alternativa:

Nombre servidor: SERVER1  
 Fecha de actividad: 03/05/2013 15:57:37  
 Nombre de actividad: USED CAPACITY OF PRIMARY TAPE STORAGE  
 Nombre de elemento: USED CAPACITY OF PRIMARY TAPE STORAGE  
 Valor numérico de elemento: 0  
 Valor de serie de elemento:  
 Estado de elemento: NORMAL  
 Detalles de elemento:  
 Sugerencia de reparación principal:  
 Primera sugerencia de reparación alternativa:  
 Segunda sugerencia de reparación alternativa:

## Descripciones de los campos

Nombre del servidor  
 El nombre del servidor.

Fecha de la actividad  
 Fecha y hora a las que se notificó la última actividad.

Nombre de actividad  
 Nombre de la actividad.

Nombre de elemento  
 Nombre del elemento.

Valor numérico de elemento  
 Valor numérico del elemento.

Valor de serie de elemento  
 Valor de serie del elemento.

Estado de elemento  
 Estado del elemento.

Detalles de elemento  
 Información detallada del elemento.

Sugerencia de reparación principal  
 Sugerencia de reparación principal.

Sugerencia principal de reparación alternativa  
 Sugerencia de reparación en caso de que la sugerencia principal no sea la adecuada.

Sugerencia secundaria de reparación alternativa  
 Sugerencia de reparación en caso de que la sugerencia principal y la primera alternativa no sean adecuadas.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY MONITORSTATUS

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.

Comando	Descripción
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## QUERY MOUNT (Visualizar información sobre volúmenes de acceso secuencial montados)

Utilice este comando para visualizar información sobre el estado de uno o varios volúmenes de acceso secuencial que están montados.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query MOunt-----*----->
      '-nombre_volumen-'

.-Format-----Standard-----.
>--+-----+-----><
      '-Format-----+Standard--'
      '-Detailed-'

```

### Parámetros

nombre\_volumen

Especifica el nombre del volumen de acceso secuencial montado. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado es todos los volúmenes montados.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

### Ejemplo: obtener una lista de todos los volúmenes secuenciales montados

Visualizar información acerca de todos los volúmenes de medios secuenciales montados.

```
query mount
```

 Sistemas operativos AIX

```

ANR8330I El volumen 3590 D6W992 está montado R/O
en la unidad RMT1 (/dev/rmt1), estado: EN USO.
ANR8334I 1 volúmenes encontrados.
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W
en la unidad 8MM.1 (/dev/mt0), estado: DESMONTÁNDOSE.
ANR8334I 1 volúmenes encontrados.

```

## Sistemas operativos Linux

```
ANR8330I El volumen 3590 D6W992 está montado R/O
en la unidad RMT1/dev/IBMtape1, estado: EN USO.
ANR8334I 1 volúmenes encontrados.
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W
en la unidad 8MM.1 (/dev/tsm SCSI/mt0), estado: DESMONTÁNDOSE.
ANR8334I 1 volúmenes encontrados.
```

## Sistemas operativos Windows

```
ANR8330I El volumen 3590 D6W992 está montado R/O
en la unidad RMT1(/dev/rmt1), estado: EN USO.
ANR8334I 1 volúmenes encontrados.
ANR8331I El volumen 8MMTAPE WPD000 está montado R/W
en la unidad 8MM.1 (mt3.0.0.0), estado: DESMONTÁNDOSE.
ANR8334I 1 volúmenes encontrados.
```

### Recuerde:

1. Si el estado de un volumen es lleno o si su modalidad de acceso es de sólo lectura (R/O), la modalidad de montaje del volumen es R/O. Para determinar el estado y la modalidad de acceso de un volumen, emita el mandato `QUERY VOLUME FORMAT=DETAILED`. Si se puede grabar en un volumen (es decir, el estado es llenando o vacío), la modalidad de montaje del volumen es Lectura/Grabación (R/W), aunque únicamente se esté leyendo.
2. En una agrupación de almacenamiento que está asociada con el tipo de dispositivo FILE o CENTERA, el servidor puede realizar varios accesos de lectura simultáneos y un único acceso de grabación al mismo volumen. Como resultado de ello, un volumen de una agrupación de almacenamiento con el tipo de dispositivo FILE o CENTERA puede aparecer montado más de una vez.
3. `anr8448i` en el mensaje, el nombre de la unidad se muestra como `unknown` para los volúmenes del tipo de dispositivo FILE con una clase de dispositivo no compartida. La razón es que no hay ninguna unidad asociada con los volúmenes; los nombres de unidades se muestran en la biblioteca basada en archivos.
4. Si emite el mandato `QUERY MOUNT` mientras la unidad se está limpiando, la salida del mandato continuará mostrando el estado `DISMOUNTING` para el volumen desmontado hasta que se complete la limpieza.

## Ejemplo: visualizar información detallada sobre los volúmenes secuenciales montados

Visualice detalles sobre los volúmenes montados.

```
query mount format=detailed
```

```
ANR2017I El administrador SERVER_CONSOLE ha emitido el mandato: QUERY
Formato MOUNT=detallado
ANR8487I El punto de montaje de la clase de dispositivo FILE está esperando
a que se complete
el montaje del volumen -- servidor propietario: SERVER1, estado: EN ESPERA DE VOLUMEN
(sesión: 0, proceso: 1).
ANR8488I El volumen LTO 015005L4 está montado para L/G en la unidad IBMVTL1
(/dev/rmt37) -- servidor
propietario: SERVER1, estado: EN USO (sesión: 0, proceso: 2).
ANR8486I El punto de montaje de la clase de dispositivo FILE está reservado -- servidor
propietario: SERVER1,
estado: RESERVADO (sesión: 5, proceso: 0).
ANR8334I          3 coincidencias encontradas
```

## Comandos relacionados

Tabla 1. Comandos relacionados con `QUERY MOUNT`

Comando	Descripción
<code>DISMOUNT VOLUME</code>	Desmonta un volumen secuencial extraíble según el nombre de volumen.
<code>REPLY</code>	Permite que una petición siga procesándose.

## QUERY NASBACKUP (Consultar imágenes de copia de seguridad de NAS)

Utilice este comando para visualizar información acerca de los objetos de imagen de sistema de archivos de los que se ha efectuado una copia de seguridad para un nodo NAS y un espacio de archivos específicos. Sólo puede emplear este comando para visualizar los objetos de los que se ha hecho copia de seguridad para un nodo NAS mediante NDMP.



El servidor muestra todos los objetos coincidentes, las fechas en las que se ha efectuado una copia de seguridad de esos objetos e información sobre una tabla de contenido (TOC) para el objeto.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query NASBackup--nombre_nodo--nombre_espacioarchivos----->
    .-BEGINDate----TODAY - 7-. .-BEGINTime----00:00:00-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  '-BEGINDate----fecha-' '-BEGINTime----hora-'

    .-ENDDate----TODAY-. .-ENDTime----23:59:59-.
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  '-ENDDate----fecha-' '-ENDTime----hora-'

    .-TYPE----BACKUPImage-----
>+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
  '-TYPE----BACKUPImage-+-'
      '-SNAPMirror--'
```

## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo NAS para el que se visualizan los objetos de copia de seguridad. No puede utilizar caracteres comodín para especificar este nombre.

nombre\_espacio\_archivos (Obligatorio)

Especifica el nombre del espacio de archivos para el que se visualizan los objetos de copia de seguridad. Puede utilizar caracteres comodín para especificar este nombre.

BEGINDate

Especifica la fecha inicial para seleccionar los objetos de copia de seguridad que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados en la fecha especificada o a partir de ella. El valor predeterminado es siete días antes de la fecha actual. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la hora y la fecha. Este parámetro es opcional.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/2002
TODAY	La fecha actual	TODAY
TODAY-días o-días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY -7 o -7. Para visualizar la información sobre los mensajes creados una semana atrás, puede especificar BEGINDATE=TODAY-7 o BEGINDATE= -7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

BEGINTime

Especifica la hora inicial para seleccionar los objetos de copia de seguridad que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados a la hora especificada o a partir de ella. Este parámetro es opcional. El valor predeterminado es la medianoche (00:00:00) de la fecha especificada para BEGINDATE.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	10:30:08
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00.  Si emite este mandato a las 9:00 con BEGINTIME=NOW+3 o BEGINTIME=+3, el servidor visualizará los registros que tengan la hora 12:00 o posterior en la fecha inicial.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-04:00 o -04:00.  Si emite este mandato a las 9:00 con BEGINTIME=NOW-3:30 o BEGINTIME=-3:30, el servidor visualiza los objetos de imágenes con la hora 5:30 o posterior en la fecha inicial.

#### ENDDate

Especifica la fecha final utilizada para seleccionar los objetos que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados en la fecha especificada o antes de ella. Este parámetro es opcional. El valor predeterminado es la fecha actual. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha finales.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/2002
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY-1 o -1.  Para visualizar la información creada hasta ayer, puede especificar ENDDATE=TODAY-1, o simplemente, ENDDATE= -1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final utilizada para seleccionar los objetos que se visualizarán. Se mostrarán todos los objetos de copia de seguridad creados a la hora especificada o antes de ella. Este parámetro es opcional. El valor predeterminado son las 23:59:59. Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW

Valor	Descripción	Ejemplo
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite este mandato a las 9:00 con ENDTIME=NOW+3:00 o ENDTIME= +3:00, el servidor visualiza los objetos de imágenes con la hora 12:00 o posterior en la fecha final especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30.  Si emite este mandato a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME= -3:30, el servidor visualizará los objetos de imágenes con la hora 5:30 o posterior en la fecha final especificada.

TYPE

Especifica el tipo de imágenes de copia de seguridad NDMP sobre el que desea visualizar información. El valor predeterminado para este parámetro es BACKUPIIMAGE. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser específicos para un servidor de archivos determinado. Los valores posibles son:

#### BACKUPIImage

Especifica que la salida sólo debe mostrar las imágenes diferenciales y básicas estándares de NAS. Este es el valor predeterminado para este parámetro.

#### SNAPMirror

Especifica si ha de visualizarse información sobre las imágenes NetApp SnapMirror. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos. Una imagen SnapMirror solo puede restaurarse en un sistema de archivos que se haya preparado como volumen de destino SnapMirror. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más información. Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM N-Series.

## Ejemplo:

Emitir el mandato QUERY NASBACKUP para que se visualice información acerca de un nodo, nas1, y un espacio de archivos, /vol/vol1.

```
query nasbackup nas1 /vol/vol1
```

Node Name	Filespace Name	Object Type (MB)	Object Size (MB)	Creation Date Contents	Has Table of Contents (TOC)	Mgmt Class Name	Image Storage Pool
NAS1	vol/vol1	Imag.	1050.5	10/22/2002 10:50:57	YES	DEFAULT NASBACKUPS	
NAS1	vol/vol1	Imagen diferenc.	9.1	10/22/2002 11:03:21	YES	DEFAULT NASBACKUPS	
NAS1	vol/vol1	Imag. compl.	1050.5	10/22/2006 10:43:00	YES	STANDARD FILEPOOL	
NAS1	vol/vol1	Imagen diferencial	9.1	10/25/2006 11:53:21	YES	STANDARD FILEPOOL	

## Ejemplo:

Emita el mandato QUERY NASBACKUP para mostrar información sobre todas las imágenes de NetApp SnapMirror to Tape para un nodo, nas2, y para un espacio de archivos, /vol/vol2.

```
query nasbackup nas2 /vol/vol2 type=snapmirror
```

Nombre de nodo	Nombre de espacio de archivos	Tipo de objeto de imagen	Tamaño de objeto (MB)	Fecha de creación	Nombre clase de gestión de imagen	Nombre de agrupac. almacen.
NAS2	vol/vol2	SnapMirror	1050.5	04/02/2008 10:50:57	ESTÁNDAR	MIAGRUPACIÓN
NAS2	vol/vol2	SnapMirror	1450.5	04/02/2008 11:03:21	ESTÁNDAR	MIAGRUPACIÓN

## Descripciones de los campos

Nombre del nodo

- El nombre del nodo cliente.
- Nombre de espacio de archivos
  - Nombre del espacio de archivos.
- Tipo de objeto
  - Tipo de objeto del que se ha realizado una copia de seguridad.
- Tamaño de objeto (MB)
  - Tamaño del objeto en megabytes.
- Fecha de creación
  - Fecha de creación de la copia de seguridad.
- Nombre clase gestión
  - El nombre de la clase de gestión.
- Nombre de agrupación de almacenamiento de imágenes
  - Nombre del almacenamiento donde se encuentra la copia de seguridad.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY NASBACKUP

Comando	Descripción
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).
BACKUP NAS (Comando de cliente de IBM Spectrum Protect)	Crea una copia de seguridad de datos de un nodo NAS.
QUERY TOC	Visualiza detalles sobre la tabla de contenido para una imagen de copia de seguridad especificada.
RESTORE NODE	Restaura un nodo de almacenamiento conectado a red (NAS).

## QUERY NODE (Consultar nodos)

Utilice este comando para ver información sobre uno o varios nodos registrados.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-*-----
>>-Query Node----->
      '-nombre_nodo-'

>----->
|           .-,'-----' |
|           v             |
| '-Domain-----nombre_dominio-+' |

.-Format-----Standard-----
>----->
      '-Format-----+Standard-+'
              '-Detailed-'

.-Type-----Client-----
>-----<
      '-AUTHentication-----+Local-+'   '-Type-----+Client-+'
              '-LDap--'                   +-NAS-----+
                                          +-Server-+
                                          '-Any-----'

```

### Parámetros

- nombre\_nodo
  - Especifica el nombre del nodo cliente que se ha de consultar. Puede utilizar caracteres comodín para especificar este nombre. Se consultarán todos los nodos clientes que coincidan. Si no especifica un valor para este parámetro, se consultarán todos los nodos clientes. El parámetro es opcional.

## Domain

Especifica una lista de dominios de políticas que limitan la consulta del nodo cliente. Únicamente se visualizarán los nodos asignados a los dominios de políticas especificados. Este parámetro es opcional. Debe separar los elementos de la lista con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar un dominio. Se muestran todos los clientes asignados a un dominio coincidente. Si no especifica un valor para este parámetro, se incluirán todos los dominios de políticas en la consulta.

## Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Puede especificar uno de los siguientes valores:

### Standard

Especifica que se visualizará información parcial sobre los nodos clientes especificados.

### Detailed

Especifica que se visualizará información completa sobre los nodos clientes especificados.

## Type

Especifica el tipo de nodo que se incluye en el resultado de la consulta. El parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

### Any

Especifica todos los tipos de nodo.

### Client

Especifica los nodos cliente que son clientes de copia de seguridad/archivado, clientes IBM Spectrum Protect for Space Management o clientes de aplicación.

### NAS

Especifica nodos NAS.

### Server

Especifica los nodos cliente que son otros servidores de .

## Authentication

Especifica el método de autenticación de contraseña para el nodo.

### Local

Muestra aquellos nodos que se autentican en el servidor de IBM Spectrum Protect.

### LDap

Muestra aquellos nodos que se autentican en el servidor de directorios LDAP. La contraseña del nodo es sensible a las mayúsculas/minúsculas.

## Ejemplo: visualizar información acerca de los nodos de cliente registrados

Visualizar información sobre todos los nodos de cliente registrados.

```
query node
```

Nombre	Platafor.	Nombre nodo	Días desde dominio políticas	Días desde último acceso	Bloqueo asignación contraseña
CLIENT1	AIX	STANDARD	6	6	No
GEORGE	AIX	STANDARD	1	1	No
JANET	AIX	STANDARD	1	1	No
JARED	Linux86	STANDARD	1	1	No
JOE2	Mac	STANDARD	<1	<1	No
TOMC	WinNT	STANDARD	1	1	No

## Ejemplo: visualizar información detallada acerca de un nodo cliente

Visualizar información completa sobre el nodo cliente llamado Joe.



```
query node joe format=detailed
```

```
Nombre nodo: JOE
Plataforma: WinNT
Nivel SO cliente: 4.00
Versión cliente: Versión 5, Release 4, Nivel 0.0
Versión de la aplicación: Versión 6, Release 4, Nivel 0.4
Nombre dominio políticas: STANDARD
Fecha/hora último acceso: 09/24/2012 18:55:46
Días desde último acceso: 6
```

```

Fecha/hora asignación contraseña: 24/09/2012 18:26:43
Días desde asignación contraseña: 6
Número conexiones no válidas: 0
    Bloqueo: No
    Contacto:
        Compresión: Cliente
¿Supresión copias archivadas?: Sí
¿Supresión copias seguridad?: No
Fecha/hora de inscripción: 24/09/2012 18:26:43
Inscrito por administrador: SERVER_CONSOLE
Último método comunicación utilizado: Tcp/Ip
Bytes recibidos última sesión: 108,731
Bytes enviados última sesión: 698
Duración de última sesión: 0,00
Porcentaje de esperas desocupado última sesión: 0,00
Porcentaje de Método comunicaciones última sesión: 0.00
Porcentaje de esperas medio última sesión: 0,00
    Conjunto opciones:
        URL: http://joe.host.name:1581
        Tipo de nodo: Cliente
    Período caducidad contraseña: 60
        ¿Mantener punto de montaje?: No
Número máximo de puntos de montaje permitidos: 2
Cambiar nombre de espacio de archivos automáticamente: No
Protocolo de validación: No
    Nombre TCP/IP:
        Dirección TCP/IP: 9.11.153.39
        ID exclusivo global: 11.9c.54.e0.8a.b5.11.d6.b3.c3.00.06.29.45.c1
Archivos máximos en grupo de transacción: 0
Ruta de grabación de datos: ANY
Ruta de lectura de datos: ANY
Iniciación de sesión: ClientOrServer
Dirección de alto nivel:
Dirección de bajo nivel: 1501
Nombre de grupo de proximidad:
Nodo proxy destino:
Agente de nodo proxy:
    Grupos de nodo:
        Dirección de correo electrónico:
        Eliminación de duplicados: ServerOnly

```

 Sistemas operativos AIX  Sistemas operativos Linux Usuarios permitidos para realizar copias de seguridad: ALL

```

Estado de réplica: activado
Modalidad de réplica: Enviar
Regla de réplica de copia de seguridad: DEFAULT
Regla de réplica de archivado: ALL_DATA
Regla de réplica de gestión de espacio: Ninguna
Servidor primario de réplica: PRODSERVER1
Última réplica en servidor: DRSERVER1
Nombre de sistema operativo cliente: WIN: Windows XP
Arquitectura de procesador de cliente: x86
Productos de cliente instalados: WIN, FCM, VE
Versión de destino de cliente: Versión 6, Release 2, Nivel 0.0
    Autenticación: Local
        SSL necesario: No
        Session Security: Strict
        Método de transporte: TLS 1.2
    Dividir objetos grandes: Sí
        Tipo de riesgo: Intervalo predeterminado
        Intervalo de riesgo:
        URL de utilidad:
Recuperación de duplicación de archivos dañados: sí
Fuera de servicio:
Fecha de fuera de servicio:

```

## Descripciones de los campos

---

### Nombre del nodo

El nombre del nodo cliente.

### Plataforma

Sistema operativo del nodo de cliente existente la última vez que el nodo de cliente contactó con el servidor. El signo de interrogación (?) se visualizará hasta que el nodo de cliente acceda al servidor por primera vez e informe acerca de su tipo de sistema operativo.

### Nivel SO cliente

Nivel del sistema operativo para el cliente existente la última vez que el nodo de cliente contactó con el servidor.

Versión del cliente

La versión del cliente instalado en el nodo cliente.

Este campo no se aplica a los nodos NAS.

Versión de la aplicación

Versión del cliente de Data Protection for VMware.

Nombre de dominio de políticas

El dominio de políticas asignado del nodo de cliente.

Fecha/hora último acceso

La última fecha y hora en que el nodo cliente ha accedido al servidor.

Días desde último acceso

Número de días que han transcurrido desde la última vez que el nodo de cliente accedió al servidor.

Fecha/hora asignación contraseña

Fecha y hora del establecimiento de la contraseña del nodo de cliente.

Días desde asignación contraseña

Número de días que han transcurrido desde que se estableció la contraseña para el nodo de cliente.

Contador de conexiones no válidas

Número de intentos de inicio de sesión no válidos que se han realizado desde el último inicio de sesión satisfactorio. Este número puede ser distinto de cero solo cuando el límite de contraseña no válida (SET INVALIDPWLIMIT) es mayor que cero. Cuando el número de intentos no válidos es igual al límite establecido por el mandato SET INVALIDPWLIMIT, el nodo queda bloqueado respecto al sistema.

Bloqueo

Si el nodo de cliente está bloqueado en IBM Spectrum Protect.

Contacto

Cualquier información de contacto del nodo cliente.

Compresión

Si la compresión está activada en el nodo cliente.

Este campo no se aplica a los nodos NAS.

¿Supresión copias archivadas?

Si el nodo cliente puede suprimir sus propias copias archivadas.

¿Supresión copias seguridad?

Si el nodo cliente puede suprimir sus propias copias archivadas.

Fecha/hora registro

La fecha y la hora en que se ha inscrito el nodo cliente.

Registrado por administrador

El nombre del administrador que ha inscrito el nodo cliente.

Último método comunicación utilizado

El método de comunicación que ha utilizado por última vez el nodo cliente para contactar con el servidor.

Bytes recibidos última sesión

El número de bytes que ha recibido el servidor durante la última sesión del nodo cliente.

Este campo no se aplica a los nodos NAS.

Bytes enviados última sesión

El número de bytes enviados al nodo cliente.

Este campo no se aplica a los nodos NAS.

Duración última sesión

Cuánto tiempo ha durado la última sesión del nodo de cliente, en segundos.

Este campo no se aplica a los nodos NAS.

Porcentaje de esperas desocupado última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente no ha estado ejecutando ninguna función.

Este campo no se aplica a los nodos NAS.

Porcentaje de Método comunicaciones última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando una respuesta del servidor.

Este campo no se aplica a los nodos NAS.

Porcentaje de esperas soporte última sesión

El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando que se montara un volumen extraíble.

Este campo no se aplica a los nodos NAS.

#### Conjunto de opciones

El nombre del conjunto de opciones del cliente.

#### URL

El URL del cliente web de IBM Spectrum Protect que está configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

#### Tipo de nodo

El tipo de nodo cliente. Son posibles los valores siguientes:

- Cliente: un cliente de archivado y copia de seguridad, un cliente de IBM Spectrum Protect for Space Management o un cliente de aplicaciones
- Servidor: un servidor de IBM Spectrum Protect
- NAS: servidor de archivos de almacenamiento conectado a red

#### Período de caducidad de contraseña

El período de caducidad de contraseña del nodo de cliente.

#### ¿Mantener punto de montaje?

Si el nodo de cliente retiene un punto de montaje durante una sesión.

#### Número máximo de puntos de montaje permitidos

El número de puntos de montaje que un nodo de cliente puede utilizar en el servidor para las operaciones de migración de IBM Spectrum Protect for Space Management y de copia de seguridad y archivado. Este parámetro no se aplica a los nodos con un tipo NAS o SERVER. Si un nodo de cliente se ha registrado en un servidor de la Versión 3.7 o posterior, el valor estará comprendido entre 0 y 999, en función del valor que se ha establecido con el parámetro MAXNUMMP del comando REGISTER NODE. Si el nodo cliente se ha registrado en versiones anteriores del servidor y el parámetro MAXNUMMP no se ha establecido explícitamente con el comando UPDATE NODE, el valor se establece en NOLIMIT. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos de las operaciones de almacenamiento de datos simultáneas del mismo nodo de cliente. Esta evaluación puede impedir que las operaciones de almacenamiento de datos adquieran puntos de montaje.

#### Cambiar nombre de espacio de archivos automáticamente

Si IBM Spectrum Protect solicita al cliente que redetermine los espacios de archivos cuando el sistema cliente se actualiza a un cliente que admite Unicode. Este campo sólo es válido para los sistemas cliente que utilizan los sistemas operativos Windows, Macintosh OS X o NetWare.

#### Protocolo de validación (en desuso)

Si el cliente tiene activada la validación de datos. Si el cliente tiene activada la validación, este campo especifica si IBM Spectrum Protect valida sólo los datos del archivo o todos los datos, incluidos los metadatos del archivo. Puede habilitar la validación de datos con los mandatos REGISTER NODE o UPDATE NODE. Este campo está en desuso.

#### Nombre TCP/IP

Nombre de host del nodo cliente existente la última vez que el nodo cliente contactó con el servidor. El campo se deja vacío si el software de cliente no admite la notificación de esta información al servidor.

#### Dirección TCP/IP

Dirección TCP/IP del nodo cliente existente la última vez que el nodo cliente contactó con el servidor. El campo se deja vacío si el software de cliente no admite la notificación de esta información al servidor.

#### ID exclusivo global



Identificador exclusivo global (GUID) utilizado la última vez que el nodo cliente estableció contacto con el servidor. Este GUID identifica el sistema principal donde está ubicado el nodo.

#### Archivos máximos en grupo de transacción

Especifica el número de archivos por validación de transacción que se transfieren entre un cliente y un servidor. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.



#### Ruta de grabación de datos

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento. Si no hay disponible una ruta, el nodo no puede enviar ningún dato.

 Sistemas operativos AIX  Sistemas operativos Linux Las opciones de la ruta de transferencia de datos son ANY, LAN o fuera de LAN.

#### Ruta de lectura de datos

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. Si no hay disponible una ruta, no es posible leer datos.

 Sistemas operativos AIX  Sistemas operativos Linux Las opciones de la ruta de transferencia de datos son ANY, LAN o fuera de LAN.



## Iniciación de sesión

Controla si el servidor o el cliente ha de iniciar las sesiones. Están disponibles las dos opciones siguientes:

- ClientOrServer
- Serveronly

## Dirección alto nivel

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados cuando SESSIONINITIATION se define con el valor SERVERONLY.

## Dirección bajo nivel

Especifica el número de puerto del cliente en el que éste está a la escucha de las sesiones del servidor cuando SESSIONINITIATION se define con el valor SERVERONLY.

## Nombre de grupo de proximidad

Especifica el nombre del grupo de proximidad al que pertenece un nodo. Si un nodo no pertenece a un grupo de proximidad, este campo está en blanco.

Consejo: Si el nodo contiene espacios de archivos que son miembros de un grupo de proximidad de espacio de archivos, este campo se deja en blanco. Puede encontrar nombres de espacio de archivos emitiendo el mandato QUERY FILESPACE.

## Destino nodo proxy

Especifica qué nodos son nodos proxy (agentes) de otros nodos, en una lista separada por espacios. Si no hay ningún nodo en ese tipo de asociación, este campo está en blanco.

## Agente de nodo proxy

Especifica el nombre de nodo originador (destino) para una sesión de nodo proxy en una lista separada por espacios. Si no hay ningún nodo en ese tipo de asociación, este campo está en blanco.

## Grupos de nodos



Especifica el nombre del grupo de nodos al que pertenece un nodo. Si un nodo no pertenece a un grupo de nodos, este campo está en blanco.



## Dirección de correo electrónico

Especifica la dirección de correo electrónico del nodo de cliente.

## Eliminación de duplicados

La ubicación donde se eliminan los duplicados de los datos. El valor ServerOnly especifica que los duplicados de los datos almacenados en este nodo solo se pueden eliminar en el servidor. El valor Clientorserver especifica que los datos almacenados por este nodo se pueden deduplicar en el cliente o en el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux Usuarios que pueden realizar copias de seguridad

 Sistemas operativos AIX  Sistemas operativos Linux Especifica si un ID de usuario no root o sólo un ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor. ALL indica que todos los usuarios pueden realizarla, mientras que ROOT indica que sólo el ID de usuario root puede realizar la copia de seguridad de los archivos en el servidor. Esta salida no está disponible si el sistema operativo del nodo cliente se considera un sistema operativo de usuario único.

## Estado de réplica

Indica si el nodo está habilitado para la réplica. Son posibles los siguientes valores:

### Habilitado

El nodo está configurado para la réplica y preparado para replicarse.

### Inhabilitado

El nodo está configurado para la réplica pero no está preparado para replicarse.

### Ninguno

El nodo no está configurado para la réplica.

## Modalidad de réplica

Indica si el nodo está configurado como origen o destino de los datos replicados. Si este campo está en blanco, el nodo no está configurado para la réplica. Son posibles los siguientes valores:

### Enviar

El nodo está configurado como origen de los datos para la réplica.

### Recibir

El nodo está configurado como destino de los datos para la réplica.

### SyncSend

Los datos que pertenecen al nodo van a estar sincronizados con los datos de nodo que hay en el servidor de réplica de destino. La sincronización se aplica sólo a los nodos cuyos datos se han importado desde un servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

### SyncReceive

Los datos que pertenecen al nodo van a estar sincronizados con los datos de nodo que hay en el servidor de réplica de origen. La sincronización se aplica sólo a los nodos cuyos datos se han importado desde un servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

### Ninguno

El nodo no está configurado para la réplica.

#### Servidor primario de réplica

Especifica el servidor de réplica de origen para el nodo de cliente.

#### Norma de réplica de copia de seguridad

##### Norma de réplica archivada

##### Norma de réplica de gestión de espacio

La regla de réplica que se aplica a los datos de copia de seguridad, archivado y gestionados por espacio que pertenecen al nodo. Son posibles los siguientes valores:

##### ALL\_DATA

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad normal.

##### ACTIVE\_DATA

Replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro FORCERECONCILE=YES.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

##### ALL\_DATA\_HIGH\_PRIORITY

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad alta.

##### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta.

##### DEFAULT

Replica los datos de copia de seguridad, archivado o gestionados por espacio según la regla de dominio para el tipo de datos.

##### NONE

No se replica ningún dato. Por ejemplo, si la regla de réplica de los datos de archivado es NONE, los datos de archivado que pertenecen al nodo no se replican.

#### Última duplicación en el servidor

Especifica el nombre del servidor al que se ha replicado por última vez el nodo y el nombre del servidor al que el cliente realiza la recuperación de errores durante las operaciones de restauración.

#### Nombre SO cliente

El sistema operativo del cliente. El asistente de despliegue del cliente utiliza esta información para desplegar un paquete en el cliente. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

#### Arquitectura de procesador de cliente

La arquitectura del cliente. El asistente de despliegue del cliente utiliza este valor para determinar qué paquete se desplegará cuando se esté actualizando el cliente. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

#### Productos cliente instalados

Los productos que se encuentran en el nodo. Se podrían listar los productos siguientes:

- BA (cliente de archivado y copia de seguridad)
- VE (entornos virtuales)
- FCM (FlashCopy Manager)

#### Versión de destino de cliente

La versión del cliente que se instalará en el momento planificado a través del mandato DEFINE SCHEDULE o UPDATE SCHEDULE. Este campo se notifica solo para clientes de IBM Spectrum Protect en V6.2.0.0 y posterior.

#### Autenticación

Especifica el método de autenticación de contraseña: LOCAL, LDAP o LDAP (pendiente).

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP

Destino de autenticación	Método de autenticación
Este nodo está configurado para autenticarse con un servidor de directorio LDAP, pero el nodo aún no se autenticó.	LDAP (pendiente)

SSL necesario (en desuso)

Especifica si la configuración de seguridad para el nodo requiere capa de sockets seguros (SSL). Los valores pueden ser SI, NO o predeterminado. Debe tener autorización de nivel de sistema para actualizar el valor de nodo SSLREQUIRED . Este campo está en desuso.

Seguridad de sesión

Especifica el nivel de seguridad de sesión que se aplica para el nodo. Los valores pueden ser STRICT o TRANSITIONAL.

Método de transporte

Especifica el método de transporte que se ha utilizado la última vez para el nodo especificado. Los valores pueden ser TLS 1.2, TLS 1.1 o NONE. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

Dividir objetos grandes

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. Sí indica que el servidor divide los objetos grandes (más de 10 GB) en fragmentos más pequeños cuando un nodo de cliente los almacena. No indica que este proceso se omite. El valor predeterminado es Yes (sí).

Tipo de riesgo

Especifica el tipo de evaluación de riesgo. Los valores pueden ser Predeterminado, Eludido o Personalizado. Predeterminado especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el mandato SET STATUSATRISKINTERVAL. Eludido especifica que el nodo no se evalúa para el estado de riesgo por el supervisor de estado. Personalizado indica que el nodo se evalúa con el intervalo que se ha especificado mediante el mandato SET NODEATRISKINTERVAL, en lugar del intervalo que se ha especificado mediante el mandato SET STATUSATRISKINTERVAL.

Intervalo de riesgo

Especifica el número de horas entre dos actividades de copia de seguridad del cliente, o dos actividades de réplica, después de lo cual el supervisor de estado indica que la actividad está en riesgo. Este campo contiene un valor únicamente cuando el campo Tipo en riesgo contiene el valor Personalizado.

URL de programa de utilidad

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde Centro de operaciones.

Recuperación de duplicación de archivos dañados

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino.

Fuera de servicio

Especifica si el nodo de cliente está fuera de servicio. Son posibles los siguientes valores:

YES

Especifica que el nodo está fuera de servicio.

Valor nulo

Especifica que el nodo no está fuera de servicio.

PENDING

Especifica que el nodo se está poniendo fuera de servicio o que el proceso para ponerlo fuera de servicio ha fallado.

Consejo: Si desea determinar el estado de un proceso para poner fuera de servicio pendiente, siga las instrucciones de Poner fuera de servicio un nodo de cliente.

Fecha de fuera de servicio

Especifica la fecha en la que el nodo de cliente se quedó fuera de servicio.

## Ejemplo: visualizar información acerca de los roles de nodo

La salida de ejemplo es sólo una porción de la pantalla completa.

```
query node alvin f=d
```

```

Agente de nodo proxy:
  Grupos de nodo:
    Dirección de correo electrónico:
    Optimización de almacenamiento: ServerOnly
  Usuarios permitidos para realizar copias de seguridad: Todos
  Rol: Servidor
  Alteración temporal de rol: UseReported
  Proveedor del procesador: ORACLE
  Marca del procesador: UltraSPARC-T2
  Tipo de procesador: 4
  Modelo de procesador:

```

Número de procesadores: 1  
 Hipervisor:  
 Aplicación de la API: NO  
 Error de exploración: NO  
 Dirección MAC:

## Descripciones de los campos

Rol	El rol de procesador que notifica el cliente.
Alteración temporal de rol	El valor de alteración temporal del rol, especificado con el mandato UPDATE NODE.
Proveedor de procesador	El proveedor de procesador que notifica el cliente.
Marca de procesador	La marca de procesador que notifica el cliente.
Tipo de procesador	El tipo de procesador que notifica el cliente. Este valor especifica el número de núcleos de procesador utilizados para el cálculo de PVU.
Modelo de procesador	El modelo de procesador que notifica el cliente.
Recuento de procesadores	El número de procesadores que notifica el cliente.
Hypervisor	El hipervisor que notifica el cliente.
Aplicación de API	El indicador del cliente que indica que el cliente es una aplicación de la API.
Error de escaneo	El indicador de si la última exploración de información del procesador falla y necesita alguna investigación.
Dirección MAC	La dirección MAC que notifica el cliente.

## Ejemplo: ver todos los nodos que se autentican en el servidor de IBM Spectrum Protect

Si desea ver todos los nodos que se autentican localmente, especifique el mandato siguiente:

```
query node * authentication=local
```

Nombre nodo	Platafor.	Nombre dominio política	Días desde últ. acceso	Días desde contraseña	Bloqueado?
NODE1	WinNT	STANDARD	3	3	No
LOCAL	(?)	STANDARD	7	7	No

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY NODE

Comando	Descripción
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.
RENAME NODE	Cambia el nombre de un nodo cliente.

Comando	Descripción
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## QUERY NODEDATA (Consultar datos de cliente en volúmenes)

Utilice este comando para visualizar la información sobre los datos de uno o varios nodos de una agrupación de almacenamiento de acceso secuencial. QUERY NODEDATA visualiza el nombre del volumen en el que se escriben los datos de un nodo y la cantidad de espacio que ocupan los datos en dicho volumen. Esta información resulta útil al determinar la forma de agrupar nodos en agrupaciones de almacenamiento ubicadas próximas.

### Clase de privilegio

Restricción: No puede utilizar este mandato para ver información de las agrupaciones de almacenamiento de contenedor.

Cualquier administrador puede emitir este comando.

### Sintaxis

```

      .-,-----
      v          |
>>-Query NODEData+-----nombre_nodo+-----+----->
      '-COLLOCGroup-----grupo_proximidad-'

>--+-----+-----+-----+-----+----->
      '-STGpool-----nombre_agrupación-'

>--+-----+-----+-----+-----+-----<
      '-VOLume-----nombre_vol-'

```

### Parámetros

#### nombre\_nodo

Especifica el nombre del nodo de cliente para el que desea localizar datos. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas; no utilice espacios intercalados. También puede utilizar caracteres comodín para especificar varios nombres. Debe especificar un nombre de nodo o un nombre de grupo de proximidad, pero no ambos.

#### COLLOCGroup

Especifica el nombre del grupo de proximidad para el que desea localizar datos. Debe especificar un nombre de nodo o un nombre de grupo de proximidad, pero no ambos.

Importante: Si la cantidad de espacio necesaria para completar la consulta sobre un grupo de proximidad supera el límite del almacenamiento intermedio SQL, el mandato QUERY NODEDATA puede fallar. Si el comando falla por esta razón, emita el comando QUERY COLLOCGroup para visualizar una lista de los nodos del grupo. A continuación, emita el mandato QUERY NODEDATA para cada nodo del grupo.

#### STGpool

Especifica el nombre de la agrupación de almacenamiento secuencial que se va a consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar los nombres. Si un comodín coincide con el nombre de una agrupación de almacenamiento de disco, se pasará por alto el nombre de la agrupación de almacenamiento de disco. Si no especifica un valor para este parámetro, se consultarán todas las agrupaciones de almacenamiento secuenciales.

#### VOLume

Especifica el volumen que contiene los datos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar varios nombres. Si no especifica un valor para este parámetro, se consultarán todos los volúmenes de la agrupación de almacenamiento.

## Utilizar comodines para visualizar datos de nodo para una agrupación de almacenamiento de acceso secuencial

Visualizar información sobre el lugar de almacenamiento de los datos de nodo de una agrupación de almacenamiento secuencial. Utilice un carácter de comodín para indicarlos nombres de nodo. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodedata e*
```

Nombre	Nombre volumen	Nombre agrupación	Espacio físico almacen. ocupado (MB)
EDU_J2	E:\tsm\server\00000117.BFS	EDU512	0,01
EDU_J2	E:\tsm\server\00000122.BFS	EDU319	0,01
EDU_J3	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_J3	E:\tsm\server\00000120.BFS	EDU319	0,01
EDU_J7	E:\tsm\server\00000118.BFS	EDU512	0,04
EDU_J7	E:\tsm\server\00000123.BFS	EDU319	0,04
EDU_JJ1	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_JJ1	E:\tsm\server\00000121.BFS	EDU512	0,01

## Visualizar información de datos de nodo para un grupo de proximidad específico

Visualizar la información sobre la ubicación de los datos de nodo de una agrupación de almacenamiento secuencial de un grupo de proximidad determinado. En este ejemplo, los nodos EDU\_J3 y EDU\_JJ1 son los únicos miembros que pertenecen al grupo de proximidad, grp1, e incluyen datos en una agrupación de almacenamiento de acceso secuencial.

```
query nodedata collogroup=grp1
```

Nombre	Nombre volumen	Nombre agrupación	Espacio físico almacen. ocupado (MB)
EDU_J3	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_J3	E:\tsm\server\00000120.BFS	EDU319	0,01
EDU_JJ1	E:\tsm\server\00000116.BFS	EDU512	0,01
EDU_JJ1	E:\tsm\server\00000121.BFS	EDU512	0,01

Si especifica un grupo de proximidad de espacio de archivos, solo se visualizarán los volúmenes de los espacios de archivos pertenecientes al grupo de proximidad. Si especifica un grupo de proximidad de espacio de archivos y un volumen, se visualizarán los volúmenes del espacio de archivos dentro del grupo de proximidad que estén también en el volumen especificado.

## Descripciones de los campos

Nombre del nodo

Especifica el nombre del nodo.

Nombre de volumen

Especifica el nombre del volumen que contiene los datos de nodo.

Nombre de la agrupación de almacenamiento

Especifica el nombre de la agrupación de almacenamiento a la que se asigna el volumen.

Espacio físico ocupado (MB)

Especifica la cantidad de espacio físico que ocupan los datos del nodo. El espacio físico incluye el espacio vacío dentro de los agregados, de donde pueden haberse suprimido o donde pueden haber caducado los archivos.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY NODEDATA

Comando	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.

Comando	Descripción
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE COLLOGROUP	Actualiza la descripción de un grupo de proximidad.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## QUERY NODEGROUP (Consultar un grupo de nodos)

Utilice este comando para visualizar los grupos de nodos definidos en el servidor.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query NODEGroup-+-----+----->
                        .-*-----
                        '-nombre_grupo-'

.-Format----Standard----.
>-+-----+-----<
  '-Format----+Standard-+'
                        '-Detailed-'

```

### Parámetros

#### nombre\_grupo

Especifica el nombre del grupo de nodos que se visualizará. Para especificar varios nombres, utilice un carácter comodín. Este parámetro es opcional. El valor predeterminado es visualizar todos los grupos de nodos.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información. Para visualizar los miembros del grupo de nodos, debe especificar FORMAT=DETAILED.

### Ejemplo: obtener una lista de los grupos de nodos del servidor

Visualizar los grupos de nodos definidos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodegroup
```

Nombre del grupo de nodos	Descripción del grupo de nodos
DEPT_ED	Departamento de formación
GROUP1	Nodos cliente de baja capacidad.

## Ejemplo: visualizar información detallada del grupo de nodos

Visualizar información completa sobre todos los grupos de nodos y determinar qué nodos cliente pertenecen a qué grupos de nodos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query nodegroup format=detailed
```

```

Nombre del grupo de nodos: DEPT_ED
Descripción del grupo de nodos: Departamento de formación
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 04/21/2006 10:59:03
Miembro(s) del grupo de nodos: EDU_1 EDU_7

Nombre del grupo de nodos: GROUP1
Descripción del grupo de nodos: nodos cliente de baja
capacidad.
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 04/21/2006 10:59:16
Miembro(s) del grupo de nodos: CHESTER REX NOAH JARED

```

## Descripciones de los campos

Nombre de grupo de nodos

El nombre del grupo de nodos.

Descripción de grupo de nodos

La descripción del grupo de nodos.

Última actualización por (administrador)

El nombre del administrador que ha definido o ha actualizado más recientemente el grupo de nodos.

Fecha/hora última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente el grupo de nodos.

Miembro(s) de grupos de nodos

Los miembros del grupo de nodos.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY NODEGROUP

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.



# QUERY OCCUPANCY (Consultar espacios de archivos de cliente en agrupaciones de almacenamiento)

Utilice este comando para ver dónde están almacenados los espacios de archivos de cliente y cuánto espacio ocupan.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query OCCupancy----->
. -*----- .
>+-----+----->
|          .-*-----|
|'-nombre_nodo--+'|
|          '-nombre_espacio_archivos-'|
+-----+----->
'-STGpool----nombre_agrupación-'
>+-----+----->
'-DEVclass----nombre_clase_dispositivo-'
. -Type----ANY----- . -NAMEType----SERVER----- .
>+-----+-----+-----+----->
|'-Type----+-ANY-----+' |'-NAMEType----+-SERVER---+'|
|          +-Backup--+          +-UNICODE+|
|          +-Archive+          '-FSID----'|
|          '-SPacem--'|
. -CODEType----BOTH----- .
>+-----+-----<<
|'-CODEType----+-UNICODE-----+'|
|          +-NONUNICODE+|
|          '-BOTH-----'|
```

## Parámetros

### nombre\_nodo

Especifica el nodo propietario de los espacios de archivos que desea localizar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los nodos.

### nombre\_espacio\_archivos

Especifica el espacio de archivos que desea localizar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los espacios de archivos. Debe especificar un nombre de nodo si especifica un nombre de espacio de archivos.

Para un servidor que tenga clientes con soporte de Unicode, es posible que necesite hacer que el servidor convierta el nombre de espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre entrado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para obtener información detallada. Si no especifica ningún nombre de espacio de archivos o especifica sólo un carácter comodín para dicho nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

### STGpool

Especifica la agrupación de almacenamiento en la que se consultan los archivos del espacio de archivos especificado. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todas las agrupaciones de almacenamiento.

### DEVclass

Especifica la clase de dispositivo asociada con los dispositivos donde están almacenados los espacios de archivos. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán las agrupaciones de almacenamiento asociadas con cualquier clase de dispositivo.

### Type

Especifica los tipos de archivos a consultar en los espacios de archivos. Este parámetro es opcional. El valor predeterminado es ANY. Los valores posibles son:

#### ANY

Especifica que se consulten todos los tipos de archivos: las versiones de copia de seguridad de los archivos, las copias archivadas de los archivos y los archivos migrados de los clientes de IBM Spectrum Protect for Space Management.

#### Backup

Especifica que se consultarán todos los archivos de copia de seguridad.

#### Archive

Especifica que se consultarán todas las copias archivadas.

#### SPacem

Especifica que se consultan los archivos bajo gestión de espacio (archivos que se migraron mediante un cliente de IBM Spectrum Protect for Space Management).

#### NAMEType

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Un cliente de copia de seguridad/archivado con soporte Unicode sólo está disponible para Windows, Macintosh OS 9, Macintosh OS X y NetWare. Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado.

El valor predeterminado es SERVER. Los valores posibles son:

#### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

#### UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contienen los nombres y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

#### FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

#### CODEType

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre del espacio de archivos o cuando no especifique ningún nombre de espacio de archivos.

El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Los valores posibles son:

#### UNICODE

Incluir espacios de archivos que sólo están habilitados para Unicode.

#### NONUNICODE

Incluir espacios de archivos que no sólo están habilitados para Unicode.

#### BOTH

Incluir espacios de archivos independientemente del tipo de página de códigos.

## Ejemplo: visualizar los espacios de archivos asignados a un nodo específico

Visualizar información sobre dónde se almacenan todos los espacios de archivos asignados al nodo denominado DAISY. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query occupancy daisy
```

Nombre nodo	Tipo	Nombre espacio	FSID	Nombre agrup. almac.	Número de archivos	Espacio físico ocupado (MB)	Espacio lógico ocupado (MB)
DAISY	C.S.	DRIVED	1	COPYFILE	38	0,45	0,42

## Ejemplo: visualizar los espacios de archivos asignados a un nodo específico que tienen un tipo de archivo de copia de seguridad

Visualizar información sobre los espacios de archivos que pertenecen al nodo WAYNE y que tienen un tipo de archivo de copia de seguridad. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query occupancy wayne type=backup
```

Nombre nodo	Tipo	Nombre espacio	FSID	Nombre agrup.	Número de	Espacio físico	Espacio lógico
-------------	------	----------------	------	---------------	-----------	----------------	----------------

			almac.	archivos	ocupado (MB)	ocupado (MB)	
WAYNE	C.S.	DWG1	1	BACKUPPOOL1	2.330	53,19	50,01
WAYNE	C.S.	OS2C	2	BACKUPPOOL1	1.554	32,00	31,30

## Descripciones de los campos

### Node Name

El nodo propietario del espacio de archivos. Si el nodo se ha suprimido anteriormente, se visualiza el nombre de nodo DELETED.

### Type

El tipo de datos. Los valores posibles son:

#### Arch

Datos que se han archivado.

#### C.S.

Datos de los que se ha realizado una copia de seguridad.

#### G.E.

Datos que se han migrado desde un cliente IBM Spectrum Protect for Space Management.

### Filespace Name

El nombre del espacio de archivos que pertenece al nodo.

Si el espacio de archivos se suprimió anteriormente, se visualiza el nombre de espacio de archivos DELETED.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

### Nombre agrupación almacenamiento

La agrupación de almacenamiento donde está ubicado el espacio de archivos.

### Número de archivos

El número de archivos lógicos que pertenecen al espacio de archivos y están almacenados en esta agrupación de almacenamiento. Al almacenar un archivo superior a 10 GB, el servidor divide el archivo en fragmentos de 10 GB. El número de fragmentos también está incluido en este valor para cálculos de ocupación.

### Espacio físico ocupado (MB)

La cantidad de espacio físico ocupado por el espacio de archivos. El espacio físico incluye el espacio vacío dentro de los agregados, de donde pueden haberse suprimido o donde pueden haber caducado los archivos. Para este valor, 1 MB = 1048576 bytes.

Consejo: Este campo no visualiza un valor para las agrupaciones de almacenamiento que se han configurado para la eliminación de datos duplicados. Si desactiva la eliminación de datos duplicados para una agrupación de almacenamiento, no se visualizará ningún valor para la ocupación física hasta que no exista ningún archivo al que se haya aplicado la eliminación de duplicados en la agrupación de almacenamiento.

### Espacio lógico ocupado (MB)

La cantidad de espacio ocupado por los archivos lógicos en el espacio de archivos. El espacio lógico es el espacio que se utiliza realmente para almacenar archivos, excluido el espacio vacío en los agregados. Para este valor, 1 MB = 1048576 bytes.

### FSID

El identificador del espacio de archivos (FSID). El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY OCCUPANCY

Comando	Descripción
---------	-------------

Comando	Descripción
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.

## QUERY OPTION (Consultar opciones del servidor)

Utilice este comando para visualizar la información sobre las opciones del servidor.

Cambie las opciones de servidor editando el archivo de opciones de servidor o bien emitiendo el mandato SETOPT. Cuando edita el archivo de opciones del servidor, debe volver a arrancar el servidor para que los cambios entren en vigor. Cualquier cambio que realice al emitir el mandato SETOPT entrará en vigor de forma inmediata.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query OPTion--+-----+-----><
                    .-*----- .
                    '-nombre_opción-'
```

### Parámetros

nombre\_opción

Especifica el nombre de una opción del archivo de opciones del servidor. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Se visualizarán todas las opciones del servidor que coincidan. Si no especifica este parámetro, se visualizará información acerca de todas las opciones.

### Ejemplo: visualizar todas las opciones del servidor

Visualizar información acerca de todas las opciones del servidor. En la salida se indicarán todas las opciones y los valores que se han especificado para éstas.

```
query option
```

### Ejemplo: visualizar los valores de las opciones empleando un carácter comodín

Ver los valores de todas las opciones que comienzan por L.

```
query option l*
```

```
Opción servidor      Valor opción
-----
Language             AMENG
```

### Ejemplo: visualizar los servidores de directorios LDAP

Ver los valores de todos los servidores de directorios LDAP.

```
query option ldapurl
```

```
Opción servidor      Valor opción
-----
LDAP URL             ldap:\\tophoy.tucson.com\cn=tsmdata
LDAP URL             ldap:\\krypton.ibm.com\ou=tsmdata,dc=ibm,dc=com
```



Especifica que sólo se visualizarán rutas con el tipo de origen DATAMOVER.

**SERVer**

Especifica que sólo se visualizarán rutas con el tipo de origen SERVER. (Un origen de tipo SERVER es un agente de almacenamiento.)

**DESTType**

Especifica el tipo de destino. Este parámetro es opcional. El valor predeterminado es visualizar las rutas de todos los tipos de destino. Los valores posibles son:

**ANY**

Especifica que se visualizarán las rutas con cualquier tipo de destino.

**DRive**

Especifica que sólo se visualizarán rutas con el tipo de destino DRIVE. Cuando el tipo de destino es una unidad, debe especificar el nombre de biblioteca. Puede especificar las rutas que deben visualizarse especificando un nombre en el parámetro LIBRARY.

**LIBRary**

Especifica que sólo se visualizarán las rutas cuyo tipo de destino sea LIBRARY.

**LIBRary**

Especifica el nombre de la biblioteca a la que pertenece la unidad. Este parámetro es necesario cuando el tipo de destino es una unidad (DESTTYPE=DRIVE).

**Format**

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

**Standard**

Especifica que se visualizará información parcial.

**Detailed**

Especifica que se visualizará toda la información.

## Ejemplo: visualizar información de ruta de resumen

---

Visualizar información acerca de las rutas para el origen NETAPP1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path netapp1
```

Nombre orig	Tipo origen	Nombre destino	Tipo destino	Activado
NETAPP1	DATAMOVER	DRIVE1	DRIVE	Yes
NETAPP1	DATAMOVER	NASLIB	LIBRARY	Yes

## Ejemplo: visualizar información de ruta detallada

---

Visualizar información detallada acerca de las rutas para el origen NETAPP1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path  
netapp1 format=detailed
```

 **Sistemas operativos Linux**

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: NASLIB  
Tipo destino: LIBRARY  
Biblioteca:  
Dispositivo: /dev/tmsmcsi/mc0  
Directorio:  
Activado: Yes  
Última actualización por (administrador): SERVER_CONSOLE  
Fecha/hora última actualización: 21/06/2002 20:52:56
```

```
Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: DRIVE1  
Tipo destino: DRIVE  
Biblioteca: NASLIB  
Dispositivo: rst01  
Directorio:  
Activado: Yes
```

Última actualización por (administrador): SERVER\_CONSOLE  
Fecha/hora última actualización: 21/06/2002 20:55:23

 Sistemas operativos AIX  Sistemas operativos Windows

Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: NASLIB  
Tipo destino: LIBRARY  
Biblioteca:  
Dispositivo: mc0  
Directorio:  
Activado: Yes

Última actualización por (administrador): SERVER\_CONSOLE  
Fecha/hora última actualización: 06/21/2001 20:52:56

Nombre origen: NETAPP1  
Tipo origen: DATAMOVER  
Nombre destino: DRIVE1  
Tipo destino: DRIVE  
Biblioteca: NASLIB  
Dispositivo: rst01  
Directorio:  
Activado: Yes

Última actualización por (administrador): SERVER\_CONSOLE  
Fecha/hora última actualización: 06/21/2001 20:55:23

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplo: mostrar información de ruta detallada de un servidor de medios de z/OS

---

Mostrar la información detallada sobre una ruta de servidor de medios de z/OS. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query path format=detailed
```

Source Name: SERVER1  
Tipo origen: SERVER  
Nombre destino: ZOSMEDIA  
Tipo destino: LIBRARY  
Biblioteca:  
Nombre nodo:  
Dispositivo:  
Gestor externo:  
Servidor de medios ZOS: MEDSERV1  
Método Método:  
LUN:  
Iniciador: 0  
Directorio:  
Activado: Yes

Última actualización por (administrador): ADMIN  
Fecha/hora última actualización: 08/06/2011 15:33:39

## Descripciones de los campos

---

Nombre de origen

El nombre del origen.

Nombre de destino

El nombre del destino.

Tipo de origen

El tipo del origen.

Tipo de destino

El tipo de destino.

Biblioteca

El nombre de la biblioteca que contiene la unidad de destino.

Este campo estará en blanco si el tipo de destino es una biblioteca. El nombre de biblioteca se encontrará en el campo de nombre de destino cuando el destino sea una biblioteca.

Node Name

El nombre del dispositivo que es el destino.

Dispositivo

El nombre del dispositivo que es el destino.

- Gestor externo  
El nombre del gestor externo.
- Servidor de medios ZOS  
El nombre del servidor de medios z/OS.
- Método comunicaciones  
Especifica el tipo de método de comunicación.
- LUN  
Especifica el nombre de unidad lógica mediante el cual el origen puede acceder al disco.
- Iniciador  
Especifica el iniciador de la comunicación.
- Directorio  
Especifica la ubicación de directorio de un archivo en el origen.
- En línea  
Especifica si la ruta está activada y disponible para utilizarla.
- Última actualización por (administrador)  
El ID del administrador que ha realizado la última actualización.
- Fecha/hora de la última actualización  
Fecha y hora en las que tuvo lugar la última actualización.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY PATH

Comando	Descripción
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE PATH	Suprime una ruta de un origen a un destino.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## QUERY POLICYSET (Consultar un juego de políticas)

Utilice este comando para visualizar información sobre uno o varios juegos de políticas.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query Policyset----->
      .-*-----
>--+-----+----->
|          .-*-----          |
|'-nom_dominio--+-----+-'|
|          '-nombre_conjunto_políticas-'|
      .-Format----Standard----.
>--+-----+-----><
|'-Format----+Standard-+'|
|          '-Detailed-'|
```

### Parámetros

- nombre\_dominio  
Especifica el dominio de políticas asociado al juego de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un valor para este parámetro, se consultarán todos los dominios de políticas. Debe especificar este parámetro cuando consulte un juego de políticas denominado explícitamente.
- nombre\_juego\_políticas  
Especifica el juego de políticas que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica ACTIVE o el nombre de un juego de políticas, se consultarán todos los juegos de políticas.
- Format



Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

## Ejemplo: obtener una lista de los juegos de políticas de todos los dominios

Consultar todos los juegos de políticas de todos los dominios de políticas. Crear la salida en formato estándar. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query policyset
```

Nombre dominio políticas	Nombre juego políticas	Nombre clase gestión archivos	Descripción del cliente
EMPLOYEE- _RECORDS	ACTIVE	ACTIVEFI- LES	Dpto. de personal
EMPLOYEE- _RECORDS	HOLIDAY	ACTIVEFI- LES	Dpto. de personal
EMPLOYEE- _RECORDS	VACATION	ACTIVEFI- LES	Dpto. de personal
PROG1	SUMMER		Políticas grupo de programación
PROG2	SUMMER		Políticas grupo de programación
STANDARD	ACTIVE	STANDARD	Juego políticas predeterminado instalado.
STANDARD	STANDARD	STANDARD	Juego políticas predeterminado instalado.

## Ejemplo: visualizar información detallada acerca de un juego de políticas específico

Consultar el juego de políticas VACATION que está en el dominio de políticas EMPLOYEE\_RECORDS. Crear la salida en formato detallado. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query policyset employee_records vacation  
format=detailed
```

```
Nombre dominio políticas: EMPLOYEE_RECORDS  
Nombre juego políticas: VACATION  
Nombre clase gestión predeterminada: ACTIVEFILES  
Descripción: Dpto. de personal  
Última actualización por (administrador): $$CONFIG_MANAGER$$  
Fecha/hora última actualización: 31/05/1998 13:15:50  
Perfil gestión: ADSM_INFO  
Cambios pendientes: Si
```

## Descripciones de los campos

Nombre de dominio de políticas

El nombre del dominio de políticas.

Nombre de juego de políticas

El nombre del juego de políticas.

Nombre clase gestión predeterminada

La clase de gestión asignada como la clase de gestión predeterminada para el juego de políticas.

Descripción

La descripción del juego de políticas.

Última actualización por (administrador)

El nombre del administrador o del servidor que ha actualizado por última vez el juego de políticas. Si este campo contiene \$\$CONFIG\_MANAGER\$\$, el conjunto de políticas está asociado a un dominio que gestiona el gestor de configuración.

Fecha/hora última actualización

La fecha y la hora en que se ha definido o actualizado por última vez el juego de políticas.

Perfil de gestión

El perfil o los perfiles que gestionan el dominio al que pertenece este juego de políticas.

Cambios pendientes

Si están realizándose o no cambios que no se han activado. Cuando los cambios se han activado, el campo se restablece en No.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## QUERY PROCESS (Consultar uno o más procesos de servidor)

Utilice este comando para que se visualice información acerca de los procesos subordinados activos.

Para cancelar los procesos subordinados, emita el comando CANCEL PROCESS. Para mostrar información detallada sobre los procesos de réplica de nodos, emita el comando QUERY REPLICATION.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query PRocess--+-+-----+----->
                    '-process_number-'
>--+-----+--+-----+-----<
    '-DESCRiption----serie-' '-STATus----serie-'
```

### Parámetros

número\_proceso

Especifica el número de proceso subordinado que se ha de consultar. Este parámetro es opcional. Si no especifica, se visualizará información sobre todos los procesos subordinados.

DESCRiption

Especifica la serie de texto que desea buscar en la lista de descripciones de procesos activos. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

STATus

Especifica la serie de texto que desea buscar en la lista de estados de procesos activos. La expresión de texto debe estar delimitada por comillas si contiene algún carácter en blanco. Puede utilizar un carácter comodín para especificar esta serie. Este parámetro es opcional.

### Ejemplo: consultar un único proceso subordinado

Visualizar información acerca del proceso en segundo plano 202. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process 202
```

Número proceso	Descripción proceso	Estado proceso
202	EXPORT SERVER	ANR0NNNI EXPORT Identificador MYEXPORTSERVER ANR0648I Se ha copiado lo siguiente: 8 dominios 2 juegos de políticas 10 Clases de gestión 4 Grupos de copia 1 administrador 746 Bytes (Se han detectado 0 errores) Volúmenes de entrada actuales: C:\BUILD\540\GA\BUILD\NT\I386\DEBUG\ -00000014.BFS, (6 segundos)

## Ejemplo: consultar todos los procesos subordinados

Visualizar información acerca de todos los procesos en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

proceso de consulta

Número proceso	Descripción proceso	Estado proceso
304	IDENTIFY DUPLICATES	Agrupación de almacenamiento FILEPOOL, Volumen /tsmpool2/00006664. BFS, Archivos procesados: 2000, Extensiones duplicadas encontradas: 344, Bytes duplicados encontrados: 3.238.123, Archivo físico actual (bytes): 2.626.676.296. Estado: Procesando
284	IDENTIFY DUPLICATES	Agrupación almacenamiento FILEPOOL, Volumen /tsmpool2/00006666. BFS, Archivos procesados: 2000, Extensiones duplicadas encontradas: 344, Bytes duplicados encontrados: 3.238.123, Archivo físico actual (bytes): Ninguno. Estado: En espera
4	Replicar nodo	Replicando nodo(s) IRONMAN. Espacios de archivos completos: 0. Espacios de archivos identificándose y replicándose: 1. Espacios de archivos replicándose: 0. Espacios de archivos no iniciados: 3. Archivos actuales: 11.920. Archivos replicados: 0 de 0. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 11.482 KB de 11.482 KB. Cantidad transferida: 11.482 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).
37	Caducidad	Procesados 12 nodos de un total de nodos, examinados 411 objetos, suprimiendo 411 de copia de seguridad, 0 objetos de archivado, 0 volúmenes de copia de seguridad de BD, 0 archivos del plan de recuperación; 0 objetos reintentados y 0 errores encontrados.

## Ejemplo: consultar todos los procesos de réplica en segundo plano

Visualizar información acerca de todos los procesos de réplica en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process desc="replicate node"
```

Número proceso	Descripción proceso	Estado proceso
4	Replicar nodo	Replicando nodo(s) IRONMAN. Espacios de archivos completos: 0. Espacios de archivos identificándose y replicándose: 1. Espacios de archivos replicándose: 0. Espacios de archivos no iniciados: 3. Archivos actuales: 11.920. Archivos replicados: 0 de 0. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 11.482 KB de 11.482 KB. Cantidad transferida: 11.482 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).

### Ejemplo: consultar todos los procesos de réplica en segundo plano para un nodo específico

Visualizar información acerca de todos los procesos de réplica en segundo plano. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query process desc="replicate node" status=ironman
```

Número proceso	Descripción proceso	Estado proceso
4	Replicar nodo	Replicando nodo(s) IRONMAN. Espacios de archivos completos: 0. Espacios de archivos identificándose y replicándose: 1. Espacios de archivos replicándose: 0. Espacios de archivos no iniciados: 3. Archivos actuales: 11.920. Archivos replicados: 0 de 0. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 11.482 KB de 11.482 KB. Cantidad transferida: 11.482 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).

### Ejemplo: Verificar que se ha iniciado un proceso de recuperación de réplica

Después de iniciar un proceso de réplica de nodo con la recuperación de archivos habilitada, verifique que el servidor de réplica de destino ha iniciado el proceso de recuperación de archivo. Emita el mandato QUERY PROCESS en el servidor de réplica de destino. Para ver una descripción de los campos, consulte Descripciones de los campos.

```
proceso de consulta
```

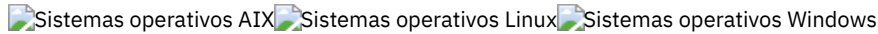
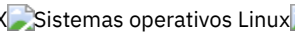
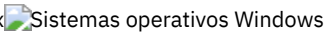
Proceso proceso	Descripción proceso	Estado proceso
4	Replicar nodo - Recuperación.	Replicando nodo(s) 3MAUTOIMPORT. Espacios de archivos completos: 87. Espacios de archivos identificándose y replicándose: 0. Espacios de archivos replicando: 6. Espacios de archivos iniciados: 0. Archivos actuales: 0. Archivos replicados: 0 de 14. Archivos actualizados: 0 de 0. Archivos suprimidos: 0 de 0. Cantidad replicada: 0 KB de 11.688 bytes. Cantidad transferida: 0 KB. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minuto(s).

### Ejemplo: Verificar que se recuperan los archivos dañados durante un proceso de réplica

Después de iniciar un proceso de réplica de nodo con la recuperación de archivos habilitada, verifique que los archivos dañados se están recuperando. Emita el mandato QUERY PROCESS en el servidor de réplica de origen. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Proceso proceso	Descripción proceso proceso	Estado proceso
6	Replicar nodo (Como recuperación secundaria)	Recuperando archivos dañados del servidor SERVER2, proceso 4, número de sesiones activas 10.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Ejemplo: verificar que los archivos se convierten

Después de iniciar un proceso de conversión de agrupación de almacenamiento, verifique que los archivos se convierten. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Número proceso	Descripción proceso	Estado proceso
6	Convert Stgpool	Convirtiendo agrupación de almacenamiento FILEPOOL1 en una agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Volúmenes convertidos: 1 de 6, Volúmenes erróneos: 0, Archivos convertidos: 975, Bytes convertidos: 196.27 MB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 151,27 MB
7	Convert Stgpool	Convirtiendo agrupación de almacenamiento DEDUPPOOL en agrupación de almacenamiento de contenedores de directorio DIRPOOL. Archivos convertidos: 150 de 360, Bytes convertidos: 79.598 KB de 388 MB. Archivos no convertidos: 12. Bytes no convertidos: 27 MB. Volumen de entrada actual: /fvt/srv/BK01. Tiempo transcurrido: 0 Day(s), 0 hora(s), 1 minuto(s).
8	Convert Stgpool	Convirtiendo agrupación de almacenamiento FILEPOOL1 en agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Archivos convertidos: 0, Bytes convertidos: 0 B de 1,00 GB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 0 B, Volumen de entrada actual: /STORAGE/file1/00000005.BFS, Tiempo transcurrido: 0 días, 0 horas, 1 minuto.
10	Convert Stgpool	Convirtiendo agrupación de almacenamiento FILEPOOL1 en agrupación de almacenamiento de contenedores de directorio NEWDEDUP1. Archivos convertido: 1007, Bytes convertidos: 285.44 MB of 1.33 GB, Archivos omitidos: 0, Bytes omitidos: 0 B, Total de bytes transferidos: 196.28 MB, Volumen de entrada actual: /STORAGE/file1/00000004.BFS, Tiempo transcurrido: 0 días, 0 horas, 1 minuto.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Ejemplo: Verificar el movimiento del disco local a la nube

Una vez iniciada la operación de transferencia de datos del disco local a la nube, verifique que los datos se están transfiriendo. Para ver una descripción de los campos, consulte Descripciones de los campos.

proceso de consulta

Número proceso	Descripción proceso	Estado proceso
-----	-----	-----

4	Transfer local a nube	Transferencia de disco local a nube para la agrupación de almacenamiento de contenedores de directorio CLOUDPOOL. 1 contenedor procesado. 2.100 KB en 4 extensiones de datos transferidos. Tiempo transcurrido: 0 día(s), 0 hora(s), 1 minutos(s).
---	-----------------------	--

## Descripciones de los campos

Número de proceso

Especifica el número que se asigna al proceso en segundo plano activo.

Descripción de proceso

Especifica una descripción del proceso subordinado activo.

Estado de proceso

Especifica el estado del proceso subordinado activo.

Consejo: Cuando un proceso de réplica de nodo ha finalizado en el servidor de réplica de destino, sólo se almacena el proceso final en el servidor de réplica de destino, sólo la información de proceso final se almacena en la tabla de resumen de actividades. El resumen completo para el proceso de réplica se almacena en la tabla de resumen de actividad en el servidor de réplica de origen.

## Comandos relacionados

Tabla 1. Comando relacionado con QUERY PROCESS

Comando	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
IDENTIFY DUPLICATES	Identifica datos duplicados en una agrupación de almacenamiento.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
RESTART EXPORT	Reinicia una operación de exportación suspendida.
SUSPEND EXPORT	Suspende una operación de exportación en ejecución.

## QUERY PROFILE (Consultar un perfil)

Utilice este comando para visualizar la información sobre perfiles y objetos asociados. Emita este comando desde un gestor de configuración o desde un servidor gestionado. Puede utilizar este comando para obtener información de perfiles de cualquier gestor de configuración definido en el servidor, aunque el servidor no esté inscrito en ningún perfil.

Si consulta un perfil bloqueado desde el gestor de configuración al que pertenece el perfil, se visualizará la información completa sobre el perfil. Si consulta un perfil bloqueado desde otro servidor, la salida de la consulta sólo visualizará que el perfil está bloqueado.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```

>>-Query PROFILE-----.*-----
                        |-----+----->
                        |'-nombre_perfil-'
>-----+----->
  |-----+-----+-----+----->
  |          (1) |
  |'-SERVer-----nombre_servidor-----'
  |-----+-----+-----+----->
  |.-Format-----Standard----- .-USELocal-----Yes-----
>-----+-----+-----+-----><

```

```
'-Format-----Standard-+-'  '-USELocal-----Yes-+-'
      '-Detailed-'                '-No--'
```

Notas:

1. El nombre del servidor depende del servidor desde donde se emita el comando: Consulte la descripción del parámetro SERVER.

## Parámetros

---

nombre\_perfil

Especifica el perfil que se visualiza. Para especificar varios nombres, utilice un carácter comodín. Este parámetro es opcional. El valor predeterminado es visualizar todos los perfiles.

SERVER

Especifica el gestor de configuración del que se ha de visualizar la información de perfil. Los requisitos del nombre dependen de dónde se emite la consulta:

- Desde un gestor de configuración: Este parámetro es opcional. El valor predeterminado es el nombre del gestor de configuración.
- Desde un servidor gestionado: Este parámetro es opcional. El valor predeterminado es el nombre del gestor de configuración para este servidor gestionado.
- Desde un servidor que no es un gestor de configuración ni un servidor gestionado: Debe especificar un nombre.

Format

Especifica si se visualiza la información parcial o detallada. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará información detallada.

USELocal

Al realizar la consulta desde un servidor gestionado, este parámetro especifica si la información del perfil se obtiene del gestor de configuración o del servidor gestionado. Si la información del perfil no existe en el servidor gestionado, la información se obtiene del gestor de configuración, independientemente del valor de este parámetro.

Si utiliza este parámetro en un servidor que no gestiona el gestor de configuración propietario del perfil, se hace caso omiso del parámetro. El valor predeterminado es YES. Los valores posibles son:

Yes

Especifica que la información del perfil, si está disponible, se obtiene del servidor gestionado. Si no hay información disponible del servidor gestionado, se establece contacto con el gestor de configuración.

No

Especifica que la información del perfil se obtiene del gestor de configuración aunque haya información disponible del servidor gestionado. De este modo se garantiza que recibirá información actual sobre el perfil.

## Ejemplo: obtener una lista de perfiles de un gestor de configuración.

---

Visualizar la información de perfil de un gestor de configuración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query profile
```

Gestor configuración	Nombre perfil	Bloqueo
SERVER1	DEFAULT_PROFILE	No
SERVER1	ADMIN_INFO	No
SERVER1	EMPLOYEE	No
SERVER1	PERSONNEL	Yes

## Ejemplo: visualizar información detallada de perfil para un servidor gestionado

---

Desde un servidor gestionado, visualizar información detallada actual para el perfil ADMIN\_INFO. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

Nota: Si el perfil está bloqueado, la mayoría de los campos no se visualizan.

```
query profile admin_info
format=detailed useLocal=no
```

```

Gestor configuración: SERVER1
Nombre perfil: ADMIN_INFO
Bloqueo: No
Descripción: Planificaciones de
              administración
              distribuidas
Administradores de servidor: DENNIS EMILY ANDREA
Dominios políticas: ADMIN RECORDS
Planificaciones comandos administración: ** todos los objetos **
Scripts comandos servidor:
Conjuntos opciones cliente:
Servidores:
Grupos servidores:

```

## Descripciones de los campos

Gestor de configuración  
El nombre del gestor de configuración propietario del perfil.

Nombre de perfil  
El nombre del perfil.

Bloqueo  
Si el perfil está bloqueado.

Descripción  
La descripción del perfil.

Administradores de servidor  
Los administradores que están asociados al perfil.

Dominios de políticas  
Los dominios de políticas que están asociados al perfil.

Planificaciones de comandos de administración  
Las planificaciones de administración que están asociadas al perfil.

Scripts de comandos del servidor  
Los scripts de comandos que están asociados al perfil.

Conjuntos de opciones de cliente  
Los conjuntos de opciones de cliente que están asociados al perfil.

Servidores  
Los servidores que están asociados al perfil.

Grupos de servidores  
Los nombres de los grupos de servidores que están asociados al perfil.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.
UPDATE PROFILE	Cambia la descripción de un perfil.

## QUERY PROTECTSTATUS (Consultar estado de protección de una agrupación de almacenamiento)



Utilice este mandato para mostrar información sobre el estado de protección de las agrupación de almacenamiento de contenedores de directorio.

## Clase de privilegio

Cualquier administrador puede emitir este mandato.

## Sintaxis

```
.-*-----.  
>>-Query PROTECTStatus--+-+-----+----->  
                               '-nombre_agrupación-'  
  
.-Format-----Standard-----.  
>--+-+-----+-----<<  
   '-Format-----+--Standard-+-'  
       '-Detailed-'
```

## Parámetros

### nombre\_agrupación

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que se va a consultar. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor, se mostrará el estado de todas las agrupaciones de almacenamiento de contenedores de directorio.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

## Ejemplo: Visualización de información de resumen de una agrupación de almacenamiento específica

Visualizar información para una agrupación de almacenamiento denominada POOL1. Emita el mandato siguiente:

```
query protectstatus pool1
```

Source	Source	Target	Target	Pct.	Last Complete
Server Name	Storage Pool	Server Name	Storage Pool	Protected	Protect
NEXT	POOL1	NEXT	POOL1COPY	96.55	02/17/2017 11:15:07
NEXT	POOL1	NEXT1	POOL2	99.99	02/17/2017 11:14:53
NEXT	POOL1	UNKNOWN	UNKNOWN	UNKNOWN	02/17/2017 11:13:44
NEXT1	POOL2	NEXT	POOL1	100.00	02/17/2017 12:56:58

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Ejemplo: Visualización de información detallada de una agrupación de almacenamiento específica

Visualizar información detallada acerca de la agrupación de almacenamiento denominada EZLIFE. Emita el mandato siguiente:

```
query protectstatus pool1 format=detailed
```

```
Source Server Name: NEXT  
Source Storage Pool: POOL1  
Target Server Name: NEXT  
Target Storage Pool: POOL1COPY  
Porcentaje de Protected: 96.55  
Data Extents Protected: 1,747  
Data Extents Total: 1,852  
Protected (MB): 165.33  
Total (MB): 171.23  
Last Completed Protection: 02/17/2017 11:15:07  
Last Refresh Date/Time: 02/19/2017 00:27:12
```

Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

## Descripciones de los campos

Source Server Name	El nombre del servidor de origen.
Agrupación de almacenamiento de origen	El nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de origen.
Target Server Name	El nombre del servidor de destino.
Agrupación de almacenamiento de destino	El nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de destino.
Porcentaje de Protegido	El porcentaje de datos protegidos en la agrupación de almacenamiento de contenedores de directorio.
Data Extents Protected	Número de extensiones de datos de la agrupación de almacenamiento de contenedores de directorio protegidas.
Data Extents Total	Número total de extensiones de datos en la agrupación de almacenamiento de contenedores de directorio.
Protected (MB)	Cantidad total de datos protegidos que se encuentran en la agrupación de almacenamiento de contenedores de directorio, en megabytes.
Total (MB)	Cantidad total de datos que se encuentran en la agrupación de almacenamiento de contenedores de directorio, en megabytes.
Last Completed Protection	La fecha y la hora de la última protección de la agrupación de almacenamiento de contenedores de directorio.
Last Refresh Date/Time	La fecha y la hora de la última actualización de la agrupación de almacenamiento de contenedores de directorio.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY PROTECTSTATUS

Comando	Descripción
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.

## QUERY PROXYNODE (Consulta la autorización de proxy de un nodo cliente)

Utilice este comando para visualizar los nodos cliente que tienen autorización para actuar como proxy con otros nodos cliente del servidor de IBM Spectrum Protect.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query PROXynode----TArget---+-----+-----><
                               .-*-----+-----+-----><
                               '-nombre_nodo_destino-'
```

### Parámetros

**TArget**  
Especifica el nombre del nodo señalado por el nodo con autoridad proxy. Opcionalmente, se puede especificar un nombre de nodo de destino. Pueden utilizarse nombres comodín para especificar el nombre de nodo de destino. También se permite una lista separada por comas de nombres de nodo.

### Ejemplo: obtener una lista de los nodos cliente que disponen de autorización de proxy

Para que se visualicen todos los nodos cliente de IBM Spectrum Protect que disponen de autorización de proxy para el nodo de destino denominado MYCLUSTER, emita el comando siguiente.

```
query proxynode target=mycluster
```

```
Nodo destino      Nodo agente
-----
FRED              MOE MINIE MICKEY
ALPHA            BETA GAMMA DELTA
```

## Descripciones de los campos

**Nodo destino**  
Especifica el nombre del nodo señalado por el nodo con autoridad proxy.

**Nodo agente**  
Especifica el nombre del nodo de agente.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY PROXYNODE

Comando	Descripción
GRANT PROXYNODE	Concede autorización de proxy a un nodo agente.
REVOKE PROXYNODE	Revocar la autoridad de proxy a un nodo de agente.

## QUERY PVUESTIMATE (Mostrar la estimación de unidades de valor de procesador)

Utilice este comando para obtener una estimación de los dispositivos de cliente y los dispositivos de servidor que gestiona este servidor de IBM Spectrum Protect. Asimismo, este comando proporciona una estimación de los totales de unidades de valor de procesador (PVU) para los dispositivos de servidor.

Este comando genera una estimación de PVU basada en el número de nodos lógicos que hay definidos en el servidor de IBM Spectrum Protect. En cambio, el cálculo de obligaciones de licencia se basa en el número de sistemas físicos. Es posible que no exista una correlación unívoca entre el número de nodos lógicos y el número de sistemas físicos. El informe que genera el comando QUERY PVUESTIMATE es una estimación, que no es vinculante jurídicamente.

Para el comando QUERY PVUESTIMATE, los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de cliente. Los nodos en las demás plataformas se consideran dispositivos de servidor. El servidor en el que se ejecuta IBM Spectrum Protect también se clasifica como un dispositivo de servidor. No obstante, puede volver a clasificar los dispositivos de servidor como dispositivos de cliente si es necesario. Si el sistema incluye estaciones de trabajo retiradas, estaciones de trabajo de prueba u otras que puedan ignorarse a efectos de cálculo de PVU, especifíquelas como el tipo Otros. Para cambiar una clasificación de nodo, utilice el mandato UPDATE NODE o el mandato REGISTER NODE.

Nota: La información de PVU proporcionada por IBM Spectrum Protect no se considera un sustituto aceptable de IBM® License Metric Tool.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query PVUESTIMATE--+-Format--Standard-----<<
                        '-Format--+-Standard-+-'
                        '-Detailed-'
```

## Parámetros

**Format**  
Especifica el formato de salida. Este parámetro es opcional. El valor predeterminado es Standard. Se pueden utilizar los siguientes valores:

**Standard**  
Especifica la salida estándar.

Detailed

Especifica la salida detallada.

## Ejemplo: visualizar el número estimado de dispositivos y PVU

Visualice el número estimado de dispositivos de cliente y dispositivos de servidor, y la PVU estimada de los dispositivos de servidor para un servidor de IBM Spectrum Protect. Emita el comando siguiente:

```
query pvestimate
```

Tabla 1. Salida de ejemplo de varios productos gestionados por un servidor de IBM Spectrum Protect

Producto	Número de dispositivos de cliente	Número de dispositivos de servidor	PVU de dispositivos de servidor
IBM Spectrum Protect Extended Edition	1.000	905	90.500
IBM Spectrum Protect para redes de área de almacenamiento	50	10	1.000
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect para correo	0	25	5.000
IBM Spectrum Protect para bases de datos	0	1.025	20.500
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
IBM Spectrum Protect para recuperación y copia de seguridad del sistema	0	0	0
Otras clasificaciones de nodos	Número		
Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente	10		
Nodos de la versión 6.3 o posteriores sin coincidencia de PVU	9		
Nodos clasificados por el administrador como "otros dispositivos"	8		
Nodos definidos como una aplicación de API sin licencia	6		

La lista siguiente incluye detalles sobre los campos de ejemplo:

### Producto

El nombre de producto IBM Spectrum Protect.

### Número de dispositivos de cliente

El número estimado de dispositivos de cliente que gestiona el producto. De forma predeterminada, solo los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de cliente.

### Número de dispositivos de servidor

El número estimado de dispositivos de servidor que gestiona el producto. De forma predeterminada, solo los nodos de los sistemas Microsoft Windows 7, Microsoft Windows XP Professional y Apple se supone que son dispositivos de servidor. Este número también incluye el servidor en el que se ejecuta IBM Spectrum Protect.

### PVU de dispositivos de servidor

Las PVU estimadas de todos los nodos que están conectados como dispositivos de servidor.

### Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente

Los dispositivos que no notifican información de procesador al servidor.

### Nodos de la versión 6.3 o posteriores sin coincidencia de PVU

Dispositivos que no notifican todos los valores necesarios o que notifican algunos valores como "Desconocido".

### Nodos clasificados por el administrador como "otros dispositivos"

Los nodos que el administrador excluye del recuento de PVU utilizando el comando `update node roleoverride=other`.

### Nodos definidos como una aplicación de API sin licencia

Nodos como, por ejemplo, las aplicaciones de API personalizadas o de copia de seguridad de DB2.

## Ejemplo: visualizar información detallada del nodo

Visualice información de nodos individuales especificando el valor detallado (d) para el parámetro Format. Emita el mandato siguiente:

```
tsm: PATMOS_630> query pvestimate f=d
```

Tabla 2. Clasificaciones de nodos para productos específicos

Producto	Número de dispositivos de cliente	Número de dispositivos de servidor	PVU de dispositivos de servidor
----------	-----------------------------------	------------------------------------	---------------------------------

<b>Producto</b>	<b>Número de dispos. de cliente</b>	<b>Número de dispos. de servidor</b>	<b>PVU de dispos. de servidor</b>
IBM Spectrum Protect Extended Edition	1.000	905	90.500
- banode1	1		
- banode2		1	200
- banode3	1		
- banode3		1	100
IBM Spectrum Protect para redes de área de almacenamiento	50	10	1.000
- stagent1		1	50
- stagent2		1	100
IBM Spectrum Protect for Space Management	0	0	0
IBM Spectrum Protect para correo	0	25	5.000
- mailnode1		1	200
- mailnode2		1	100
IBM Spectrum Protect para bases de datos	0	1.025	20.500
- dbnode1		1	200
- dbnode2		1	100
IBM Spectrum Protect for Enterprise Resource Planning	0	25	5.000
- erpnode1		1	50
- erpnode2		1	100
IBM Spectrum Protect para recuperación y copia de seguridad del sistema	0	0	0
<b>Otras clasificaciones de nodos</b>	<b>Número</b>		
Nodos anteriores a la versión 6.3 sin información de PVU disponible actualmente	10		
- oldnode1	1		
- oldnode2	1		
- mailnote44	1		
- erpnode66	1		
Nodos de la versión 6.3 o posteriores sin coincidencia de PVU	10		
- badcitnode1	1		
- badcitnode2	1		
- mailnode23	1		
- erpnode34	1		
Nodos clasificados por el administrador como "otros dispositivos"	8		
- overriddennode1	1		
- overriddennode2	1		

Otras clasificaciones de nodos	Número
- mailnode77	
Nodos definidos como una aplicación de API sin licencia	6
- vendorapinode1	1
- vendorapinode2	1

## Comandos relacionados

Tabla 3. Comandos relacionados con QUERY PVUESTIMATE

Comando	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## QUERY RECOVERYMEDIA (Consultar medio de recuperación)

Utilice este comando para visualizar información sobre el medio (por ejemplo, medio de arranque) necesario para efectuar la recuperación de una máquina. Los medios se visualizan por orden alfabético de nombres.

Recuerde: IBM Spectrum Protect no utiliza la información. Sólo está disponible para ayudar a planificar la recuperación ante siniestro de las máquinas cliente.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query RECOVERYMedia----->
      .-*-----
      '-nombre_medio-'

>+-----+-----+----->
      '-Type---+---B0ot---+' '-L0cation---+---ubicación-'
      '-Other-'

      .-Format---+---Standard-----
>+-----+-----+-----<<
      '-Format---+---Standard---+'
      '-Detailed-'

```

### Parámetros

nombre\_medio

Especifica el nombre del medio de recuperación. Puede utilizar caracteres comodín para especificar el nombre. Este parámetro es opcional. El valor predeterminado son todos los medios de recuperación.

#### Type

Especifica el tipo de medios que se han de consultar. Este parámetro es opcional. Si no se especifica este parámetro, se consultarán todos los medios de recuperación. Los valores posibles son:

BOot

Sólo se consultan los medios de arranque.

Other

Se consultan todos los medios excepto los de arranque.

#### Location

Especifica la ubicación del medio de recuperación que se ha de consultar. Este parámetro es opcional. Puede especificar hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. Los valores posibles son:

Standard

Visualiza información parcial. Este es el valor predeterminado.

Detailed

Visualiza toda la información.

## Ejemplo: visualizar información de resumen acerca de medios de recuperación específicos

---

Visualizar información para el medio de recuperación denominado RECMED1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query recoverymedia RECMED1
```

Nombre medio recuperación	Nombres volúmenes	Ubicación	Nombre máquina
RECMED1	vol1 vol2 vol3 vol4	IRONMOUNTAIN	MACH1

## Ejemplo: visualizar información detallada acerca de medios de recuperación específicos

---

Visualizar información detallada acerca del medio de recuperación denominado RECMED1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query recoverymedia RECMED1 format=detailed
```

```
Nombre medio recuperación: RECMED1
  Tipo: Arranque
  Nombres volúmenes: vol1 vol2 vol3 vol4
  Ubicación: IRONMOUNTAIN
  Descripción:
  Producto:
Información producto:
  Nombre máquina: MACH1
```

## Descripciones de los campos

---

### Nombre del medio de recuperación

El nombre del medio de recuperación.

### Tipo

Si el medio de recuperación es de tipo arranque o de otro tipo. Los valores posibles son:

#### Arranque

El medio de recuperación es de tipo arranque.

#### Otro

El medio de recuperación no es de tipo arranque.

### Nombres de volúmenes

Especifica el conjunto de volúmenes que contiene los datos necesarios para efectuar la recuperación para las máquinas asociadas a este medio.

### Ubicación

Lugar donde se almacena el medio de recuperación.

### Descripción

- La descripción del medio de recuperación.
- Producto
  - El producto utilizado para crear el medio de arranque.
- Información de producto
  - Información acerca del producto que ha creado el medio de arranque. Es posible que esta información sea necesaria para restaurar la máquina.
- Nombre de máquina
  - Las máquinas que están asociadas a este medio de recuperación.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY RECOVERYMEDIA

Comando	Descripción
DEFINE RECMEDMACHASSOCIATION	Asocia un medio de recuperación con una máquina.
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
UPDATE RECOVERYMEDIA	Cambia los atributos de un medio de recuperación.

## QUERY REPLICATION (Consultar los procesos de réplica de nodos)

Utilice este comando para visualizar la información sobre la ejecución y la finalización de procesos de réplica de nodos.

Emita este comando en el servidor que actúe como origen para los datos replicados.

Importante: No puede visualizar información sobre la ejecución de los procesos de réplica para los nodos cliente que se están convirtiendo de operaciones de importación y exportación a operaciones de réplica. El proceso de conversión podría ejecutarse durante un largo periodo de tiempo, pero sólo se produce una vez para un nodo cliente que se está convirtiendo.

De forma predeterminada, los registros sobre los procesos de réplica de nodos completados se retienen durante 30 días naturales. Un *día natural* consta de 24 horas, de medianoche a mediodía.

Para visualizar el periodo de retención, emita el mandato QUERY STATUS. Compruebe el valor en el campo Período de retención de registros de réplica. Para cambiar el periodo de retención, emita el mandato SET REPLRETENTION.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query REPLIcation--nombre_nodo----->
.
.*-----
>-----
| (1) |
'-----+--nombre_espacio_archivos--+--'
| '-----' |
'--+FSID--+-----'
| (2) |
|-----'
.
.-NAMEType----SERVER-----
>-----
'-NAMEType----+SERVER--+
+UNICODE--+
| (2) |
'-FSID-----'
.
.-CODEType----BOTH-----
>-----
'-CODEType----+BOTH--+
+UNICODE----+
'-NONUNICODE-'
.
.-DISplay----1-----.
```





El servidor interpreta los nombres de espacio de archivos utilizando los identificadores de espacios de archivos.

#### CODEType

Especifica el tipo de espacios de archivos que se van a incluir en la consulta. El valor predeterminado es BOTH, lo que significa que se incluyen los espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo si especifica un único carácter comodín para el nombre del espacio de archivos. Puede especificar uno de los siguientes valores:

##### UNICODE

Incluir solo espacios de archivos que están en Unicode.

##### NONUNICODE

Incluir únicamente espacios de archivos que no estén en Unicode.

##### BOTH

Incluir todos los espacios de archivos independientemente del tipo de página de códigos.

#### DISplay

Especifica el número de días de historial de réplicas de nodos que se muestran. El valor predeterminado es 1, que muestra información sobre la ejecución de procesos de réplica de nodo y sobre procesos que se han completado durante el día natural actual. El valor máximo es 9999.

Puede especificar un número que sea igual o menor que el número de días que se han especificado como periodo de retención para los registros de historial de réplicas. Si especifica un valor que es superior al valor del periodo de retención de réplica o superior al número de días en los que se recopilan registros de réplica, el servidor sólo muestra el número de registros de historial de réplica que están disponibles. Por ejemplo, suponga que el periodo de retención de réplica es 30 días y que el proceso de réplica se ejecuta sólo durante 10 días. Si especifica `DISPLAY=20`, sólo se visualizan 10 días del historial de réplica.

#### PROcessid

Especifica el historial de réplicas de nodos asociado con un determinado proceso identificado por el identificador de proceso. Este parámetro es opcional. Si no especifica este parámetro, se visualizarán todos los procesos para el número de días que especifica el parámetro `DISPLAY`.

El reinicio del servidor puede hacer que este reutilice los ID de proceso. La reutilización de ID de proceso puede generar ID de proceso duplicados para procesos diferentes.

#### STatus

Especifica el estado de los espacios de archivos a consultar. Este parámetro es opcional. El valor predeterminado es ALL. Puede especificar uno de los siguientes valores:

##### ALL

Especifica todos los espacios de archivos que se están replicando, espacios de archivos que se han replicado correctamente y espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

##### RUNning

Especifica todos los espacios de archivos que se están replicando en el servidor de réplica de destino.

##### ENded

Especifica todos los espacios de archivos que se han replicado correctamente y espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

##### FAiled

Especifica todos los espacios de archivos para los que no ha finalizado la replicación o que se han replicado con errores.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Puede especificar uno de los siguientes valores:

##### Standard

Especifica que se visualizará información parcial sobre los procesos de réplica de nodos.

##### Detailed

Especifica que se visualizará toda la información disponible sobre los procesos de réplica de nodos.

## Ejemplo: visualizar información sobre los procesos de réplica para un espacio de archivos

Visualice información sobre los procesos de réplica para un espacio de archivos en el nodo de cliente PAYROLL. El identificador del espacio de archivos es 10.

```
query replication ironman
```

```
NodeName Nombre FSID Hora de inicio Hora de finalización Estado Fase
archivos del cliente
```

```
-----  
IRONMAN    /space    2      02/08/11    02/08/11    Finalizado    Ninguna  
                21:44:19    21:48:14
```

query replication ironman format=detailed

```
Nombre nodo: IRONMAN  
Nombre de espacio de archivos: /space  
FSID: 2  
Hora de inicio: 02/08/11 21:44:19  
Hora de finalización: 02/08/11 21:48:14  
Estado: Finalizado  
Número de proceso: 4  
Comando: replicate node ironman  
Fase: Ninguna  
Tiempo de ejecución de proceso: 0 día(s) 0 hora(s)  
4 Minuto(s)  
Estado de terminación: Completo  
Razón de no completarse: Ninguna  
Fecha/hora última actualización de copia de seguridad:  
Servidor de destino de copia de seguridad:  
Archivos de copia de seguridad que no necesitan ninguna acción: 0  
Archivos de copia de seguridad que se replican: 0  
Archivos de copia de seguridad replicados: 0  
Archivos de copia de seguridad no replicados debido a errores: 0  
Archivos de copia de seguridad no replicados todavía: 0  
Archivos de copia de seguridad que se suprimen: 0  
Archivos de copia de seguridad suprimidos: 0  
Archivos de copia de seguridad no suprimidos debido a errores: 0  
Archivos de copia de seguridad que se actualizan: 0  
Archivos de copia de seguridad actualizados: 0  
Archivos de copia de seguridad no actualizados debido a errores: 0  
Bytes de copia de seguridad que se replican (MB): 0  
Bytes replicados de copia de seguridad (MB): 0  
Bytes transferidos de copia de seguridad (MB): 0  
Bytes de copia de seguridad no replicados  
debido a errores (MB): 0  
Bytes no replicados todavía de copia de seguridad (MB): 0  
  
Fecha/hora última actualización de archivado: 02/08/11 21:48:14  
Servidor de destino de archivado: NIGLINA  
Archivos de archivado que no necesitan ninguna acción: 0  
Archivos de archivado que se replican: 39.416  
Archivos de archivado replicados: 39.206  
Archivos de archivado no replicados debido a errores: 210  
Archivos de archivado no replicados todavía: 0  
Archivos de archivado que se suprimen: 0  
Archivos de archivado suprimidos: 0  
Archivos de archivado no suprimidos debido a errores: 0  
Archivos de archivado que se actualizan: 0  
Archivos de archivado actualizados: 0  
  
Archivos de archivado no actualizados debido a errores: 0  
Bytes de archivado que se replican (MB): 4.335  
Bytes replicados de archivado (MB): 4.335  
Bytes transferidos de archivado (MB): 0  
Bytes de archivado no replicados  
debido a errores (MB): 0  
Bytes no replicados todavía de archivado (MB): 0  
  
Fecha/hora última actualización de gestionados por espacio:  
Servidor destino de gestión de espacio:  
Archivos gestionados por espacio que no necesitan ninguna acción: 0  
Archivos gestionados por espacio que se replican: 0  
Archivos gestionados por espacio replicados: 0  
Archivos gestionados por espacio no replicados  
debido a errores: 0  
Archivos gestionados por espacio no replicados todavía: 0  
Archivos gestionados por espacio que se suprimen: 0  
Archivos gestionados por espacio suprimidos: 0  
Archivos de archivado no suprimidos  
debido a errores: 0  
Archivos gestionados por espacio que se actualizan: 0  
Archivos gestionados por espacio actualizados: 0  
Archivos gestionados por espacio no actualizados  
debido a errores: 0  
Bytes gestionados por espacio que se replican (MB): 0
```

```

Bytes replicados gestionados por espacio (MB): 0
Bytes transferidos gestionados por espacio (MB): 0
  Bytes gestionados por espacio no replicados
    debido a errores (MB): 0
Bytes no replicados todavía gestionados por espacio (MB): 0
  Total de archivos que no necesitan ninguna acción: 0
    Total de archivos que se replican: 39.416
    Total de archivos replicados: 39.206
Total de archivos no replicados debido a errores: 210
  Total de archivos no replicados todavía: 0
    Total de archivos que se suprimen: 0
    Total de archivos suprimidos: 0
Total de archivos no suprimidos debido a errores: 0
  Total de archivos que se actualizan: 0
  Total de archivos actualizados: 0
Total de archivos no actualizados debido a errores: 0
  Total de bytes que se replican (MB): 4.335
  Total de bytes replicados (MB): 4.335
  Total de bytes transferidos (MB):
  Total de Bytes no replicados
    Debido a errores (MB):
  Total de bytes no replicados todavía (MB):
  Porcentaje de terminación estimado: 100
  Tiempo estimado restante:
  Hora estimada de terminación:

```

## Descripciones de los campos

---

### Nombre del nodo

El nombre del nodo de cliente cuyos datos se están mostrando.

### Nombre de espacio de archivos

El nombre del espacio de archivos de cliente cuyos datos se están mostrando.

### FSID

El identificador del espacio de archivos.

### Hora de inicio

La fecha y la hora en que se ha iniciado el proceso de réplica de nodo.

### Hora de finalización

La fecha y la hora en que ha finalizado el proceso de réplica de nodo.

### Estado

El estado del proceso de réplica de nodo. Son posibles los siguientes valores:

#### Ejecutando

El proceso está activo y está buscando datos seleccionables o enviando datos al servidor de réplica de destino.

#### Finalizado

El proceso ha finalizado o ha fallado.

#### No válido

El proceso ha fallado.

### Número de proceso

El identificador del proceso de réplica de nodo.

El mismo número de proceso puede tener distintas horas de inicio. Si se inicia un proceso de réplica y se reinicia el servidor, el servidor empieza a asignar números de proceso que empiezan por el número 1. Los procesos de réplica que se inician después de un reinicio del servidor pueden obtener los números de proceso que ya se han asignado a otros procesos de réplica en el historial de réplicas. Para identificar procesos de réplica exclusivos, utilice la hora de inicio.

### Comando

El comando que se ha emitido para iniciar el proceso de réplica de nodo.

### Fase

La fase de un proceso de réplica de nodo en ejecución. Las siguientes fases se muestran en el orden en el que se producen:

#### Identificando

El proceso de réplica de nodo ha empezado a identificar los datos que se van a replicar, pero los datos no se están enviando todavía al servidor de réplica de destino.

#### Identificando y replicando

El proceso de réplica de nodo está identificando los datos que se van a replicar y transfiriendo los datos al servidor de réplica de destino.

#### Replicando

El proceso de réplica de nodo ha identificado los datos y transfiere los archivos al servidor de réplica de destino.

Ninguno

El proceso de réplica de nodo no se está ejecutando.

Tiempo de ejecución de proceso

El tiempo de ejecución del proceso de réplica de nodo.

Estado de finalización

El estado del proceso de réplica de nodo. Son posibles los siguientes valores:

Completo

El proceso de réplica de nodo se ha completado.

No completo

El proceso de réplica de nodo ha finalizado sin ejecutarse completamente. Para determinar la razón, compruebe el valor en el campo Razón de no completarse.

Razón de la no finalización

La razón por la que ha finalizado el proceso de réplica de nodo sin completarse. Los valores posibles incluyen *canceled* y *other*. El valor *other* puede indicar que se ha parado el servidor durante la réplica o que el servidor ha fallado.

Fecha/hora última actualización de copia de seguridad

La fecha y la hora en que se han actualizado por última vez las estadísticas de copia de seguridad. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Fecha/hora última actualización de archivado

La fecha y la hora en que se han actualizado por última vez las estadísticas de archivado. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Fecha/hora de la última actualización de gestionados por espacio

La fecha y la hora en que se han actualizado por última vez las estadísticas de los archivos gestionados por espacio. La hora especificada es la hora en que se han identificado para la réplica los archivos en el espacio de archivos o cuando se ha enviado cada lote de archivos al servidor de réplica de destino.

Servidor destino de copia de seguridad

El nombre del servidor de réplica de destino para los archivos de copia de seguridad.

Servidor destino de archivado

El nombre del servidor de réplica de destino para los archivos de archivado.

Servidor destino de gestión de espacio

El nombre del servidor de réplica de destino para los archivos gestionados por espacio.

Archivos de copia de seguridad que no necesitan acción

El número de archivos de copia de seguridad del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Copias archivadas que no necesitan acción

El número de archivos de archivado del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Archivos de espacio gestionado que no necesitan acción

El número de archivos gestionados por espacio del espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Archivos de copia de seguridad para replicar

El número de archivos de copia de seguridad que deben replicarse en el servidor de réplica de destino.

Copias archivadas para replicar

El número de archivos de archivado que deben replicarse en el servidor de réplica de destino.

Archivos gestionados por espacio para replicar

El número de archivos gestionados por espacio que deben replicarse en el servidor de réplica de destino.

Archivos de copia de seguridad replicados

El número de archivos de copia de seguridad que se han replicado en el servidor de réplica de destino.

Archivos de archivado replicados

El número de archivos de archivado que se han replicado en el servidor de réplica de destino.

Archivos gestionados por espacio replicados

El número de archivos gestionados por espacio que se han replicado en el servidor de réplica de destino.

Archivos de copia de seguridad no replicados debido a errores

El número de archivos de copia de seguridad que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos de archivado no replicados debido a errores

El número de archivos de archivado que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no replicados debido a errores

El número de archivos gestionados por espacio que no se han replicado en el servidor de réplica de destino debido a errores.

Archivos de copia de seguridad aún no replicados

El número de archivos de copia de seguridad que no se han replicado todavía en el servidor de réplica de destino.

Archivos de archivado aún no replicados

El número de archivos de archivado que no se han replicado todavía en el servidor de réplica de destino.

Archivos gestionados por espacio aún no replicados

El número de archivos gestionados por espacio que no se han replicado todavía en el servidor de réplica de destino.

Archivos de copia de seguridad para suprimir  
El número de archivos de copia de seguridad que deben suprimirse en el servidor de réplica de destino.

Archivos de archivado para suprimir  
El número de archivos de archivado que deben suprimirse en el servidor de réplica de destino.

Archivos gestionados por espacio para suprimir  
El número de archivos gestionados por espacio que deben suprimirse en el servidor de réplica de destino.

Archivos de copia de seguridad suprimidos  
El número de archivos de copia de seguridad que se han suprimido en el servidor de réplica de destino.

Archivos de archivado suprimidos  
El número de archivos de archivado que se han suprimido en el servidor de réplica de destino.

Archivos gestionados por espacio suprimidos  
El número de archivos gestionados por espacio que se han suprimido en el servidor de réplica de destino.

Archivos de copia de seguridad no suprimidos debido a errores  
El número de archivos de copia de seguridad que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos de archivado no suprimidos debido a errores  
El número de archivos de archivado que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no suprimidos debido a errores  
El número de archivos gestionados por espacio que no se han suprimido del servidor de réplica de destino debido a errores.

Archivos de copia de seguridad para actualizar  
El número de archivos de copia de seguridad que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos de archivado para actualizar  
El número de archivos de archivado que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos gestionados por espacio para actualizar  
El número de archivos gestionados por espacio que deben actualizarse en el servidor de réplica de destino. Si los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Archivos de copia de seguridad actualizados  
El número de archivos de copia de seguridad que se han actualizado en el servidor de réplica de destino.

Archivos de archivado actualizados  
El número de archivos de archivado que se han actualizado en el servidor de réplica de destino.

Archivos gestionados por espacio actualizados  
El número de archivos gestionados por espacio que se han actualizado en el servidor de réplica de destino.

Archivos de copia de seguridad no actualizados debido a errores  
El número de archivos de copia de seguridad que no se han actualizado en el servidor de réplica de destino debido a errores.

Archivos de archivado no actualizados debido a errores  
El número de archivos de archivado que no se han actualizado en el servidor de réplica de destino debido a errores.

Archivos gestionados por espacio no actualizados debido a errores  
El número de archivos gestionados por espacio que no se han actualizado en el servidor de réplica de destino debido a errores.

Bytes de copias de seguridad para replicar (MB)  
El número de bytes de copia de seguridad que deben replicarse en el servidor de réplica de destino.

Bytes de archivado para replicar (MB)  
El número de bytes de archivado que deben replicarse en el servidor de réplica de destino.

Bytes gestionados por espacio para replicar (MB)  
El número de bytes gestionados por espacio que deben replicarse en el servidor de réplica de destino.

Bytes de copias de seguridad replicados (MB)  
El número de bytes de copia de seguridad que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes de archivados replicados (MB)  
El número de bytes de archivado que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes gestionados por espacio replicados (MB)  
El número de bytes gestionados por espacio que se han replicado en el servidor de réplica de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Bytes de copias de seguridad transferidos (MB)

El número de bytes de copia de seguridad que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes de archivados transferidos (MB)

El número de bytes de archivado que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes gestionados por espacio transferidos (MB)

El número de bytes gestionados por espacio que se han transferido al servidor de réplica de destino.

El valor de este campo representa el número real de bytes de archivo enviados al servidor de réplica de destino. Este valor se calcula restando el número de bytes no enviados debido a la eliminación de duplicados del número de bytes que se van a replicar.

Bytes de copia de seguridad no replicados debido a errores (MB)

El número de bytes de copia de seguridad que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes de archivado no replicados debido a errores (MB)

El número de bytes de archivado que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes gestionados por espacio no replicados debido a errores (MB)

El número de bytes gestionados por espacio que no se han replicado en el servidor de réplica de destino debido a errores.

Bytes de copia de seguridad aún no replicados (MB)

El número de bytes de copia de seguridad que aún no se han replicado en el servidor de réplica de destino.

Bytes de archivados aún no replicados (MB)

El número de bytes de archivado que aún no se han replicado en el servidor de réplica de destino.

Bytes gestionados por espacio aún no replicados (MB)

El número de bytes gestionados por espacio que aún no se han replicado en el servidor de réplica de destino.

Total de archivos que no necesitan acción

El número total de archivos en el espacio de archivos que no han necesitado replicarse, actualizarse o suprimirse.

Total de archivos para replicar

El número total de archivos que se replican en el servidor de réplica de destino.

Total de archivos replicados

El número total de archivos que se han replicado en el servidor de réplica de destino.

Total de archivos no replicados debido a errores

El número total de archivos que no se han replicado debido a errores.

Total de archivos no replicados todavía

El número total de archivos que no se han replicado todavía en el servidor de réplica de destino.

Total de archivos para suprimir

El número total de archivos que se han suprimido en el servidor de réplica de destino.

Total de archivos suprimidos

El número total de archivos que se han suprimido en el servidor de réplica de destino.

Total de archivos no suprimidos debido a errores

El número total de archivos de copia de seguridad, archivado y gestionados por espacio que no se han suprimido en el servidor de réplica de destino debido a errores.

Total de archivos para actualizar

El número total de archivos que se van a actualizar en el servidor de réplica de destino. Cuando los metadatos de un archivo cambian, los campos modificados se envían al servidor de réplica de destino.

Total de archivos actualizados

El número total de archivos que se han actualizado en el servidor de réplica de destino.

Total de archivos no actualizados debido a errores

El número total de archivos de copia de seguridad, archivado y gestionados por espacio que no se han actualizado en el servidor de réplica de destino debido a errores.

Total de bytes para replicar (MB)

El número total de bytes que se replican en el servidor de réplica de destino.

Total de bytes replicados (MB)

El número total de bytes que se han replicado en el servidor de destino.

Si un archivo se ha almacenado en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el número de bytes en el archivo almacenado puede ser menor que el número de bytes en el archivo original. Este campo representa el número de bytes físicos en el archivo original.

Total de bytes transferidos (MB)

El número total de bytes que se han transferido al servidor de réplica de destino.

Para los archivos almacenados en una agrupación de almacenamiento donde se han eliminado los datos duplicados, el valor en este campo incluye el número de bytes en el archivo original antes de que se hayan eliminado las extensiones duplicadas. Si todavía hay extensiones duplicadas en el servidor de réplica de destino, el número de bytes en el archivo original es mayor que el número de bytes transferidos.

Total de bytes no replicados debido a errores (MB)

El número total de bytes que se han omitido porque el servidor de réplica de origen no ha podido transferirlos al servidor de réplica de destino.

Total de bytes aún no replicados (MB)

El número total de bytes que no se han transferido todavía al servidor de réplica de destino.

Porcentaje de finalización estimado

El porcentaje de terminación estimado basado en el número de bytes.

Tiempo restante estimado

El tiempo estimado que queda antes de que el proceso de réplica de nodo se haya completado.

Tiempo de finalización estimado

La hora estimada en que finalizará el proceso de réplica de nodo.

Tabla 1. Comandos relacionados con QUERY REPLICATION

Comando	Descripción
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLRETENTION	Especifica el periodo de retención de los registros de historial de réplicas.

## QUERY REPLNODE (Mostrar información sobre el estado de réplica de un nodo de cliente)

Utilice este mandato para mostrar el número de archivos almacenados para cada espacio de archivos replicado. Se muestra información sobre los espacios de archivo para cada nodo de cliente configurado para la réplica.

Se configura un nodo de cliente para la réplica si está activado o desactivado.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

      .-|-----|
      v
>>-Query REPLNode-----nombre_nodo-----+----->
>--+-----+-----<
    '-nombre_servidor_destino-'

```



## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nodo de cliente que es propietario de los archivos sobre los que desea información. Puede especificar uno o más nombres. Si especifica varios nombres, sepárelos con comas. No utilice espacios intercalados. Puede utilizar caracteres comodín para especificar varios nombres.

No se muestra la información sobre los nodos de cliente que coinciden con los criterios de archivo, pero que no están configurados para la réplica.

nombre\_servidor\_destino

Especifica el nombre del servidor de réplica que se va a consultar para obtener información de réplica. Este parámetro es opcional. Si no especifica un valor para este parámetro, se consulta el servidor que es el destino predeterminado para los datos replicados.

Como valor para este parámetro, también puede especificar un servidor que haya sido previamente un destino de los datos replicados.

Los nodos de cliente definidos en un servidor de réplica pueden ser el origen o el destino de los datos replicados. Para determinar si un nodo de cliente en particular está enviando o recibiendo datos, emita el comando QUERY NODE. Busque el valor *Send* o *Receive* en el campo Modalidad de réplica de la salida.

Para visualizar el nombre del servidor de réplica de destino activo, emita el comando QUERY STATUS y busque el nombre en el campo Servidor de réplica de destino.

## Ejemplo: listar los archivos de nodo de cliente en un servidor de réplica de origen y un servidor de réplica de destino

El nombre del nodo de cliente es NODE1.

```
query replnode *
```

Nodo Nombre	Tipo	Espacio de archivos Nombre	FSID	Archivos en Servidor	Réplica Servidor (1)	Archivos en Servidor (1)
NODE1	SpMg	/hmsmfs	1	1		
NODE1	Bkup	/lspace2	2	27		
NODE1	Arch	/lspace2	2	22	TGTSRV	22
NODE1	Bkup	/lspace	3	18.096		
NODE1	Arch	/lspace	3	61.150	TGTSRV	61.150
NODE2						

El número de archivos visualizados para los servidores de réplica puede ser diferente por los motivos siguientes:

- La salida del comando QUERY REPLNODE visualiza el número de archivos obtenidos de la tabla de ocupación. La tabla de ocupación sólo contiene archivos con una longitud mayor que cero. Los archivos que tienen una longitud de 0 y que se han replicado no se reflejan en esta salida.
- Si sólo se replican datos activos en el servidor de destino, el número de archivos visualizados para el servidor de origen será mayor que el número de archivos visualizados en el servidor de destino. El motivo de esta diferencia es que el servidor de réplica de origen tiene datos activos e inactivos y el servidor de destino sólo tiene datos activos.
- Un nodo de cliente puede tener datos exportados desde el servidor de réplica de origen e importados al servidor de réplica de destino. Si se han sincronizado los datos y el nodo de cliente también ha almacenado datos en el servidor de réplica de destino, el número de archivos en el servidor de réplica de destino será mayor que el número de archivos almacenados como resultado de las operaciones de exportación e importación y de la réplica.
- Cuando se replican datos de nodo desde un servidor de origen anterior a la versión 7.1 a un servidor de destino de la versión 7.1 o posterior, los archivos más grandes de 10 GB se dividen en archivos más pequeños si el parámetro SPLITLARGEOBJECTS de la definición de nodo está definido a *Yes*. Cada uno de estos archivos divididos se cuenta en el servidor de destino.

## Descripciones de los campos

Nombre del nodo

El nombre del nodo de cliente que es propietario de los archivos.

Tipo

El tipo de datos. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica. En la salida de ejemplo, NODE2 está configurado para la réplica, pero no tiene datos de copia de seguridad, archivado o gestionados por espacio.

Son posibles los siguientes valores:

Arch

Datos de archivado

C.S.

Datos de copia de seguridad

G.E.

Datos que IBM Spectrum Protect ha migrado para los clientes de gestión de espacio

Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

FSID

El identificador de espacio de archivos del espacio de archivos. El servidor asigna un FSID único cuando un espacio de archivo se almacena inicialmente en el servidor. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Archivos en el servidor

El número de archivos de copia de seguridad, archivado y gestionados por espacio en el servidor en el que se emite este comando. Si este campo está en blanco, el nodo de cliente está configurado para la réplica, pero no tiene datos en el servidor de réplica.

Servidor de réplica (1)

El nombre del servidor de réplica para el que se está consultando información. Si este campo está en blanco, pueden existir una o varias de las condiciones siguientes:

- El espacio de archivos del nodo en el servidor de réplica donde se ha emitido el comando no tiene ningún dato.
- El nodo de cliente no está definido en el servidor de réplica (1).
- El nodo de cliente está definido en el servidor de réplica (1), pero el nodo no está configurado para la réplica.
- El espacio de archivos correspondiente en el servidor de réplica (1) no tiene datos o el espacio de archivos no está definido.

Archivos en el servidor (1)

El número de archivos para el tipo de datos almacenados en el servidor de réplica de destino. Este campo puede estar en blanco. Si lo está, pueden existir una o varias de las condiciones siguientes:

- El servidor de réplica (1) no tiene datos.
- El nodo de cliente no está definido en el servidor de réplica (1).
- El nodo de cliente está definido en el servidor de réplica (1), pero el nodo no está configurado para la réplica.
- El espacio de archivos correspondiente en el servidor de réplica (1) no tiene datos o el espacio de archivos no está definido.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY REPLNODE

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.

Comando	Descripción
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.

## QUERY REPLRULE (Consultar reglas de réplica)

Utilice este mandato para visualizar la información sobre las reglas de réplica.

Emita este comando en el servidor que actúe como origen para los datos replicados.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query REPLRule-----*-----<<
'--ALL_DATA-----+'
+-ACTIVE_DATA-----+
+-ALL_DATA_HIGH_PRIORITY-----+
'-ACTIVE_DATA_HIGH_PRIORITY-'

```

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Parámetros

nombre\_regla

Especifica el nombre de la regla de réplica sobre la que desea mostrar información. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar una o varias reglas. Si no especifica este parámetro, se visualizará información sobre todas las reglas en la salida de la consulta. Puede especificar los siguientes valores:

ALL\_DATA

Muestra información sobre la regla de réplica ALL\_DATA. Esta regla replica los datos de copia de seguridad, archivado o gestionados por espacio. Los datos se replican con una prioridad normal.

ACTIVE\_DATA

Muestra información sobre la regla de réplica ACTIVE\_DATA. Esta regla replica sólo los datos de copia de seguridad activos. Los datos se replican con una prioridad normal. Esta regla no es válida para los datos de archivado o gestionados por espacio.

Atención: Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

ALL\_DATA\_HIGH\_PRIORITY

Muestra información sobre la regla ALL\_DATA\_HIGH\_PRIORITY. Esta regla replica los datos de copia de seguridad, archivado o gestionados por espacio. Los datos se replican con una prioridad normal. En un proceso de réplica, los datos de prioridad alta se replican antes que los datos de prioridad normal.

ACTIVE\_DATA\_HIGH\_PRIORITY

Muestra información sobre la regla ACTIVE\_DATA\_HIGH\_PRIORITY.

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta.

## Ejemplo: visualizar información sobre una regla de réplica de servidor

El nombre de la regla es ALL\_DATA\_HIGH\_PRIORITY

```
query replrule all_data_high_priority
```

Nombre de regla de réplica: ALL\_DATA\_HIGH\_PRIORITY

Servidor de réplica de destino:

Sólo activos: No

Activado: Sí

## Descripciones de los campos

Nombre de norma de réplica

Especifica el nombre de la regla que se ha consultado.

Servidor de réplica destino

Especifica el nombre del servidor de réplica de destino.

Sólo activos

Especifica si la regla se aplica sólo a los datos de copia de seguridad activos. Son posibles los siguientes valores:

Sí

Especifica que sólo se replican los datos de copia de seguridad activos para los espacios de archivos a los que se ha asignado esta regla.

No

Especifica que se replican todos los datos de copia de seguridad para los espacios de archivos a los que se ha asignado esta regla.

Habilitado

Especifica si la regla está activada o desactivada. Son posibles los siguientes valores:

Sí

Especifica que la regla está activada para la réplica. Los datos en los espacios de archivos a los que se ha asignado la regla se replican.

No

Especifica que la regla no está activada para la réplica. Los datos en los espacios de archivos a los que se ha asignado la regla no se replican.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY REPLRULE

Comando	Descripción
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.

## QUERY REPLSERVER (Consultar un servidor de réplica)

Utilice este mandato para ver información sobre todos los servidores de réplica que conoce el servidor. El resultado de este mandato incluye información del servidor para el servidor desde donde se ha emitido el mandato. El mandato indica si una definición de servidor de réplica se suprime como resultado de un mandato REMOVE REPLSERVER.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query REPLServer-+-----+----->>
                    .-*-----
                    '-nombre_servidor-'
```

## Ejemplo: visualizar estadísticas de resumen acerca de todos los servidores de réplica

---

Visualizar información sobre el servidor de réplica. Emita el mandato desde el servidor de réplica de origen o de destino:

```
query replserver *

ID exclusivo global de réplica: 4d.83.fc.30.67.c1.11.e1.b8.
                                40.f0.de.f1.5e.f1.89
      Nombre de servidor: Server1
      Última réplica:
      Pulsación:
Dirección de alto nivel de migración tras error: server1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas:

ID exclusivo global de réplica: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
      Nombre de servidor: DRServer1
      Última réplica: 30/06/2012 08:16:30
      Pulsación: 07/09/2012 22:15:22
Dirección de alto nivel de migración tras error: drserver1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas: On

ID exclusivo global de réplica: 90.4f.53.b0.8e.cb.11.e3.a8.
                                2f.00.14.5e.55.b3.67
      Nombre de servidor: DRSERVER2
      Última réplica: 01/04/2014 12:38:28
      Pulsación: 29/05/2014 11:15:44
Dirección de alto nivel de migración tras error: drserver2.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error:
Supresión en curso: No
                                Políticas heterogéneas: Off
```

## Ejemplo: visualizar estadísticas de resumen acerca de un servidor de réplica específico

---

Visualizar información sobre el servidor de réplica DRServer1. Emita el mandato desde el servidor de réplica de origen o de destino:

```
query replserver drserver1

ID exclusivo global de réplica: 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.27.00.58.dc
      Nombre de servidor: DRServer1
      Última réplica: 30/06/2012 08:16:30
      Pulsación: 07/09/2012 22:15:22
Dirección de alto nivel de migración tras error: drserver1.example.com
Número de puerto TCP de migración tras error: 1500
Número de puerto SSL de migración tras error: 1542
Supresión en curso: No
Políticas distintas: On
```

## Parámetros

---

nombre\_servidor

Especifica el nombre del servidor de réplica a consultar. Puede utilizar caracteres comodín para especificar este nombre. Se consultarán todos los servidores coincidentes. Si no especifica un valor para este parámetro, se consultarán todos los servidores. El parámetro es opcional.

## Descripciones de los campos

---

ID exclusivo global de réplica

El identificador exclusivo para el servidor de IBM Spectrum Protect. Los valores para el ID exclusivo global de réplica se crea cuando un servidor se utiliza por primera vez en un proceso de réplica.

Consejo: El ID que aparece en el campo ID exclusivo global de duplicación no es el mismo valor que el del ID en el campo ID exclusivo global de máquina que se muestra en el mandato QUERY STATUS.

Nombre servidor

Nombre del servidor de réplica.

Última réplica

La fecha del proceso de réplica último que utiliza el servidor.

#### Pulsación

La última vez que el servidor ha finalizado una sesión de comunicación de prueba satisfactoria.

#### Número de puerto TCP de migración tras error

El activo Transmission Control Protocol (TCP) de puerto de cliente en el servidor de réplica que se utiliza para las conexiones de cliente. Si el cliente está configurado para TCP, el puerto se utiliza para conectar con el servidor de migración tras error.

#### Número de puerto SSL de migración tras error

El puerto SSL activo en el servidor de réplica que se utiliza para las conexiones de cliente. Si el cliente está configurado para SSL, el puerto se utiliza para conectar con el servidor de migración tras error.

#### Dirección de alto nivel de migración tras error

La dirección de alto nivel que el cliente utiliza para conectar con el servidor de réplica durante la migración tras error.

#### Supresión en curso

Especifica si se ha emitido un mandato REMOVE REPLSERVER para este servidor de réplica y si todavía está en curso. Son posibles los siguientes valores:

Sí

La supresión del servidor de réplica está en curso.

No

La supresión de este servidor de réplica no está en curso.

#### Políticas distintas

Especifica si las políticas que están definidas en el servidor de réplica de destino están habilitadas. Son posibles los siguientes valores:

Activo

Las políticas en el servidor de réplica de destino gestionan datos de nodo cliente replicados.

Inactivo

Las políticas en el servidor de réplica de origen gestionan datos de nodos cliente replicados.

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con QUERY REPLSERVER

Comando	Descripción
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	Elimina un nodo de la réplica.
REMOVE REPLSERVER (Eliminar un servidor de réplica)	Elimina un servidor de la réplica.

## QUERY REQUEST (Consultar una o más peticiones de montaje pendientes)

---

Utilice el mandato QUERY REQUEST para mostrar información acerca de una o varias solicitudes de montaje pendientes. El servidor realiza peticiones al administrador para llevar a cabo una acción, como insertar un volumen de cinta en una biblioteca después de haberse emitido un comando CHECKIN LIBVOL.

### Clase de privilegio

---

Cualquier administrador puede emitir este comando.

### Sintaxis

---

```
>>-Query REQuest--+-+-----+----->>  
                '-número_petición-'
```

### Parámetros

---

número\_petición

Especifica el número de identificación de la petición de montaje pendiente. Este parámetro es opcional. El valor predeterminado son todas las peticiones de montaje pendientes.

### Ejemplo: obtener una lista de todas las peticiones de montaje pendientes

---

Visualizar información acerca de todas las peticiones de montaje pendientes después de haberse emitido un comando CHECKIN LIBVOL.



## Parámetros

---

### nombre\_nodo

Especifica el nombre del nodo cliente que se consultará. Este parámetro es opcional. Si no especifica un valor, se visualizarán todos los nodos cliente con sesiones de restauración reiniciables. Debe especificar un valor para este parámetro si especifica un nombre de espacio de archivos.

### nombre\_espacio\_archivos

Especifica el nombre del espacio de archivos que se consultará. Este parámetro es opcional. Si no especifica un valor, se compararán todos los espacios de archivos para el nodo especificado.

Para un servidor que tenga clientes que admiten Unicode, es posible que deba utilizar el servidor para que éste convierta el nombre del espacio de archivos que especifica. Por ejemplo, es posible que deba hacer que el servidor convierta el nombre especificado de la página de códigos del servidor a Unicode. Consulte el parámetro NAMETYPE para conocer los detalles.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

### NAMETYPE

Especifique cómo desea que el servidor interprete los nombres de espacios de archivos entrados. Este parámetro es útil cuando el servidor tiene clientes que admiten Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS 9, Macintosh OS X y NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente calificado. El valor predeterminado es SERVER. Los valores posibles son:

#### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

#### Unicode

El servidor convierte el nombre de espacio de archivos especificado de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o bien si el servidor tiene problemas para acceder a las rutinas de conversión del sistema.

#### FSID

El servidor interpreta los nombres de espacios de archivos como sus identificadores de espacios de archivos (FSID).

## Ejemplo: visualizar una sesión de restauración reiniciable en un nodo cliente específico

---

Visualizar información detallada sobre el nodo cliente JAMES asociado al espacio de archivos DRIVE\_F\_R. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query restore james drive_f_r format=detailed
```

```

Número sesión: -1
Estado restauración: Reiniciable
Minutos transcurridos: 2
Nombre nodo: JAMES
FSID: 1
Nombre espacio archivos: DRIVE_F_R:
Espec. archivo: /RESTORE/TESTDIRF\

```

## Descripciones de los campos

---

### Número de sesión

Especifica el número de sesión de la sesión de restauración reanunciable. El número de las sesiones de restauración activas es el mismo número que se visualiza en el comando QUERY SESSION. Para las sesiones de restauración que están en estado reiniciable, se visualiza un número negativo como número de sesión. Cualquier número de sesión que se visualice en la salida de QUERY RESTORE puede especificarse desde la salida de QUERY RESTORE.

### Estado restauración



- Activo: Especifica que la sesión de restauración está activa, restaurando los archivos en el cliente.
- Reinicializable: Especifica que la sesión de restauración no se ha ejecutado correctamente y que puede reiniciarse desde donde ha quedado interrumpida.

#### Minutos transcurridos

Especifica el número de minutos desde que se ha arrancado la sesión de restauración. Todas las sesiones de restauración reinicializables con un tiempo transcurrido mayor que el valor de la opción del servidor RESTOREINTERVAL pueden suprimirse automáticamente de la base de datos del servidor cuando sea necesario, o durante el proceso de caducidad. Si el tiempo transcurrido es inferior al valor de RESTOREINTERVAL, esta entrada sólo puede suprimirse (y desbloquearse el espacio de archivos) mediante la emisión del comando CANCEL RESTORE y la reducción del valor de RESTOREINTERVAL.

#### Node Name

Especifica el nodo asociado a la sesión de restauración reinicializable.

#### FSID

Especifica el identificador del espacio de archivos.

#### Filespace Name

Especifica el espacio de archivos asociado a la sesión de restauración reinicializable.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

#### Especificación de archivo

Indica la especificación de archivo utilizada en la operación de restauración. Debe indicarse la misma especificación de archivo si se va a reiniciar una operación de restauración que no se ha podido ejecutar desde el punto en que se detuvo.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY RESTORE

Comando	Descripción
CANCEL RESTORE	Cancela una sesión de restauración reinicializable.

## QUERY RPFCONTENT (Consultar el contenido del archivo del plan de recuperación almacenado en un servidor de destino)

Utilice este mandato para visualizar el contenido de un archivo del plan de recuperación almacenado en un servidor de destino (es decir, cuando el parámetro DEVCLASS se ha especificado en el mandato PREPARE). Puede emitir este mandato desde el servidor que ha creado el archivo (el servidor de origen) o desde el servidor que almacena el archivo del plan de recuperación (el servidor de destino). Este mandato no se puede emitir en la consola del servidor.

La salida se puede retardar si el archivo está en cinta.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Query RPFContent--nombre_archivo_plan----->
>--+DEVclass---nombre_clase_dispositivo+-----<
'-NODENAME---nombre_nodo-----'
```

## Parámetros

nombre\_archivo\_plan (Obligatorio)

Especifica el nombre del archivo del plan de recuperación que se ha de consultar. El formato del nombre de archivo es nombreservidor.aaaammdd.hhmmss. Para ver los nombres de los archivos existentes, emita el comando QUERY RPFFILE.

DEVclass

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear el archivo del plan de recuperación. Los caracteres comodín no están permitidos.

Especifique este parámetro cuando:

- Desea visualizar el contenido del archivo del plan de recuperación creado para este servidor.
- Emita este mandato en el mismo servidor en el que se ha emitido el mandato PREPARE (el servidor de origen).
- Se haya utilizado el nombre de clase de dispositivo especificado en el mandato PREPARE que ha creado el archivo del plan de recuperación.

NODENAME

Especifica el nombre de nodo, registrado en el servidor de destino, del servidor de origen que ha creado el archivo del plan de recuperación. Los caracteres comodín no están permitidos.

Especifique este parámetro cuando:

- Desea visualizar el contenido del archivo del plan de recuperación que estaba almacenado en servidor.
- Emita este mandato para el servidor que era el destino del mandato PREPARE que ha creado el archivo del plan de recuperación.
- El nombre de nodo especificado esté registrado en este servidor con un tipo de nodo de SERVER.
- El servidor de IBM Spectrum Protect que ha creado el archivo del plan de recuperación no esté disponible.

## Ejemplo: visualizar el plan de recuperación del servidor de origen

En el servidor origen, visualizar el contenido de un archivo del plan de recuperación que se ha creado para este servidor el 19 de marzo de 1998 a las 6:10 A.M. El mandato PREPARE especifica la clase de dispositivo REMOTE. La salida de este comando es el contenido completo del archivo del plan de recuperación.

```
query rpfcontent branch1.19980319.061000 devclass=remote
```

## Ejemplo: visualizar el plan de recuperación del servidor de destino

En el servidor de destino, visualizar el contenido de un archivo del plan de recuperación que se ha almacenado en este servidor el 19 de marzo de 1998 a las 6:10 A.M. El servidor que ha creado el archivo está inscrito en el servidor destino como el nodo denominado POLARIS y tiene el tipo de nodo SERVER. La salida de este comando es el contenido completo del archivo del plan de recuperación.

```
query rpfcontent branch1.19980319.061000 nodename=polaris
```

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY RPFCONTENT

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFFILE	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.

**Información relacionada:**

 Archivo del plan de recuperación tras siniestro

## QUERY RPFFILE (Consultar la información del archivo del plan de recuperación almacenado en un servidor de destino)

Utilice este comando para visualizar la información sobre los archivos del plan de recuperación almacenados en un servidor destino. Puede emitir este comando desde el servidor que ha creado el archivo (el servidor origen) o desde el servidor que almacena el archivo del plan de recuperación (el servidor destino).

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
>>-Query RPFile--+--DEVclass-----nombre_clase_dispositivo+----->
      '-NODEName-----nombre_nodo-----'

.-Source-----DBBackup-----.-Format-----Standard-----
>-----+-----+-----+-----<
'-Source-----+--DBBackup---+' '-Format-----+--Standard-+-'
      '-DBSnapshot-'           '-Detailed-'
```

## Parámetros

---

### DEVclass

Especifica el nombre de la clase de dispositivo que se ha utilizado para crear los archivos del plan de recuperación. Utilice este parámetro si ha iniciado la sesión en el servidor que ha creado el archivo del plan de recuperación. Puede utilizar caracteres comodín en el nombre de clase de dispositivo. En la consulta se incluirán todos los archivos del plan de recuperación que se han creado con la clase de dispositivo especificada.

### NODENAME

Especifica el nombre de nodo, registrado en el servidor destino, del servidor origen que ha creado los archivos del plan de recuperación. Utilice este parámetro si ha iniciado la sesión en el servidor destino. Puede utilizar este parámetro si el servidor origen no está disponible. Puede utilizar caracteres comodín para especificar el nombre de nodo. En esta consulta se incluyen todos los objetos de archivo que están almacenados con el nombre de nodo especificado.

### Source

Especifica el tipo de copia de seguridad de base de datos indicada al preparar el archivo del plan de recuperación. Este parámetro es opcional. El valor predeterminado es DBBACKUP. Los valores posibles son:

#### DBBackup

El archivo del plan de recuperación se preparó con copias de seguridad completas e incrementales especificadas.

#### DBSnapshot

El archivo del plan de recuperación se preparó con las copias de seguridad de instantánea de base de datos especificadas.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Visualiza información parcial para el archivo del plan de recuperación.

#### Detailed

Visualiza toda la información para el archivo del plan de recuperación.

## Ejemplo: visualizar información detallada acerca de los planes de recuperación

---

Visualizar los archivos de plan de recuperación que se han creado para este servidor empleando la clase de dispositivo especificada. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query rpfile devclass=* format=detailed

Nombre archivo plan recuperación: ALASKA.20000406.170423
      Nombre nodo: BRANCH1
      Nombre clase dispositivo: REMOTE
Tipo archivo plan recuperación: RPFIL
      Nombre clase gestión: STANDARD
Tamaño archivo plan recuperación: 16.255 Bytes
      Marca supresión: Si
      Fecha supresión: 06/12/2000 13:05:31

Nombre archivo plan recuperación: ALASKA.20000407.170845
      Nombre nodo: BRANCH1
      Nombre clase dispositivo: REMOTE
Tipo archivo plan recuperación: RPF
      Nombre clase gestión: STANDARD
Tamaño archivo plan recuperación: 16.425 Bytes
      Marca supresión: No
      Fecha supresión:
```

## Ejemplo: visualizar una lista de los planes de recuperación para un nombre de nodo específico

---

Visualizar una lista de todos los objetos de archivo del plan de recuperación que están almacenados con el nombre de nodo especificado (TIPO=SERVER). Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query rpfile nodename=branch1
```

Nombre archivo plan recuperación	Nombre nodo	Nombre clase dispositivo
ALASKA.19980406.170423	BRANCH1	REMOTE
ALASKA.19980407.170845	BRANCH1	REMOTE

## Descripciones de los campos

**Nombre del archivo del plan de recuperación**

El nombre del archivo del plan de recuperación.

**Node Name**

El nombre del nodo que está registrado con el servidor destino y se utiliza para almacenar los objetos de archivo del plan de recuperación.

**Nombre clase dispositivo**

El nombre de clase de dispositivo que está definido en el servidor origen y se utiliza para crear los archivos del plan de recuperación.

**Tipo de archivo del plan de recuperación**

Indica el tipo de archivo del plan de recuperación:

**RPFIL**

El plan presupone copias de seguridad completas e incrementales.

**RPFNSNAPSHOT**

El plan presupone copias de seguridad de instantánea de base de datos.

**Nombre clase gestión**

El nombre de la clase de gestión a la que el archivo del plan de recuperación está asociado en el servidor destino.

**Tamaño del archivo del plan de recuperación**

Tamaño estimado del objeto archivo del plan de recuperación del servidor destino.

**Marcado para suprimir**

Si el objeto que contiene el archivo del plan de recuperación se ha suprimido del servidor origen y se ha marcado para suprimir en el servidor destino si el período de gracia no ha caducado. Los valores posibles son:

**Sí**

El objeto se marca para suprimirlo.

**No**

El objeto no se marca para suprimirlo.

**Fecha supresión**

Fecha en la que el objeto se ha suprimido del servidor origen y se ha marcado para supresión en el servidor destino. Este campo está en blanco si el objeto no está marcado para supresión.


## Comandos relacionados


Tabla 1. Comandos relacionados con QUERY RPFIL


Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.

## QUERY SAN (Consultar los dispositivos de la SAN)

Utilice este mandato para obtener información acerca de los dispositivos que se pueden detectar en una red de área de almacenamiento (SAN) para poder configurar IBM Spectrum Protect para un traspaso de datos libre de LAN.

 Sistemas operativos AIX El mandato QUERY SAN requiere que libhbaapi.a dé soporte a la API de adaptador de bus de host (HBA) SNIA común. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBA API común SNIA.

 Sistemas operativos Windows El mandato QUERY SAN requiere que hbaapi.dll dé soporte a la API del adaptador de bus de host (HBA) común SNIA. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBAAPI común SNIA.

 Sistemas operativos Linux El mandato QUERY SAN requiere que libhaapi.so dé soporte a la API de adaptador de bus de host (HBA) SNIA común. Con este objeto de biblioteca, IBM Spectrum Protect puede llamar a las funciones hbaapi que se han especificado en el estándar HBAAPI común SNIA.

Puede que el mandato QUERY SAN no muestre todos los dispositivos si la opción del servidor SANDISCOVERY no está establecida en ON.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
.-Type-----Any-----.  
>>-Query SAN-----+----->  
      '-Type-----+Any-----+'  
              +-DRive---+  
              '-LIBRARY-'  
  
. -Format-----Standard-----.  
>-----+-----<<  
      '-Format-----+Standard-+-'  
              '-Detailed-'
```

## Parámetros

---

### Type

Especifica el tipo de dispositivo que se visualiza. Este parámetro es opcional. El valor predeterminado es Any. Los valores posibles son:

#### Any

Especifica que se puede visualizar cualquier dispositivo que se detecte en SAN.

#### DRive

Especifica que solamente se visualizarán los dispositivos de unidad.

#### LIBRARY

Especifica que solamente se visualizarán los dispositivos de biblioteca.

### Format

Especifica el tipo de información que se visualiza. Este parámetro es opcional. El valor predeterminado es Standard. Los valores posibles son:

#### Standard

Especifica que la información visualizada está resumida.

#### Detailed

Especifica que se visualizará toda la información.

Consejo: Puede que la salida no visualice el número de serie del dispositivo. Si esto es así, busque en la parte posterior del dispositivo o póngase en contacto con el fabricante del dispositivo.

## Ejemplo: obtener una lista de los dispositivos de unidad

---

Visualizar información resumida de los dispositivos de unidad de una SAN. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query san type=drive
```

Tipo dispo.	Proveedor	Producto	Serie	Dispositivo
LIBRARY	STK	L180		MPC01000128 /dev/smc1
DRIVE	STK	9840D	331001017229	/dev/rmt3
DRIVE	Quantum	DLT4000	JF62806275	/dev/rmt4
DRIVE	Quantum	DLT4000	JP73213185	/dev/rmt5
DRIVE	STK	9840D	331000028779	/dev/rmt6

## Ejemplo: visualizar información de dispositivo de unidad

---

Visualizar información detallada de todos los dispositivos de unidad de una SAN. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query san type=drive format=detailed
```

```
Tipo dispositivo:    DRIVE
Proveedor:         IBM
Producto:          03570B02
Número de serie:
Dispositivo:       mt10.2.0.3
Transportador de datos: No
Nodo WWN:          5005076206039E05
Puerto WWN:        5005076206439E05
LUN:               0
Puerto SCSI:       3
Bus SCSI:          0
Destino SCSI:      10
```

## Descripciones de los campos

### Tipo dispositivo

El tipo de dispositivo que se está visualizando.

### Proveedor

El nombre del proveedor del dispositivo.

### Producto

El nombre del producto que asigna el proveedor.

### Número de serie

El número de serie del dispositivo.

### Dispositivo

El nombre del archivo de dispositivo especial.

### Transportador de datos

Si el dispositivo es un transportador de datos.

### WWN de nodo

Nombre de ámbito mundial del dispositivo.

### WWN de puerto

Nombre de ámbito mundial del dispositivo, que es específico del puerto con el que se ha conectado el dispositivo.

### LUN

El número de unidad lógica del dispositivo.

### Puerto de SCSI

El puerto del adaptador de bus de host de canal de fibra (o SCSI)

### Bus de SCSI

El bus de la tarjeta adaptadora del bus de host.

### Destino de SCSI

El número de destino del dispositivo.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SAN

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.

## QUERY SCHEDULE (Consultar planificaciones)

Utilice este comando para visualizar información acerca de una o varias planificaciones.

El comando QUERY SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones del cliente o a los comandos de administración. La sintaxis y los parámetros de cada operación se definen por separado. Algunas opciones de la visualización de la consulta estarán en blanco, en función de si el estilo de planificación es clásico o mejorado.

Tabla 1. Comandos relacionados con QUERY SCHEDULE



El formato estándar muestra un espacio en blanco en la columna de periodo y un asterisco en la columna de día en las planificaciones mejoradas. Para visualizar información completa acerca de una planificación mejorada, emita `FORMAT=DETAILED`.

## Ejemplo: obtener una lista de las planificaciones de un dominio de políticas específico

Visualizar todas las planificaciones que pertenecen al dominio de políticas `EMPLOYEE_RECORDS`. Consulte el apartado Descripciones de los campos: planificaciones de un dominio de políticas específico para obtener las descripciones de los campos.

```
query schedule employee_records
```

El formato estándar muestra un espacio en blanco en la columna de periodo y un asterisco en la columna de día en las planificaciones mejoradas. Para visualizar información completa acerca de una planificación mejorada, emita `FORMAT=DETAILED`.

Domain	* Schedule Name	Action	Start Date/Time	Duration	Period	Day
EMPLOYEE_RECORDS	WEEKLY_BACKUP	Inc Bk	2004.06.04 17.04.20	1 H	1 D	Any
EMPLOYEE_RECORDS	EMPLOYEE_BACKUP	Inc Bk	2004.06.04 17.04.20	1 H		(*)

## Descripciones de los campos: planificaciones de un dominio de políticas específico

### Domain

Especifica el nombre del dominio de políticas al que pertenece la planificación especificada.

### \* (asterisco)

Especifica si ha caducado la planificación correspondiente. Si existe un asterisco en esta columna, ha caducado la planificación correspondiente.

### Schedule Name

Especifica el nombre de la planificación.

### Acción

Especifica la acción que se produce cuando se procesa esta planificación.

### Fecha/hora inicio

Especifica la fecha y hora de inicio de esta planificación.

### Duración

Especifica la duración del margen de puesta en marcha de esta planificación.

### Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que `DAYOFWEEK=ANY`). La columna está en blanco en las planificaciones mejoradas.

### Día

Especifica el día de la semana en que se inician los márgenes de puesta en marcha de esta planificación. La columna contiene un asterisco en las planificaciones mejoradas.

## Ejemplo: visualizar información detallada acerca de las planificaciones de cliente

Desde un servidor gestionado, visualizar información detallada sobre las planificaciones de cliente. Consulte el apartado Descripciones de los campos: información detallada acerca de las planificaciones de cliente para obtener las descripciones de los campos.

```
query schedule * type=client format=detailed
```

```
Nombre dominio políticas: ADMIN_RECORDS
Nombre planificación: ADMIN_BACKUP
Descripción:
  Acción: Backup
  Subacción: vApp
  Opciones:
  Objetos:
  Prioridad: 5
Fecha/hora inicio: 04/06/2013 17.04.20
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Clásico
Período: 1 día(s)
Día semana: Cualquiera
Mes:
Día del mes:
Semana del mes:
```



```

Caducidad:
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/hora de la última actualización: 06/04/2013 17.51.49
Perfil de gestión: ADMIN_INFO

Nombre dominio políticas: EMPLOYEE_RECORDS
Nombre planificación: EMPLOYEE_BACKUP
Descripción:
Acción: Incremental
Subacción:
Opciones:
Objetos:
Prioridad: 5
Fecha/hora inicio: 2004.06.04 17.04.33
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
Estilo de planificación: Mejorado
Periodo:
Día semana: Cualquiera
Mes: Mar,Jun,Nov
Día del mes: -14,14,22
Semana del mes: Última
Caducidad:
Última actualización por (administrador): $$CONFIG_MANAGER$$
Fecha/hora última actualización: 2004.06.04 17.18.30
Perfil de gestión: EMPLOYEE

```

## Descripciones de los campos: información detallada acerca de las planificaciones de cliente

---

Nombre dominio políticas

Especifica el nombre del dominio de políticas.

Schedule Name

Especifica el nombre de la planificación.

Descripción

Especifica la descripción de la planificación.

Acción

Especifica el tipo de acción que se produce cuando se ejecuta esta planificación. Consulte el comando DEFINE SCHEDULE para obtener un listado de las acciones.

Subacción

Especifica que el tipo de operación identificado por el parámetro ACTION se debe planificar. Consulte el comando DEFINE SCHEDULE para obtener un listado de las subacciones.

Opciones

Especifica las opciones que se suministran al comando DSMC cuando se procesa la planificación.

Objetos

Especifica los objetos para los que se realiza la acción especificada.

Prioridad

Especifica el valor de prioridad de la planificación.

Fecha/hora inicio

Especifica la fecha y hora de inicio de la planificación.

Duración

Especifica la duración del margen de puesta en marcha de la planificación.

Tiempo máximo de ejecución(Minutos)

Especifica el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Estilo de planificación

Especifica si se utilizan reglas de planificación clásicas o mejoradas.

Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que DAYOFWEEK=ANY). No se visualiza para las planificaciones de sintaxis mejoradas.

Día de la semana

Especifica el día de la semana en que se inician los márgenes de puesta en marcha de esta planificación. Mediante la utilización de un formato estándar, visualiza un asterisco en el campo del día de la semana para las planificaciones mejoradas.

Mes

Especifica los meses durante los cuales se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Día del mes

Especifica los días durante los cuales se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Semana del mes

Especifica las semanas (primera, segunda, tercera, cuarta o última) del mes durante el cual se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

Caducidad

Especifica la fecha y hora en la que caduca esta planificación. Si esta columna está en blanco, la planificación no caducará.

Última actualización por (administrador)

Especifica el nombre del administrador que ha actualizado por última vez la planificación. Si este campo contiene \$\$CONFIG\_MANAGER\$\$, la planificación está asociada a un dominio que gestiona el gestor de configuración.

Fecha/hora de la última actualización

Especifica la fecha y hora en que se ha actualizado por última vez la planificación.

Perfil de gestión

Especifica el perfil o los perfiles en los que se ha inscrito el servidor gestionado para obtener la definición de esta planificación.

## QUERY SCHEDULE (Consultar una planificación de administración)

---

Utilice este mandato para visualizar información acerca de una o varias planificaciones de administración.

### Clase de privilegio

---

Cualquier administrador puede emitir este comando.

### Sintaxis

---

```
.-*-----
>>-Query SCHEDULE--+-----+----->
      '-nombre_planificación-'

      .-Format----Standard----.
>>-Type----Administrative--+-----+-----<
      '-Format----+Standard+-'
                        '-Detailed-'
```

### Parámetros

---

nombre\_planificación

Especifica el nombre de la planificación que se consultará. Puede utilizar un carácter comodín para especificar este nombre.

Type=Administrative (Necesario)

Especifica que la consulta visualiza las planificaciones de comando de administración.

Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial acerca de las planificaciones.

Detailed

Especifica que se visualizará información detallada acerca de las planificaciones.

El formato estándar presenta una columna de periodo en blanco y un asterisco en la columna de día en las planificaciones mejoradas. Emita el comando FORMAT=DETAILED para visualizar la información completa sobre una planificación mejorada.

### Ejemplo: visualizar información detallada acerca de planificaciones de mandatos de administración

---

Desde un servidor gestionado, visualizar información detallada sobre las planificaciones de mandato de administración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query schedule * type=administrative
format=detailed

Nombre planificación: BACKUP_ARCHIVEPOOL
Descripción:
  Comando: backup db
  Prioridad: 5
Fecha/hora inicio: 2004.06.04 16.57.15
Duración: 1 Hora(s)
Tiempo máximo de ejecución (minutos): 0
```

Estilo de planificación: Clásico  
Período: 1 día(s)  
Día semana: Cualquiera  
Mes:  
Día del mes:  
Semana del mes:  
Caducidad:  
Activo: No  
Última actualización por (administrador): \$\$CONFIG MANAGER\$\$  
Fecha/hora última actualización: 2004.06.04 17.51.49  
Perfil de gestión: ADMIN\_INFO

Nombre planificación: MONTHLY\_BACKUP  
Descripción:  
Comando: q status  
Prioridad: 5  
Fecha/hora inicio: 2004.06.04 16.57.14  
Duración: 1 Hora(s)  
Tiempo máximo de ejecución (minutos): 0  
Estilo de planificación: Mejorado  
Período:  
Día de la semana: Mar,Jue,Vie  
Mes: Ago,Nov  
Día del mes:  
Semana del mes: Segunda,Tercera  
Caducidad:  
Activo: No  
Última actualización por (administrador): \$\$CONFIG MANAGER  
Fecha/hora última actualización: 2004.06.04 17.51.49  
Perfil de gestión: ADMIN\_INFO

## Descripciones de los campos

---

### Schedule Name

Especifica el nombre de la planificación.

### Descripción

Especifica la descripción de la planificación.

### Comando

Especifica el comando que se ha planificado.

### Prioridad

Especifica el valor de prioridad de esta planificación.

### Fecha/hora inicio

Especifica la fecha y hora de inicio de esta planificación.

### Duración

Especifica la duración del margen de puesta en marcha.

### Tiempo máximo de ejecución(Minutos)

Especifica el número de minutos durante los cuales los procesos de servidor que se inician mediante los mandatos planificados deben completarse. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

### Consejos:

- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

### Estilo de planificación

Especifica si se utilizan reglas de planificación clásicas o mejoradas.

### Período

Especifica el tiempo entre márgenes de puesta en marcha (presuponiendo que DAYOFWEEK=ANY). No se visualiza para las planificaciones de sintaxis mejoradas.

### Día de la semana

Especifica el día de la semana en que se inician los márgenes de puesta en marcha.

### Mes

Especifica los meses durante los cuales se ejecutará la planificación. No se visualiza para las planificaciones de sintaxis clásicas.

### Día del mes



Datos de anotación: Toronto 5A24  
Fecha/hora de creación: 2013-09-10, 10:15:50  
Fecha/hora última actualización: 2013-09-10, 10:15:50  
Última actualización por (administrador): CODJO

Categoría principal de anotación: admin\_info  
Categoría secundaria de anotación: location  
Asunto de anotación: jane  
Número de línea de anotación: 1  
Datos de anotación: Raleigh GF85  
Fecha/hora de creación: 2013-09-09, 14:29:40  
Fecha/hora última actualización: 2013-09-09, 14:29:40  
Última actualización por (administrador): JANE\_W

Categoría principal de anotación: admin\_info  
Categoría secundaria de anotación: location  
Asunto de anotación: jane  
Número de línea de anotación: 2  
Datos de anotación: Fuera de la oficina del 1-15 Nov.  
Fecha/hora de creación: 2013-09-09, 14:30:05  
Fecha/hora última actualización: 2013-10-31, 16:55:52  
Última actualización por (administrador): JANE\_W

Categoría principal de anotación: admin\_info  
Categoría secundaria de anotación: location  
Asunto de anotación: montse  
Número de línea de anotación: 1  
Datos de anotación: Barcelona B19  
Fecha/hora de creación: 2013-09-10, 04:34:37  
Fecha/hora última actualización: 2013-09-10, 04:34:37  
Última actualización por (administrador): MONTSERRAT

## Descripciones de los campos

---

### Datos de registro

Los datos que se almacenan en la entrada del área de registro.

### Fecha/hora de creación

Fecha y hora en la que se creó la entrada de registro.

### Fecha/hora última actualización

Fecha y hora en la que se actualizó por última vez la entrada de registro.

### Última actualización por (administrador)

El administrador que actualizó por última vez la entrada de registro.

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con QUERY SCRATCHPADENTRY

Comando	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

## QUERY SCRIPT (Consultar scripts IBM Spectrum Protect)

---

Utilice este comando para visualizar la información sobre scripts.

Puede utilizar este comando con el comando DEFINE SCRIPT para crear un nuevo script utilizando el contenido de otro script.

### Clase de privilegio

---

La clase de privilegios necesaria para este comando depende de si se ha especificado el parámetro Outputfile en el comando.

- Si no se especifica el parámetro Outputfile, cualquier administrador puede emitir este comando.
- Si se ha especificado el parámetro Outputfile y la opción del servidor REQSYSAUTHOUTFILE está establecida en YES, el administrador debe tener privilegio de sistema.

- Si se ha especificado el parámetro Outputfile y la opción del servidor REQSYSAUTHOUTFILE está establecida en NO, el administrador debe tener privilegio de operador, de políticas, de almacenamiento o de sistema.

## Sintaxis

```

>>-Query SCript-.-*----->
      +-----+----->
      '-nombre_script-'

.-FORMAT----Standard----->
>--+-----+-----><
  '-FORMAT----+Standard-----+'
      +-Detailed-----+
      +-Lines-----+
  '-Raw--+-----+'
      '-Outputfile----nombre_archivo-'

```

## Parámetros

### nombre\_script

Especifica el nombre del script cuya información se va a visualizar. Puede incluir un carácter comodín para especificar este nombre.

Importante: Si no especifica un script, la consulta visualizará la información sobre todos los scripts. El tiempo utilizado para procesar este comando y la cantidad de información visualizada pueden ser considerables.

### Format

Especifica el formato de salida para visualizar la información de script. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que sólo se visualizarán el nombre del script y la descripción.

#### Detailed

Especifica que se visualiza información detallada sobre el script. Esta información incluye los mandatos del script y los números de línea, la fecha de la última actualización y el administrador que ha realizado las actualizaciones.

#### Lines

Especifica que se visualizan el nombre del script, el número de línea de los comandos, las líneas de comentarios y los comandos que hay en el script.

#### Raw

Especifica que los comandos incluidos en el script se graban en un archivo indicado con el parámetro Outputfile. Este formato es un modo de dirigir la salida de un script a un archivo para poder copiarlo en otro script con el comando DEFINE SCRIPT.

Si no se especifica ningún archivo de salida, el servidor de IBM Spectrum Protect enviará la salida de "query script" con "format=raw" a la consola.

### Outputfile

Especifica el nombre del archivo al que se dirige la salida si se especifica FORMAT=Raw. El archivo que especifique debe estar en el servidor que ejecuta este comando. Si existe el archivo, la salida de la consulta se agrega al final del archivo.

## Ejemplo: obtener una lista de las descripciones de los scripts

Visualizar la información estándar relativa a scripts.

```
query script *
```

Nombre	Descripción
QCOLS	Visualiza columnas para una tabla SQL especificada
QSAMPLE	Consulta SQL de ejemplo
EXAMPLE	Copia de seguridad de las agrupaciones de almacenamiento y base de datos cuando no hay sesiones

## Ejemplo: visualizar el contenido de un script con números de líneas

Visualizar la información de líneas del script denominado Q\_AUTHORITY.

```
query script q_authority format=lines
```

Nombre	Núm. líneas	Comando
Q_AUTHORITY	1	/* -----*/
	5	/* Nombre script: Q_AUTHORITY */
	10	/* Descripción: Visualizar administradores */
	15	/* con autorización para emitir */
	20	/* comandos que requieran un */
	25	/* privilegio específico. */
	30	/* Parámetro 1: nombre privilegio - formato */
	35	/* x_priv - EX. policy_priv */
	40	/* Ejemplo: run q_authority storage_priv */
	45	/* -----*/
	50	select admin_name from admins where -
	55	upper(system_priv) <> 'NO' or -
	60	upper(\$1) <> 'NO'

## Ejemplo: crear un script a partir de un script existente

Consultar el script ENGDEV y dirigir la salida a un archivo denominado MY.SCRIPT.

```
query script engdev format=raw outputfile=my.script
```

## Ejemplo: visualizar información detallada acerca del script

Visualizar la información detallada sobre los scripts. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query script * format=detailed
```

```

Nombre: QCOLS
Número líneas: DESCRIPTION
Comando: Visualizar columnas para
una tabla
SQL especificada
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 12/02/1997 16:05:29

Nombre: QCOLS
Número líneas: 1
Comando: select colname from
columns where
tabname='$1'
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 12/02/1997 16:05:29

```

## Descripciones de los campos

Nombre

El nombre del script.

Número de línea

El número de línea del script o la serie DESCRIPTION.

Comando

El comando incluido en el número de línea visualizado en el campo anterior.

Última actualización por (administrador)

El nombre del administrador que ha definido o ha actualizado más recientemente el script.

Fecha/hora de la última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente el script.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SCRIPT

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.

Comando	Descripción
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

**Conceptos relacionados:**

Scripts de servidor

## QUERY SERVER (Consultar un servidor)

Utilice este mandato para visualizar información acerca de una definición de servidor.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

>>-Query SERver-----+----->
      '-nombre_servidor-'

.-Format-----Standard-----
>--+-----+-----<
      '-Format-----+Standard+-'
      '-Detailed-'

```

### Parámetros

nombre\_servidor

Especifica el nombre del servidor que se va a consultar. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado son todos los nombres de servidores.

Format

Especifica cómo se ha de visualizar la información. El parámetro es opcional. El valor predeterminado es STANDARD.

Standard

Especifica que se visualizará información parcial.

Detailed

Especifica que se visualizará toda la información.

### Ejemplo: obtener una lista de todos los servidores

Visualizar información en el formato estándar relativa a todos los servidores. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query server *
```

Nombre servidor	Método com.	Dirección alto nivel	Dirección bajo nivel	Días desde últ. acceso	Contras. servidor asignada	Contras. volumen virtual asignada	Permitir sustit.
SERVER_A	TCPIP	9.115.35.6	1501	11	Yes	No	No
SERVER_B	TCPIP	9.115.45.24	1500	<1	Yes	No	No
ASTRO	TCPIP	9.115.32.21	1500	24	Yes	No	No

### Ejemplo: visualizar información detallada acerca de un servidor específico

Desde un servidor gestionado, visualizar información detallada sobre el SERVER\_A. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query server server_a format=detailed
```

```

Nombre servidor: SERVER_A
Método comunicaciones: TCPIP
Método de transferencia: TCPIP

```



```

Dirección alto nivel: 9.115.4.15
Dirección bajo nivel: 1500
Descripción:
Permitir sustitución: No
Nombre nodo:
Fecha/hora último acceso : 09.07.2013 09:00:00
Días desde último acceso: <1
Compresión: Elección del cliente
¿Supresión copias archivadas?: No
URL:
Fecha/hora registro: 07/08/2013 09:15:09
Registrado por administrador: $$CONFIG_MANAGER$$
Bytes recibidos última sesión: 362
Bytes enviados última sesión: 507
Duración de última sesión: 0,00
Porcentaje de esperas desocupado
última sesión: 0,00
Porcentaje de Método comunicaciones
última sesión: 0.00
Porcentaje de esperas medio
última sesión: 0,00
Período gracia supresión: 5
Perfil de gestión:
Contraseña servidor asignada: Si
Fecha/hora asignación contraseña servidor: 07/08/2013 09:15:09
Días desde establecimiento de contraseña de servidor: 1
Número inicios sesión no válidos servidor: 0
Contraseña volumen virtual asignada: No
Fecha/hora asignación volúmenes volumen virtual:(?)
Días desde asignación contraseña volumen
virtual:(?)
Número inicios sesión no válidos nodo
volumen virtual: 0
Protocolo de validación: No
Versión: 7
Release: 1
Nivel: 0.0
Rol(es): Réplica
SSL: No
Session Security: Strict
Transport Method: TLS 1.2

```

## Descripciones de los campos

---

### Nombre del servidor

El nombre del servidor.

### Método comunicaciones

El método de comunicación que se utiliza para conectarse al servidor.

### Método de transferencia

El método que se utiliza para la transferencia de datos de servidor a servidor.

### Dirección alto nivel

La dirección IP (con formato de puntos) del servidor.

### Dirección bajo nivel

El número de puerto del servidor.

### Descripción

La descripción del servidor.

### Permitir sustitución

Especifica si una definición de servidor en un servidor gestionado puede sustituirse por una definición de un gestor de configuración.

### Nombre del nodo

El nombre del nodo de cliente.

### Fecha/hora último acceso

La última fecha y hora en que el nodo de cliente ha accedido al servidor.

### Días desde último acceso

El número de días transcurridos desde que el nodo cliente accedió al servidor.

### Compresión

El tipo de compresión que IBM Spectrum Protect completa en los archivos de cliente.

### ¿Supresión copias archivadas?

Especifica si el nodo de cliente puede suprimir sus propias copias archivadas. Un valor de (?) indica que este campo no se ha establecido y no se aplica a esta definición.

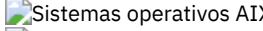
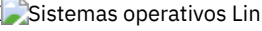
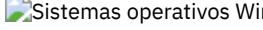
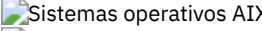
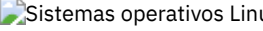
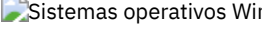
### URL

- El URL utilizado para acceder a este servidor desde una interfaz basada en un navegador web.
- Fecha/hora registro  
La fecha y la hora en que se ha inscrito el nodo cliente.
- Registrado por administrador  
El nombre del administrador que ha inscrito el nodo cliente.
- Bytes recibidos última sesión  
El número de bytes que ha recibido el servidor durante la última sesión del nodo de cliente.
- Bytes enviados última sesión  
El número de bytes enviados al nodo de cliente.
- Duración última sesión  
El tiempo que ha durado la última sesión del nodo de cliente, en segundos.
- Porcentaje de esperas desocupado última sesión  
El porcentaje del tiempo total de la sesión durante la cual el cliente no ha realizado ninguna función.
- Porcentaje de Método comunicaciones última sesión  
El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando una respuesta del servidor.
- Porcentaje de esperas soporte última sesión  
El porcentaje del tiempo total de la sesión durante el cual el cliente ha estado esperando que se montara un volumen extraíble.
- Periodo de gracia de supresión  
El número de días que un objeto permanece en el servidor de destino después de que se haya marcado para suprimirlo.
- Perfil de gestión  
El perfil del que el servidor gestionado ha obtenido la definición de este servidor.
- Contraseña servidor establecida  
Especifica si la contraseña del servidor se ha establecido.
- Fecha/hora de establecimiento de contraseña de servidor  
Especifica cuándo se ha establecido la contraseña del servidor.
- Días desde asignación de contraseña de servidor  
Especifica el número de días transcurridos desde que se ha asignado la contraseña del servidor.
- Número inicios sesión no válidos para el servidor  
El número máximo de intentos de inicio de sesión no válidos que el servidor puede aceptar.
- Contraseña de volumen virtual establecida  
Especifica si la contraseña que se utiliza para iniciar la sesión en el servidor de destino se ha establecido.
- Fecha/hora de establecimiento de contraseña de volumen virtual  
Especifica cuándo se ha establecido la contraseña del soporte de volumen virtual.
- Días desde establecimiento de contraseña de volumen virtual  
Especifica el número de días transcurridos desde que se ha asignado la contraseña del soporte de volúmenes virtuales.
- Número de inicios de sesión no válidos para nodo de volumen virtual  
El número máximo de intentos de inicio de sesión no válidos que se aceptan en el servidor de destino.
- Protocolo de validación (en desuso)  
  
Especifica si el agente de almacenamiento tiene activada la función de validación de datos. Este campo está en desuso.
- Versión  
La versión de software del servidor de IBM Spectrum Protect.
- Release  
El release del software del servidor de IBM Spectrum Protect.
- Nivel  
El nivel de software del servidor de IBM Spectrum Protect.
- Rol(es)  
El rol del servidor. Por ejemplo, uno de los roles para los que se utiliza el servidor es la duplicación.
- SSL  
Especifica si se utiliza la comunicación de la capa de sockets seguros (SSL).
- Seguridad de sesión  
Especifica el nivel de seguridad de sesión que se impone para el servidor. Los valores pueden ser STRICT o TRANSITIONAL.
- Método de transporte  
Especifica el método de transporte que se ha utilizado la última vez para el servidor especificado. Los valores pueden ser TLS 1.2, TLS 1.1 o NONE. El signo de interrogación (?) se muestra hasta que se la autenticación es correcta.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SERVER

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

Comando	Descripción
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
   PROTECT STGPOOL	   Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLSERVER	Especifica un servidor de réplica de destino.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE SERVER	Actualiza la información sobre un servidor.

## QUERY SERVERGROUP (Consultar un grupo de servidores)

Utilice este comando para visualizar información sobre grupos de servidores y miembros de grupos.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-QUERY SERVERGroup--*-----+-----<<
                        '-nombre_grupo-'
```

### Parámetros

nombre\_grupo

Especifica el grupo de servidores que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre.

### Ejemplo: obtener una lista de grupos de servidores

Desde un servidor gestionado, consultar todos los grupos de servidores. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query servergroup *
```

```
Grupo
serv.  Miembros      Descripción      Perfil gestión
-----
ADMIN_GROUP  SERVER_A      Headquarters      ADMIN_INFO
```



Especifica visualizar las sesiones que han tenido como mínimo este número de minutos transcurridos desde la hora en que el cliente ha enviado datos al servidor para su almacenamiento. Este parámetro es opcional. El número mínimo de minutos es 1. El número máximo de minutos es 99999999.

#### MAXTHROUGHPUT

Especifica visualizar sesiones que están transfiriendo datos a una velocidad inferior a este número de kilobytes por segundo. Este parámetro es opcional. El número mínimo de kilobytes por segundo es de 0. El número máximo de kilobytes por segundo es de 99999999.

#### Format

Especifica cómo se visualiza la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Son posibles los siguientes valores:

##### Standard

Especifica que se visualizará información parcial para la sesión.

##### Detailed

Especifica que se visualizará información completa para la sesión.

#### Type

Especifica el tipo de sesiones a incluir en el resultado de la consulta. Si no especifica un valor para este parámetro, se consultarán todos los tipos de sesión. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### Admin

Especifica que se visualizan las sesiones administrativas.

##### Node

Especifica que se visualizan las sesiones de nodo.

##### Server

Especifica que se visualizan las sesiones de servidor.

#### CLIENTName

Especifica el nombre de un administrador, nodo de cliente o servidor a consultar. Puede especificar uno o más nombres. También puede especificar grupos de nodos y nodos proxy. Si especifica varios nombres, sepárelos mediante comas, no utilice espacios intercalados. Puede utilizar caracteres comodín con nombres de nodo pero no con nombres de grupos de nodos. El parámetro es opcional.

Durante la replicación de nodos, el nombre de cliente del servidor de destino se visualiza como *nombre\_nodo* (*nombre\_servidor*), donde *nombre\_nodo* es el nodo cuyos datos se están replicando y *nombre\_servidor* es el nombre del servidor de origen. Puede especificar el nombre del nodo o bien el nombre del servidor en el parámetro CLIENTName para visualizar las sesiones de replicación.

## Ejemplo: obtener una lista de las sesiones de nodo cliente activas

---

Visualizar información acerca de todas las sesiones de nodo cliente y de administración que están comunicándose con el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query session
```

Núm. sesión	Método comun.	Estado sesión	Tiempo espera	Bytes env. rec.	Bytes sesión	Tipo sesión	Plataf.	Nombre cliente
4	TCP/IP	Run	0 S	1.4 K	162	Admin	WinNT	ADMIN

## Ejemplo: visualizar información detallada acerca de las sesiones de nodo cliente activas

---

Visualizar información detallada acerca de todas las sesiones de nodo de cliente y de administración que están comunicándose con el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query session format=detailed
```

```
Número sesión: 4
Método comunicaciones: Tcp/Ip
Estado sesión: Run
Tiempo de espera: 0 S
Bytes enviados: 1,4 K
Bytes recibidos: 162
Tipo de sesión: Admin
Plataforma: WinNT
Nombre de cliente: ADMIN
Estado del acceso al soporte:
Nombre usuario:
Fecha/hora primer envío datos:
Proxy mediante agente de almacenamiento:
```

## Descripciones de los campos

---

### Número sesión

Especifica un número de identificación de sesión exclusivo que asigna el servidor.

### Método comunicaciones

Especifica el método que está utilizando el cliente para comunicarse con el servidor.

### Estado sesión

Especifica el estado actual de las comunicaciones del servidor. Son posibles los siguientes estados:

#### END

La sesión está finalizando (se liberan los recursos de sesión).

#### IDLEW

En espera de la siguiente petición del cliente (la sesión está en estado de desocupación).

#### Espera medio

La sesión está a la espera de acceso a un volumen de acceso secuencial.

#### RECVW

A la espera de recibir un mensaje del cliente.

#### RUN

El servidor está ejecutando una petición del cliente (y no a la espera de enviar datos).

#### SENDW

El servidor está a la espera de enviar datos al cliente (a la espera de que los datos que ya se han enviado se entreguen al nodo de cliente).

#### SSLiW

La sesión está esperando a que finalice la inicialización de la capa de sockets seguros (SSL).

#### START

Se está iniciando la sesión (la autenticación está en proceso).

### Tiempo espera

Especifica la cantidad de tiempo (segundos, minutos u horas) en que el servidor ha estado en el estado actual mostrado.

### Bytes enviados

Especifica el número de bytes de datos enviados al nodo de cliente desde que se ha iniciado la sesión.

### Bytes rec.

Especifica el número de bytes de datos recibidos del nodo de cliente desde que se ha iniciado la sesión.

### Tipo

Especifica el tipo de sesión en curso: ADMIN para una sesión de administración, NODE para una sesión de nodo de cliente o SERVER. SERVER especifica que el servidor inicia una sesión e inicia operaciones de servidor como la configuración central, compartimiento de biblioteca y sesiones de agente de almacenamiento.

### Plataforma

Especifica el tipo de sistema operativo asociado con el cliente.

### Nombre cliente

Especifica el nombre del nodo cliente o el administrador.

Para las sesiones de réplica de nodo, el nombre del cliente se actualiza a *nombre\_nodo (nombre\_servidor)* en el servidor de destino tras iniciar la transferencia de datos.

### Estado de acceso al medio

Especifica el tipo de estado de espera del medio. Cuando una sesión se encuentra en un estado de espera de medios, este campo muestra una lista de todos los puntos de montaje y los volúmenes secuenciales de la sesión. La lista de puntos de montaje especifica la clase de dispositivo y la agrupación de almacenamiento asociada. La lista de volúmenes especifica los volúmenes de agrupación de almacenamiento primaria además de los volúmenes de agrupación de almacenamiento de copia y de agrupación de datos activos con su agrupación de almacenamiento asignada.

El servidor permite a varias sesiones la lectura y a una sesión la grabación en un volumen simultáneamente en una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA. Como resultado, un volumen en una agrupación de almacenamiento con el tipo de dispositivo FILE o CENTERA puede aparecer como el volumen actual en más de una sesión.

### Proxy mediante agente de almacenamiento

Especifica el agente de almacenamiento que es el proxy de movimiento de datos fuera de la LAN para el nodo.

### Nombre usuario

Especifica el identificador de usuario del nodo en un sistema de multiusuario, que se conecta con el servidor cuando no es el mismo usuario del sistema que se ha conectado originalmente con el servidor.

### Fecha/hora primer envío datos

Especifica la fecha y hora en que el cliente ha enviado por primera vez datos al servidor para su almacenamiento.

## Acciones

Muestra una lista de acciones que se realizan durante la sesión. Una acción se lista una sola vez, aunque se produzca varias veces durante una sesión. Son posibles las acciones siguientes:

### BkIns

Se han almacenado uno o más objetos de copia de seguridad en el servidor. La operación puede haberse basado en una copia de seguridad incremental o selectiva.

### BkUpd

Se han actualizado uno o más atributos para un objeto de copia de seguridad que está almacenada en el servidor.

### BkDel

Se han eliminado uno o más objetos de copia de seguridad en el servidor.

### BkRebind

Uno o más objetos de copia de seguridad almacenados en el servidor están vinculados a una clase de gestión diferente.

### NoQueryRestore

Una operación de restauración sin consulta se ha iniciado desde el cliente para restaurar los archivos de copia de seguridad del servidor al sistema cliente.

### ArIns

Se han almacenado uno o más objetos de archivado en el servidor.

### ObjRtrv

Se han recuperado uno o más archivos del servidor. Puede servir para recuperar archivos de copia archivada, o para restaurar datos de copia de seguridad (excepto para datos de copia de seguridad procedentes de una operación de restauración no solicitada).

### MigIns

Uno o más archivos se han migrado y almacenado en el servidor mediante IBM Spectrum Protect for Space Management (cliente HSM).

### MigDel

Se han suprimido uno o más archivos gestionados por espacio que estaban almacenados en el servidor.

### MigRebind

Uno o más archivos gestionados por espacio que estaban almacenados en el servidor se han vinculado a una clase de gestión distinta.

### MigRecall

Se han recuperado uno o más archivos gestionados por espacio almacenados en el servidor.

### MigUpd

Se han actualizado los atributos de uno o más archivos gestionados por espacio que estaban almacenados en el servidor.

### FSAdd

El nodo de cliente ha agregado uno o más espacios de archivo nuevos al almacenamiento del servidor.

### FSUpd

El nodo de cliente ha actualizado los atributos para uno o más espacios de archivo que están definidos en el servidor.

### DefAuth

El nodo de cliente ha procesado un mandato SET ACCESS, lo que ha hecho que se agregara una regla de autorización para el acceso a los datos del nodo de cliente.

## Modalidad de migración tras error

Especifica si la sesión de cliente se ha iniciado en modalidad de recuperación de errores. Son posibles los siguientes valores:

### Fuerza

Se especifica FORCEFAILOVER en el cliente y se fuerza la modalidad de migración tras error de sesión.

### Sí

La sesión de cliente se ha iniciado en modalidad de recuperación de errores.

### No

La sesión de cliente no se ha iniciado en modalidad de recuperación de errores.

## Comandos relacionados

---

Tabla 1. Comando relacionado con QUERY SESSION

Comando	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.

## QUERY SHREDSTATUS (Consultar estado de destrucción)

---

Utilice este comando para visualizar información acerca de los datos en espera de ser destruidos.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegios de administrador.

## Sintaxis

```
>>-QUERY SHREDstatus--+-Format-----Standard-----><
                        '-Format-----+Standard+-'
                        '-Detailed-'
```

## Parámetros

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial. Este es el valor predeterminado.

#### Detailed

Especifica que se visualizará toda la información.

## Ejemplo: visualizar información de destrucción de resumen

Muestra información parcial sobre la destrucción de datos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query shredstatus
```

```
Destrucción  Objetos
 activa      para
            destruir
-----
          NO          4
```

## Ejemplo: visualizar información de destrucción detallada

Muestra información detallada sobre la destrucción de datos en el servidor. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query shredstatus format=detailed
```

```
Destrucción  Objetos  Espacio  Datos restantes
 Active      Awaiting  Space    To Shred
            Shred   (MB)     (MB)
-----
          NO          4        182       364
```

## Descripciones de los campos

### Destrucción activa

Indica si el servidor está destruyendo datos de forma activa en este momento.

### Objetos para destruir

El número de objetos en espera de destruirse.

### Espacio ocupado (MB)

La cantidad de espacio de almacenamiento del servidor ocupado por los objetos que actualmente están en espera de destruirse, en megabytes. Es la cantidad de espacio que pasará a estar disponible cuando se destruyan los objetos.

### Datos restantes para destruir (MB)

La cantidad de datos que todavía se tienen que destruir.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SHREDSTATUS

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.



Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
MOVE DATA	Mueve los datos de un volumen de agrupación de almacenamiento a otro volumen de agrupación de almacenamiento.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
SETOPT	Actualiza una opción del servidor sin parar y reiniciar el servidor.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## QUERY SPACETRIGGER (Consultar los desencadenantes de espacio)

Utilice este comando para visualizar los valores de los desencadenantes de espacio de agrupación de almacenamiento.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query SPACETriGger--STG----->
>--+-----+----->
  '-STGPOOL----agrupación_almacenamiento-'
  .-Format----Standard----.
>--+-----+-----<<
  '-Format----+Standard-+'
      '-Detailed-'
```

### Parámetros

#### STG

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

#### STGPOOL

Especifica una o varias agrupaciones de almacenamiento (mediante un comodín) para las que se visualizará información de desencadenantes de agrupación. Si STG está especificado, pero STGPOOL no, se visualiza el desencadenante de espacio predeterminado de la agrupación de almacenamiento, si lo hay.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

##### Standard

Especifica que se visualizará información parcial.

##### Detailed

Especifica que se visualizará toda la información.

## Ejemplo: visualizar información detallada acerca de los valores de un desencadenante de espacio de agrupación de almacenamiento

Emita este comando:

```
query spacetrigger stg stgpool=archivepool format=detailed
```

#### Sistemas operativos AIX

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: /usr/tivoli/tsm/
                             server/filevol/
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

#### Sistemas operativos Linux

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: /opt/tivoli/tsm/server
                             /filevol/
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

#### Sistemas operativos Windows

```
Porcentaje llenado STGPOOL: 50
Porcentaje ampliación STGPOOL: 20
STGPOOL Prefijo ampliación: c:\program files\tivoli
                             \filevol\
STGPOOL: ARCHIVEPOOL
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 10/05/2004 11:59:59
```

## Descripciones de los campos

---

### STGPOOL Full Percentage

El porcentaje de utilización de desencadenante en que IBM Spectrum Protect asigna más espacio para la agrupación de almacenamiento.

### STGPOOL Expansion Percentage

Porcentaje de espacio según el cual se amplía la agrupación de almacenamiento.

### Prefijo de ampliación STGPOOL

El prefijo asociado al desencadenante de espacio.

### STGPOOL

Nombre de la agrupación de almacenamiento asociado a la consulta.

### Última actualización por (administrador)

Administrador que actualizó por última vez el desencadenante de espacio de la agrupación de almacenamiento.

### Fecha/hora de la última actualización

Fecha y hora de la última actualización por parte del administrador del desencadenante de espacio de la agrupación de almacenamiento.

## Comandos relacionados

---

Tabla 1. Comandos relacionados con QUERY SPACETRIGGER

Comando	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
UPDATE SPACETRIGGER	Cambia los atributos del desencadenante de espacio de agrupación de almacenamiento.

## QUERY STATUS (Consultar parámetros del sistema)

---

Utilice el comando QUERY STATUS para visualizar información sobre los parámetros del sistema.

Utilice este mandato para las tareas siguientes:

- Para visualizar el nivel de servicio del servidor

- Para visualizar información acerca de los parámetros generales del servidor, como por ejemplo los definidos mediante los comandos SET.
- Para solicitar información acerca de las sesiones cliente, como por ejemplo la disponibilidad del servidor, la autenticación de contraseñas, los valores de contabilidad, o el período de retención de la información retenida en el registro de actividad.
- Para visualizar información acerca del planificador central, como por ejemplo la modalidad de planificación central del servidor.
- Para visualizar el número máximo de intentos repetidos que se permiten después de un intento anómalo de ejecutar un mandato planificado.
- Para visualizar si se pueden hacer copias de seguridad de los subarchivos en este servidor, como indica el comando SET SUBFILE
- Para visualizar información sobre un servidor de réplica de destino
- Para mostrar información de licencias

Consejo: Para visualizar información sobre un servidor de réplica de destino, debe emitir el mandato desde el servidor de réplica de destino.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-Query SStatus-----><
```


## Parámetros

Ninguno.

## Ejemplo: consultar el estado de un gestor de configuración

Visualizar información general acerca de los parámetros del servidor. El comando se ejecuta desde un gestor de configuración. Para ver una descripción de los campos mostrados, consulte Descripciones de los campos.

```
query status
```

 Sistemas operativos AIX

```

Nombre de servidor: SETSHOT
Nombre host servidor o dirección IP: setshot
Número puerto TCP/IP servidor: 1500
Autenticación: Activada
Contraseña servidor asignada: Si
Fecha/hora de instalación de servidor: 2016-07-08, 09:45:53
Fecha/hora de reinicio de servidor: 2016-10-10, 05:38:49
Autenticación: Desactivada
Período caducidad contraseña: 9.999 día(s)
Límite conexiones no válidas: 0
Longitud mínima contraseña: 0
Inscripción: Cerrada
Copia de seguridad de subarchivos: Cliente
Disponibilidad: Activada
Sesiones de entrada desactivadas:
Sesiones de salida desactivadas:
Contabilidad: Desactivada
Período retención registro actividades: 30 día(s)
Número de registros de registro de actividad: 222919
Tamaño del registro de actividad: 6 M
Período retención resumen actividades: 30 día(s)
Período auditoría licencia: 30 día(s)
Última auditoría de licencia: 2016-10-21, 07:40:20
Cumplimiento licencia servidor: Válido
Planificador central: Activo
Sesiones máximas: 300
Sesiones planificadas máximas: 75
Período retención registros eventos: 14 día(s)
Duración acción cliente: 5 día(s)
Porcentaje aleatorización planificaciones: 25
Período consulta planificaciones: Opción cliente
Máximo reintentos comandos: Opción cliente
Período reintento: Opción cliente
Nivel de verificación de desduplicación del lado del cliente: 0%
```

Modalidades planificación: Cualquiera  
 Receptores activos: CONSOLE ACTLOG  
 Gestor configuración: Desactivado  
 Intervalo renovación: 60  
 Fecha/hora última renovación:  
 Envío de mensajes de contexto: Activado  
 Período retención de carga tabla contenido (TOC): 120 Minuto(s)  
 ID exclusivo global de máquina: d4.cg.f6.ae.04.6e.11.e3.80.1f.00.21.5e.18.df.01  
 Protección retención copias archivadas: desactivada  
 Directorios de base de datos: /TSMserver/DB1,/TSMserver/DB2  
 Espacio total de sistema de archivos (MB): 222.720,00  
 Espacio utilizado en el sistema de archivos (MB): 47.780,74  
 Espacio libre disponible (MB): 174.939,26  
 Nivel de cifrado: AES  
 Intervalo de renovación de información de CPU de cliente: 180  
 Réplica de salida: activado  
 Servidor de réplica de destino: POWER  
 Regla de réplica predeterminada de archivado: ALL\_DATA  
 Regla de réplica predeterminada de copia de seguridad: ALL\_DATA  
 Regla de réplica predeterminada para gestión de espacio: ALL\_DATA  
 Período de retención de registros de réplica: 30 día(s)  
 Usuario LDAP:  
 Contraseña LDAP establecida: No  
 Autenticación predeterminada: Local  
 Dirección de alto nivel de migración tras error:  
 Retención de anotación: 365 día(s)  
 Recuperación de duplicación de archivos dañados: activado  
 Ocupación SUR (TB): 5.66  
 Fecha/hora de ocupación SUR: 2016-10-10, 05:39:33  
 Capacidad inicial (MB): 226.331  
 Recuento de cliente inicial: 6  
 Fecha de capacidad inicial: 2016-10-13, 09:20:02  
 Oferta de producto: IBM Spectrum Protect

#### Sistemas operativos Linux

Nombre de servidor: GOBI  
 Nombre host servidor o dirección IP:  
 Número puerto TCP/IP servidor: 1500  
 Autenticación: Activada  
 Contraseña servidor asignada: Sí  
 Fecha/hora de instalación de servidor: 2016-07-08, 11:29:03  
 Fecha/hora de reinicio de servidor: 2016-11-10, 14:25:03  
 Autenticación: Activada  
 Período caducidad contraseña: 90 día(s)  
 Límite conexiones no válidas: 0  
 Longitud mínima contraseña: 0  
 Inscripción: Cerrada  
 Copia de seguridad de subarchivos: No  
 Disponibilidad: Activada  
 Sesiones de entrada desactivadas:  
 Sesiones de salida desactivadas:  
 Contabilidad: Desactivada  
 Período retención registro actividades: 30 día(s)  
 Número de registros de registro de actividad: 21346  
 Tamaño del registro de actividad: <1 M  
 Período retención resumen actividades: 30 día(s)  
 Período auditoría licencia: 30 día(s)  
 Última auditoría de licencia: 2016-10-21, 23:27:23  
 Cumplimiento licencia servidor: Válido  
 Planificador central: Activo  
 Sesiones máximas: 500  
 Sesiones planificadas máximas: 250  
 Período retención registros eventos: 14 día(s)  
 Duración acción cliente: 5 día(s)  
 Porcentaje aleatorización planificaciones: 25  
 Período consulta planificaciones: Opción cliente  
 Máximo reintentos comandos: Opción cliente  
 Período reintento: Opción cliente  
 Nivel de verificación de desduplicación del lado del cliente: 0%  
 Modalidades planificación: Cualquiera  
 Receptores activos: CONSOLE ACTLOG  
 Gestor configuración: Desactivado  
 Intervalo renovación: 60  
 Fecha/hora última renovación:  
 Envío mensajes contexto: Desactivado  
 Período retención de carga tabla contenido (TOC): 120 Minuto(s)

ID exclusivo global de máquina: fc.e7.be.58.4a.a7.11.e0.8a.c8.e4.1f.13.34.11.e0  
Protección retención copias archivadas: desactivada  
Dir. base datos:  
/TSMdbspace1/gpcinst1,/TSMdbspace2/gpcinst1,/TSMdbspace3/gpcinst1  
Espacio total de sistema de archivos (MB): 302.379,84  
Espacio utilizado en sistema de archivos (MB): 106.793,65  
Espacio libre disponible (MB): 195.586,20  
Nivel de cifrado: AES  
Intervalo de renovación de información de CPU de cliente: 180  
Réplica de salida: activado  
Servidor de réplica de destino:  
Regla de réplica predeterminada de archivado: ALL\_DATA  
Regla de réplica predeterminada de copia de seguridad: ALL\_DATA  
Regla de réplica predeterminada para gestión de espacio: ALL\_DATA  
Período de retención de registros de réplica: 30 día(s)  
Usuario LDAP:  
Contraseña LDAP establecida: No  
Autenticación predeterminada: Local  
Dirección de alto nivel de migración tras error:  
Retención de anotación: 365 día(s)  
Recuperación de duplicación de archivos dañados: desactivado  
Ocupación SUR (TB): 0,00  
Fecha/hora ocupación SUR: 2016-10-10, 14:25:35  
Capacidad inicial (MB): 226.331  
Recuento de cliente inicial: 6  
Fecha de capacidad inicial: 2016-10-13, 09:20:02  
Oferta de producto: IBM Spectrum Protect

#### Sistemas operativos Windows

Nombre de servidor: EXCELSIOR  
Nombre host servidor o dirección IP: excelsior.storage.  
newyork.example.com  
Número puerto TCP/IP servidor: 1500  
Autenticación: Activada  
Contraseña servidor asignada: Si  
Fecha/hora de instalación de servidor: 2016-07-08, 18:02:50  
Fecha/hora de reinicio de servidor: 2016-11-10, 11:48:32  
Autenticación: Activada  
Período caducidad contraseña: 90 día(s)  
Límite conexiones no válidas: 0  
Longitud mínima contraseña: 0  
Inscripción: Cerrada  
Copia de seguridad de subarchivos: No  
Disponibilidad: Activada  
Sesiones de entrada desactivadas:  
Sesiones de salida desactivadas:  
Contabilidad: Activada  
Período retención registro actividades: 30 día(s)  
Número de registros de registro de actividad: 1346376  
Tamaño del registro de actividad: 37 M  
Período retención resumen actividades: 30 día(s)  
Período auditoría licencia: 30 día(s)  
Última auditoría de licencia: 2016-10-21, 17:05:16  
Cumplimiento licencia servidor: Válido  
Planificador central: Activo  
Sesiones máximas: 25  
Sesiones planificadas máximas: 12  
Período retención registros eventos: 14 día(s)  
Duración acción cliente: 5 día(s)  
Porcentaje aleatorización planificaciones: 25  
Período consulta planificaciones: Opción cliente  
Máximo reintentos comandos: Opción cliente  
Periodo reintento: Opción cliente  
Nivel de verificación de deduplicación del lado del cliente: 0%  
Modalidades planificación: Cualquiera  
Receptores activos: CONSOLE ACTLOG  
NTEVENTLOG  
Gestor configuración: Desactivado  
Intervalo renovación: 60  
Fecha/hora última renovación:  
Envío mensajes contexto: Desactivado  
Período retención de carga tabla contenido (TOC): 120 Minuto(s)  
ID exclusivo global de máquina: e9.3e.f1.70.ff.c5.11.e2.  
a5.67.5c.f3.fc.0c.5e.60  
Protección retención copias archivadas: desactivada

Directorios de base de datos: e:\Server1\TSMDBdir  
 Espacio total de sistema de archivos (MB): 102.270,00  
 Espacio utilizado en sistema de archivos (MB): 22.032,79  
 Espacio libre disponible (MB): 80.237,20  
 Nivel de cifrado: AES  
 Intervalo de renovación de información de CPU de cliente: 180  
 Réplica de salida: activado  
 Servidor de réplica de destino: EXPLORER  
 Regla de réplica predeterminada de archivado: ALL\_DATA  
 Regla de réplica predeterminada de copia de seguridad: ALL\_DATA  
 Regla de réplica predeterminada para gestión de espacio: ALL\_DATA  
 Período de retención de registros de réplica: 30 día(s)  
 Usuario LDAP: cn=excelsior\_ldapadmin,ou=excelsior,  
 ou=John Doe,dc=tsmadldap,dc=storage,  
 dc=newyork, dc=example,dc=com  
 Contraseña LDAP establecida: Yes  
 Autenticación predeterminada: LDAP  
 Dirección de alto nivel de migración tras error:  
 Retención de anotación: 365 día(s)  
 Recuperación de duplicación de archivos dañados: activado  
 Ocupación SUR (TB): 8,98  
 Fecha/hora de ocupación SUR: 2016-10-10, 11:49:27  
 Capacidad inicial (MB): 226.331  
 Recuento de cliente inicial: 6

 Sistemas operativos Windows

Fecha de capacidad inicial: 2016-10-13, 09:20:02  
 Oferta de producto: IBM Spectrum Protect

## Descripciones de los campos

---

- Nombre del servidor  
Especifica el nombre del servidor.
- Nombre del host del servidor o dirección IP  
Especifica la dirección TCP/IP del servidor.
- Número de puerto TCP/IP del servidor  
Especifica la dirección del puerto del servidor.
- Crossdefine  
Especifica si otro servidor que ejecuta el mandato DEFINE SERVER se define automáticamente a sí mismo en este servidor. Consulte el mandato SET CROSSDEFINE.
- Contraseña servidor establecida  
Especifica si se ha asignado la contraseña para el servidor.
- Fecha/hora instalación servidor  
Especifica la fecha y hora en que se ha instalado el servidor.
- Fecha/hora reinicio servidor  
Especifica la última fecha y hora en que se ha iniciado el servidor.
- Autenticación  
Especifica si está activada o desactivada la autenticación del servidor.
- Período de caducidad de contraseña  
Especifica el período, en días, después del cual caduca la contraseña del nodo cliente o del administrador.
- Límite de conexiones no válidas  
Especifica el número de intentos de inicio de sesión permitidos antes de bloquear un nodo.
- Longitud mínima contraseña  
Especifica el número de caracteres mínimo que debe tener la contraseña.
- Inscripción  
Especifica si la modalidad de inscripción de nodos cliente es abierta o cerrada.
- Copia de seguridad de subarchivos  
Especifica si se pueden hacer copias de seguridad de los subarchivos en este servidor, como indica el comando SET SUBFILE.
- Disponibilidad  
Especifica si el servidor está activado o desactivado.
- Sesiones de entrada inhabilitadas  
Especifica los nombres de los servidores desde los que no están permitidas las comunicaciones de servidor a servidor. Para activar las sesiones de servidor de entrada, utilice el comando ENABLE SESSIONS.
- Sesiones de salida inhabilitadas  
Especifica los nombres de los servidores hacia los que no están permitidas las comunicaciones de servidor a servidor. Para activar las sesiones de servidor de salida, utilice el comando ENABLE SESSIONS.
- Contabilidad  
Especifica si se genera un registro de contabilidad al final de cada sesión del nodo cliente.

Período de registro de actividades  
Especifica el número de días en que se retiene la información de las anotaciones de actividades o el tamaño del registro.

Número de registros de anotaciones de actividades  
Especifica el número de registros de anotaciones de actividades.

Tamaño del registro de actividades  
Especifica el tamaño de los registros de anotaciones de actividades.

Período retención resumen actividades  
Especifica el número de días en que se retiene la información de la tabla resumen de actividad de SQL.

Período auditoría licencia  
Especifica el período, en días, después del cual el gestor de licencias realiza automáticamente una auditoría de la licencia de IBM Spectrum Protect. Se puede disponer de información de auditorías adicional mediante el comando QUERY LICENSE.

Última auditoría licencia  
Especifica la fecha y hora en que se ha producido la última auditoría de licencia. Se puede disponer de información de auditorías adicional mediante el comando QUERY LICENSE.

Cumplimiento licencia servidor  
Especifica si el servidor de ADSM cumple (Válido) o no (No válido) con los términos de la licencia. Utilice el comando QUERY LICENSE para ver cuáles son los factores que hacen que el servidor no cumpla los términos de la licencia.

Planificador central  
Especifica si está ejecutándose la planificación central (activo o cancelado).

Máximo de sesiones  
Especifica el número máximo de sesiones cliente/servidor.

Máximo de sesiones planificadas  
Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.

Período de retención de registros de eventos  
Especifica el número de días en que se retienen los registros de eventos del planificador central.

Duración acción de cliente  
Especifica la duración del período durante en el que el cliente procesa la planificación definida con el mandato DEFINE CLIENTACTION.

Porcentaje de aleatorización de planificaciones  
Especifica la cantidad de margen de puesta en marcha que se utiliza para ejecutar los eventos planificados en modalidad de sondeo de cliente.

Período de consulta de planificaciones  
Especifica la frecuencia con la que los clientes sondan el servidor para obtener el trabajo planificado, en modalidad de sondeo de cliente. Si el valor de este campo es Opción cliente, la frecuencia de sondeo la determina el nodo cliente.

Máximo reintentos comandos  
Especifica el número máximo de veces que un planificador del cliente intenta ejecutar un comando planificado después de un intento fallido. Si el valor de este campo es Opción cliente, el número máximo lo determina el nodo de cliente.

Período de reintento  
Especifica el número de minutos entre intentos fallidos de un planificador del cliente de contactar con el servidor o de ejecutar un comando planificado. Si el valor de este campo es Opción cliente, el número de minutos lo determina el nodo de cliente.

Nivel de verificación de deduplicación del lado del cliente  
Especifica un porcentaje de extensiones que debe verificar el servidor de IBM Spectrum Protect. Las extensiones se crean durante la eliminación de duplicados de datos del lado del cliente.

Modalidades de planificación  
Especifica las modalidades de planificación central que soporta el servidor.

Receptores activos  
Especifica los receptores para los que se ha iniciado la anotación de eventos.

¿Gestor de configuración?  
Especifica si el servidor es un gestor de configuración.

Intervalo de renovación  
Especifica el intervalo que transcurre antes de que el servidor gestionado solicite una renovación de todos los cambios de un gestor de configuración.

Fecha/hora última renovación  
Si el servidor es un servidor gestionado, especifica la fecha y la hora de la última renovación ejecutada correctamente de la información de configuración del gestor de configuración.

Envío de mensajes de contexto  
Especifica si el envío de mensajes de contexto está activado o desactivado.

Retención de carga de la tabla de contenido (TOC)  
Especifica el número aproximado de minutos que se retienen en la base de datos los datos de tabla de contenido sin referencia.

ID exclusivo global de máquina  
El identificador exclusivo global (GUID) existente la última vez que se inició el servidor. Este GUID identifica el sistema host al que pertenece el servidor actual.

Protección de retención de copias archivadas  
Especifica si la protección de retención de datos de copia archivada está activa.

#### Directorios de base de datos

Especifica las ubicaciones de los directorios de base de datos.

#### Espacio total de sistema de archivos (MB)

Especifica el tamaño total del sistema de archivos.

#### Espacio utilizado en sistema de archivos (MB)

Especifica la cantidad de espacio que se utiliza en el sistema de archivos.

#### Espacio libre disponible (MB)

Especifica la cantidad de espacio disponible.

#### Nivel de cifrado

Indica el nivel de cifrado de los datos: AES o DES.

#### Intervalo de renovación de la información de CPU de cliente

Especifica el número de días transcurridos entre exploraciones de cliente para la información de CPU utilizada para la estimación de PVU.

#### Réplica de salida

Especifica si el proceso de réplica está activado o desactivado. Si la réplica de salida está desactivada, no pueden iniciarse nuevos procesos de réplica en el servidor.

#### Servidor de réplica destino

Especifica el nombre del servidor que es el destino de las operaciones de réplica de nodo. Si un servidor de réplica de destino no existe, el campo está en blanco.

#### Norma de réplica predeterminada para archivado

Especifica la regla de réplica del servidor que se aplica a los datos de archivado. Son posibles los siguientes valores:

##### ALL\_DATA

Replica los datos de archivado. Los datos se replican con una prioridad normal.

##### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de archivado. Los datos se replican con una prioridad alta.

##### NONE

Los datos de archivado no se replican.

#### Norma de réplica predeterminada para copia de seguridad

Especifica la regla de réplica del servidor que se aplica a los datos de copia de seguridad. Son posibles los siguientes valores:

##### ALL\_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

##### ACTIVE\_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

##### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

##### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta.

##### NONE

Los datos de copia de seguridad no se replican.

#### Norma de réplica predeterminada para gestión de espacios

Especifica la regla de réplica del servidor que se aplica a los datos gestionados por espacio. Son posibles los siguientes valores:

##### ALL\_DATA

Replica los datos gestionados por espacio. Los datos se replican con una prioridad normal.

##### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos gestionados por espacio. Los datos se replican con una prioridad alta.

##### NONE

Los datos gestionados por espacio no se replican.

#### Período de retención de registros de réplicas



Especifica el número de días que se retienen los registros de historial de réplicas en la base de datos del servidor de réplica de origen.

#### Usuario LDAP

Especifica el ID de usuario que se nombra en el mandato SET LDAPUSER. Este ID de usuario puede emitir mandatos administrativos en el espacio de nombres reservado para IBM Spectrum Protect en el servidor de directorios LDAP.

#### Establecer contraseña de LDAP

Este campo de salida muestra si se define una contraseña para el ID de usuario que se especifica en el SET LDAPUSER mandato. Los valores son YES y NO. Si es YES, el ID de usuario que se especifica en el mandato SET LDAPUSER puede emitir mandatos administrativos en el espacio de nombres de LDAP que está reservado para IBM Spectrum Protect. Si NO, emita el mandato SET LDAPPASSWORD para definir la contraseña para el ID de usuario que se nombra en el mandato SET LDAPUSER.

#### Autenticación predeterminada

Especifica el método de autenticación de contraseña predeterminada: LOCAL o LDAP.

Destino de autenticación	Método de autenticación
Servidor de IBM Spectrum Protect	LOCAL
Servidor de directorios LDAP	LDAP

Cuando emite el mandato SET DEFAULTAUTHENTICATION define el método de autenticación resultante para todos los mandatos REGISTER ADMIN y REGISTER NODE. El valor predeterminado es LOCAL.

#### Dirección de alto nivel de migración tras error

Especifica la dirección de alto nivel para el servidor de migración tras error que utiliza el cliente. Las operaciones de restauración de cliente migran tras error en esta dirección de nivel superior cuando la interfaz que utiliza el cliente es distinta a la interfaz utilizada por la réplica.

#### Retención de anotación

Especifica el número de días para el que se retienen entradas de anotación desde que se actualizó por última vez.

#### Recuperación de duplicación de archivos dañados

Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino. Este es un valor del lado del sistema. Si se especifica Activado, el proceso de réplica del nodo se puede configurar para detectar los archivos dañados en un servidor de réplica de origen y sustituirlos por archivos sin dañar de un servidor de réplica de destino. Si se especifica Desactivado, los archivos dañados no se recuperan de un servidor de réplica de destino.

#### Ocupación SUR (TB)

Si tiene una licencia de IBM Spectrum Protect Suite (SUR), este campo especifica la ocupación de SUR en el servidor. La *ocupación SUR* es la cantidad de espacio que se utiliza para almacenar datos que gestionan productos de IBM Spectrum Protect que están incluidos en el paquete SUR.

#### Fecha y hora de ocupación SUR

Especifica la fecha y hora en las que se recopilaron los datos de ocupación SUR por última vez.

#### Capacidad inicial (MB)

Especifica la cantidad de datos primarios de los cuales se ha notificado que los clientes están haciendo una copia de seguridad. Los clientes pueden ser aplicaciones, máquinas virtuales y sistemas. Este valor se utiliza para el modelo de licencias frontal.

#### Recuento del cliente inicial

Especifica el número de clientes que han notificado el uso de la capacidad basado en el modelo de licencias frontales.

#### Fecha de capacidad inicial

Especifica la fecha y hora cuando se recopilaron por última vez los datos de capacidad inicial.

#### Oferta de producto

Especifica una oferta de producto.

Valor especificado por el mandato SET PRODUCTOFFERING	Valor mostrado en la salida del mandato QUERY STATUS
ENTry	IBM Spectrum Protect Entry
DATARet	IBM Spectrum Protect para retención de datos
BASIC	IBM Spectrum Protect
EE	IBM Spectrum Protect Extended Edition
SUIte	IBM Spectrum Protect Suite
SUITEEntry	IBM Spectrum Protect Suite Entry
SUITEArchive	IBM Spectrum Protect Suite - Archive
SUITEProtectier	IBM Spectrum Protect Suite - ProtecTier
SUITEFrontend	IBM Spectrum Protect Suite - FrontEnd
SUITEENTRYFrontend	IBM Spectrum Protect Suite Entry - FrontEnd
CLEAR	NULO

Tabla 1. Comandos relacionados con QUERY STATUS

Comando	Descripción
BEGIN EVENTLOGGING	Inicia la anotación de eventos en un receptor especificado.
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
DISABLE SESSIONS	Impide que las nuevas sesiones accedan a IBM Spectrum Protect, pero permite que continúen las sesiones existentes.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
END EVENTLOGGING	Finaliza el registro de eventos en un receptor especificado.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
SET ACCOUNTING	Especifica si se crean registros de contabilidad al final de cada sesión cliente.
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.
SET CONTEXTMESSAGING	Especifica que debe activarse el envío de mensajes de contexto para depurar un mensaje ANR9999D
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET EVENTRETENTION	Especifica el número de días que se retienen los registros de las operaciones planificadas.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un comando planificado.
SET MAXSCHEDESESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET PRODUCTOFFERING	Establece la oferta de producto para la que su empresa tiene licencia.
SET QUERYSCHEDPERIOD	Especifica la frecuencia en que los clientes pueden obtener el trabajo planificado, en modalidad por sondeo de cliente.
SET RANDOMIZE	Especifica la aleatorización de las horas de inicio de un margen de las planificaciones en modalidad por sondeo de cliente.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.

Comando	Descripción
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERNAME	Especifica el nombre por el que se identifica al servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.
SET SUMMARYRETENTION	Especifica el número de días que se debe mantener la información en la tabla resumen de actividades.
SET TOCLOADRETENTION	Especifica el número de minutos que se debe mantener la información de los conjuntos de tabla de contenido sin referencia.

## QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)

Utilice este mandato para visualizar información sobre los umbrales de supervisión de estado.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-*-----
>>-Query STAtusthreshold-+----->
                          '-nombre_umbral-'

.-Format----Standard----.
>-+-----+-----+-----+----->
  '-Format----+Standard-+'  '-Activity----actividad-'
                          '-Detailed-'

>-+-----+-----+-----+----->
  '-Condition----+EXists-+'  '-Value----nombre_valor-'
                          +-GT-----+
                          +-GE-----+
                          +-LT-----+
                          +-LE-----+
                          '-Equal--'

>-+-----+-----+-----+-----<
  '-Status----+Normal--+-'
                          +-Warning-+
                          '-Error--'

```

### Parámetros

nombre\_umbral

Especifica el nombre de umbral. El nombre de no puede tener más 48 caracteres de longitud.

Format

Especifica cómo se ha de visualizar la información. El valor predeterminado es STANDARD. Los valores posibles son:

Standard

Especifica que se visualizará información parcial para los umbrales de estado especificados.

Detailed

Especifica que se visualizará información completa para los umbrales de estado especificados.

## actividad

Especifica la actividad para la que desea visualizar indicadores de estado. Si no especifica un valor, se visualizará información para todas las actividades. Para obtener una lista de actividades, consulte el mandato DEFINE STATUSTHRESHOLD.

## Condition

Restringe la salida a sólo aquellos que coincidan con el valor especificado. Los valores posibles son:

### EXists

Visualiza umbrales de estado donde la condición es igual a EXISTS.

### GT

Visualiza umbrales de estado donde la condición es igual a GT.

### GE

Visualiza umbrales de estado donde la condición es igual a GE.

### LT

Visualiza umbrales de estado donde la condición es igual a LT.

### LE

Visualiza umbrales de estado donde la condición es igual a LE.

### EQual

Visualiza umbrales de estado donde la condición es igual a EQUAL.

## Value

Visualiza umbrales que tienen el valor especificado. Si no especifica un valor, se visualizará información para todos los valores. Puede especificar un entero de 0 a 9223372036854775807.

## Status

Visualiza umbrales de estado que tienen el valor de estado especificado. Si no especifica un valor, se visualizará información para todos los valores. Los valores posibles son:

### Normal

Visualiza los umbrales de estado que tienen un valor de estado normal.

### Aviso

Visualiza los umbrales de estado que tienen un valor de estado de aviso.

### Error

Visualiza los umbrales de estado que tienen un valor de estado de error.

## QUERY status threshold

---

Consulte todos los umbrales de estado emitiendo el mandato siguiente:

```
query statusthreshold
```

Nombre umbral	Nomb.actividad	Nombre condición	Valor	Estado informe
-----	-----	-----	-----	-----
ACTIVELOGCHECK	ACTIVE LOG UTILIZATION (%)	>	90	ERROR
AVGSTGPLW	AVERAGE STORAGE POOL UTILIZATION (%)	>	85	WARNING
AVGSTGPLE	AVERAGE STORAGE POOL UTILIZATION (%)	>	90	ERROR

## Consultar umbrales de estado y visualizar formato detallado

---

Consulte los umbrales de estado y visualice la salida en formato detallado, emitiendo el mandato siguiente:

```
query statusthreshold f=d
```

```
Nombre de umbral: ACTIVELOGCHECK
Nombre de la actividad: ACTIVE LOG UTILIZATION (%)
Nombre de la condición: >
Valor: 90
Estado del informe: ERROR
Nombre de servidor: TSMAWP24

Nombre de umbral: AVGSTGPLW
Nombre de la actividad: AVERAGE STORAGE POOL UTILIZATION (%)
Nombre de la condición: >
```

Valor: 85  
 Estado del informe: WARNING  
 Nombre de servidor: TSMAWP24

Nombre de umbral: AVGSTGPLE  
 Nombre de la actividad: AVERAGE STORAGE POOL UTILIZATION (%)  
 Nombre de la condición: >  
 Valor: 95  
 Estado del informe: ERROR  
 Nombre de servidor: TSMAWP24

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY STATUSTHRESHOLD

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## QUERY STGPOOL (Consultar agrupaciones de almacenamiento)

Utilice este comando para visualizar información acerca de una o varias agrupaciones de almacenamiento. También puede utilizar este mandato para supervisar procesos de migración para agrupaciones de almacenamiento.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

      .-*----- .
>>-Query STGpool---+----->
      '-nombre_agrupación-'

      .-Format----Standard----.
>>+-----+----->
      '-Format---+Standard-+'
      '-Detailed-'

      .-Pooltype----ANY----- .
>>+-----+-----<<
      '-Pooltype----+ANY-----+'
      +-Primary-----+
      +-Copy-----+
      +-COPYCONTAINER+
      '-ACTIVEdata----'
  
```

## Parámetros

---

### nombre\_agrupación

Especifica la agrupación de almacenamiento que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar este nombre. Si no especifica un valor para este parámetro, se visualizarán todas las agrupaciones de almacenamiento.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Especifique uno de los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

### POoltype

Especifica el tipo de agrupación de almacenamiento que se consulta. Este parámetro es opcional. El valor predeterminado es ANY. Especifique uno de los siguientes valores:

#### ANY

Se consultan las agrupaciones de almacenamiento primarias, las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos.

#### PRimary

Sólo se consultan las agrupaciones de almacenamiento primarias.

#### COpy

Sólo se consultan las agrupaciones de almacenamiento de copia.

#### COPYCONTainer

Sólo se consultan las agrupaciones de almacenamiento de copia de contenedor.

#### ACTIVEdata

Sólo se consultan las agrupaciones de almacenamiento de datos activos.

## Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de disco de acceso aleatorio

---

Consejo: En los ejemplos de la salida detallada, algunos campos están en blanco porque el elemento no se aplica en el entorno especificado.

Mostrar detalles para una agrupación de almacenamiento llamada DISKPOOL. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool diskpool format=detailed
```

```
Nombre agrupación almacenamiento: DISKPOOL
Tipo agrupación almacenamiento: Primaria
Nombre de clase de dispositivo: DISK
  Tipo de almacenamiento: DEVCLASS
    Tipo de nube:
      URL de nube:
        Identidad de nube:
          Ubicación de nube:
            Capacidad estimada: 66 G
            Desencadenante de espacio: 0,0
              % Util: 0,0
              % Migr: 3,1
              % Lógico: 100,0
              % Migr alto: 90
              % Migr bajo: 70
            Retardo migración: 0
            Continuar migración: Yes
            Procesos migración: 1
            Procesos reclamación: 1
              Siguiendo agrupación almacenamiento:
              Agrupación de almacenamiento de reclamación:
              Tamaño máximo umbral: Ilimitado
                Acceso: Lectura/Grabación
                Descripción:
                Ubicación desbordamiento:
                ¿Caché de archivos migrados?:
                ¿Función proximidad?: Grupo
                Umbral reclamación: 60
                Límite de reclamación fuera del local:
```

```

Máximo de volúmenes reutilizables: 32
Número volúmenes reutilizables utilizados: 1
Periodo de retardo para reutilización de contenedor: 1 día(s)
  ¿Migración en curso?: No
    Cantidad migrada (MB): 0,00
Tiempo transcurrido en migración (segundos): 0
  ¿Reclamación en curso?: No

Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 01/03/2014 13:57:16
Formato datos agrupación almacenamiento: nativo
Agrupaciones almacenamiento copias:
  Agrupaciones de datos activos:
    ¿Continuar la copia en caso de error?: No
      Datos CRC: sí
    Tipo de reclamación: Umbral
  Grabar sobre datos cuando se supriman: 2 veces
    ¿Eliminar duplicados de datos?: No
Procesos para identificar duplicados:
  Comprimido:
  Ahorro de la deduplicación:
  Ahorro de compresión:
  Espacio total ahorrado:
  Modalidad de copia automática: Cliente
¿Contiene eliminaciones de datos duplicados por clientes?: No
Máximo de grabadores simultáneos:
  Procesos de protección:
  Agrupación de almacenamiento de protección:
  Proteger agrupaciones de almacenamiento locales:
  Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
  ¿La eliminación de duplicados requiere una copia seguridad?:
    Cifrada:
      Pct cifrado:
    Espacio de nube utilizado (MB):
      Nombre de grupo:
    Capacidad estimada local:
      Pct. util local:
      Pct. lógico local:

```

## Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de disco de acceso secuencial

Mostrar detalles para una agrupación de almacenamiento denominada FILEPOOL. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool filepool format=detailed
```

```

Nombre agrupación almacenamiento: FILEPOOL
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo: FILEC
  Tipo de almacenamiento: DEVCLASS
    Tipo de nube:
      URL de nube:
  Identidad de nube:
  Ubicación de nube:
  Capacidad estimada: 66 G
  Desencadenante de espacio: 0,0
    % Util: 0,0
    % Migr: 3,1
    % Lógico: 100,0
    % Migr alto: 90
    % Migr bajo: 70
  Retardo migración: 0
  Continuar migración: Yes
  Procesos migración: 1
  Procesos reclamación: 1
  Siguiendo agrupación almacenamiento:
  Agrupación de almacenamiento de reclamación:
  Tamaño máximo umbral: Ilimitado
  Acceso: Lectura/Grabación
  Descripción:
  Ubicación desbordamiento:
  ¿Caché de archivos migrados?:

```

```

                ¿Función proximidad?: Grupo
                Umbral reclamación: 60
                Límite de reclamación fuera del local:
                Máximo de volúmenes reutilizables: 32
                Número volúmenes reutilizables utilizados: 1
                Período de retardo para reutilización de contenedor: 1 día(s)
                ¿Migración en curso?: No
                Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
                ¿Reclamación en curso?: No
                Última actualización por (administrador): SERVER_CONSOLE
                Fecha/hora última actualización: 01/02/2014 13:57:16
                Formato datos agrupación almacenamiento: nativo
                Agrupaciones almacenamiento copias:
                Agrupaciones de datos activos:
                ¿Continuar la copia en caso de error?: No
                Datos CRC: sí
                Tipo de reclamación: Umbral
                Grabar sobre datos cuando se supriman:
                ¿Eliminar duplicados de datos?: Sí
                Procesos para identificar duplicados: 1
                Comprimido:
                Ahorro de deduplicación: 65.396 K (49,99%)
                Ahorro de compresión:
                Espacio total ahorrado: 65.396 K (49,99%)
                Modalidad de copia automática: Cliente
                ¿Contiene eliminaciones de datos duplicados por clientes?: Sí
                Máximo de grabadores simultáneos:
                Procesos de protección:
                Agrupación de almacenamiento de protección:
                Proteger agrupaciones de almacenamiento locales:
                Límite del volumen de reclamación:
                Fecha de última protección de la agrupación local:
                Fecha de última protección de la agrupación local:
                ¿La eliminación de duplicados requiere una copia seguridad?:
                Cifrada:
                Pct cifrado:
                Espacio de nube utilizado (MB):
                Nombre de grupo:
                Capacidad estimada local:
                Pct. util local:
                Pct. lógico local:

```

## Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento de acceso secuencial

Mostrar detalles para una agrupación de almacenamiento secuencial de datos activos que se llama FILEPOOL que utiliza una clase de dispositivo de tipo FILE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool filepool format=detailed
```

```

Nombre agrupación almacenamiento: FILEPOOL
Tipo de agrupación de almacenamiento: Datos activo
Nombre clase dispositivo: FILEC
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 0,0 M
Desencadenante de espacio: 0,0
    % Util: 0,0
    % Migr: 0,0
    % Lógico: 0,0
    % Migr alto: 90
    % Migr bajo: 70
Retardo migración: 0
Continuar migración: Yes
Procesos migración: 1
Procesos reclamación: 1
Siguiete agrupación almacenamiento:
Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral: Ilimitado
Acceso: Lectura/Grabación
Descripción:

```



```

Ubicación desbordamiento:
¿Caché de archivos migrados?:
  ¿Función proximidad?: Grupo
Umbral reclamación: 60
Límite de reclamación fuera del local:
Máximo de volúmenes reutilizables: 99
Número volúmenes reutilizables utilizados: 0
Período de retardo para reutilización de contenedor: 1 día(s)
¿Migración en curso?: No
Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
¿Reclamación en curso?: No
Última actualización por (administrador): SERVER_CONSOLE
Fecha/hora última actualización: 01/02/2014 11:37:57
Formato datos agrupación almacenamiento: nativo
Agrupaciones almacenamiento copias:
Agrupaciones de datos activos:
¿Continuar la copia en caso de error?:
  Datos CRC: sí
  Tipo de reclamación: Umbral
Grabar sobre datos cuando se supriman:
  ¿Eliminar duplicados de datos?: Sí
Procesos para identificar duplicados: 1
  Comprimido:
  Ahorro de deduplicación: 65.396 K (49,99%)
  Ahorro de compresión:
  Espacio total ahorrado: 65.396 K (49,99%)
  Modalidad de copia automática:
¿Contiene eliminaciones de datos duplicados por clientes?: No
Máximo de grabadores simultáneos:
  Procesos de protección:
  Agrupación de almacenamiento de protección:
  Proteger agrupaciones de almacenamiento locales:
  Límite del volumen de reclamación:
Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
  ¿La eliminación de duplicados requiere una copia seguridad?:
  Cifrada:
  Pct cifrado:
Espacio de nube utilizado (MB):
  Nombre de grupo:
Capacidad estimada local:
  Pct. util local:
  Pct. lógico local:

```

## Ejemplo: visualizar información de resumen acerca de una agrupación de almacenamiento específica

Mostrar información para una agrupación de almacenamiento que se llama POOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool pool1
```

Nombre agrupación	Nombre clase	Capacidad estimada (MB)	% Util	% Migr	% Mig sup.	% Mig inf.	Siguiente agrupación almac. dispositivo
POOL1	DISK	58,5 M	0,8	0,7	90	70	POOL2

## Ejemplo: Visualizar información detallada acerca de la agrupación de almacenamiento de cinta de 8 mm

Visualizar los detalles sobre la agrupación de almacenamiento denominada 8MMPool. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool 8mmpool format=detailed
```

```

Nombre agrupación almacenamiento: 8MMPool
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo: 8MMTAPE
Tipo de almacenamiento: DEVCLASS
Tipo de nube:

```

```

        URL de nube:
        Identidad de nube:
        Ubicación de nube:
        Capacidad estimada: 0,0 M
        Desencadenante de espacio: 0,0
            % Util: 0,0
            % Migr:
                % Lógico: 0,0
                % Migr alto: 90
                % Migr bajo: 70
        Retardo migración: 0
        Continuar migración: Yes
        Procesos migración: 1
        Procesos reclamación: 1
        Siguiete agrupación almacenamiento:
        Agrupación de almacenamiento de reclamación:
        Tamaño máximo umbral: 5 M
            Acceso: Lectura/Grabación
            Descripción: Agrupación de
                                almacenamiento
                                principal
        Ubicación desbordamiento: Room1234/Bldg31
        ¿Caché de archivos migrados?:
        ¿Función proximidad?: No
        Umbral reclamación: 60
        Límite de reclamación fuera del local:
        Máximos volúmenes reutilizables: 5
        Volúmenes reutilizables utilizados: 3
        Período de retardo para reutilización de contenedor: 1 día(s)
        ¿Migración en curso?: No
        Cantidad migrada (MB): 0,00

Tiempo transcurrido en migración (segundos): 0
    ¿Reclamación en curso?: No
    Última actualización por (administrador): ADMIN
    Fecha/hora última actualización: 01/08/2014 06:55:45
    Formato datos agrupación almacenamiento: nativo
    Agrupaciones de almacenamiento de copia: COPYPOOL1
    Agrupaciones de datos activos: ACTIVEPOOL1 ACTIVEPOOL2
    ¿Continuar la copia en caso de error?: Yes
        Datos CRC: sí
        Tipo de reclamación: Umbral
    Grabar sobre datos cuando se supriman:
        ¿Eliminar duplicados de datos?: No
    Procesos para identificar duplicados:
        Comprimido:
        Ahorro de la deduplicación:
        Ahorro de compresión:
        Espacio total ahorrado:
        Comprimido: No
        Ahorro de la deduplicación:
        Ahorro de compresión:
        Espacio total ahorrado:
        Modalidad de copia automática: Cliente
    ¿Contiene eliminaciones de datos duplicados por clientes?: No
    Máximo de grabadores simultáneos:
    Procesos de protección:
        Agrupación de almacenamiento de protección:
    Proteger agrupaciones de almacenamiento locales:
        Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
    ¿La eliminación de duplicados requiere una copia seguridad?:
        Cifrada:
        Pct cifrado:
    Espacio de nube utilizado (MB):
        Nombre de grupo:
    Capacidad estimada local:
        Pct. util local:
        Pct. lógico local:

```

## Ejemplo: visualizar información detallada acerca de la agrupación de almacenamiento NAS2CLASS

---

Visualizar los detalles sobre la agrupación de almacenamiento NAS2LIBPOOL. Cuando configure esta agrupación de almacenamiento, debe establecer el formato de datos en NETAPPDUMP. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool nas2libpool format=detailed
```

```
Nombre agrupación almacenamiento: NAS2
Nombre de agrupación de almacenamiento: NAS2LIBPOOL
Tipo agrupación almacenamiento: Primaria
Nombre de clase de dispositivo: NAS2CLASS
Tipo de almacenamiento: DEVCLASS
Tipo de nube:
URL de nube:
Identidad de nube:
Ubicación de nube:
Capacidad estimada: 0,0 M
Util. desencadenante de espacio:
    % Util: 0,0
    % Migr:
    % Lógico: 0,0
    % Migr alto:
    % Migr bajo:
Retardo migración:
Continuar migración:
Procesos migración:
Procesos reclamación:
    Siguiente agrupación almacenamiento:
Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral:
    Acceso: Lectura/Grabación
    Descripción:
    Ubicación desbordamiento:
    ¿Caché de archivos migrados?:
    ¿Función proximidad?: Grupo
Umbral reclamación:
Límite de reclamación fuera del local:
Máximos volúmenes reutilizables: 50
Número volúmenes reutilizables utilizados: 0
Período de retardo para reutilización de contenedor: 1 día(s)
    ¿Migración en curso?:
    Cantidad migrada (MB):

Tiempo transcurrido en migración (segundos):
    ¿Reclamación en curso?:
    Última actualización por (administrador): SERVER_CONSOLE
    Fecha/hora última actualización: 01/02/2014 16:24:43
    Formato datos agrupación almacenamiento: vuelco NetApp
    Agrupaciones almacenamiento copias:
    Agrupaciones de datos activos:
    ¿Continuar la copia en caso de error?: No
    Datos CRC: No
    Tipo de reclamación:
    Grabar sobre datos cuando se supriman:
    ¿Eliminar duplicados de datos?: No
Procesos para identificar duplicados:
    Comprimido:
    Ahorro de la deduplicación:
    Ahorro de compresión:
    Espacio total ahorrado:
    Modalidad de copia automática: Cliente
¿Contiene eliminaciones de datos duplicados por clientes?: No
Máximo de grabadores simultáneos:
    Procesos de protección:
    Agrupación de almacenamiento de protección:
    Proteger agrupaciones de almacenamiento locales:
    Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
    ¿La eliminación de duplicados requiere una copia seguridad?:
    Cifrada:
    Pct cifrado:
Espacio de nube utilizado (MB):
    Nombre de grupo:
Capacidad estimada local:
    Pct. util local:
    Pct. lógico local:
```

## Ejemplo: Visualizar información detallada para una agrupación de almacenamiento de contenedores de directorios utilizada para deduplicación de datos

---

Visualizar detalles para una agrupación de almacenamiento de contenedores de directorios, DPOOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool dpool1 format=detailed

Nombre agrupación almacenamiento: DPOOL1
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo:
  Tipo de almacenamiento: Directorio
  Tipo de nube:
  URL de nube:
  Identidad de nube:
  Ubicación de nube:
Capacidad estimada: 798 G
Util. desencadenante de espacio:
  % Util: 3,4
  % Migr:
  % Lógico: 100,0
  % Migr alto:
  % Migr bajo:
  Retardo migración:
  Continuar migración:
  Procesos migración:
Procesos reclamación:
  Siguiete agrupación almacenamiento:
  Agrupación de almacenamiento de reclamación:
  Tamaño máximo umbral: Ilimitado
  Acceso: Lectura/Grabación
  Descripción:
  Ubicación desbordamiento:
  ¿Caché de archivos migrados?:
  ¿Función proximidad?:
  Umbral reclamación:
  Límite de reclamación fuera del local:
Máximo permitido de volúmenes reutilizables:
Número de volúmenes reutilizables utilizados:
Período de retardo para reutilización de contenedor: 1 día(s)
  ¿Migración en curso?:
  Cantidad migrada (MB):

Tiempo transcurrido en migración (segundos):
  ¿Reclamación en curso?:
  Última actualización por (administrador): SERVER_CONSOLE
  Fecha/hora última actualización: 01/02/2014 16:24:43
  Formato datos agrupación almacenamiento: nativo
  Agrupaciones almacenamiento copias:
  Agrupaciones de datos activos:
  ¿Continuar la copia en caso de error?:
  Datos CRC: No
  Tipo de reclamación:
  Grabar sobre datos cuando se supriman:
  ¿Eliminar duplicados de datos?: Sí
Procesos para identificar duplicados:
  Comprimido: Sí
  Espacio utilizado para datos protegidos: 1.599 M
  Total de espacio pendiente: 100 M
  Ahorro de deduplicación: 1.331 M (67,56%)
  Ahorro de compresión: 194.805 K (29,82%)
  Espacio total ahorrado: 1.521 M (77,22%)
  Modalidad de copia automática:
  ¿Contiene datos deduplicados por el cliente?:
  Máximo de grabadores simultáneos: Sin límite
  Procesos de protección:
  Agrupación de almacenamiento de protección: DPOOL2
  Proteger agrupaciones de almacenamiento locales:
  Límite del volumen de reclamación:

Fecha de última protección de la agrupación local:
Fecha de última protección de la agrupación local:
  ¿La eliminación de duplicados requiere una copia seguridad?:
  Cifrada:
  Pct cifrado: 34.56%
```

Espacio de nube utilizado (MB):  
Nombre de grupo:  
Capacidad estimada local:  
Pct. util local:  
Pct. lógico local:

## Ejemplo: Visualizar información detallada para una agrupación de almacenamiento de contenedores de nubes utilizada para deduplicación de datos

---

Visualizar detalles para una agrupación de almacenamiento de contenedores de nubes, CPOOL1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpool cpool1 format=detailed

Nombre agrupación almacenamiento: CPOOL1
Tipo agrupación almacenamiento: Primaria
Nombre clase dispositivo:
  Tipo de almacenamiento: CLOUD
  Tipo de nube: SWIFT
  URL de nube: http://localhost.local
Identidad de nube: Bailey
Ubicación de nube: ONPREMISE
Capacidad estimada:
Util. desencadenante de espacio:
  Pct. util:
  % Migr:
  % Lógico: 0,0
  % Migr alto:
  % Migr bajo:
Retardo migración:
Continuar migración:
Procesos migración:
Procesos reclamación:
  Siguiente agrupación almacenamiento:
  Agrupación de almacenamiento de reclamación:
Tamaño máximo umbral: Ilimitado
  Acceso: Lectura/Grabación
  Descripción:
  Ubicación desbordamiento:
¿Caché de archivos migrados?:
¿Función proximidad?:
Umbral reclamación:
Límite de reclamación fuera del local:
Máximo permitido de volúmenes reutilizables:
Número de volúmenes reutilizables utilizados:
Período de retardo de la reutilización de un volumen: 1
¿Migración en curso?:
Cantidad migrada (MB):

Tiempo transcurrido en migración (segundos):
¿Reclamación en curso?:
Última actualización por (administrador): CODY
  Fecha/hora última actualización: 2015-05-28, 10:47:52
Formato datos agrupación almacenamiento: nativo
  Agrupaciones almacenamiento copias:
  Agrupaciones de datos activos:
¿Continuar la copia en caso de error?:
  Datos CRC: No
  Tipo de reclamación:
Grabar sobre datos cuando se supriman:
¿Eliminar duplicados de datos?: Sí
Procesos para identificar duplicados:
  Comprimido: Sí
  Ahorro deduplicación: 9.241 K (89,76%)
  Ahorro compresión: 1.033 K (98,81%)
  Espacio total ahorrado: 10.274 K (99,79%)
  Modalidad de copia automática:
¿Contiene datos deduplicados por el cliente?:
  Máximo de grabadores simultáneos: Sin límite
  Procesos de protección:
  Agrupación de almacenamiento de protección:
  Proteger agrupaciones de almacenamiento locales:
  Límite del volumen de reclamación:
Fecha de última protección de la agrupación remota:
Fecha de última protección de la agrupación local:
```

¿La eliminación de duplicados requiere una copia seguridad?:  
Cifrado: Yes  
Pct cifrado: 34.56%  
Espacio de nube utilizado (MB): 4,231  
Nombre de grupo: ibmsp.  
C8ae4ec058cf11e680fe0a270000000  
Capacidad estimada local: 168 G  
Pct. util local: 0.1  
Pct. lógico local: 100.0

## Descripciones de los campos

---

### Nombre de la agrupación de almacenamiento

El nombre de la agrupación de almacenamiento.

### Tipo agrupación de almacenamiento

El tipo de agrupación de almacenamiento.

### Nombre clase dispositivo

El nombre de la clase de dispositivo asignada a la agrupación de almacenamiento.

### Tipo de almacenamiento

El tipo de almacenamiento que está definido para la agrupación de almacenamiento. Se pueden visualizar los siguientes tipos de almacenamiento:

#### DEVCLASS

La agrupación de almacenamiento especifica una clase de dispositivo que determina el tipo de dispositivo donde se almacenan los datos.

#### DIRECTORY

La agrupación de almacenamiento crea contenedores lógicos para datos en los directorios del sistema de archivos.

#### CLOUD

La agrupación de almacenamiento crea contenedores lógicos para datos en un entorno de nube.

### Tipo de nube

Para agrupaciones de almacenamiento en la nube, el tipo de plataforma de la nube.

### URL de nube

Para agrupaciones de almacenamiento en la nube, el URL para acceder a la nube privada local o a la nube pública externa.

### Identidad de nube

Para agrupaciones de almacenamiento en la nube, el ID de usuario para acceder a la nube privada local o a la nube pública externa.

### Ubicación de nube

Para agrupaciones de almacenamiento en la nube, indica si la nube es una nube privada local o una nube pública externa.

### Capacidad estimada

La capacidad estimada de la agrupación de almacenamiento en megabytes (M) o gigabytes (G).

Para dispositivos DISK, la capacidad estimada es la capacidad de todos los volúmenes de la agrupación de almacenamiento, incluido cualquier volumen que se haya desactivado.

Para agrupaciones de almacenamiento de acceso secuencial, la capacidad estimada es el espacio total estimado de todos los volúmenes de acceso secuencial en la agrupación de almacenamiento, independientemente de su modo de acceso. Se debe utilizar al menos un volumen en una agrupación de almacenamiento de acceso secuencial (ya sea un volumen reutilizable o un volumen privado) para calcular la capacidad estimada.

Para dispositivos de cinta y FILE, la capacidad estimada para la agrupación de almacenamiento incluye los factores siguientes:

- La capacidad de todos los volúmenes reutilizables que ya ha adquirido y puede adquirir la agrupación de almacenamiento. El número de volúmenes reutilizables se define mediante el parámetro MAXSCRATCH en el mandato DEFINE STGPOOL o UPDATE STGPOOL.
- Número total de volúmenes reutilizables disponibles en la biblioteca de cintas.
- La capacidad estimada es el número más pequeño entre el valor MAXSCRATCH y el número total de volúmenes reutilizables disponibles en la biblioteca de cintas.

Los cálculos de la capacidad estimada dependen del espacio disponible de almacenamiento del dispositivo asignado a la agrupación de almacenamiento. Para las agrupaciones de almacenamiento FILE, la capacidad de la agrupación de almacenamiento se reduce si el almacenamiento disponible es menos que el total de espacio estimado de todos los volúmenes FILE de la agrupación de almacenamiento. El valor que se visualiza para la capacidad se reduce por el tamaño de un volumen FILE de manera incremental a medida que el espacio disponible continúa disminuyendo.

Para Centera, este valor representa la capacidad total del dispositivo de almacenamiento Centera que se está consultando.

#### Util. desencadenante de espacio

Utilización de la agrupación de almacenamiento, calculada por el desencadenante de espacio de la agrupación de almacenamiento, si existe alguno, para esta agrupación de almacenamiento. Puede definir desencadenantes de espacio solo para las agrupaciones de almacenamiento asociadas a tipos de dispositivo DISK o FILE.

Para los dispositivos de acceso secuencial, la utilización del desencadenante de espacio se expresa como un porcentaje del número de bytes utilizados en cada volumen de acceso secuencias relativo al tamaño del volumen, y la capacidad estimada de todos los volúmenes existentes de la agrupación de almacenamiento. No incluye volúmenes reutilizables potenciales. A diferencia del cálculo del porcentaje de utilización, en el cálculo de la utilización del desencadenante de espacio es más preferible la creación de nuevos volúmenes de archivos privados por parte del desencadenante de espacio que la utilización de más volúmenes reutilizables.

Para los dispositivos de disco, la utilización del desencadenante de espacio se expresa en forma de porcentaje de la capacidad estimada, incluidos los datos en caché. Sin embargo, excluye datos que están en cualquier volumen que se haya desactivado. El valor de la utilización del desencadenante de espacio puede ser mayor que el valor del porcentaje de migración si emite el mandato QUERY STGPOOL mientras tiene lugar la creación de un archivo. El valor de la utilización de desencadenante de espacio lo determina la cantidad de espacio asignada mientras la transacción está en curso. El valor del porcentaje de migración representa solo el espacio ocupado por los archivos validados. Al final de la transacción, estos valores se sincronizan.

El valor de la utilización del desencadenante de espacio incluye los datos almacenados en caché en los volúmenes de disco. Por lo tanto, cuando se activa la caché y se produce una migración, el valor permanece igual porque los datos migrados continúan en el volumen como datos en caché. El valor solo disminuye cuando los datos de la memoria caché caducan o cuando el espacio que ocupan los archivos de la memoria caché se deben utilizar para archivos que no están en la memoria caché.

#### Pct. util

Un cálculo de la utilización de la agrupación de almacenamiento especificado como porcentaje.

Para los dispositivos de acceso secuencial, es un porcentaje del número de bytes activos en cada volumen de acceso secuencial y la capacidad estimada de todos los volúmenes de la agrupación de almacenamiento. El porcentaje incluye el número de volúmenes reutilizables potenciales que se pueden asignar.

Para dispositivos de disco, es un porcentaje de la capacidad estimada, incluyendo los datos en caché y los datos que residen en todos los volúmenes que están desactivados. El valor de Pct Util puede ser mayor que el valor de Pct Migr, si emite este mandato mientras está en proceso una transacción de creación de archivos. El valor de Pct Util se determina por la cantidad de espacio asignado, mientras la transacción está en proceso. El valor de Pct Migr sólo representa el espacio que ocupan los archivos validados. Al final de la transacción, se sincronizan estos valores.

El valor de Pct Util incluye los datos almacenados en caché en los volúmenes de disco. Por lo tanto, cuando se activa la caché y se produce una migración, el valor de Pct Util permanece igual porque los datos migrados continúan en el volumen como datos en caché. El valor de Pct Util sólo disminuye cuando los datos en caché caducan o cuando el espacio que ocupan los archivos en caché debe utilizarse para archivos que no están en caché.

Para Centera, esto representa un cálculo del uso de todo el dispositivo de almacenamiento Centera completo, no el espacio de la agrupación de almacenamiento que se está consultando.

#### Pct Migr (sólo agrupaciones de almacenamiento primario)

Un cálculo del porcentaje de los datos de la agrupación de almacenamiento que se pueden migrar. El servidor utiliza este valor y el de los umbrales superior e inferior de migración para determinar cuándo debe iniciarse y pararse la migración.

Para dispositivos de disco de acceso aleatorio, este valor se especifica como un porcentaje del valor de la capacidad estimada, excluidos los datos en caché, pero incluidos los datos de todos los volúmenes desactivados.

Para dispositivos de disco de acceso secuencial, este valor se especifica como un porcentaje del valor de la capacidad estimada. Este valor incluye la capacidad de todos los volúmenes reutilizables que se han especificado para la agrupación. Para otros tipos de dispositivos de acceso secuencial, este valor se especifica como el porcentaje del número total de volúmenes de la agrupación de almacenamiento que contienen como mínimo un byte de datos activos. El número total de volúmenes incluye el número máximo de volúmenes reutilizables.

El valor de Pct Util incluye los datos en caché de un volumen; el valor de Pct Migr excluye los datos en caché. Por lo tanto, cuando se activa la caché y se produce una migración, el valor de Pct Migr disminuye pero el valor de Pct Util permanece igual porque los datos migrados permanecen en el volumen como datos en caché. El valor de Pct Util sólo disminuye cuando los datos en caché caducan o cuando el espacio que ocupan los archivos en caché debe utilizarse para archivos que no están en caché.

#### Pct. lógico

La ocupación lógica de la agrupación de almacenamiento como un porcentaje de la ocupación total. La ocupación lógica es el espacio que ocupan los archivos de cliente que podrían formar parte o no de una agregación de archivos. Un valor de Pct Lógico menor al 100% indica que hay espacio libre en los agregados de archivos de la agrupación de almacenamiento.

#### Pct. migr alto (sólo agrupaciones de almacenamiento primario)

El umbral superior de migración, que especifica cuándo puede el servidor empezar la migración de la agrupación de almacenamiento. El servidor empieza los procesos de migración cuando la utilización de la capacidad alcanza este umbral.

Pct. migr bajo (sólo agrupaciones de almacenamiento primario)  
El umbral inferior de migración, que especifica cuándo puede el servidor terminar la migración de la agrupación de almacenamiento. El servidor detiene los procesos de migración cuando la utilización de la capacidad alcanza este umbral.

Retardo de migración (sólo agrupaciones de almacenamiento primario)  
El número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el servidor pueda migrar el archivo a la siguiente agrupación de almacenamiento. Para una agrupación de almacenamiento de disco, los días se cuentan a partir del momento en que el archivo se ha almacenado en la agrupación de almacenamiento o un cliente lo ha recuperado por última vez. Para una agrupación de almacenamiento de acceso secuencial, los días se cuentan a partir del momento en que el archivo se ha almacenado en la agrupación de almacenamiento.

Continuar migración (sólo agrupaciones de almacenamiento primario)  
Si el servidor continúa migrando archivos a la siguiente agrupación de almacenamiento aunque los archivos no hayan estado en la agrupación el número de días que especifica el retardo de migración.

Procesos migración  
El número de procesos paralelos que se utilizan para migrar archivos desde una agrupación de almacenamiento principal aleatoria o secuencial.

Procesos de reclamación  
Número de procesos paralelos utilizados para reclamar los volúmenes de una agrupación de almacenamiento de copia o principal de acceso secuencial.

Siguiente agrupación de almacenamiento (sólo agrupaciones de almacenamiento primario)  
La agrupación de almacenamiento que es el destino de los datos que se migran desde esta agrupación de almacenamiento.

Agrupación de almacenamiento de reclamación (sólo agrupaciones de almacenamiento primario de acceso secuencial)  
Si se especifica, la agrupación de almacenamiento que es el destino de los datos que se traspasan de los volúmenes durante el proceso de reclamación. Si no se especifica ninguna agrupación, de forma predeterminada, el proceso de reclamación sólo traspasa datos entre los volúmenes de la misma agrupación de almacenamiento.

Umbral de tamaño máximo (sólo agrupaciones de almacenamiento primario)  
Tamaño máximo de los archivos que se pueden almacenar en la agrupación de almacenamiento.

Acceso  
La modalidad de acceso a los datos de la agrupación de almacenamiento. Son posibles las modalidades de acceso siguientes:

Lectura/ Grabación  
Puede accederse a los datos en modalidad de lectura-grabación.

Sólo lectura  
Puede accederse a los datos en modalidad de sólo lectura.

Convirtiendo  
La agrupación de almacenamiento se está convirtiendo en una agrupación de almacenamiento de contenedores de directorio.

Conversión detenida  
El proceso de conversión de la agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio se ha detenido.

Limpieza de conversión necesaria  
Para convertir satisfactoriamente la agrupación de almacenamiento, debe limpiarla. La conversión no ha podido completarse porque hay datos dañados. Emita el mandato QUERY CLEANUP para identificar los archivos dañados.

Convertido  
La agrupación de almacenamiento se ha convertido en una agrupación de almacenamiento de contenedores de directorio.

Descripción  
La descripción de la agrupación de almacenamiento.

Ubicación de desbordamiento (sólo agrupaciones de almacenamiento de acceso secuencial)  
La ubicación donde se almacenan los volúmenes de la agrupación de almacenamiento cuando se expulsan de una biblioteca automatizada con el mandato MOVE MEDIA.

¿Archivos migrados en caché? (sólo agrupaciones de almacenamiento de acceso aleatorio)  
Si está activada la función de caché para los archivos migrados a la siguiente agrupación de almacenamiento.

¿Función proximidad? (sólo agrupaciones de almacenamiento de acceso secuencial)  
Si está desactivada o activada la función de proximidad. Si la función de proximidad está desactivada, el valor de este campo es No. Si la función de proximidad está activada, los valores posibles son Group, Node y Filespace.

Umbral de reclamación (sólo agrupaciones de almacenamiento de acceso secuencial)  
El umbral que determina cuándo se reclaman los volúmenes de una agrupación de almacenamiento. El servidor compara con este valor el porcentaje de espacio reclamable que hay en un volumen para determinar si es necesaria la operación de reclamación.

Límite de reclamación fuera del local  
El número de volúmenes fuera del local que tienen espacio que se reclama durante la reclamación de esta agrupación de almacenamiento. Este campo se aplica sólo cuando POOLTYPE=COPY.

Máximo de volúmenes reutilizables permitidos (sólo almacenamientos de acceso secuencial)



El número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento.

Número de volúmenes reutilizables utilizados (sólo agrupaciones de almacenamiento de acceso secuencial)

El número de volúmenes reutilizables utilizados en la agrupación de almacenamiento.

Período de retardo para reutilización de contenedor (sólo agrupaciones de almacenamiento de contenedor)

El número de días que deben transcurrir después de suprimir todos los archivos de un contenedor antes de que el servidor reutilice el contenedor.

¿Migración en curso? (sólo agrupaciones de almacenamiento primario)

Si hay como mínimo un proceso de migración activo para la agrupación de almacenamiento.

Cantidad migrada (MB) (sólo agrupaciones de almacenamiento primario)

La cantidad de datos, en megabytes, que se migran, si la migración está en proceso. Si la migración no está en proceso, este valor indica la cantidad de datos migrados durante la última migración. Cuando se utilizan varios procesos de migración paralelos para la agrupación de almacenamiento, este valor indica la cantidad total de datos que migran todos los procesos.

Tiempo transcurrido en migración (segundos) (sólo agrupaciones de almacenamiento primario)

La cantidad de tiempo que ha transcurrido desde que ha empezado la migración, si la migración está activa. Si la migración no está activa, este valor indica la cantidad de tiempo que se necesita para completar la última migración. Cuando se utilizan varios procesos de migración paralelos para la agrupación de almacenamiento, este valor indica la cantidad total de tiempo desde el inicio del primer proceso hasta la finalización del último proceso.

¿Reclamación en curso? (sólo agrupaciones de almacenamiento de acceso secuencial)

Si hay como mínimo un proceso de reclamación activo para la agrupación de almacenamiento.

Última actualización por (administrador)

El nombre del administrador que está definido o que ha actualizado más recientemente la agrupación de almacenamiento.

Fecha/hora última actualización

La fecha y hora en que el administrador ha definido o actualizado más recientemente la agrupación de almacenamiento.

Formato de datos de agrupación de almacenamiento

Tipo de formato de datos utilizado para grabar datos en esta agrupación de almacenamiento (por ejemplo, NATIVE, NETAPPDUMP, CELERRADUMP o NDMPDUMP).

Agrupaciones de almacenamiento de copia

Las agrupaciones de almacenamiento de copia que se enumeran tienen datos que se graban simultáneamente en las mismas cuando se realiza una copia de seguridad de los datos o se archivan dichos datos en una agrupación de almacenamiento primaria consultada mediante este mandato.

Agrupaciones de datos activos

Las agrupaciones de almacenamiento de datos activos que se enumeran aquí tienen datos que se graban simultáneamente en las mismas cuando se realiza una copia de seguridad de los datos en la agrupación de almacenamiento primaria consultada mediante este mandato.

¿Continuar la copia en caso de error?

Indica si un servidor debe continuar grabando datos en otras agrupaciones de almacenamiento de copia de la lista o debe finalizar la transacción por completo cuando se produce un fallo en una de las agrupaciones de copia de la lista. Este campo se aplica únicamente a agrupaciones de almacenamiento de acceso aleatorio y de acceso secuencial primarias.

Datos CRC

Especifica si los datos se validan mediante la comprobación de redundancia cíclica (CRC) cuando se transfieren los datos durante el almacenamiento o la recuperación de datos en un dispositivo.

Tipo de reclamación

Si los volúmenes están reclamado por el umbral o por la fecha de retención de SnapLock.

Grabar sobre datos cuando se supriman

Número de veces que los datos se sobrescriben físicamente después de haberse suprimido de la base de datos.

¿Eliminar duplicados de datos?

Si han de eliminarse o no los datos duplicados de la agrupación de almacenamiento.

Procesos para identificar duplicados

Número de procesos de identificación de duplicados especificado como valor predeterminado para la agrupación de almacenamiento. El número de procesos de identificación de duplicados especificado en este campo podría no ser igual al número de procesos de identificación de duplicados que están en ejecución.

Comprimido

Indica si la agrupación de almacenamiento está comprimida.

Espacio adicional para datos protegidos

La cantidad de espacio, en MB, que se utiliza para proteger datos de los servidores remotos. Se trata de la cantidad total de espacio utilizado para los datos recibidos de otros servidores como resultado de ejecutar el mandato PROTECT STGPOOL.

Espacio no utilizado total pendiente

La cantidad de espacio que está planificado para que vuelva a estar disponible en una agrupación de almacenamiento de contenedor de directorio. El espacio lo ocupan las extensiones con datos eliminados que se suprimirán de la agrupación de almacenamiento cuando caduque el periodo de tiempo especificado mediante el parámetro REUSEDELAY en el mandato DEFINE STGPOOL.

Ahorro de deduplicación

La cantidad y el porcentaje de datos que se conseguido ahorrar en la agrupación de almacenamiento mediante la deduplicación de datos.

#### Ahorro de compresión

La cantidad de datos que se ha ahorrado en la agrupación de almacenamiento mediante la compresión.

#### Espacio total ahorrado

La cantidad total de datos que se ha ahorrado en la agrupación de almacenamiento.

#### Modalidad de copia automática

Indica si los datos se graban de forma simultánea en agrupaciones de almacenamiento de copia o de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor, los procesos de migración de datos del servidor o las tres operaciones. El valor CLIENT indica operaciones de almacenamiento del cliente o de importación del servidor. El valor ALL indica que la grabación simultánea se produce cuando esta agrupación es el destino de cualquiera de las operaciones elegibles.

Si la agrupación de almacenamiento es una agrupación de almacenamiento de copia o una agrupación de datos activos o si la función de grabación simultánea está inhabilitada, este campo está vacío.

#### ¿Contiene eliminaciones de datos duplicados por clientes?

Indica si la agrupación de almacenamiento contiene datos cuyos duplicados han eliminado los clientes. Los agentes de almacenamiento V6.1 o anteriores no pueden acceder a las agrupaciones de almacenamiento que contienen eliminaciones de datos realizadas por los clientes para el traspaso de datos fuera de la LAN.

Consejo: Este campo está en blanco para agrupaciones de almacenamiento de contenedor. No puede utilizar las agrupaciones de almacenamiento de contenedores para el movimiento de datos sin LAN.

#### Máximo de grabadores simultáneos

El número máximo de E/S que pueden ejecutarse simultáneamente en la agrupación de almacenamiento.

#### Procesos de protección

El conjunto de procesos de protección.

#### Agrupación de almacenamiento de protección

El nombre de la agrupación de almacenamiento de contenedores donde se protegen los datos en el servidor de réplica de destino.

#### Protección de agrupaciones de almacenamiento local

Indica si las agrupaciones de almacenamiento local están protegidas.

#### Límite del volumen de reclamación

En el caso de agrupaciones de almacenamiento de copia de contenedor, indica el número máximo de volúmenes que reclama el servidor durante la protección de la agrupación de almacenamiento.

#### Fecha de última protección de la agrupación remota

La fecha en que se protegió por última vez la agrupación de almacenamiento en una agrupación de almacenamiento de un servidor remoto.

#### Fecha de última protección en agrupación local

La fecha en que se protegió por última vez la agrupación de almacenamiento en una agrupación de almacenamiento de un servidor local.

#### ¿Necesita una copia de seguridad para eliminar los archivos duplicados?

Indica si debe realizarse una copia de seguridad de la agrupación de almacenamiento secuencial si la agrupación de almacenamiento contiene datos con duplicados eliminados.

#### Cifrado

Para las agrupaciones de contenedores de directorio o de almacenamiento en la nube, indica si los datos de cliente se cifran antes de que se graben en la agrupación de almacenamiento.

#### Pct cifrado

El porcentaje de datos de cliente deduplicados que se han cifrado en la agrupación de almacenamiento en la nube de contenedores de directorio o de contenedor en la nube.

#### Espacio de nube utilizado (MB)

Para las agrupaciones de almacenamiento de nube, esto es el espacio utilizado por la agrupación, expresado en megabytes.

#### Nombre de grupo

En el caso de agrupaciones de almacenamiento en la nube que utilizan Simple Storage Service (S3), el nombre que IBM Spectrum Protect asigna al grupo de S3 o la caja fuerte de IBM® Cloud Object Storage. Este valor también puede ser el nombre que ha asignado al grupo utilizando el parámetro BUCKETNAME en el mandato DEFINE STGPOOL o en el mandato UPDATE STGPOOL.

#### Capacidad estimada local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, la capacidad estimada de almacenamiento local en megabytes (M) o gigabytes (G).

#### Pct. util local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, una estimación del uso del componente de almacenamiento local de la agrupación de almacenamiento en la nube, como un porcentaje.




#### Pct. lógico local

En las agrupaciones de almacenamiento en la nube que utilizan el almacenamiento local, la ocupación lógica de la agrupación de almacenamiento en la nube como un porcentaje del total de la ocupación. La ocupación lógica es el espacio que ocupan los archivos de cliente que podrían formar parte o no de una agregación de archivos. Un valor de Pct Lógico local menor que un 100% indica que hay espacio libre en los agregados de la agrupación de almacenamiento.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY STGPOOL

Comando	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## QUERY STGPOOLDIRECTORY (Consulta de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para visualizar información acerca de uno o varios directorios de agrupaciones de almacenamiento.

### Clase de privilegio

Cualquier administrador puede emitir este mandato.

### Sintaxis

```
>>-Query STGPOOLDIRECTORY .-*-----+----->
                          +-----+----->
                          '-directorio-'

>--+-----+----->
  '-STGpool----nombre_agrupación-'

  .-ACCESS----Any----- .
>--+-----+----->
  '-ACCESS----+READWrite---+
                    +-READOnly----+
                    +-DESTROYED---+
                    +-Any-----+
                    '-UNAVAILABLE-'

  .-Format----Standard---- .
>--+-----+-----><
  '-Format----+Standard-+-'
                    '-Detailed-'
```

## Parámetros

---

### directorio

Especifica el directorio de agrupaciones de almacenamiento que se consulta. Este parámetro es opcional.

\*

Especifica que un asterisco (\*) representa un carácter comodín. Utilice los caracteres comodín como, por ejemplo, un asterisco para que coincida con cualquier carácter. De forma alternativa, puede utilizar un signo de interrogación (?) o un signo de porcentaje (%) para hacer coincidir con exactitud un carácter. Este es el valor predeterminado.

### directorio

Especifica el directorio de la agrupación de almacenamiento. Si no especifica un valor para este parámetro, se visualizarán todos los directorios de agrupaciones de almacenamiento. La longitud máxima del directorio de la agrupación de almacenamiento es de 1024.

### STGpool

Especifica el nombre de la agrupación de almacenamiento que se va a consultar. Si no especifica un valor para este parámetro, se visualizarán todos los directorios de agrupaciones de almacenamiento. La longitud máxima del nombre de la agrupación de almacenamiento es de 30. Este parámetro es opcional.

### ACcEss

Especifica que la salida está restringida por la modalidad de acceso de directorio. Este parámetro es opcional. Especifique uno de los siguientes valores:

#### READWrite

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `READWRITE`.

#### READOnly

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `READONLY`.

#### DESTroyed

Visualizar todos los directorios de agrupaciones de almacenamiento con una modalidad de acceso `DESTROYED`. Los directorios se han designado como dañados permanentemente en el directorio de la agrupación de almacenamiento.

#### Any

Visualizar todos los directorios de agrupación de almacenamiento. Este es el valor predeterminado.

#### UNAVailable

Visualizar directorios con una modalidad de acceso `UNAVAILABLE`.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es `STANDARD`. Puede especificar uno de los siguientes valores:

#### Standard

Especifica que se visualizará información parcial.

#### Detailed

Especifica que se visualizará toda la información.

## Ejemplo: Visualización de información de resumen acerca de un directorio específico de agrupaciones de almacenamiento

---

Visualice información del directorio de agrupaciones de almacenamiento denominado `DPOOL`. Consulte Descripciones de los campos para obtener las descripciones de los campos.

```
query stgpooldirectory C:\data
```

Storage	Directory	Access
Pool Name		
-----	-----	-----
DPOOL	C:\data	Read/Write

## Ejemplo: Visualización de información detallada del directorio de agrupaciones de almacenamiento


---

Visualizar detalles del directorio de agrupaciones de almacenamiento denominado `DPOOL`.

```
query stgpooldirectory stgpool=dpool format=detailed
```

 Sistemas operativos AIX  Sistemas operativos Linux

Nombre agrupación almacenamiento: DPOOL  
 Directorio: /storage/sampleDir  
 Acceso: Lectura/Grabación  
 Espacio libre (MB): 323,170  
 Total espacio (MB): 476,938  
 Sistema de archivos: /storage  
 Vía de acceso absoluta: /storage/data

 Sistemas operativos Windows

Nombre agrupación almacenamiento: DPOOL  
 Directorio: /storage2/sampleDir  
 Acceso: Lectura/Grabación  
 Espacio libre (MB): 323,170  
 Total espacio (MB): 476,938  
 Sistema de archivos: /storage  
 Vía de acceso absoluta: /storage2/sampleDir

## Descripciones de los campos

**Nombre de la agrupación de almacenamiento**

El nombre de la agrupación de almacenamiento.

**Directorio**

El nombre del directorio de la agrupación de almacenamiento.

**Acceso**

La modalidad de acceso de los datos en el directorio de la agrupación de almacenamiento.

**Espacio libre (MB)**

La cantidad de espacio en el directorio de agrupaciones de almacenamiento, en megabytes, que no se utiliza.

**Espacio total (MB)**

La cantidad total de espacio en el directorio de agrupaciones de almacenamiento, en megabytes.










**Sistema de archivos**

El nombre del sistema de archivos donde se halla el directorio de agrupaciones de almacenamiento.

**Vía de acceso absoluta**

El nombre de la vía de acceso absoluta donde se halla el directorio de agrupaciones de almacenamiento. El nombre de la vía de acceso absoluta contiene el nombre del directorio raíz y todos los subdirectorios en el nombre de la vía de acceso. Todos los enlaces simbólicos se resuelven en el nombre de vía de acceso absoluta.

Tabla 1. Mandatos relacionados con QUERY STGPOOLDIRECTORY

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.

## QUERY SUBSCRIBER (Visualizar información de suscriptor)

Utilice este mandato en un gestor de configuración para visualizar información sobre los suscriptores y sus inscripciones en perfiles.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

      .-*-----*
>>-Query SUBSCRIBer--+-----+----->
      '-nombre_servidor-'

.-PROFIle-----*-----*
>--+-----+-----<
      '-PROFIle-----nombre_perfil-'

```

## Parámetros

### nombre\_servidor

Especifica el nombre de un servidor gestionado para el que se visualiza la información de inscripción. Puede utilizar caracteres comodín para especificar varios nombres de servidores. Este parámetro es opcional. El valor predeterminado son todos los servidores gestionados.

### PROFIle

Especifica un nombre de perfil para el que se visualiza la información. Puede utilizar caracteres comodín para especificar varios nombres de perfiles. Este parámetro es opcional. El valor predeterminado son todos los perfiles.

## Ejemplo: obtener una lista de las suscripciones de perfil de un gestor de configuración

Visualizar la información de los suscriptores de todas las inscripciones en perfiles para este gestor de configuración. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query subscriber
```

Suscriptor	Nombre perfil	¿Actual?	Última actualización actualización
SERVER2	DEFAULT_PROFILE	Sí	Jue, 14 Mayo 1998 01:14:42 PM
SERVER2	SETUP	Sí	Jue, 14 Mayo 1998 01:14:42 PM

## Descripciones de los campos

### Suscriptor

El nombre del suscriptor (servidor gestionado).

### Nombre de perfil

El nombre del perfil.

### ¿Es actual?

Si la inscripción se ha renovado con la información actual asociada al perfil. Los valores posibles son:

Sí

El servidor gestionado es actual.

No

El servidor gestionado no es actual. Si este campo tiene el valor NO una vez renovado el perfil, compruebe si en los mensajes del servidor hay condiciones de error que puedan ocasionar que no se haya ejecutado la renovación.

Desconocido

El servidor gestionado tiene una versión más reciente del perfil que el gestor de configuración, o bien, el perfil ya no existe en el gestor de configuración, pero la inscripción sigue estando asociada al perfil.

### Fecha/hora última actualización

Especifica la fecha y la hora en que se ha distribuido correctamente al suscriptor la información de configuración para la inscripción.

## Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY SUBSCRIBER

Comando	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.

Comando	Descripción
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
QUERY SUBSCRIPTION	Muestra información sobre suscripciones a perfiles.

## QUERY SUBSCRIPTION (Visualizar información de inscripción)

Utilice este comando en un servidor gestionado para visualizar la información de suscripción de un perfil.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query SUBSCRIPTION--.*-----+-----<<
                        +-----+-----<<
                        '-nombre_perfil-'
```

### Parámetros

nombre\_perfil

Especifica el nombre del perfil sobre el que se visualiza información de inscripciones. Puede utilizar caracteres comodín para especificar varios nombres. Este parámetro es opcional. El valor predeterminado son todos los perfiles.

### Ejemplo: visualizar información de descripción

Visualizar la información de inscripción de todos los perfiles.

```
query subscription
```

Gestor configuración	Nombre perfil	Fecha/hora últ. act.
-----	-----	-----
SERVER1	ADMIN_INFO	Jue, 14 Mayo 1998 01:35:13 PM
SERVER1	DEFAULT_PROFILE	Jue, 14 Mayo 1998 01:35:13 PM
SERVER1	EMPLOYEE	Jue, 14 Mayo 1998 01:35:13 PM

### Descripciones de los campos

Gestor de configuración

El nombre del gestor de configuración.

Nombre de perfil

El nombre del perfil.

Fecha/hora última actualización

El momento en que se ha distribuido correctamente la información de configuración más reciente al suscriptor.

### Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SUBSCRIPTION

Comando	Descripción
DEFINE SUBSCRIPTION	Suscribe un servidor gestionado a un perfil.
DELETE SUBSCRIBER	Suprime las inscripciones obsoletas de un servidor gestionado.
DELETE SUBSCRIPTION	Suprime una suscripción de perfil especificada.

Comando	Descripción
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
QUERY SUBSCRIBER	Muestra información sobre los suscriptores y sus suscripciones a perfiles.

## QUERY SYSTEM (Consultar la configuración y la capacidad de configuración)

Utilice este comando para obtener información consolidada acerca de la configuración y la capacidad del servidor.

Este mandato consolida la salida de sentencias select, mandatos SHOW, y otros mandatos de IBM Spectrum Protect. La salida se genera desde varios mandatos de IBM Spectrum Protect, por ejemplo:

- QUERY ASSOCIATION
- QUERY COPYGROUP
- QUERY DATAMOVER
- QUERY DB
- QUERY DBSPACE
- QUERY DEVCLASS
- QUERY DIRSPACE
- QUERY DOMAIN
- QUERY LIBRARY
- QUERY LOG
- QUERY MGMTCLASS
- QUERY OPTION
- QUERY PROCESS
- QUERY REPLRULE
- QUERY SCHEDULE
- QUERY SERVER
- QUERY SESSION
- QUERY STATUS
- QUERY STGPOOL
- QUERY VOLHISTORY
- QUERY VOLUME

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query SYStem-----<<
```

### Ejemplo: visualizar información consolidada del sistema

Emita el comando QUERY SYSTEM para obtener información consolidada acerca del sistema. Para obtener ejemplos de salidas de estos comandos de consulta, consulte los comandos individuales.

```
query system
```

### Comandos relacionados

Tabla 1. Comandos relacionados con QUERY SYSTEM

Comando	Descripción
QUERY ASSOCIATION	Visualiza los clientes asociados a una o más planificaciones.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DB	Visualiza información de asignación acerca de la base de datos.



Comando	Descripción
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY LOG	Visualiza información acerca de las anotaciones de recuperación.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.

## QUERY TAPEALERTMSG (Visualizar estado del comando SET TAPEALERTMSG)

Utilice este comando para visualizar el estado del comando SET TAPEALERTMSG. Puede activar o desactivar las alertas de cinta. Si se activan, IBM Spectrum Protect puede recuperar información de diagnóstico de un dispositivo de cinta o biblioteca y visualizarla mediante mensajes ANR. Si se desactivan, IBM Spectrum Protect no consultará ningún dispositivo para obtener esta información.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-Query TAPEAlertmsg-----<<
```

### Ejemplo: visualizar el estado del comando QUERY TAPEALERTMSG

Utilizar el comando QUERY TAPEALERTMSG para determinar si deben recuperarse las alertas de cinta de los dispositivos y visualizarse en forma de mensajes ANR.

```
query tapealertmsg
```

```
ANR2017I El administrador SERVER_CONSOLE
emitió el comando:
QUERY TAPEALERTMSG
ANR8960I QUERY TAPEALERTMSG: la visualización de alertas de cinta de
dispositivos SCSI
está Activada.
```

### Comandos relacionados

Tabla 1. Comandos relacionados con QUERY TAPEALERTMSG

Comando	Descripción
---------	-------------

Comando	Descripción
SET TAPEALERTMSG	Especifica si los dispositivos de cinta y biblioteca reportan la información de diagnóstico al servidor.

## QUERY TOC (Visualizar tabla de contenido para una imagen de copia de seguridad)

Utilice este mandato para visualizar la información sobre los directorios y archivos que contiene la tabla de contenido (TOC) para una imagen de copia de seguridad especificada. Este mandato no carga la información de la tabla de contenido en la base de datos de IBM Spectrum Protect. La tabla de contenido especificada se lee desde una agrupación de almacenamiento cada vez que se emita el mandato QUERY TOC.

Este comando no se puede emitir desde la consola del servidor. Si la tabla de contenido está almacenada en un medio extraíble, se necesita un punto de montaje y la salida se retardará mientras se monte el volumen de agrupación de almacenamiento.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de política para el dominio al que está asignado el nodo o autorización de propietario de cliente en el nodo.

### Sintaxis

```
>>-Query TOC--nombre_nodo--nombre_espacioarchivos----->
>--+-----+----->
  '-CREATIONDate---- fecha--CREATIONTime---- hora-'
.-Format----Standard----.
>--+-----+-----<
  '-Format---+-Standard-+-'
    '-Detailed-'
```

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo NAS al que pertenece la tabla de contenido (TOC). No puede utilizar caracteres comodín para especificar este nombre.

nombre\_espacio\_archivos (Obligatorio)

Especifica el nombre del espacio de archivos al que pertenece la tabla de contenido. El nombre de espacio de archivos especificado no puede contener caracteres comodín.

CREATIONDate

Especifica la fecha de creación de la imagen de copia de seguridad para la que debe visualizarse la tabla de contenido. Este parámetro es opcional. Si especifica CREATIONDATE, también debe especificar CREATIONTIME. Si no especifica estos parámetros, se mostrará el contenido de la imagen de copia de seguridad más reciente para el nodo y el espacio de archivos especificados, siempre que esta imagen tenga una tabla de contenido. Sólo puede especificar la fecha de creación como uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	05/15/2002

Especifica que desea visualizar el contenido de la imagen de copia de seguridad creada en esta fecha. Puede obtener esta fecha de la salida del mandato QUERY NASBACKUP.

CREATIONTime

Especifica la hora de creación de la imagen de copia de seguridad para la que debe visualizarse la tabla de contenido. Este parámetro es opcional. Si especifica CREATIONTIME, también debe especificar CREATIONDATE. Si no especifica estos parámetros, se mostrará el contenido de la imagen de copia de seguridad más reciente para el nodo y el espacio de archivos especificados, siempre que esta imagen tenga una tabla de contenido. Sólo puede especificar la hora de creación como uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha de creación especificada	10:30:08

Especifica que desea visualizar el contenido de la imagen de copia de seguridad creada a esta hora para la fecha especificada. Puede obtener esta hora en la salida del mandato QUERY NASBACKUP.

#### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial para los archivos.

#### Detailed

Especifica que se visualizará información completa para los archivos, incluida la representación hexadecimal de cada nombre de archivo o directorio.

## Ejemplo: visualizar información de tabla de contenido detallada para un nodo específico

Utilice el mandato QUERY TOC para visualizar la información de la tabla de contenido que pertenece al nodo NAS NETAPP del espacio de archivos /vol/vol1 creado el 12/06/2002 a las 11:22:46. Especificar un formato detallado.

```
query toc netapp /vol/vol1 creationdate=12/06/2002 creationtime=11:22:46
format=detailed
```

Objetos en la imagen de la que se ha realizado una copia el 12/06/2002 a las 11:22:46 para el espacio de archivos /vol/vol1 en el nodo NETAPP:

```
Nombre de objeto: /.etc
Nombre de objeto hexadecimal: 2f657463
Tipo objeto: Directorio
Tamaño objeto: 4.096
Fecha/hora de última modificación de datos: 07/31/2002 14:21:19

Nombre de objeto: /.etc/oldmaps/ndmp
Nombre de objeto hexadecimal: 2f6574632f6f6c646d6170
732f6e646d70
Tipo objeto: Directorio
Tamaño objeto: 4.096
Fecha/hora de última modificación de datos: 07/31/2002 14:21:19

Nombre de objeto: /.etc/oldmaps/ndmp/
TSM
/vol/vol1/3df0e8fd
Nombre de objeto hexadecimal: 2f6574632f6f6c646d6170
732f6e646d702f54534d2
02f766f6c2f766f6c312f3
364663065386664
Tipo de objeto: Archivo
Tamaño de objeto: 36,864
Fecha/hora de última modificación de datos: 12/06/2002 11:14:22
```

## Descripciones de los campos

Nombre de objeto

Nombre del objeto.

Nombre de objeto hexadecimal

Nombre del objeto en formato hexadecimal.

Tipo de objeto

Tipo de objeto.

Tamaño de objeto

Tamaño del objeto.

Fecha/hora de última modificación de datos

Fecha y hora de la última modificación del objeto.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY TOC

Comando	Descripción
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).

Comando	Descripción
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
RESTORE NODE	Restaura un nodo de almacenamiento conectado a red (NAS).

## QUERY VIRTUALFSMAPPING (Consultar una correlación de espacios de archivos virtuales)

Utilice este mandato para consultar una definición de correlación de espacios de archivos virtuales.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-Query VIRTUALFSmapping ----->
      .-*-----
>--+-----+-----<
  |          .-*-----|
  |'-nombre_nodo-----+'
  |          '-nombre_espacio_archivos_virtual-'
```

### Parámetros

#### nombre\_nodo

Especifica el nodo de cliente al que pertenece el espacio de archivos virtual. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. El valor predeterminado es especificar todos los nombres de nodo. Debe especificar un valor para este parámetro si especifica un nombre de espacio de archivos virtual.

#### nombre\_espacio\_archivos\_virtual

Especifica el nombre de las correlaciones de espacios de archivos virtuales que consultará. Puede utilizar caracteres comodín para especificar este nombre. Este parámetro es opcional. Si no especifica ningún valor, se consultan todas las correlaciones de espacios de archivos virtuales. Los nombres de correlaciones de espacios de archivos virtuales son sensibles a las mayúsculas/minúsculas. Utilice el comando QUERY VIRTUALFSMAPPING para determinar el uso correcto de mayúsculas/minúsculas para la correlación de espacios de archivos virtuales que va a consultarse.

### Ejemplo: visualizar los espacios de archivos virtuales para un nodo específico

Visualizar los espacios de archivos virtuales definidos actualmente para el nodo NAS1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query virtualfsmapping nas1
```

Nombre nodo	Nombre correlación de espacios de archivos virtuales	Nombre espacio archivos	Ruta	¿Ruta hexadecimal?
NAS1	/mikesdir	/vol/vol2	/mikes	No
NAS1	/tmpdir	/vol/vol1	/tmp	No
NAS1	/nonASCIIDir	/vol/vol3	2f73657276657231	Sí

### Descripciones de los campos

#### Node Name

Especifica el nombre del nodo cliente.

#### Virtual Filespace Mapping Name

Especifica el nombre de la correlación de espacios de archivos virtuales.

#### Filespace Name

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

Ruta

Especifica la ruta al nodo de cliente.

Hexadecimal Path

Indica si la ruta es hexadecimal.

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY VIRTUALFSMAPPING

Comando	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
UPDATE VIRTUALFSMAPPING	Actualiza una correlación de espacios de archivos virtuales.

## QUERY VOLHISTORY (Visualizar información histórica de volúmenes secuenciales)

Utilice este mandato para visualizar la información histórica de volúmenes secuenciales. Para guardar la información histórica de volúmenes secuenciales en uno o varios archivos, utilice el comando BACKUP VOLHISTORY.

Utilice la opción de servidor VOLUMEHISTORY para especificar uno o varios archivos históricos de volúmenes. Una vez reiniciado el servidor, IBM Spectrum Protect actualiza la información de volúmenes en la base de datos y en los archivos.

Utilice el mandato QUERY BACKUPSET para consultar la información correspondiente al conjunto de copias de seguridad especificado.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```

      .-BEGINDate-----fecha_anterior-.
>>-Query VOLHistory-+-----+----->
      '-BEGINDate-----fecha-----'

      .-ENDDate-----fecha_actual-.  .-BEGINTime-----00:00:00-.
>-+-----+-----+-----+----->
      '-ENDDate-----fecha-----'  '-BEGINTime-----hora-----'

      .-ENDTime-----hora_actual-.  .-Type-----All----->
>-+-----+-----+-----+-----<
      '-ENDTime-----hora-----'  '-Type-----+All-----+'
                                     +-BACKUPSET---+
                                     +-DBBackup----+
                                     +-DBRpf-----+
                                     +-DBSnapshot--+
                                     +-EXPort-----+
                                     | (1) |
                                     +-REMOte-----+
                                     +-RPFile-----+
                                     +-RPFSnapshot-+
                                     +-STGDelete---+

```

Notas:

1. Este parámetro sólo está disponible en sistemas operativos AIX, HP-UX, Linux, Solaris y Windows.

## Parámetros

### BEGINDate

Especifica que desea visualizar la información empezando por los registros creados en la fecha especificada. Este parámetro es opcional. El valor predeterminado es la fecha más antigua en la que existe información histórica.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados	TODAY-7 o -7.  Para visualizar la información empezando por los registros creados hace una semana, especifique BEGINDATE=TODAY-7 o BEGINDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

### ENDDate

Especifica que desea visualizar la información acabando por los registros creados en la fecha especificada. Este parámetro es opcional. El valor predeterminado es la fecha actual.

Para especificar la fecha utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY-días o -días	La fecha actual menos los días especificados. El número máximo de días es 9999.	TODAY-1 o -1.  Para visualizar los registros creados hasta ayer, especifique ENDDATE=TODAY-1 o ENDDATE=-1.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

### BEGINTime

Especifica que desea visualizar la información empezando por los registros creados a la hora especificada. Este parámetro es opcional. El valor predeterminado es medianoche (00:00:00).

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha inicial especificada	12:33:28
NOW	La hora actual en la fecha inicial especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha inicial especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 con BEGINTIME=NOW+03:00 o BEGINTIME=+03:00, IBM Spectrum Protect visualizará los registros que tengan la hora 12:00:00 o posterior, en la fecha inicial especificada.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30.  Si emite este comando a las 9:00 con BEGINTIME=NOW-03:30 o BEGINTIME=-03:30, IBM Spectrum Protect visualizará los registros que tengan la hora 5:30 o posterior en la fecha inicial.

#### ENDTime

Especifica que desea visualizar la información acabando por los registros creados a la hora especificada en la fecha final. Este parámetro es opcional. El valor predeterminado es la hora actual.

Para especificar la hora utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha final especificada	10:30:08
NOW	La hora actual en la fecha final especificada	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+03:00 o +03:00.  Si emite este comando a las 9:00 con ENDTIME=NOW+03:00 o ENDTIME=+03:00, IBM Spectrum Protect visualizará los registros que tengan la hora 12:00 o posterior, en la fecha final.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-03:30 o -03:30  Si emite este comando a las 9:00 con ENDTIME=NOW-3:30 o ENDTIME=-3:30, IBM Spectrum Protect visualizará los registros que tengan la hora 5:30 o anterior, en la fecha final.

#### Type

Especifica el tipo de registros a visualizar del archivo histórico de volúmenes. Este parámetro es opcional. El valor predeterminado es ALL. Los valores posibles son:

##### All

Especifica todos los registros.

##### BACKUPSET

Especifica que se visualizará sólo la información sobre los volúmenes de juego de copias de seguridad.

##### DBBackup

Especifica que sólo se visualizarán los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos, es decir, los tipos de volumen BACKUPFULL y BACKUPINCR.

##### DBRpf

Especifica que sólo se visualizarán los registros que contienen información sobre los volúmenes de copia de seguridad completa e incremental de la base de datos y los volúmenes de objetos del archivo del plan de recuperación (los tipos de volúmenes BACKUPFULL, BACKUPINCR y RPFIL).

##### DBSnapshot

Especifica que se visualizarán sólo los registros que contienen información sobre los volúmenes utilizados para las copias de seguridad de instantánea de base de datos.

##### EXPort

Especifica sólo los registros que contienen información sobre los volúmenes de exportación.

##### REMOte

Especifica que sólo se visualizarán los registros que contienen información acerca de los volúmenes que los clientes de biblioteca han utilizado.

#### RPFile

Especifica que sólo se muestren los registros que contienen información sobre los objetos de archivos de un plan de recuperación que están guardados en un servidor de destino y que se han creado presuponiendo copias de seguridad de base de datos completas e incrementales. El parámetro muestra sólo los registros de los archivos de plan de recuperación que se han guardado en otro servidor IBM Spectrum Protect utilizando la función de volumen virtual de servidor a servidor para IBM Spectrum Protect.

#### RPFSnapshot

Especifica que sólo se muestren los registros que contienen información sobre los objetos de archivos de un plan de recuperación que están guardados en un servidor de destino y que se han creado suponiendo copias de seguridad de instantánea de base de datos. RPFSnapshot sólo visualiza registros acerca de archivos de plan de recuperación que se han guardado en otro servidor IBM Spectrum Protect utilizando la función de volumen virtual de servidor a servidor para IBM Spectrum Protect.

#### STGDelete

Especifica sólo los registros que contienen información sobre los volúmenes de agrupaciones de almacenamiento secuenciales suprimidos.

#### STGNew

Especifica sólo los registros que contienen información sobre los nuevos volúmenes de almacenamiento de acceso secuencial.

#### STGReuse

Especifica sólo los registros que contienen información sobre los volúmenes de agrupaciones de almacenamiento secuenciales reutilizados.

## Ejemplo: Visualizar información histórica de volúmenes de un volumen de agrupación de almacenamiento

---

Visualizar información histórica de volúmenes de un volumen de agrupación de almacenamiento almacenado en la base de datos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos. Emita el comando:

```
query volhistory type=stgnew
```

```
                Fecha/hora: 02/25/2011 18:28:06
                Tipo volumen: STGNEW
                Serie copia seguridad:
                Operación copia seguridad:
                Sec. volumen:
                Clase dispositivo: FILE
                Nombre volumen: /adsmfct/server/prvoll
                Ubicación volumen:
                Comando:
                ID superior copia de seguridad base de datos:
                ID inferior copia de seguridad base de datos:
                Posición de reposo de copia de seguridad de base de datos:
                HLA copia de seguridad base de datos:
                LLA de copia de seguridad base de datos:
Bytes de datos totales de copia seguridad base de datos (MB):
Bytes de registro totales de copia seguridad base de datos:
Número de bloque superior de copia de seguridad base de datos:
Número de bloque inferior de copia de seguridad base de datos:
                ID de corriente de copia de seguridad de base de
datos:
Secuencia de volumen de copia de seguridad de base de datos para corriente:
```

Nota: El archivo histórico de volúmenes contendrá campos adicionales que no aparecen en la salida de la consulta. Estos campos son específicos del soporte de copia de seguridad y restauración de base de datos. No son para que los utilicen o modifiquen los administradores de IBM Spectrum Protect. Los campos aparecerán entre corchetes con un mensaje que indica que son sólo para uso interno de IBM Spectrum Protect y que no deben ser modificados.

## Ejemplo: la información histórica de volúmenes de visualización para un volumen de copia de seguridad de base de datos

---

Visualizar información histórica de volúmenes de un volumen de copia de seguridad de base de datos almacenado en la base de datos. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos. Emita el comando:

```
query volhistory type=dbb
```

```
                Fecha/hora: 02/25/2011 18:28:06
                Tipo volumen: BACKUPFULL
                Serie copia seguridad: 176
```



```

Operación copia seguridad: 0
  Sec. volumen: 0
  Clase dispositivo: FILE
  Nombre volumen: /adsmfct/server/prv011
  Ubicación volumen:
  Comando:
    ID superior copia de seguridad base de datos: 0
    ID inferior copia de seguridad base de datos: 0
  Posición inicial de copia de seguridad base de datos: 0
  HLA copia de seguridad base de datos:
  LLA de copia de seguridad base de datos:
  Bytes de datos totales de copia seguridad base de datos (MB): 0
  Bytes de registro totales de copia seguridad base de datos (MB): 0
  Número de bloque superior de copia de seguridad base de
datos: 0
  Número de bloque inferior de copia de seguridad base de
datos: 0
  ID de corriente de copia de seguridad de base de datos: 1
  Secuencia de volumen de copia de seguridad de base de datos para
corriente: 10.001

```

Nota: El archivo histórico de volúmenes contendrá campos adicionales que no aparecen en la salida de la consulta. Estos campos son específicos del soporte de copia de seguridad y restauración de base de datos. No son para que los utilicen o modifiquen los administradores de IBM Spectrum Protect. Los campos aparecerán entre corchetes con un mensaje que indica que son sólo para uso interno de IBM Spectrum Protect y que no deben ser modificados.

## Descripciones de los campos

---

### Fecha/Hora

La fecha y la hora de la creación del volumen.

### Volume Type

El tipo del volumen:

#### BACKUPFULL

Volumen de copia de seguridad de base de datos completa.

#### BACKUPINCR

Volumen de copia de seguridad de base de datos incremental.

#### BACKUPSET

Volumen de juego de copias de seguridad de cliente.

#### DBSNAPSHOT

Volumen de copia de seguridad de instantánea de base de datos.

#### EXPORT

Exportar volumen.

#### REMOTE

Volumen que se utiliza en el cliente de biblioteca, que es el servidor de IBM Spectrum Protect que se ha especificado en el campo Ubicación del volumen. Consulte el histórico de volúmenes del servidor que es el cliente de biblioteca para obtener información detallada acerca de cómo se ha utilizado el volumen.

#### RPFIL

Volumen de objeto de archivo del plan de recuperación dándose por supuesto copias de seguridad de base de datos incrementales y completas.

#### RPFSnapshot

Volumen de objeto de archivo del plan de recuperación que se ha creado dándose por supuesto copias de seguridad de instantánea de base de datos.

#### STGDELETE

Volumen de agrupación de almacenamiento de acceso secuencial suprimido.

#### STGNEW

Volumen de agrupación de almacenamiento de acceso secuencial agregado.

#### STGREUSE

Volumen de agrupación de almacenamiento de acceso secuencial reutilizado.

### Backup Series

El valor de este campo depende del tipo de volumen:

- Para los tipos de volumen BACKUPFULL o BACKUPINCR: el identificador de la serie de copia de seguridad.
- Para el tipo de volumen DBSNAPSHOT: el identificador de la serie de copia de seguridad que está asociado a la entrada DBSNAPSHOT.
- Para el tipo de volumen RPFIL: el identificador de la serie de copia de seguridad que está asociado a la entrada RPFIL.

- Para el tipo de volumen RPFSSNAPSHOT: el identificador de la serie de copia de seguridad que está asociado a la entrada RPFSSNAPSHOT.
- En tipos de volumen BACKUPSET este campo está en blanco.
- Para todos los demás tipos de volumen: siempre 0.

Una serie de copia de seguridad es un copia de seguridad completa y todas las copias de seguridad incrementales que se aplican a esa copia de seguridad completa. Otra serie empieza con la siguiente copia de seguridad completa de la base de datos.

#### Backup Operation

Para los tipos de volumen BACKUPFULL o BACKUPINCR: el número de operación de este volumen de copia de seguridad dentro de la serie de copia de seguridad. La copia de seguridad completa en una serie de copia de seguridad es la operación 0. La primera copia de seguridad incremental para dicha copia de seguridad completa es la operación 1, la segunda copia de seguridad incremental es la operación 2, y así sucesivamente.

Para los tipos de volumen DBSNAPSHOT: el número de operación de este volumen DBSNAPSHOT dentro de la serie DBSNAPSHOT.

Para todos los demás tipos de volumen: siempre 0.

Este campo está en blanco cuando el tipo de volumen es BACKUPSET.

#### Volume Seq

La secuencia o posición del volumen dentro de la serie de copia de seguridad.

- Para los tipos de volumen BACKUPFULL o BACKUPINCR: la secuencia, o posición, del volumen dentro de la serie de copia de seguridad. La secuencia de volumen 1 identifica el primer volumen utilizado para la primera operación (una copia de seguridad completa), etc. Por ejemplo, si la copia de seguridad completa ocupa tres volúmenes, estos volúmenes se identifican como la secuencia de volúmenes 1, 2 y 3. El primer volumen de la siguiente operación (la primera copia de seguridad incremental) es la secuencia de volumen 4.
- Para los tipos de volumen BACKUPSET: la secuencia, o posición, del volumen dentro de la serie de BACKUPSET.
- Para los tipos de volumen DBSNAPSHOT: la secuencia, o posición, del volumen dentro de la serie de DBSNAPSHOT. La secuencia de volumen 1 identifica el primer volumen utilizado para la primera operación DBSNAPSHOT, y así sucesivamente.
- Para los tipos de volumen EXPORT: el número de secuencia del volumen al utilizarlo para exportar los datos.
- Para los tipos de volumen RPFSSNAPSHOT: el valor de este campo siempre es uno (1).
- Para todos los demás tipos de volumen: siempre 0.

#### Device Class

El nombre de la clase de dispositivo asociado a este volumen.

#### Volume Name

El nombre del volumen.

#### Volume Location

La ubicación del volumen. Esta información sólo está disponible para los siguientes tipos de volúmenes:

- BACKUPFULL
- BACKUPINCR
- EXPORT
- REMOTE
- RPFSSNAPSHOT

Para el tipo de volumen REMOTE, este campo de ubicación es el nombre de servidor del cliente de biblioteca que es el propietario de este volumen.

Para el tipo de volumen RPFSSNAPSHOT, este campo de ubicación es el nombre de servidor que se ha definido en la definición de clase de dispositivo que el comando PREPARE utiliza cuando se especifica el parámetro DEVCLASS.

#### Comando

Cuando el tipo de volumen es EXPORT o BACKUPSET y el número de secuencia del volumen es 1 (por ejemplo, el primer volumen), este campo muestra el comando que se utilizó para generar el volumen. Si EXPORT o BACKUPSET están presentes en más de un volumen, el comando visualiza el primer volumen, pero no visualiza ninguno de los demás volúmenes.

Para los tipos de volúmenes distintos de EXPORT o BACKUPSET, este campo está en blanco.

Consejo: Los campos siguientes no los utilizan los servidores de IBM Spectrum Protect que son de la versión 6.3 o posteriores. Sin embargo, los campos se visualizan con fines de compatibilidad con releases anteriores.

- ID superior de copia de seguridad base de datos
- ID inferior copia de seguridad base de datos

- Posición inicial de copia de seguridad base de datos
- HLA copia de seguridad base de datos
- LLA copia de seguridad base de datos
- Bytes de datos totales de copia seguridad base de datos (MB)
- Bytes de registro totales de copia seguridad base de datos (MB)
- Número de bloque superior de copia de seguridad base de datos
- Número de bloque inferior de copia de seguridad base de datos

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY VOLHISTORY

Comando	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
PREPARE	Crea un archivo de plan de recuperación.
QUERY RPFIL	Muestra información sobre archivos del plan de recuperación.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
UPDATE VOLHISTORY	Agrega o cambia la información de ubicación de un volumen del archivo histórico de volúmenes.

## QUERY VOLUME (Consultar volúmenes de agrupación de almacenamiento)

Utilice este mandato para visualizar información acerca de uno o varios volúmenes de agrupación de almacenamiento.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```

.-*-----
>>-Query Volume-----+----->
      '-nombre_volumen-'

>-----+----->
|          .-,-----|
|          v          |
| '-ACCess-----+READWrite---+-'
|                   +-READOnly---+
|                   +-UNAVailable-+
|                   +-OFFsite-----+
|                   '-DESTroyed---'

>-----+----->
|          .-,-----|
|          v          |
| '-STatus-----+ONline---+-'
|                   +-OFFline-+
|                   +-EMPTy---+
|                   +-PENding-+
|                   +-FILLing-+
|                   '-FULl----'

.-STGpool-----*-----
>-----+----->
      '-STGpool-----nombre_agrupación-'

.-DEVclass-----*-----
>-----+----->
      '-DEVclass-----nombre_clase_dispositivo-'

.-Format-----Standard-----
>-----+-----<

```

## Parámetros

---

### nombre\_volumen

Especifica el volumen que se consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre, en la consulta se incluirán todos los volúmenes de agrupación de almacenamiento.

### ACCess

Especifica que la salida está restringida por la modalidad de acceso a volumen. Este parámetro es opcional. Puede especificar varias modalidades de acceso separando las modalidades con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la salida no estará limitada según la modalidad de acceso. Los valores posibles son:

#### READWrite

Se visualizan los volúmenes con la modalidad de acceso READWRITE. Los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes.

#### READOnly

Se visualizan los volúmenes con la modalidad de acceso READONLY. Los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en los archivos almacenados en los volúmenes.

#### UNAVailable

Se visualizan los volúmenes con la modalidad de acceso UNAVAILABLE. Los nodos cliente y los procesos del servidor no pueden acceder a archivos que están almacenados en los volúmenes.

#### OFFsite

Se visualizan los volúmenes de agrupaciones de almacenamiento de copia con la modalidad de acceso OFFSITE. Los volúmenes se encuentran en ubicaciones fuera de local desde las que no pueden montarse.

#### DESTroyed

Se visualizan los volúmenes de agrupaciones de almacenamiento primarias con la modalidad de acceso DESTROYED. Los volúmenes se han designado como dañados permanentemente.

### Status

Especifica que la salida está restringida por el estado de volumen. Este parámetro es opcional. Puede especificar varios valores de estado separando los valores con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la salida no estará limitada según el estado del volumen. Los valores posibles son:

#### ONline

Se visualizan volúmenes de acceso aleatorio que están disponibles en el servidor.

#### Offline

Se visualizan volúmenes de acceso aleatorio que no están disponibles en el servidor.

#### EMPTy

Se visualizan volúmenes de acceso secuencial que no tienen datos.

#### PENding

Se visualizan los volúmenes con el estado PENDING. Estos volúmenes pueden ser de acceso secuencial de los que se han suprimido todos los archivos pero para los que no ha transcurrido el tiempo especificado por el parámetro REUSEDELAY en el mandato DEFINE STGPOOL. Estos volúmenes también podrían ser volúmenes de disco de acceso aleatorio que se suprimieron, pero que todavía contienen datos descartados que están a la espera de ser destruidos. Después de destruir los datos, el volumen se suprimirá físicamente.

#### FILLing

Se visualizan los volúmenes de acceso secuencial en los que el servidor ha grabado pero que todavía no ha llenado hasta su capacidad.

#### FULL

Se visualizan los volúmenes de acceso secuencial que el servidor ha llenado.

### STGPool

Especifica la agrupación de almacenamiento que se incluye en la consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de agrupación de almacenamiento, se incluirán en la consulta todas las agrupaciones de almacenamiento.

### DEVclass

Especifica la clase de dispositivo que se incluye en la consulta. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de clase de dispositivo, se incluirán en la consulta todos los dispositivos.

### Format

Especifica cómo se ha de visualizar la información. Este parámetro es opcional. El valor predeterminado es STANDARD. Los valores posibles son:

#### Standard

Especifica que se visualizará información parcial.

## Detailed

Especifica que se visualizará toda la información.

### Ejemplo: obtener una lista de todos los volúmenes de agrupación de almacenamiento de archivo

Visualizar información acerca de todos los volúmenes de agrupación de almacenamiento que tengan el nombre de clase de dispositivo FILE. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume devclass=file
```

Nombre volumen	Nombre agrupación almacenam.	Nombre clase	Capacidad estimada	% Util	Estado volumen
/FCT/SERVER/COVOL1	COPYSTG	FILE	0.0 M	0.0	Pend.
/FCT/SERVER/COVOL2	COPYSTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/COVOL3	COPYSTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/PRVOL1	PRIMESTG	FILE	0.0 M	0.0	Vacío
/FCT/SERVER/PRVOL2	PRIMESTG	FILE	0.0 M	0.0	Vacío



### Ejemplo: obtener una lista de todos los volúmenes de agrupación de almacenamiento que tienen el mismo prefijo

Visualizar información acerca de todos los volúmenes de agrupación de almacenamiento que tengan como prefijo el nombre ATF. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume atf*
```

Nombre volumen	Nombre agrupación almacenam.	Nombre clase	Capacidad estimada	% Util	Estado volumen
ATF001	8MMPPOOL	8MMTAPE	4.8 G	18.2	Llenando
ATF002	8MMPPOOL	8MMTAPE	4.8 G	18.2	Llenando

### Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

Visualizar detalles sobre el volumen de agrupación de almacenamiento denominado /fct/server/covol1. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume covol1 format=detailed
```

```
Nombre volumen: /FCT/SERVER/COVOL1
Nombre agrupación almacenamiento: COPYSTG
Nombre de clase de dispositivo: DISK
Capacidad estimada: 10,0 M
Capacidad de escala aplicada:
  % Util: 6,7
Estado volumen: Activado
Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 3,2
¿Volumen reutilizable?: Sí
¿Con error?: No
Número caras grabables: 1
Número montajes: 11
  Número pases grabación: 1
Fecha aprox. última grabación: 04/14/1998 16:17:26
Fecha aprox. última lectura: 04/01/1998 13:26:18
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
El volumen es MVS con posibilidad
  fuera de la LAN: No
Última actualización por (administrador): COLLIN
Fecha/hora última actualización: 05/01/1998 14:07:27
```

Empezar periodo de reclamación:  
Finalizar período de reclamación:  
Bloque lógico protegido:  
Gestor de claves de cifrado de unidad:



## Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

---

Visualizar detalles sobre el volumen de agrupación de almacenamiento WPDV00. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume wpdv00 format=detailed
```

```
Nombre volumen: WPDV00
Nombre agrupación almacenamiento: TAPEPOOL
Nombre clase dispositivo: TAPE
Capacidad estimada: 5,8 M
Capacidad de escala aplicada:
  % Util: 0,1
Estado volumen: Activado
Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 3,2
¿Volumen reutilizable?: Sí
¿Con error?: No
Número caras grabables: 1
Número montajes: 11
Número pases grabación: 1
Fecha aprox. última grabación: 04/14/1998 16:17:26
Fecha aprox. última lectura: 04/01/1998 13:26:18
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
El volumen es MVS con posibilidad
fuera de la LAN: No
Última actualización por (administrador): COLLIN
Fecha/hora última actualización: 05/01/1998 14:07:27
Empezar periodo de reclamación:
Finalizar período de reclamación:
Bloque lógico protegido:
Gestor de claves de cifrado de unidad:
```

## Ejemplo: visualizar información detallada acerca de un volumen de agrupación de almacenamiento que tiene una clase de dispositivo específica

---

Muestra detalles sobre un volumen en una agrupación de almacenamiento con un nombre de clase de dispositivo FILECLASS. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume devclass=fileclass format=detailed
```

```
Nombre volumen: Z:\WORM_CFS\0000000E.BFS
Nombre volumen:
/Sistemas operativos Windows
/Sistemas operativos AIX
/Sistemas operativos Linux
/WORM_FILESYS/0000000E.BFS
Nombre agrupación almacenamiento: FILEPOOL
Nombre de clase de dispositivo: FILECLASS
Capacidad estimada: 2 G
Capacidad de escala aplicada:
  % Util: 0,0
Estado volumen: Llenando
Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 0,0
¿Volumen reutilizable?: Sí
¿Con error?: No
Número caras grabables: 1
Número de montajes: 1
Número pases grabación: 1
Fecha aprox. última grabación: 03/22/2004 15:23:46
Fecha aprox. última lectura: 03/22/2004 15:23:46
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
```

```
El volumen es MVS con posibilidad
fuera de la LAN: No
Última actualización por (administrador):
Fecha/hora última actualización: 03/22/2004 15:23:46
Empezar periodo de reclamación: 03/22/2005
Finalizar periodo de reclamación: 04/22/2005
Bloque lógico protegido:
Gestor de claves de cifrado de unidad:
```

## Ejemplo: visualizar información detallada acerca de un volumen agrupación de almacenamiento específico

---

Visualizar detalles sobre un volumen de agrupación de almacenamiento que se denomina 000642. El volumen está en una agrupación de almacenamiento que está asociada con una clase de dispositivo 3592. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
query volume 000642 format=detailed

Nombre volumen: 000642
Nombre agrupación almacenamiento: 3592POOL
Nombre clase dispositivo: 3592CLASS
Capacidad estimada: 2 G
Capacidad de escala aplicada:
% Util: 0,0
Estado volumen: Llenando
Acceso: Lectura/Grabación
Porcentaje de espacio reclamable: 0,0
¿Volumen reutilizable?: Sí
¿Con error?: No
Número caras grabables: 1
Número de montajes: 1
Número pases grabación: 1
Fecha aprox. última grabación: 03/22/2004 15:23:46
Fecha aprox. última lectura: 03/22/2004 15:23:46
Fecha en que pasó a pendiente:
Número errores grabación: 0
Número errores lectura: 0
Ubicación volumen:
El volumen es MVS con posibilidad
fuera de la LAN: No
Última actualización por (administrador):
Fecha/hora última actualización: 03/22/2004 15:23:46
Empezar periodo de reclamación: 03/22/2005
Finalizar periodo de reclamación: 04/22/2005
Bloque lógico protegido: Sí
Drive Encryption Key Manager: IBM Spectrum Protect
```

## Descripciones de los campos

---

### Nombre de volumen

El nombre del volumen de agrupación de almacenamiento.

### Nombre de la agrupación de almacenamiento

La agrupación de almacenamiento en la que está definido el volumen.

### Nombre clase dispositivo

La clase de dispositivo que se asigna a la agrupación de almacenamiento.

### Capacidad estimada

La capacidad estimada del volumen, en megabytes (M), gigabytes (G) o terabytes (T).

Para dispositivos DISK, este valor es la capacidad del volumen.

Para dispositivos de acceso secuencial, este valor es un cálculo del espacio total disponible en el volumen, que se basa en la clase de dispositivo.

### Capacidad de escala aplicada

El porcentaje de la capacidad a la que se ha escalado un volumen. Por ejemplo, un valor de 20 para un volumen cuya capacidad máxima es de 300 GB indica que el volumen sólo puede almacenar 20 por ciento de 300 GB o 60 GB. Este atributo solamente se aplica a los dispositivos IBM® 3592.

### Pct. util

Un cálculo de la utilización del volumen. La utilización incluye todo el espacio que ocupan ambos archivos y agregados, incluido el espacio vacío dentro de agregados.

Para volúmenes DISK, la utilización también incluye el espacio que ocupan los datos almacenados en caché.

Estado volumen

El estado del volumen.

Acceso

Si el volumen está disponible para el servidor.

Porcentaje de Espacio reclamable (sólo volúmenes de acceso secuencial)

La cantidad de espacio de este volumen que puede reclamarse porque los datos han caducado o se han suprimido. Este valor se compara con el umbral de reclamación de la agrupación de almacenamiento para determinar si es necesaria la reclamación. El espacio reclamable incluye el espacio vacío en las agregaciones.

Cuando se determina qué volúmenes se reclaman en una agrupación de almacenamiento, el servidor determina primero el umbral de reclamación. El umbral de reclamación viene indicado por el valor del parámetro THRESHOLD en el mandato RECLAIM STGPOOL o, si no se ha especificado dicho valor, el valor del parámetro RECLAIM en una definición de agrupación de almacenamiento. A continuación, el servidor examina el porcentaje de espacio reclamable de cada volumen en la agrupación de almacenamiento. Si el porcentaje de espacio reclamable que hay en un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento, el volumen es candidato para la reclamación.

Por ejemplo, supongamos que la agrupación de almacenamiento FILEPOOL tiene un umbral de reclamación del 70 por ciento. Este valor indica que el servidor puede reclamar cualquier volumen en la agrupación de almacenamiento que tenga un porcentaje de espacio reclamable mayor del 70 por ciento. La agrupación de almacenamiento tiene tres volúmenes:

- FILEVOL1 con el 65 por ciento de espacio reclamable
- FILEVOL2 con el 80 por ciento de espacio reclamable
- FILEVOL3 con el 95 por ciento de espacio reclamable

Cuando empieza la reclamación, el servidor compara el porcentaje de espacio reclamable de cada volumen con el umbral de reclamación del 70 por ciento. En este ejemplo, FILEVOL2 y FILEVOL3 son candidatos para la reclamación porque sus porcentajes de espacio reclamable son mayores que el 70 por ciento.

Para volúmenes que pertenecen una agrupación de almacenamiento de SnapLock, el valor se visualiza pero no se utiliza.

¿Volumen reutilizable? (sólo volúmenes de acceso secuencial)

Si este volumen se puede reutilizar cuando el volumen se vacía.

¿Con error?

Si el volumen está en un estado de error. El servidor no puede grabar en volúmenes que tienen un estado de error.

Número caras grabables

Esta información está reservada para IBM Spectrum Protect.

Número montajes

El número de veces que el servidor abierto el volumen para su uso. El número de veces que el servidor ha abierto el volumen no siempre coincide con que el número de veces que se ha montado físicamente el volumen en una unidad. Una vez montado físicamente un volumen, el servidor puede abrir el mismo volumen varias veces para distintas operaciones, como por ejemplo para distintas sesiones de copia de seguridad de cliente.

Número de pases de grabación (sólo volúmenes de acceso secuencial)

El número de veces que se ha grabado en el volumen desde el principio al final.

Fecha aprox. última grabación

La fecha aproximada en que se ha grabado el volumen por última vez.

Fecha aprox. última lectura

La fecha aproximada en que se ha leído el volumen por última vez.

Fecha en que pasó a pendiente

La fecha en que el estado del volumen se ha modificado a pendiente.

Número errores grabación

El número de errores de grabación que se han producido en el volumen.

Número errores lectura

El número de errores de lectura que se han producido en el volumen.

Ubicación del volumen

La ubicación del volumen.

El volumen es MVS con posibilidad fuera de la LAN

Si el volumen es un volumen con posibilidad fuera de la LAN. Un volumen con posibilidad fuera de la LAN es aquél que ha definido y ha utilizado (como mínimo una vez) el servidor del gestor de datos de IBM Spectrum Protect z/OS.

Última actualización por (administrador)

El administrador que ha definido o que ha actualizado más recientemente el volumen.

Fecha/hora última actualización

El momento en que se ha definido o actualizado más recientemente el volumen.

Empezar período de reclamación



Representa la fecha después de la cual el servidor inicia la reclamación de este volumen, pero que no debe ser posterior a la fecha que representa el fin del período de reclamación. Si, cuando empieza el periodo de reclamación, hay archivos en el volumen que no han caducado, estos se trasladan a un nuevo volumen WORM durante el proceso de reclamación. Este campo muestra una fecha sólo si este volumen está en una agrupación de almacenamiento para la que el valor del parámetro RECLAMATIONTYPE es SNAPLOCK.

Si se almacena más de un archivo en el mismo volumen, el inicio del período de reclamación del volumen se basa en la fecha del archivo más reciente. Para los volúmenes SnapLock, el parámetro RETVer del mandato DEFINE COPYGROUP determina durante cuánto tiempo se almacenará una copia archivada. Si RETVer se define en 100 días, el período de reclamación del volumen se iniciará 100 días después de que el primer archivo se almacene en él. Si se almacena un segundo archivo en el mismo volumen, la fecha de inicio de la reclamación se ajustará a 100 días después de que se almacene el nuevo archivo. Si el valor de RETVer se modifica una vez que el primer archivo ya se ha almacenado, se aplicará la última fecha de reclamación para todos los archivos del volumen. Por ejemplo, supongamos que RETVer se define en 100 para un archivo inicial, pero luego se cambia a 50. Si se almacena un segundo archivo en el volumen tres días después del primero, el período de reclamación no empezará hasta pasados 100 días desde el almacenamiento del primer archivo.

**Finalizar período de reclamación**

Representa la fecha en la que IBM Spectrum Protect debe completar el proceso de reclamación de este volumen para garantizar la protección continuada de los datos. También representa el atributo de archivo físico Fecha de último acceso en el archivador NetApp, que impide que el archivo se suprima hasta después de esa fecha. Este campo muestra una fecha sólo si este volumen está en una agrupación de almacenamiento para la que el valor del parámetro RECLAMATIONTYPE es SNAPLOCK.

**Gestor de claves de cifrado de unidad**

El gestor de claves de cifrado de unidad. Este campo se aplica sólo a volúmenes de una agrupación de almacenamiento que está asociada a un tipo de dispositivo de 3592, LTO o ECARTRIDGE.

**Bloque lógico protegido**

Especifica si la protección de bloques lógicos está habilitada para el volumen. Puede utilizar la protección de bloques lógicos solamente con los siguientes tipos de unidades y medios:

- IBM LTO5 y posterior
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior
- Unidades Oracle StorageTek T10000C y T10000D

## Comandos relacionados

Tabla 1. Comandos relacionados con QUERY VOLUME

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.
VARY	Especifica si está disponible un volumen de disco para el servidor.

## QUIT (finalizar la modalidad interactiva del cliente de administración)

Utilice este comando para finalizar una sesión de cliente de administración en modalidad interactiva.

No puede utilizar el comando QUIT desde el identificador de administración SERVER\_CONSOLE ni desde las modalidades de consola, por lotes o de montaje del cliente de administración.

### Clase de privilegio

Cualquier administrador puede emitir este comando.

### Sintaxis

```
>>-QUIT-----><
```

## Parámetros

---

Ninguno.

## Ejemplo: finalizar una sesión de cliente de administración interactiva

---

Finalizar una sesión del cliente de administración en modalidad interactiva.

```
quit
```

## Comandos relacionados

---

Ninguno.

## RECLAIM STGPOOL (Reclamar volúmenes de una agrupación de almacenamiento de acceso secuencial)

---

Utilice este mandato para reclamar volúmenes en una agrupación de almacenamiento de acceso secuencial. La reclamación no traslada las versiones inactivas de los datos de copia de seguridad de los volúmenes en las agrupaciones de datos activos.

Este mandato no se puede utilizar para los tipos siguientes de agrupaciones de almacenamiento:

- Agrupaciones de almacenamiento de copia de contenedor. El espacio de estas agrupaciones de almacenamiento se reclama como parte del proceso realizado por mandatos PROTECT STGPOOL.
- Agrupaciones de almacenamiento con uno de los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
- Agrupaciones de almacenamiento que utilizan una clase de dispositivo de CENTERA.
- Agrupaciones de almacenamiento que utilizan dispositivos WORM (Grabar una vez leer varias). La reclamación no es necesaria porque los volúmenes WORM no son reutilizables, pero puede ejecutar la reclamación para consolidar los datos en menos volúmenes.

Utilice este mandato sólo si no va a utilizar la reclamación automática para la agrupación de almacenamiento. Este mandato acepta los valores de los atributos RECLAIMPROCESS y RECLAIMSTGPOOL de la definición de agrupación de almacenamiento. Este mandato también acepta los valores de los parámetros OFFSITERECLAIMLIMIT y RECLAIM de la definición de agrupación de almacenamiento, si no los han alterado temporalmente los parámetros de mandato OFFSITERECLAIMLIMIT y THRESHOLD.

Consejos:

- Al emitir este mandato se eliminan los datos duplicados de una agrupación de almacenamiento primaria, una agrupación de almacenamiento de copia o una agrupación de datos activos configurada para la deduplicación de datos.
- Cuando se utiliza este mandato para restaurar objetos deduplicados a la misma agrupación de almacenamiento, los bloques de datos duplicados se sustituyen por referencias a las extensiones deduplicadas.

Para las agrupaciones de almacenamiento definidas con RECLAMATIONTYPE=SNAPLOCK, este mandato también suprime los volúmenes WORM FILE vacíos que exceden su periodo de reclamación.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado para la agrupación de almacenamiento que se está reclamando y la agrupación de almacenamiento de reclamación, si procede.

## Sintaxis

---

```
>>-RECLaim STGpool--nombre_agrupación----->
>--+-----+--+-----+-----+----->
  '-Threshhold---número-' '-Duration---minutos-'

  .-Wait---No-----
>--+-----+-----+-----+----->
  '-Wait---+No---+'
      '-Yes-'
```

```
>-----<
'-OFFSITERECLAIMLimit---número_de_volúmenes-'
```

## Parámetros

---

### nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento cuyos volúmenes se reclamarán.

### DUration

Especifica el número máximo de minutos que se ejecuta la migración antes de que se cancele automáticamente. Puede especificar un número de 1 a 9999. Este parámetro es opcional.

Después de transcurrir el número de minutos especificado, la próxima vez que el servidor verifique el proceso de reclamación lo detendrá. El servidor comprueba el proceso de reclamación cuando monta otro volumen elegible de la agrupación de almacenamiento que se está reclamando. El servidor también comprueba el proceso de reclamación cuando el servidor empieza a reclamar un nuevo lote de archivos del volumen que está montado actualmente. Como consecuencia, la reclamación puede ejecutarse durante más tiempo que el valor que especifique para este parámetro.

Hasta que el servidor no verifique el proceso de reclamación, no existe ninguna indicación de que haya caducado el período de duración. Cuando el servidor detiene el proceso de reclamación, emite el mensaje ANR4927W: Se ha terminado la reclamación para el volumen xxx - se ha sobrepasado la duración.

Si no especifica este parámetro, el proceso se detendrá únicamente cuando no haya más volúmenes que satisfagan el umbral.

Si especifica un valor de duración para la reclamación de una agrupación de almacenamiento de copia con volúmenes fuera del local, puede provocar que la reclamación finalice antes de que se haya reclamado cualquier volumen. En la mayoría de situaciones al iniciar la reclamación de una agrupación de almacenamiento con volúmenes fuera del local, se recomienda limitar el número de volúmenes fuera del que deben reclamarse en lugar de limitar la duración. Para obtener información adicional, consulte el parámetro OFFSITERECLAIMLIMIT.

### THreshold

Especifica el porcentaje de espacio reclamable en un volumen que permite seleccionarlo para la reclamación. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos. El espacio reclamable también incluye el espacio no utilizado.

Puede especificar un número del 1 al 99. Este parámetro es opcional. Si no se especifica, se utiliza el atributo RECLAIM de la definición de agrupación de almacenamiento.

Para determinar el porcentaje de espacio reclamable de un volumen, emita el mandato QUERY VOLUME y especifique FORMAT=DETAILED. El valor en el campo Porcentaje de espacio reclamable es el porcentaje de espacio reclamable del volumen.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de destino.

### OFFSITERECLAIMLimit

Especifica el número máximo de volúmenes de agrupaciones de almacenamiento fuera del local que el servidor intenta reclamar. Este parámetro sólo es válido para las agrupaciones de almacenamiento de copia. Puede especificar un número del 0 al 99999. Este parámetro es opcional. Si no se especifica, se utiliza el atributo OFFSITERECLAIMLIMIT de la definición de agrupación de almacenamiento.

### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

#### No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Si cancela este proceso, pueden haberse trasladado ya algunos archivos antes de la cancelación.

#### Yes

Especifica que el servidor procesa este comando en primer plano. La operación debe estar terminada para poder continuar con otras tareas. Cuando finaliza la operación, se muestran mensajes de salida en el cliente de administración. Los mensajes también se visualizan en las anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.



- IBM Spectrum Protect marca como no disponibles los volúmenes de agrupación de almacenamiento del servidor de origen que no se pueden localizar en el servidor de destino. Los volúmenes que sólo se encuentran en el archivo histórico de volúmenes, como, por ejemplo, los volúmenes de importación y exportación y las copias de seguridad de base de datos, se registrarán como incoherentes.
- Las copias archivadas del servidor de destino que no se correspondan con ningún volumen virtual en el servidor de origen se marcan para suprimirlas del servidor de destino.

La tabla siguiente muestra los detalles de las acciones que se ejecutan:

FIX=	En el servidor origen	En el servidor destino	Acción
NO	Existen volúmenes	No existen archivos	Informar sobre error
		Los archivos existen pero están marcados para supresión	
		Existen archivos activos pero los atributos no coinciden	
	Los volúmenes no existen	Existen volúmenes activos	Informar sobre error
Los archivos existen pero están marcados para supresión		Ninguno	
YES	Existen volúmenes	No existen archivos	Informar sobre error <b>Volúmenes de agrupación de almacenamiento:</b> Marcados como no disponibles
		Los archivos existen pero están marcados para supresión	Informar sobre error <b>Volúmenes de agrupación de almacenamiento:</b> Si los atributos coinciden, marcar los archivos del servidor de destino como activos de nuevo, marcar los volúmenes del servidor de origen como no disponibles y recomendar que se ejecute un mandato AUDIT VOLUME para verificar los datos. Si los atributos no coinciden, marcar los volúmenes como no disponibles.
		Existen archivos activos pero los atributos no coinciden	Informar sobre error <b>Volúmenes de agrupación de almacenamiento:</b> Marcar como no disponibles y recomendar que se ejecute un mandato AUDIT VOLUME para verificar los datos.
	Los volúmenes no existen	Existen volúmenes activos	Marcar archivos para supresión en el servidor de destino.
		Los archivos existen pero están marcados para supresión	Ninguno

## Ejemplo: reconciliar las diferencias en las definiciones de volumen virtual

Reconciliar las diferencias que hay entre todas las definiciones de volúmenes virtuales del servidor de origen y las copias archivadas den el servidor de destino para corregir las incoherencias.

```
reconcile volumes remotel fix=yes
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RECONCILE VOLUMES

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE SERVER	Suprime la definición de un servidor.

Comando	Descripción
QUERY SERVER	Muestra información sobre servidores.
UPDATE SERVER	Actualiza la información sobre un servidor.

## Comandos REGISTER

Utilice los mandatos REGISTER para definir o agregar objetos para IBM Spectrum Protect.

- REGISTER ADMIN (Registrar un ID de administrador)
- REGISTER LICENSE (Registrar una nueva licencia)
- REGISTER NODE (Inscribir un nodo)

## REGISTER ADMIN (Registrar un ID de administrador)

Utilice este comando para agregar un administrador al servidor. Una vez registrado, el administrador puede emitir un conjunto de comandos limitado, incluidos todos los comandos de consulta. Para proporcionar privilegios adicionales, utilice el mandato GRANT AUTHORITY.

### Clase de privilegio

Para emitir este mandato, debe tener privilegios del sistema.

Al registrar un administrador con el mismo nombre que un nodo existente, tenga en cuenta el método de autenticación de administrador y el valor de SSLREQUIRED. Cualquier nodo que tiene el mismo nombre que el administrador que se está registrando hereda esos valores.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- No especifique un ID de usuario de administración que coincida con un nombre de nodo. Si el ID de usuario de administración coincide con el nombre del nodo, podría darse un comportamiento imprevisto debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

### Sintaxis

```
>>-REGister Admin--nombre_admin--+-----+----->
                                     '-password-'

>+-----+-----+-----+----->
| (1) | '-CONTACT---texto-'
|-----PASSExp---días-'

.-FORCEPwreset---No-----
>+-----+-----+-----+----->
'-FORCEPwreset---+No--+-'
                                     '-Yes-'

>+-----+-----+-----+----->
'-EMAILAddress---ID_usuario@nodo-'

(2)
.------AUTHentication---LOCAL-.
>+-----+-----+-----+----->
'-AUTHentication---+LOCAL+---'
                                     '-LDap--'

(3)
.-SSLrequired---DEFAULT-----
>+-----+-----+-----+----->
'-SSLrequired---+Yes+---+'
                                     +No-----+
                                     '-DEFAULT-'

.-SESSIONSECurity---TRANSitional-----.
```

```

>-----+----->
'-SESSIONSECurity--==--+-STRict-----+-'
          '-TRANSitional-'

.-ALert-----No-----
>-----+-----<
'-ALert-----+-Yes+-'
          '-No--'

```

**Notas:**

1. El mandato PASSEXP no se aplica a los administradores que se autentican en un servidor de directorios LDAP.
2. El valor predeterminado puede cambiar si emitió el mandato SET DEFAULTAUTHENTICATION y especificó LDAP.
3. El parámetro SSLREQUIRED está en desuso.

## Parámetros

---

**nombre\_admin (Necesario)**

Especifica el nombre del administrador que se ha de registrar. La longitud máxima del nombre es de 64 caracteres.

No puede especificar NONE como nombre de administrador.

Si tiene previsto autenticar el ID de administrador con un servidor LDAP, asegúrese de que el ID de administrador no coincida con el nombre de cualquier nodo que se autentique con un servidor LDAP.

**contraseña**

Especifica la contraseña del administrador que se ha de registrar. La longitud máxima de la contraseña es de 64 caracteres.

Si autentica contraseñas localmente con el servidor IBM Spectrum Protect, debe especificar una contraseña. La contraseña no es sensible a las mayúsculas y minúsculas.

Si autentica contraseñas con un servidor LDAP (Lightweight Directory Access Protocol), no especifique una contraseña en el mandato REGISTER ADMIN.

**PASSExp**

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña en el rango de 0 – 9999 días. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, la contraseña se establecerá con el período de caducidad global de 90 días. Este parámetro no afecta a las contraseñas que se almacenan en un servidor de directorios LDAP.

**CONtact**

Especifica información que identifica al administrador que se ha registrado. Este parámetro es opcional. La longitud máxima de esta serie es de 255 caracteres. La información de contacto debe estar encerrada entre comillas, si contiene espacios en blanco.

**FORCEPwreset**

Especifica si el administrador tiene que cambiar o restablecer la contraseña. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

**No**

Especifica que el administrador no necesita cambiar ni restablecer la contraseña al intentar conectarse al servidor.

**Yes**

Especifica que la contraseña del administrador caduca durante el próximo inicio de sesión. El cliente o el administrador deben cambiar o restablecer la contraseña en ese momento. Si no se especifica una contraseña, recibirá un mensaje de error.

Restricción: En el caso de los ID de usuarios administrativos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si especifica AUTHENTICATION=LDAP.

**EMAILAdress**

Especifica la dirección de correo electrónico de este administrador.

**AUTHentication**

Este parámetro especifica el método de autenticación para el ID de usuario administrador. Especifique uno de los siguientes valores: LDAP o LOCAL. El parámetro es opcional y toma el valor predeterminado LOCAL. El valor predeterminado se puede cambiar a LDAP si se utiliza el mandato SET DEFAULTAUTHENTICATION y especifica LDAP.

**Local**

Especifica que se está utilizando la base de datos del servidor IBM Spectrum Protect .

**LDap**

Especifica que el ID de usuario administrador autentica contraseñas con un servidor de directorio LDAP. Las contraseñas que se autentican con un servidor de directorios LDAP distinguen entre mayúsculas y minúsculas.

Consejo: No se necesita contraseña si registra un administrador y selecciona AUTHENTICATION=LDAP. Al iniciar la sesión, se le solicitará una contraseña.

## SSLrequired (en desuso)

Especifica si el ID de usuario administrador debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect y el cliente de archivado y copia de seguridad. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

## SESSIONSECurity

Especifica si el administrador debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

### STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el administrador. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el administrador. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el administrador pueda autenticarse en el servidor:

- Tanto el administrador como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el administrador para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el administrador.

Los administradores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

### TRANSitional

Especifica que se aplicarán los valores de seguridad existentes para el administrador. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el administrador no cumplen nunca los requisitos para el valor STRICT, el administrador continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un administrador cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el administrador ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el administrador se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un administrador que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como el direccionamiento de mandatos o la exportación entre servidores, cuando el administrador se autentica en el servidor IBM Spectrum Protect como administrador de otro servidor.

## ALert

Especifica si las alertas se envían a una dirección de correo electrónico de los administradores.

### Yes

Especifica que las alertas se envíen a la dirección de correo electrónico especificada de los administradores.

### No

Especifica que las alertas no se envíen a la dirección de correo electrónico especificada de los administradores. Este es el valor predeterminado.

Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

## Ejemplo: registrar un administrador

---

Definir un administrador, LARRY, con la contraseña PASSONE. Puede identificar a LARRY como personal de segundo turno, especificando esta información en el parámetro CONTACT. Emita el comando:

```
register admin larry passone contact="segundo turno"
```

## Ejemplo: registrar un ID de administrador y establecer el método de autenticación

---



Defina un ID de administrador para Harry de forma que Harry pueda autenticarse en un servidor LDAP. Emita el mandato:

```
register admin harry authentication=ldap
```

## Ejemplo: registrar un administrador y forzar la seguridad de sesión estricta

Registre un administrador llamado Harry y exija que utilice la configuración de seguridad más estricta para autenticarse en el servidor. Emita el mandato:

```
register admin harry sessionsecurity=strict
```

## Comandos relacionados

Tabla 1. Comandos relacionados con REGISTER ADMIN

Comando	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE ADMIN	Suprime un administrador de la lista de administradores registrados.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UNLOCK ADMIN	Permite que un administrador bloqueado acceda a IBM Spectrum Protect.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

### Tareas relacionadas:

Nombrar objetos de Tivoli Storage Manager

### Información relacionada:

Opción de cliente SSL

## REGISTER LICENSE (Registrar una nueva licencia)

Utilice este comando para registrar licencias nuevas para componentes del servidor, incluyendo IBM Spectrum Protect (base), IBM Spectrum Protect Extended Edition y IBM Spectrum Protect para retención de datos.

Las licencias se almacenan en los archivos de certificados de inscripción. Los archivos de certificados de inscripción contienen información de licencias para el producto del servidor. El archivo NODELOCK conserva la información de licencias de la instalación. Su acuerdo de licencia determina qué puede utilizar con su licencia, aunque no pueda usar el comando REGISTER LICENSE para registrar todos los componentes. Se espera que cumpla con el acuerdo de licencia y utilice sólo lo que ha adquirido. El uso del comando REGISTER LICENSE implica que acepta los términos de licencia de su acuerdo de licencia.

Importante:

- Antes de proceder a la actualización de una versión anterior de IBM Spectrum Protect, debe suprimir el archivo NODELOCK o cambiarle el nombre.
- Para anular licencias, debe borrar el archivo NODELOCK en el directorio de instancia del servidor de la instalación y volver a registrar las licencias registradas previamente.

- No se pueden registrar licencias de IBM Spectrum Protect para correo, IBM Spectrum Protect para bases de datos, IBM Spectrum Protect para ERP y IBM Spectrum Protect for Space Management.

Para generar un informe que pueda ayudarle a conocer los requisitos de licencia del sistema, ejecute el mandato QUERY PVUESTIMATE. El informe contiene estimaciones del número de dispositivos de cliente y los totales de PVU de los dispositivos de servidor. Las estimaciones no son vinculantes jurídicamente.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-REGister LICense--FILE--==--+-tsmbasic.lic+-----><
                                     +-tsmee.lic-----+
                                     +-dataret.lic--+
                                     '-*.lic-----'
```

## Parámetros

### FILE

Especifica el nombre del archivo de certificados de inscripción que contiene la licencia que se ha de registrar. La especificación puede contener un carácter comodín (\*). Especifique el nombre de archivo completo o un carácter comodín en lugar del nombre de archivo. Los nombres de archivos son sensibles a las mayúsculas/minúsculas. Se pueden utilizar los siguientes valores:

tsmbasic.lic

Para obtener la licencia de IBM Spectrum Protect base.

tsmee.lic

Para obtener la licencia de IBM Spectrum Protect Extended Edition. Esto incluye el gestor de recuperación ante siniestro, bibliotecas de gran tamaño y NDMP.

dataret.lic

Para obtener la licencia de IBM Spectrum Protect para retención de datos. Es necesaria para activar la protección de retención de datos y también la suspensión de caducidad y supresión (retención de supresión).

\*.lic

Para obtener la licencia de todas las licencias de IBM Spectrum Protect para componentes del servidor.

## Ejemplo: registrar una licencia

Registre la licencia de IBM Spectrum Protect base.

```
register license file=tsmbasic.lic
```

## Comandos relacionados

Tabla 1. Comandos relacionados con REGISTER LICENSE

Comando	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY PVUESTIMATE	Muestra las estimaciones de las unidades de valor de procesador.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET LICENSEAUDITPERIOD	Especifica el número de días entre auditorías automáticas de licencias.

## REGISTER NODE (Inscribir un nodo)

Utilice este comando para inscribir un nodo en el servidor.

Este mandato puede crear un ID de usuario de administración con autorización de propietario de cliente sobre el nodo. Puede utilizar este identificador de usuario de administración para acceder al cliente de copia de seguridad/archivado de web desde ubicaciones

remotas mediante un navegador web.

Consejo:

- En versiones anteriores del producto, el mandato REGISTER NODE creaba automáticamente un ID de usuario de administración cuyo nombre coincidía con el nombre de nodo. A partir de IBM Spectrum Protect V8.1, el mandato REGISTER NODE no crea automáticamente un ID de usuario de administración que coincide con el nombre del nodo.
- Si tiene previsto utilizar la opción sin LAN con este nodo, debe registrar un ID administrativo que coincida con el nombre de nodo. Para registrar el ID administrativo, utilice el parámetro USERID o registre manualmente el administrador y otórguele autoridad de propietario para el nodo.

Si un cliente necesita un dominio de políticas distinto de STANDARD, deberá inscribir el nodo cliente con este comando o actualizar el nodo inscrito.

Requisito: Cuando establece `sslrequired=serveronly` en un mandato REGISTER NODE, el valor SSLREQUIRED vuelve a ser YES. Para utilizar una sesión que no es SSL con un agente de almacenamiento, cambie el nombre al administrador por el nombre idéntico emitiendo el mandato RENAME ADMIN .

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Cuando se registra o actualiza un nodo, puede especificar si los archivos dañados en el nodo pueden recuperarse de un servidor de réplica. Los archivos sólo se pueden recuperar si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores de los parámetros a la recuperación de archivos dañados y replicados.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	No especificado	NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

## Sintaxis

```
>>-REGister Node--nombre_nodo--+-----+-----+----->
                                     '-password-'
                                     .-USerid---NONE-----
>+-----+-----+-----+-----+-----+----->
| (1)          | '-USerid---NONE-----+'
|-----PASSExp---días-'          '-id_usuario-'
                                     .-Domain---STANDARD-----
>+-----+-----+-----+-----+-----+----->
'-CONTACT---texto-' '-Domain---nombre_dominio--'
                                     .-COMPression---Client----- .-ARCHDElete---Yes-----
>+-----+-----+-----+-----+-----+----->
'-COMPression---Client+' '-ARCHDElete---Yes+'
          +-Yes----+          '-No--'
          '-No-----'
                                     .-BACKDElete---No-----
>+-----+-----+-----+-----+-----+----->
'-BACKDElete---No--+'
          '-Yes-'
>+-----+-----+-----+-----+-----+----->
'-CLOptset---option_set_name-'
                                     .-FORCEPwreset---No----- .-Type---Client-----
>+-----+-----+-----+-----+-----+----->
'-FORCEPwreset---No--+' '-Type---Client--+'
          '-Yes-'          | (2) |
                          +-NAS-----+
                          '-Servidor-'
>+-----+-----+-----+-----+-----+----->
'-URL---url-' '-UTILITYUrl---utility_url-'
                                     .-MAXNUMMP---1----- .-AUTOFSRename---No-----
>+-----+-----+-----+-----+-----+----->
'-MAXNUMMP---number-' '-AUTOFSRename---Yes--+'
                          +-No-----+
                          '-Client-'
                                     .-KEEPMP---No----- (3)
>+-----+-----+-----+-----+-----+----->
'-KEEPMP---No--+'
          '-Yes-'
                                     .-VALIDateprotocol---No-----
>+-----+-----+-----+-----+-----+----->
'-VALIDateprotocol---No--+'
          +-Dataonly+
          '-All-----'
                                     .-TXNGroupmax---0-----
>+-----+-----+-----+-----+-----+----->
'-TXNGroupmax---0-----+'
          '-número-'
                                     .-DATAWritepath---ANY-----
>+-----+-----+-----+-----+-----+----->
'-DATAWritepath---ANY--+'
          +-LAN-----+
          '-LANFree-'
                                     .-DATAReadpath---ANY-----
>+-----+-----+-----+-----+-----+----->
'-DATAReadpath---ANY--+'
          +-LAN-----+
          '-LANFree-'
```





Si se registra un nodo que tiene el mismo nombre que un administrador, el método de autenticación del administrador y el valor SSLREQUIRED cambian para que coincidan con el método de autenticación del nodo. Las contraseñas que se comparten entre nodos y administradores con el mismo nombre se mantienen sincronizadas durante un cambio de autenticación.

Si tiene previsto utilizar la opción sin LAN con este nodo, utilice el parámetro USERID para registrar un ID administrativo que coincida con el nombre de nodo.

Para usuarios de servidores LDAP: Si tiene previsto autenticar el nodo con un servidor LDAP, conserve el valor predeterminado (USERID=NONE) o especifique un ID de usuario de administración distinto del nombre de nodo. Si el ID de usuario de administración coincide con el nombre de nodo, es posible que observe un comportamiento inesperado debido a cambios automáticos de contraseña que actualizan la misma contraseña dos veces. Como resultado, la contraseña podría llegar a ser desconocida para el ID de usuario de administración. De forma alternativa, la operación de actualización de contraseña podría fallar.

#### CONtact

Especifica una serie de texto de información que identifica el nodo. El parámetro es opcional. La longitud máxima de la serie de texto es de 255 caracteres. La información de contacto debe estar encerrada entre comillas, si contiene espacios en blanco.

#### DOmain

Especifica el nombre del dominio de políticas al que se asigna el nodo. El parámetro es opcional. Si no especifica un nombre de dominio de políticas, se asigna el nodo al dominio de políticas predeterminado (STANDARD).

Si un servidor origen está inscrito como un nodo, se asigna a un dominio de políticas. Los datos del servidor de origen se almacenan en la agrupación de almacenamiento especificada en el grupo de copia archivada de la clase de gestión predeterminada de dicho dominio.

#### COMPrression

Especifica si el nodo cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado. El parámetro es opcional. El valor predeterminado es CLIENT.

Restricción: Este parámetro no se aplica a los nodos con un tipo NAS o SERVER.

Puede especificar uno de los siguientes valores:

##### Client

Especifica que el cliente determina si se han de comprimir los archivos.

##### Yes

Especifica que el nodo cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado.

##### No

Especifica que el nodo cliente no comprime sus archivos antes de enviarlos al servidor para copia de seguridad y archivado.

#### ARCHDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. El parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

##### Yes

Especifica que el nodo cliente puede suprimir sus propias copias archivadas del servidor.

##### No

Especifica que el nodo cliente no puede suprimir sus propias copias archivadas del servidor.

#### BACKDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

##### No

Especifica que el nodo cliente no puede suprimir sus propias copias de seguridad del servidor.

##### Yes

Especifica que el nodo cliente puede suprimir sus propias copias de seguridad del servidor.

#### CLOptset

Especifica el nombre del conjunto de opciones que ha de utilizar el cliente. El parámetro es opcional.

#### FORCEPwreset

Especifica si se forzará que un cliente cambie o restablezca la contraseña. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

##### No

Especifica que el período de caducidad de contraseña se establece mediante el comando SET PASSEXP. El cliente no necesita cambiar ni restablecer la contraseña cuando el cliente está iniciando la sesión en el servidor.

##### Yes

Especifica que la contraseña del nodo cliente caducará en la próxima conexión. El cliente debe cambiar o restablecer la contraseña. Si no se especifica una contraseña, recibirá un mensaje de error.

Restricción: En el caso de los nodos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si especifica AUTHENTICATION=LDAP.

#### Type

Especifica el tipo de nodo que se está inscribiendo. El parámetro es opcional. El valor predeterminado es CLIENT. Puede especificar uno de los siguientes valores:

##### Client

Especifica que el nodo de cliente es un cliente de archivado y copia de seguridad, un cliente de IBM Spectrum Protect for Space Management o un cliente de aplicaciones.

##### NAS

Especifica que el nodo es un servidor de archivos de almacenamiento conectado a red (NAS) cuyos datos se protegen mediante operaciones NDMP. El nombre de nodo no puede ser SERVER.

Nota: El nombre del nodo NAS debe ser el mismo que el del transportador de datos. Por lo tanto, el nombre no puede cambiarse después de haberse definido el transportador de datos correspondiente.

##### Server

Especifica que el nodo de cliente es un servidor de origen que se está inscribiendo en el servidor de destino.

#### URL

Especifica el URL del cliente web de IBM Spectrum Protect que se ha configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

Este parámetro es opcional. El URL debe incluir el nombre DNS o la dirección IP del sistema cliente y el número de puerto que está definido en el sistema cliente para el cliente web de IBM Spectrum Protect. Por ejemplo, `http://client.mycorp.com:1581`

#### UTILITYUrl

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza el Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde el Centro de operaciones.

Este parámetro es opcional. Puede especificar un URL de hasta 200 caracteres de longitud. El URL debe empezar por `https`. Incluye el nombre DNS o la dirección IP del sistema cliente y el número de puerto que se ha definido en el sistema cliente para los servicios de gestión de cliente de IBM Spectrum Protect. Por ejemplo, `https://client.mycorp.com:9028`

Si se omite el número de puerto, el Centro de operaciones utiliza el número de puerto 9028, que es el número de puerto predeterminado cuando se instalan los servicios de gestión del cliente en el sistema cliente.

#### MAXNUMMP

Especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor o en el agente de almacenamiento sólo para las operaciones de copia de seguridad, de archivado y de migración IBM Spectrum Protect for Space Management. El parámetro es opcional y no se aplica a los nodos con un tipo NAS o SERVER. El valor predeterminado es 1. Puede especificar un entero en el rango de 0 a 999. Un valor de 0 especifica que un nodo no puede adquirir ningún punto de montaje para una operación de almacenamiento de datos de cliente. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos de las operaciones de almacenamiento de datos simultáneas del mismo nodo cliente, y puede que impidan que las operaciones de almacenamiento de datos obtengan puntos de montaje.

En el caso de los volúmenes de una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA, el servidor puede disponer, simultáneamente, de varias sesiones que lean y de un único proceso que grabe en el mismo volumen. Para aumentar la concurrencia y proporcionar un acceso eficiente para nodos que tienen datos en agrupaciones de almacenamiento FILE o CENTERA, incremente el valor del parámetro MAXNUMMP.

En nodos que almacenan datos en agrupaciones de almacenamiento primarias con la función de grabación simultánea activada, deberá ajustar el valor del parámetro MAXNUMMP para especificar el número correcto de puntos de montaje de cada sesión de cliente. Una sesión de cliente requiere un punto de montaje para la agrupación de almacenamiento primario y un punto de montaje para cada agrupación de almacenamiento de copias y cada agrupación de datos activos.

Para una copia de seguridad de servidor a servidor, si un servidor se encuentra en una versión diferente de la de otro servidor, establezca el número de puntos de montaje en el servidor de destino en un valor superior a uno. De lo contrario, recibirá un error.

Un agente de almacenamiento hace un seguimiento del número de puntos empleados durante una sesión de cliente de forma independiente. Si un nodo tiene un agente de almacenamiento que se ha instalado, puede superar el valor de MAXNUMMP. El valor MAXNUMMP puede superarse también en condiciones en que el nodo no tiene que esperar un punto de montaje.



Nota: El servidor puede tomar el control de la operación de un cliente para una operación de prioridad superior y el cliente puede perder un punto de montaje si no hay ningún otro punto de montaje disponible.

#### KEEPMP

Especifica si el nodo cliente mantiene el punto de montaje durante toda la sesión. El parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

##### Yes

Especifica que el nodo cliente debe retener el punto de montaje durante toda la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se retendrán los puntos de montaje que mantenga la sesión.

##### No

Especifica que el nodo de cliente libera el punto de montaje durante la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se publicarán los puntos de montaje que mantenga la sesión.

#### AUTOFSRename

Especifique si el nombre de los espacios de archivos ha de cambiarse automáticamente al actualizar el sistema cliente para el soporte de Unicode o especifique si el cliente ha de realizar, si es necesario, el cambio del nombre de los espacios de archivos. El parámetro es opcional. El valor predeterminado es NO. El establecimiento del parámetro en YES activa el cambio automático del nombre, que tiene lugar cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. El cambio automático del nombre cambia los nombres de los espacios de archivos existentes de los que se ha realizado una copia de seguridad y que no están en Unicode en el almacenamiento del servidor. A continuación, se realiza una copia de seguridad de los espacios de archivos en Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS X y NetWare.

Una vez que se ha instalado el cliente que admite Unicode, los nuevos espacios de archivos de los que el cliente hace una copia de seguridad se almacenan en el almacenamiento del servidor utilizando la página de códigos UTF-8. UTF-8 es un formato de codificación orientado a bytes que especifica el estándar de Unicode.

Puede especificar uno de los siguientes valores:

##### Yes

El nombre de los espacios de archivos existentes se cambia automáticamente al actualizar a un cliente que admite Unicode y cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental o copia de seguridad parcial incremental. La red denominación se produce si el cliente utiliza una interfaz gráfica de usuario, la línea de comandos o el planificador cliente. Por ejemplo, el servidor red denomina una unidad del siguiente modo:

```
Nombre original: D_DRIVE  
Nombre nuevo: D_DRIVE_OLD
```

El nombre nuevo indica que el espacio de archivos se almacena en el servidor en un formato que no es Unicode.

##### No

Los espacios de archivos no se red denominan automáticamente cuando el sistema cliente se actualiza a un cliente que admite Unicode y el cliente ejecuta una de las siguientes operaciones: archivado, copia de seguridad selectiva, copia de seguridad incremental o copia de seguridad parcial incremental.

##### Client

La opción AUTOFSRENAME en el archivo de opciones del cliente determina si los espacios de archivos están red denominados.

De forma predeterminada, la opción de cliente se define en PROMPT. Cuando el sistema cliente se actualiza en un cliente compatible con Unicode y el cliente realiza una operación de IBM Spectrum Protect con la interfaz gráfica de usuario o la línea de mandatos, el programa pregunta una vez al usuario si desea cambiar el nombre los espacios de archivos.

Cuando el planificador cliente realiza una operación, el programa no ofrece ninguna solicitud sobre red denominación y no red denomina los espacios de archivos. Las copias de seguridad de los espacios de archivos existentes se envían como antes (no en Unicode).

#### VALIDateprotocol (en desuso)

Especifica si IBM Spectrum Protect completa una comprobación de redundancia cíclica para validar los datos que se han enviado entre el cliente y el servidor. El parámetro es opcional. El valor predeterminado es NO.

Importante: A partir de V8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

#### TXNGroupmax

Especifica el número de archivos por validación de transacción que se transfieren entre un cliente y un servidor. El parámetro es opcional. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.

El valor predeterminado es 0. Al especificar 0 se indica que el nodo utiliza el valor global del servidor que se ha establecido en el archivo de opciones del servidor. Si desea emplear un valor distinto del valor global del servidor, especifique un valor entre 4 y 65.000 para este parámetro. El valor del nodo prevalece sobre el valor del servidor.

Atención: Si aumenta el valor de TXNGROUPMAX, aumenta la utilización del registro de recuperación. Una mayor utilización del registro de recuperación puede incrementar el riesgo de quedarse sin espacio de registro. Evalúe el rendimiento de cada uno de los nodos antes de cambiar este parámetro.

#### DATAWritepath

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento tales como copia de seguridad o archivado. El parámetro es opcional. El valor predeterminado es ANY.

Nota: Si no hay disponible una ruta, el nodo no puede enviar ningún dato. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará.

Puede especificar uno de los siguientes valores:

##### ANY

Especifica que los datos se envían al servidor, agente de almacenamiento o a ambos por medio de cualquier ruta disponible. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se mueven mediante la LAN.

##### LAN

Especifica que los datos se envían utilizando la LAN.

##### LANFree

Especifica que los datos se envían utilizando una ruta fuera de la LAN.

#### DATAReadpath

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. El parámetro es opcional. El valor predeterminado es ANY.

Nota: Si no hay disponible una ruta, no es posible leer datos. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará. El valor de la vía de acceso de transferencia también se aplica a las conexiones de migración tras error. Si el valor se establece en LANFree, puede producirse la migración tras error para el nodo en el servidor secundario.

Puede especificar uno de los siguientes valores:

##### ANY

Especifica que el servidor, agente de almacenamiento o ambos utilizan cualquier ruta disponible para leer datos. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se leen utilizando la LAN.

##### LAN

Especifica que los datos se leen utilizando la LAN.

##### LANFree

Especifica que los datos se leen utilizando una ruta fuera de la LAN.

#### TARGETLevel

Especifica el paquete de despliegue del cliente que se utiliza este nodo. Puede sustituir con un paquete de release aplicable Version.Release.Modification.Fix (V.R.M.F) Level. Por ejemplo: `TARGETLevel=6.2.0.0`.

Debe especificar cada segmento con un número aplicable a un paquete de despliegue. No se puede utilizar el asterisco en ningún campo como sustituto de un número válido. El parámetro es opcional.

Restricción: El parámetro TARGETLEVEL no se aplica a los nodos con un tipo NAS o SERVER.

#### SESSIONInitiation

Controla si el servidor o el cliente ha de iniciar las sesiones. El valor predeterminado establece que el cliente ha de iniciar las sesiones. El parámetro es opcional.

##### Clientserver

Especifica que el cliente puede iniciar sesiones con el servidor comunicándose en el puerto TCP/IP que se ha definido con la opción de servidor TCPPOINT. También puede utilizarse la planificación por petición de servidor para solicitar al cliente que se conecte con el servidor.

##### SERVEROnly

Especifica que el servidor no acepta peticiones de sesiones del cliente. Todas las sesiones deberá iniciarlas la planificación por petición de servidor en el puerto que se ha definido para el cliente con los mandatos REGISTER o

UPDATE NODE. No se puede utilizar Client Acceptor, dsmscad, para iniciar el planificador si SESSIONINITIATION está establecido en SERVERONLY.

#### HLAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

#### LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

#### EMAILAddress

Este parámetro se utiliza para obtener más información de contacto. El parámetro es opcional. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

#### DEDUPLICATION

Especifica dónde puede producirse la eliminación de datos duplicados para este nodo. El parámetro es opcional. Puede especificar uno de los siguientes valores:

##### Clientserver

Indica que los datos almacenados por este nodo se pueden deduplicar en el cliente o en el servidor. Este es el valor predeterminado. Para realizar la eliminación de datos duplicados en el cliente, debe especificar el valor YES en la opción de cliente DEDUPLICATION. Puede especificar esta opción en el archivo de opciones del cliente o en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

##### SERVEROnly

Especifica que los datos almacenados por este nodo sólo se pueden deduplicar en el servidor.

#### BACKUPINITIATION

Especifica si el ID de usuario no root en el nodo de cliente puede realizar una copia de seguridad de los archivos en el servidor. El parámetro es opcional. El valor predeterminado es ALL, que indica que los ID de usuario no root pueden realizar una copia de seguridad de los datos en el servidor. Puede seleccionar uno de los siguientes valores:

##### All

Especifica que los ID de usuario no root pueden realizar una copia de seguridad de los archivos en el servidor. ALL es el valor predeterminado si no se especifica BACKUPINITIATION.

##### ROOT

Especifica que el ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor. Si utiliza el cliente de copia de seguridad-archivador V6.4 o posterior, los usuarios autorizados tiene los mismos privilegios que el ID de usuario root.

Restricción: El servidor ignora el atributo si el cliente de archivado y copia de seguridad se conecta desde un sistema operativo distinto de AIX, Linux, Solaris o Mac OS.

Recuerde: La interfaz de programación de aplicaciones (API) se ve afectada por el parámetro BACKUPINITIATION en el servidor. De forma predeterminada, a todos los usuarios de la API se les permite realizar una copia de seguridad de los datos. No se recomienda establecer el parámetro en ROOT en un nodo de la API.

#### REPLState

Especifica si los datos que pertenecen al nodo de cliente están preparados para replicarse. Este parámetro es opcional.

Especifica este parámetro sólo si emite el comando REGISTER NODE en un servidor que está configurado para replicar datos en un servidor de réplica de destino. Si registra un nodo de cliente en un servidor de réplica de origen y configura la réplica para el nodo, no registre el nodo en el servidor de réplica de destino. El nodo de cliente se crea automáticamente en el servidor de destino la primera vez que se produce la réplica.

Puede seleccionar uno de los siguientes valores:

##### Enabled

Especifica que el nodo de cliente está configurado para la réplica y preparado para replicarse. Cuando especifica este parámetro, la modalidad de réplica en la definición de nodo de cliente en el servidor de réplica de origen se establece automáticamente en SEND. Este valor indica que los datos que pertenecen al nodo de cliente se envían a un servidor de destino durante la réplica.

Cuando se realiza la réplica por primera vez para el nodo de cliente, el estado de réplica del nodo en el servidor de réplica de destino se establece automáticamente en ENABLED. La modalidad de réplica en el servidor de réplica de destino se establece en RECEIVE. Este valor indica que los datos que pertenecen al nodo de cliente se reciben de un servidor de réplica de origen. Para determinar la modalidad y el estado de la réplica, emita el comando QUERY NODE en un servidor de réplica de origen o destino.

#### DISabled

Especifica que el nodo está configurado para la réplica, pero que la réplica no se produce hasta que la activa.

#### BKREPLRuledefault, ARREPLRuledefault, y SPREPLRuledefault

Especifica la regla de réplica que se aplica a un tipo de datos si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT.

Restricción: Sólo puede especificar el parámetro BKREPLRULEDEFAULT, ARREPLRULEDEFAULT o SPREPLRULEDEFAULT si especifica el parámetro REPLSTATE.

#### BKREPLRuledefault

Especifica la regla de réplica de los datos de copia de seguridad.

#### ARREPLRuledefault

Especifica la regla de réplica de los datos de archivado.

#### SPREPLRuledefault

Especifica la regla de réplica de los datos gestionados por espacio.

Si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT y no especifica una regla para el parámetro BKREPLRULEDEFAULT, ARREPLRULEDEFAULT o SPREPLRULEDEFAULT, los datos se replican según la regla de servidor del tipo de datos.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Puede especificar las siguientes reglas:

#### ALL\_DATA

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad normal.

#### ACTIVE\_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal. Esta regla sólo es válida para BKREPLRULEDEFAULT.

Atención:

Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando se instala una versión anterior a la Versión 7.1.1 en los servidores de réplica de origen o de destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro FORCERECONCILE=YES.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la duplicación, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino de una versión anterior a V7.1.1.

Si las condiciones anteriores no son verdaderas, se duplican todos los archivos nuevos y cambiados desde la última réplica, incluidos los archivos inactivos, y los archivos se suprimen cuando caducan.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad alta.

#### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta. Esta regla sólo es válida para BKREPLRULEDEFAULT.

#### DEFAULT

Replica los datos según la regla de réplica del servidor para los datos de copia de seguridad.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es

especificar `ARREPLRULEDEFAULT=DEFAULT`. Asegúrese de que las reglas de espacio de archivos de los datos de archivado también se establezcan en `DEFAULT` y que la regla del servidor de los datos de archivado se establezca en `ALL_DATA_HIGH_PRIORITY`.

Restricción: Si se configura un nodo para la réplica, las reglas de espacio de archivos se establecen en `DEFAULT` después de que el nodo almacene datos en el servidor de réplica de origen.

#### NONE

Los datos del tipo especificado no se replican.

Por ejemplo, si no desea replicar los datos gestionados por espacio que pertenecen a un nodo de cliente, especifique `SREPLRULEDEFAULT=NONE`

#### RECOVERDAMAGED

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino. El parámetro es opcional. El valor predeterminado es `YES`. Puede especificar uno de los siguientes valores:

##### Yes

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino está habilitada para este nodo.

##### No

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino no está habilitada para este nodo.

Consejo: El valor del parámetro `RECOVERDAMAGED` es sólo uno de varios valores que determinan si se recuperan los archivos dañados. Para obtener información sobre cómo especificar los valores, consulte Valores que afectan a la recuperación de archivos dañados.

#### ROLEOVERRIDE

Especifica si se debe alterar temporalmente el rol notificado del cliente para la creación de informes de estimación de unidades de valor de procesador (PVU). El valor predeterminado es `USEREPORTED`. El parámetro es opcional.

El rol notificado por el cliente es un dispositivo de cliente (por ejemplo, una estación de trabajo) o un dispositivo de servidor (por ejemplo, un servidor de archivos/impresión, un servidor de aplicaciones o una base de datos). De forma predeterminada, el cliente notifica su rol basándose en el tipo de cliente y el sistema operativo. Todos los clientes notifican inicialmente su rol como dispositivo de servidor, excepto los clientes de archivado y copia de seguridad que ejecutan distribuciones de estaciones de trabajo de Microsoft Windows (Windows Vista) y Macintosh OS X.

Especifique uno de los siguientes valores:

##### Client

Especifica un dispositivo de cliente.

##### Server

Especifica un dispositivo de servidor.

##### Otro

Especifica que este nodo no se va a utilizar para la creación de informes de estimaciones de PVU. Este valor puede ser útil cuando se despliegan múltiples nodos para un sistema físico (por ejemplo, entornos virtuales, nodos de prueba, nodos retirados y nodos que no estén en producción ni en clúster).

##### Userreported

Utilice el rol notificado que proporciona el cliente.

#### AUTHentication

Este parámetro especifica el método de autenticación de contraseña para el nodo. Especifique uno de los siguientes valores: `LDAP` o `LOCAL`. El parámetro es opcional y toma el valor predeterminado `LOCAL`. El valor predeterminado se puede cambiar a `LDAP` si se utiliza el mandato `SET DEFAULTAUTHENTICATION` y especifica `LDAP`.

##### Local

Especifica que se está utilizando la base de datos del servidor IBM Spectrum Protect .

##### LDap

Especifica que el nodo utiliza un servidor LDAP para la autenticación de contraseñas.

#### SSLrequired (en desuso)

Especifica si el nodo debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect . El parámetro es opcional. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red

Importante: A partir de V8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro `SESSIONSECURITY`. El parámetro `SSLREQUIRED` se ignora.

Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

#### SESSIONSECURITY

Especifica si el nodo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

#### STRICT

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el nodo. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el nodo pueda autenticarse en el servidor:

- Tanto el nodo como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el nodo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el nodo.

Los nodos que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

#### TRANSITIONAL

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el nodo no cumplen nunca los requisitos para el valor STRICT, el nodo continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un nodo cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el nodo ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, el nodo ya no se puede autenticar con un protocolo menos seguro. Por ejemplo, si se actualiza un nodo que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, cuando el nodo se autentica en el servidor IBM Spectrum Protect como nodo de otro servidor.

#### SPLITLARGEObjects

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. El parámetro es opcional. Si se especifica Sí, el servidor divide los objetos grandes (más de 10 GB) en partes más pequeñas cuando se almacenan en un nodo de cliente. Si se especifica No, se ignora este proceso. Especifique No solo si lo que pretende es maximizar el rendimiento de las copias de seguridad directamente en la cinta. El valor predeterminado es Yes (sí).

## Ejemplo: registrar un nodo de cliente del que sólo puede hacer una copia de seguridad el usuario root

---

Registre el nodo de cliente `meteOrite` con la contraseña `KingK0ng` para permitir que sólo el usuario `root` pueda realizar una copia de seguridad de los archivos en el servidor.

```
register node meteOrite KingK0ng
backupinit=root
```

## Ejemplo: registrar un nodo cliente y una contraseña y activar la compresión

---

Registrar el nodo cliente `JOEOS2` con la contraseña `SECRETCODE` y asignar este nodo al dominio de políticas `DOM1`. Este nodo puede suprimir sus propias copias de seguridad y copias archivadas del servidor. Todos los archivos los comprime el nodo cliente antes de enviarlos al servidor. Este comando creará automáticamente el identificador de usuario de administración `JOEOS2` con la contraseña `SECRETCODE`. Asimismo, el administrador ahora dispondrá de autorización de propietario de cliente para el nodo `JOEOS2`.

```
register node joeos2 secretcode domain=dom1
archdelete=yes backdelete=yes
compression=yes
```

## Ejemplo: otorgar autorización de propietario de cliente a un usuario de administración existente

---

Otorgar autorización de propietario de cliente a un ID de usuario de administración existente, `HELADMIN`, al registrar el nodo cliente `JAN`. Este paso no creará automáticamente un ID de administrador denominado `JAN`, sino que otorgará autorización de propietario de cliente para este nodo al administrador `HELADMIN`.

```
register node jan pwdsafe userid=helpadmin
```

## Ejemplo: registrar un nodo servidor de archivos que utiliza operaciones NDMP

---

Registrar el nombre de nodo `NAS1` para un servidor de archivos NAS que utiliza operaciones NDMP. Asignar este nodo a un dominio NAS especial.

```
register node nas1 pw4pw domain=nasdom type=nas
```

## Ejemplo: registrar un nodo y especificar el número máximo de archivos por validación de transacción

---

Registrar el nombre de nodo `ED` y establecer el valor `TXNGroupmax` en 1.000.

```
register node ed pw45twx txngroupmax=1000
```

## Ejemplo: registrar un nodo y permitirle eliminar duplicados en el sistema cliente

---

Registre el nombre de nodo `JIM` y permítale eliminar duplicados de datos en el sistema cliente.

```
register node jim jim deduplication=clientorserver
```

## Ejemplo: registrar un nombre de nodo ED y establecer el rol como un dispositivo de servidor para la creación de informes de estimación de PVU

---

Registre un nombre de nodo `ED` y establezca el rol como un dispositivo de servidor para la creación de informes de estimación de PVU.

```
register node ed pw45twx roleoverride=server
```

## Ejemplo: registrar un nodo en un servidor de réplica de origen

---

Defina `NODE1` en un servidor de réplica de origen. Especifique una regla de réplica para los datos de copia de seguridad que pertenecen a `NODE1`, para que los datos de copia de seguridad activos se repliquen con una prioridad alta. Active la réplica para el nodo.

```
register node node1 bkreplruledefault=active_data_high_priority replstate=enabled
```

## Ejemplo: registrar un nodo que se autentique mediante un servidor LDAP

---

Registre un nombre de nodo de `NODE17` que debe autenticarse con un servidor LDAP.

```
register node node17 authentication=ldap
```

Consejo: Al registrar un nodo de esta forma, no se crea un ID de usuario de administración.

## Ejemplo: Registrar un nodo para comunicarse con un servidor utilizando la seguridad de sesión transitoria.

---

Registre un nombre de nodo, `NODE4`, para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
register node node4 sessionsecurity=strict
```

## Ejemplo: Registrar un nodo y habilitar la recuperación de archivos dañados

---

Registrar un nombre de nodo `PAYROLL`. Para el nodo `PAYROLL`, habilite la recuperación de archivos dañados a partir de un servidor de réplica de destino.

```
register node payroll recoverdamaged=yes
```

## Comandos relacionados


---

Tabla 2. Comandos relacionados con REGISTER NODE

Comando	Descripción
DEFINE ASSOCIATION	Asocia los clientes a una planificación.
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.

Comando	Descripción
DEFINE MACHNODEASSOCIATION	Asocia un nodo de IBM Spectrum Protect a una máquina.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.
RENAME NODE	Cambia el nombre de un nodo cliente.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET CPUINFOREFRESH	Especifica el número de días entre exploraciones de cliente para la información de estación de trabajo utilizada para las estimaciones de PVU.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UNLOCK NODE	Permite que un usuario bloqueado de un dominio de políticas específico acceda al servidor.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

**Conceptos relacionados:**

 Cliente raíz de UNIX y Linux y tareas de usuario autorizadas




**Información relacionada:**

Opción de cliente SSL

## Comandos REMOVE

Utilice los mandatos REMOVE para eliminar un objeto de IBM Spectrum Protect.



- REMOVE ADMIN (Suprimir un ID de usuario administrador)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)
- REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)
- REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)
- REMOVE REPLSERVER (Eliminar un servidor de réplica)

## REMOVE ADMIN (Suprimir un ID de usuario administrador)

Utilice este comando para suprimir un ID de usuario administrador del sistema.

No puede eliminar el ID de usuario administrador del sistema o el ID administrativo SERVER\_CONSOLE del sistema.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-REMOve Admin--nombre_admin--+-----+-----+>>
      .-SYNCldapdelete-----No-----
      '-SYNCldapdelete-----+No--+-'
                          '-Yes-'
```

### Parámetros

nombre\_admin (Necesario)

Especifica el ID de usuario administrador que se ha de eliminar.

SYNCldapdelete

Especifica si desea suprimir el ID de usuario de administración en el servidor LDAP (Lightweight Directory Access Protocol).

Sí

Suprime el ID de usuario de administración en el servidor LDAP.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

No suprime el ID de usuario de administración en el servidor LDAP. Este es el valor predeterminado.

### Ejemplo: Suprimir un ID de usuario administrador




Suprima el ID de usuario administrador larry que no está definido en un servidor LDAP. Emita el comando siguiente:

```
remove admin larry
```

### Comandos relacionados

Tabla 1. Comandos relacionados con REMOVE ADMIN

Comando	Descripción
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

# REMOVE DAMAGED (Eliminar los datos dañados de una agrupación de almacenamiento de origen)

Tras la conversión de la agrupación de almacenamiento, utilice este mandato para eliminar los datos dañados de una agrupación de almacenamiento que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL).

El mandato REMOVE DAMAGED suprime de forma permanente los datos dañados de la agrupación de almacenamiento. Consejo: antes de eliminar los datos dañados de la agrupación de almacenamiento, intente recuperar una versión sin daños de los datos de una agrupación de almacenamiento de copia o de datos activos emitiendo el mandato RESTORE STGPOOL. Recupere una versión sin daños de los datos de un servidor de réplica de destino emitiendo el mandato REPLICATE NODE y especificando el parámetro RECOVERDAMAGED=YES.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de almacenamiento restringido.

## Sintaxis

```
>>-REMOve DAMAged--nombre_agrupación .-*----- .
| .-,'-----' |
| V          | |
'---nombre_nodo-+-'

.-Wait----No-----
>-----+-----><
'-Wait----+No--+-'
          '-Yes-'
```

## Parámetros

- nombre\_agrupación (Obligatorio)**  
Especifique una agrupación de almacenamiento primario que utilice una clase de dispositivo FILE, una clase de dispositivo de cinta o una biblioteca virtual de cintas (VTL). La agrupación de almacenamiento contiene los datos dañados. Este parámetro es obligatorio.
- nombre\_nodo**  
Especifica el nombre del nodo cliente. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar un carácter comodín en lugar de un nombre de nodo si desea eliminar daños de todos los nodos de la agrupación de almacenamiento.
- Wait**  
Especifica si se debe esperar al servidor para eliminar datos dañados de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar este parámetro solamente desde una línea de mandatos administrativa. Puede especificar uno de los siguientes valores:
  - No**  
Especifica que el mandato se procesa de forma subordinada.
  - Yes**  
Especifica que el mandato se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

## Ejemplo: eliminar datos dañados de una agrupación de almacenamiento y esperar a que el servidor complete el proceso

Eliminar los datos dañados de una agrupación de almacenamiento llamada POOL1 y esperar a que el servidor complete el proceso en primer plano.

```
remove damaged pool1 wait=yes
```

Tabla 1. Mandatos relacionados con REMOVE DAMAGED

Comando	Descripción
CONVERT STGPOOL	Convertir una agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio.

Comando	Descripción
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.

## REMOVE NODE (Eliminar un nodo o un nodo asociado a una máquina)

Utilice este comando para suprimir un nodo del servidor. Si está utilizando el gestor de recuperación ante siniestro y el nodo que se ha de suprimir está asociado a una máquina, se suprimirá también la asociación entre el nodo y la máquina.

Si el nodo es miembro de un grupo de proximidad y elimina el nodo del servidor, el nodo también se elimina del grupo de proximidad. Si se elimina un nodo y este contenía espacios de archivos en un grupo de proximidad de espacio de archivos, estos espacios de archivos se eliminan de la lista de miembros del grupo.

Si elimina un nodo que almacenó datos en una agrupación de almacenamiento de duplicados eliminados, el nombre del nodo DELETED se visualiza en la salida del mandato QUERY OCCUPANCY hasta que todas las dependencias de eliminación de duplicados de datos se eliminan.

Cuando se elimina un nodo, el ID de administración correspondiente se elimina solamente si se cumplen las condiciones siguientes:

- El nombre del administrador es idéntico al nombre del nodo.
- El administrador tiene autorización de propietario de cliente o de acceso a cliente *solo* para el nodo que se elimina.
- El administrador no es un objeto gestionado.

Para poder suprimir un nodo, debe suprimir todos los espacios de copia de seguridad y copia archivada que pertenezcan a dicho nodo. Antes de poder eliminar un nodo NAS que tenga un transportador de datos correspondiente, debe completar las tareas siguientes en orden:

1. Suprimir las rutas desde el transportador de datos
2. Suprimir el transportador de datos
3. Suprimir todas las definiciones de espacio de archivos virtual para el nodo
4. Eliminar el nodo NAS

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol): La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

### Sintaxis

```

>>-REMOve Node--nombre_nodo--+-SYNCldapdelete-----No-----+-----<<
                               '-SYNCldapdelete-----+No---+'
                               '-Yes-'

```

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo que se ha de suprimir.

SYNCldapdelete

Especifica si debe eliminarse el nodo del servidor LDAP (Lightweight Directory Access Protocol).

Sí

Especifica que el nodo se elimina.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que el nodo no se elimina. Este es el valor predeterminado.









## Ejemplo: eliminar un nodo cliente

Eliminar el nodo cliente LARRY.

```
remove node larry
```

## Comandos relacionados

Tabla 1. Comandos relacionados con REMOVE NODE

Comando	Descripción
  DELETE MACHNODEASSOCIATION	  Suprime la asociación entre una máquina y un nodo.
DELETE DATAMOVER	Suprimir un transportador de datos.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE PATH	Suprime una ruta de un origen a un destino.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY COLLOGGROUP	Muestra información acerca de los grupos de proximidad.
  QUERY MACHINE	  Muestra información sobre máquinas.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SESSION	Muestra información sobre todas las sesiones activas de administrador y de cliente con IBM Spectrum Protect.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RENAME NODE	Cambia el nombre de un nodo cliente.

## REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)

Utilice este mandato para eliminar un nodo de la réplica si ya no desea replicar los datos que pertenecen al nodo.

No puede suprimirse los datos del nodo cliente emitiendo el mandato REMOVE REPLNODE. Puede emitir el mandato en un servidor de réplica de origen o de destino. Sólo se puede emitir este mandato desde el cliente de línea de mandatos administrativos. Este mandato no se puede emitir en la consola del servidor.

Si emite el comando REMOVE REPLNODE para un nodo de cliente cuyo nodo de réplica está establecido en SEND o RECEIVE, la modalidad se establece en NONE. El estado de réplica también se establece en NONE. Después de eliminar un nodo de cliente de la réplica, el servidor de réplica de destino puede aceptar los datos de copia de seguridad, archivado y gestionados por espacio directamente desde el nodo.

Si un nodo de cliente se elimina de la réplica, se suprime la información en la base de datos sobre la réplica del nodo. Si el nodo de cliente se activa para la réplica más adelante, el proceso de réplica replica todos los datos especificados por los valores y las reglas de réplica.

Al emitir el comando REMOVE REPLNODE, los datos que pertenecen a un nodo de cliente no se suprimen. Para suprimir los datos del espacio de archivos que pertenecen al nodo de cliente, emita el mandato DELETE FILESPACE para cada uno de los espacios de archivos que pertenecen al nodo. Si no desea mantener la definición de nodo de cliente, emita el mandato REMOVE NODE. Para suprimir los datos del espacio de archivos y la definición de nodo de cliente, emita DELETE FILESPACE y REMOVE NODE en el servidor de réplica de destino.

Restricción: Si se está ejecutando un proceso de réplica de nodo para un nodo de cliente especificado por este mandato, el mandato falla y la información de réplica del nodo no se elimina.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

## Sintaxis

```
      .------  
      v                                     |  
>>-REMOve REPLNode-----+--nombre_nodo-----+-----><  
                          '-nombre_grupo_nodos-'
```

## Parámetros

nombre\_nodo o nombre\_grupo\_nodos (Necesario)

Especifica el nombre del nodo de cliente y del grupo definido de nodos de cliente que desea eliminar de la réplica. Para especificar varios nombres de nodos de cliente y nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede utilizar caracteres comodín para especificar los nombres de nodos de cliente, pero no para especificar los nombres de grupos de nodos de cliente. No puede combinar nombres de nodo o grupo de nodos con el nombre de dominio.

## Ejemplo: eliminar tres nodos de cliente y un grupo de nodos de cliente de la réplica

Los nombres de los nodos cliente son NODE1, NODE2 y NODE3. El nombre del grupo de nodos de cliente es PAYROLL. Emita el siguiente comando en los servidores de réplica de origen y destino:

```
remove replnode node*,payroll
```

## Comandos relacionados

Tabla 1. Comandos relacionados con REMOVE REPLNODE

Comando	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.

## REMOVE REPLSERVER (Eliminar un servidor de réplica)

Utilice este mandato para eliminar o cambiar un servidor de réplica de la lista de servidores de réplica. Este mandato suprime toda la información que existe sobre el estado de la réplica de todos los nodos que se ha copiado en el servidor.

Puede emitir el mandato en un servidor de réplica de origen o de destino.

Restricción: No puede suprimirse los datos del nodo cliente emitiendo el mandato REMOVE REPLSERVER.

Utilice el mandato para conmutar servidores de réplica y eliminar información de réplica de un servidor anterior. El mandato no afecta a la modalidad de réplica ni al estado actual de todas las definiciones de nodo. Emita el mandato en los servidores de origen y de destino para mantener la coherencia de la información de estado de réplica sobre ambos servidores.

Restricción: Si especifica el servidor de réplica predeterminado en el mandato REMOVE REPLSERVER y un proceso de réplica de nodo está en ejecución, el mandato falla y no se elimina ninguna información de réplica.

Este mandato se ejecuta como una operación en segundo plano y no se puede cancelar. IBM Spectrum Protect suprime información de duplicación que está asociada al servidor especificado, como por ejemplo, una serie de transacciones de base de datos por lotes. Si se produce un problema en el sistema, puede realizarse una supresión parcial.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-REMOve REPLServer--GUID-----><
```

## Parámetros

---

guid\_ réplica (Obligatorio)

Identificador único del servidor de réplica que va a eliminarse. Puede utilizar caracteres comodín para especificar el Identifier exclusivo global de réplica (GUID); sin embargo, solamente puede coincidir un GUID con el comodín. Si la secuencia comodín coincide con más de un GUID, el mandato falla. Debe calificar la serie comodín solamente hasta que se encuentre el GUID que desea suprimir.

## Ejemplo: utilizar un comodín para eliminar un servidor de réplica

---

Elimine un servidor de réplica utilizando un carácter comodín para indicar el GUID de la réplica.

```
remove replserver e*
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con REMOVE REPLSERVER

Comando	Descripción
REMOVE REPLNODE (Eliminar un nodo de cliente de la réplica)	Elimina un nodo de la réplica.
QUERY REPLSERVER (Consultar un servidor de réplica)	Muestra información sobre servidores de réplica.

## Comandos RENAME

---

Utilice los comandos RENAME para cambiar el nombre de un objeto existente.

- RENAME ADMIN (redenominar un administrador)
- RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)
- RENAME NODE (Cambiar el nombre de un nodo)
- RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)
- RENAME SERVERGROUP (Redenominar un grupo de servidores)
- RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)

## RENAME ADMIN (redenominar un administrador)

---

Utilice este comando para cambiar un ID de usuario administrador. No se modificará la información existente para este administrador, como por ejemplo la información de contacto y las clases de privilegios.

Si asigna un ID de usuario de administración existente a otra persona, utilice el mandato UPDATE ADMIN para cambiar la contraseña.

Cuando un administrador y un nodo comparten nombres y cambia el método de autenticación de administrador, el método de autenticación de nodo también cambia. Si cambia el nombre de un administrador por el mismo nombre que un nodo existente, el método de autenticación y el valor SSLREQUIRED del nodo pueden cambiar. Si estos valores son diferentes, después del cambio de nombre, tanto el administrador y el nodo tendrá el mismo método de autenticación y el mismo valor SSLREQUIRED.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Al cambiar el nombre de un ID de usuario de administración, tenga cuidado de que no coincida con un nombre de nodo. Si los nombres coinciden, es posible que se dé un comportamiento imprevisto, debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría pasar que la actualización de la contraseña fallase.

No puede redenominar el ID de administración SERVER\_CONSOLE.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-REName Admin--nombre_admin_actual--nombre_admin_nuevo----->
.-SYNCLdapdelete---No-----,
>+-----+-----><
'-SYNCLdapdelete---No---+'
'-Yes-'
```

## Parámetros

nombre\_admin\_actual (Obligatorio)

Especifica el ID de usuario administrador cuyo nombre se ha de cambiar.

nombre\_admin\_nuevo (Obligatorio)

Especifica el nuevo ID de usuario administrador. La longitud máxima del nombre es de 64 caracteres.

SYNCLdapdelete

Especifica si desea suprimir el ID de usuario de administración en el servidor LDAP (Lightweight Directory Access Protocol) y sustituir el ID por uno nuevo.

Yes

Suprime el ID de usuario de administración en el servidor LDAP y lo sustituye por un ID nuevo.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

No suprime ni sustituye el ID de usuario de administración en el servidor LDAP. Este es el valor predeterminado.

## Ejemplo: cambiar el nombre de un administrador

Redenominar el administrador de IBM Spectrum Protect CLAUDIA como BILL.

```
rename admin claudia bill
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RENAME ADMIN

Comando	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.

## RENAME FILESPACE (Redenominar un espacio de archivos de cliente del servidor)

Utilice este mandato para redenominar un espacio de archivos de cliente existente en el servidor por un nuevo nombre de espacio de archivos o para redenominar espacios de archivos importados.

Puede que desee cambiar el nombre de un espacio de archivos que se ha importado o crear nuevos espacios de archivos activados para Unicode para clientes activados para Unicode.

Restricción: No cambie el nombre de los espacios de archivos NAS o VMware. Si cambia el nombre del espacio de archivos NAS o VMware, dejará de estar visible y no se puede restaurar. Para restaurar un espacio de archivos NAS o VMware renombrado, debe restablecer su nombre original y definir el parámetro force de la siguiente manera: force=yes

## Clase de privilegio

Puede emitir este comando un administrador con autorización de políticas ilimitada o con autorización de políticas limitada sobre el dominio de políticas del cliente.

## Sintaxis

```
>>-REName Filespace--nombre_nodo----->
```





servidor. Si la conversión no es satisfactoria, puede que desee especificar el parámetro HEXADECIMAL.  
HEXadecimal

El servidor interpreta el nombre de espacio de archivo especificado como la representación hexadecimal de un nombre en Unicode. La utilización de la representación hexadecimal asegura que el servidor pueda red denominar correctamente el espacio de archivos, independientemente de la página de códigos del servidor.

Para visualizar la representación hexadecimal de un nombre de espacio de archivos, puede utilizar el mandato QUERY FILESPACE con FORMAT=DETAILED.

Restricción: No puede especificar un nombre de nuevo de un tipo que sea distinto del nombre original. Puede red denominar un espacio de archivos que es Unicode a otro nombre en Unicode. Puede red denominar un espacio de archivos que no es Unicode utilizando un nuevo nombre en la página de códigos del servidor. No puede mezclar los dos tipos.

force

Para renombrar un espacio de archivos NAS o VMware, debe establecer este parámetro de la siguiente manera: force=yes

## Cambiar el nombre de un espacio de archivos importado para evitar la sobregrabación

Un nodo de cliente de AIX denominado LARRY ha realizado la copia de seguridad del espacio de archivos /r033 en el servidor de IBM Spectrum Protect. El espacio de archivos se ha exportado a cinta y después se ha reimportado al servidor. Al importarse este espacio de archivos, se ha creado un nombre generado por el sistema, /r031, para éste, pues /r033 ya existía para el nodo de cliente LARRY.

Sin embargo, el nodo cliente LARRY ya tenía un espacio de archivos denominado /r031 cuya copia de seguridad no se había realizado y, por lo tanto, el servidor lo desconocía. A menos que se cambie el nombre del espacio de archivos importado, éste recubrirá el espacio de archivos /r031, pues el nombre del espacio de archivos que ha generado la función IMPORT es igual al nombre de un espacio de archivos del nodo de cliente LARRY que el servidor desconoce.

Utilice el siguiente comando para cambiar el nombre del espacio de archivos importado /r031. El nuevo nombre, /imported-r033, identifica que el nuevo espacio de archivos es una imagen importada del espacio de archivos /r033.

```
rename file space larry /r031 /imported-r033
```

## Cambiar el nombre del espacio de archivos para crear un espacio de archivos activado para Unicode

El cliente JOE está utilizando un cliente de IBM Spectrum Protect activado para Unicode en inglés. JOE ha hecho copia de seguridad de varios espacios de archivos grandes que no son Unicode que está activado en el almacenamiento del servidor. El espacio de archivos \\joe\c\$ contiene algunos archivos con nombres de archivos en japonés cuya copia de seguridad no puede realizarse en un espacio de archivos que no esté activado para Unicode. Puesto que los espacios de archivos son de gran tamaño, el administrador no desea convertir ahora todos los espacios de archivos de JOE en espacios de archivos activados para Unicode. El administrador solamente desea cambiar el nombre del espacio de archivos que no es Unicode, \\joe\c\$, de modo que la próxima copia de seguridad del espacio de archivos dé lugar a la creación de un nuevo espacio de archivos activado para Unicode. El nuevo espacio de archivos activado para Unicode permitirá que se efectúe correctamente una copia de seguridad los archivos en japonés.

Utilice el siguiente mandato para cambiar el nombre \\joe\c\$:

```
rename file space joe \\joe\c$ \\joe\c$_old
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RENAME FILESPACE

Comando	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY OCCUPANCY	Muestra información de espacio de archivos según la agrupación de almacenamiento.

## RENAME NODE (Cambiar el nombre de un nodo)

---

Utilice este comando para cambiar el nombre de un nodo.

Si asigna un ID de nodo existente a otra persona, utilice el mandato UPDATE NODE para cambiar la contraseña.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- No cambie el nombre de un nodo para que coincida con un ID de usuario de administración existente. Si cambia el nombre de un nodo y este coincide con un ID de usuario de administración, podría darse un comportamiento imprevisto debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría pasar que la actualización de la contraseña fallase.

Restricciones:

- No es posible cambiar el nombre de un nodo NAS que tenga definido un transportador de datos correspondiente. Si el transportador de datos tiene rutas definidas, deben suprimirse primero.
- Si un nodo se configura para la réplica, no se puede renombrar.

Si cambia el nombre de un nodo por un nombre que tiene un administrador, el método de autenticación del administrador y el valor de SSLREQUIRED se actualizan para que coincidan con los del nodo. Cuando un nodo y un administrador comparten un nombre y cambia el método de autenticación del nodo o el valor SSLREQUIRED del nodo, los valores del administrador también cambian. Debe tener autorización de nivel de sistema para actualizar el método de autenticación del nodo o el valor SSLREQUIRED del nodo y también actualizar un administrador con el mismo nombre.

### Clase de privilegio

---

Debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

### Sintaxis

---

```
>>-REName Node--nombre_nodo_actual--nuevo_nombre_nodo----->
.-SYNClapdelete---No-----
>>+-----+----->>
'-SYNClapdelete---+No--+-'
      '-Yes-'
```

### Parámetros

---

nombre\_nodo\_actual (Obligatorio)

Especifica el nombre del nodo que debe cambiarse.

nombre\_nodo\_nuevo (Obligatorio)

Especifica el nuevo nombre del nodo. La longitud máxima es de 64 caracteres.

SYNClapdelete

Especifica si el nombre de nodo se suprime y se sustituye en el servidor LDAP (Lightweight Directory Access Protocol).

Sí

Especifica que el nombre de nodo se suprime y se sustituye.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

No

Especifica que el nombre de nodo no se suprime ni se sustituye. Este es el valor predeterminado.

### Ejemplo: cambiar el nombre de un nodo

---

Cambiar el nombre del nodo JOE por JOYCE.

```
rename node joe joyce
```

## Ejemplo: Cambiar el nombre de un nodo que comparte un espacio de nombres con otros servidores

Cambie el nombre del nodo de JOYCE a JOE sin suprimir el nombre anterior de los servidores LDAP correspondientes.

```
rename node joyce joe
```

### Comandos relacionados

Tabla 1. Comandos relacionados con RENAME NODE

Comando	Descripción
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

#### Tareas relacionadas:

Gestión de los nodos de servidor de archivos de NAS

## RENAME SCRIPT (cambie el nombre de un script de IBM Spectrum Protect)

Utilice este mandato para cambiar el nombre de un script de IBM Spectrum Protect.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de operador, políticas, almacenamiento o sistema.

### Sintaxis

```
>>-REName SCRIpt--nombre_script_actual--nombre_nuevo_script----<<
```

### Parámetros

nombre\_script\_actual (Obligatorio)

Especifica el nombre del script que se va a red denominar.

nombre\_script\_nuevo (Obligatorio)

Especifica el nuevo nombre del script. El nombre puede contener hasta 30 caracteres.

### Ejemplo: cambiar el nombre de un script

Redenominar SCRIPT1 con el nuevo nombre de script SCRIPT2.

```
rename script script1 script2
```

### Comandos relacionados

Tabla 1. Comandos relacionados con RENAME SCRIPT

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RUN	Ejecuta un script.
UPDATE SCRIPT	Cambia o añade líneas a un script.

## RENAME SERVERGROUP (Redenominar un grupo de servidores)

Utilice este comando para redenominar un grupo de servidores.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-REName SERVERGroup--nombre_grupo_actual--nombre_nuevo_grupo-><
```

## Parámetros

---

nombre\_grupo\_actual (Obligatorio)

Especifica el grupo de servidores que se redenomina.

nombre\_grupo\_nuevo (Obligatorio)

Especifica el nuevo nombre del grupo de servidores. La longitud máxima del nombre es de 64 caracteres.

## Ejemplo: cambiar el nombre de un grupo de servidores

---

Redenominar el grupo de servidores WEST\_COMPLEX como BIG\_WEST.

```
rename servergroup west_complex big_west
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con RENAME SERVERGROUP

Comando	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
UPDATE SERVERGROUP	Actualiza un grupo de servidores.

## RENAME STGPOOL (Cambiar el nombre de una agrupación de almacenamiento)

---

Utilice este mandato para cambiar el nombre de una agrupación de almacenamiento. Puede cambiar los nombres de agrupaciones de almacenamiento de forma que se utilicen los mismos nombres en un gestor de configuración y en sus servidores gestionados.

Al cambiar el nombre de una agrupación de almacenamiento, todos los administradores con privilegio de almacenamiento restringido para la agrupación de almacenamiento anterior retienen el privilegio de almacenamiento restringido para la agrupación de almacenamiento renombrada. Si la agrupación de almacenamiento renombrada se encuentra en una jerarquía de agrupaciones de almacenamiento, se conserva la jerarquía. Debe actualizar la clase de gestión o el grupo de copia para especificar el nuevo nombre de agrupación de almacenamiento como destino para los archivos.

Si hay procesos activos cuando se renombra una agrupación de almacenamiento, puede que se siga mostrando el nombre antiguo en los mensajes o consultas de esos procesos.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-REName STGpool--nombre_agrupación_actual--nuevo_nombre_agrupación-><
```

## Parámetros

---

nombre\_agrupación\_actual (Obligatorio)

Especifica la agrupación de almacenamiento que se redenomina.  
 nombre\_agrupación\_nueva (Obligatorio)  
 Especifica el nuevo nombre de la agrupación de almacenamiento. La longitud máxima del nombre es de 30 caracteres.

## Ejemplo: cambiar el nombre de una agrupación de almacenamiento




Redenominar la agrupación de almacenamiento STGPOOLA con el nombre STGPOOLB:

```
rename stgpool stgpoola stgpoolb
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RENAME STGPOOL

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## REPAIR STGPOOL (Reparar una agrupación de almacenamiento de contenedores de directorio)

Utilice este mandato para reparar extensiones con duplicados eliminados en una agrupación de almacenamiento de contenedores de directorio. Las extensiones con duplicados eliminados que están dañadas se reparan con extensiones de las que se ha hecho copia de seguridad en el servidor de réplica de destino o en las agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.

Restricciones:

- Sólo puede emitir el mandato REPAIR STGPOOL si ya ha emitido el mandato PROTECT STGPOOL para hacer una copia de seguridad de datos en otra agrupación de almacenamiento en un servidor de destino de réplica o en el mismo servidor.
- Cuando repara una agrupación de almacenamiento de contenedores de directorio del servidor de réplica, el mandato REPAIR STGPOOL falla cuando se produce cualquiera de las condiciones siguientes:
  - El servidor de destino no está disponible.
  - La agrupación de almacenamiento de destino está dañada.
  - Se produce una parada de red.
- Cuando repara una agrupación de almacenamiento de contenedores de directorio de agrupaciones de copia de contenedor, el mandato REPAIR STGPOOL falla cuando se produce cualquiera de las condiciones siguientes:
  - La agrupación de almacenamiento de copia de contenedor no está disponible.
  - La agrupación de almacenamiento de copia de contenedor está dañada.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis cuando el origen es el servidor de réplica

```
>>-REPAir STGPool--nombre_agrupación----->
      .-SRCLOCation----Replserver-.
>--+-----+-----+-----+-----+----->
      '-SRCLOCation----Replserver-'
```

```

.-MAXSESSions----1-----
>-----+----->
'-MAXSESSions-----número_sesiones--'

.-Preview ----No----- .-Wait----No-----
>-----+-----<
'-Preview-----+No--+-' '-Wait-----+No--+-'
'-Yes-' '-Yes-'

```

## Sintaxis cuando el origen es una agrupación de almacenamiento en el mismo servidor

```

>>-REPAir STGPool--nombre_agrupación--SRCLOcation-----Local----->

.-Preview ----No----- .-Wait----No-----
>-----+-----<
'-Preview-----+No--+-' '-Wait-----+No--+-'
'-Yes-' '-Yes-'

```

## Parámetros

### nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio que contiene los datos que se deben reparar.

### SRCLocation

Especifica la ubicación de origen utilizada para reparar los datos. El valor predeterminado es REPLSERVER. Este parámetro sólo es necesario cuando la ubicación de origen está en el mismo servidor. Puede especificar uno de los siguientes valores:

#### Local

Especifica que los datos se reparan de agrupaciones de almacenamiento de copia de contenedor en el mismo servidor.

#### Replserver

Especifica que los datos se reparan de una agrupación de almacenamiento de contenedores de directorio en el servidor de réplica de destino.

### MAXSESSions

Especifica el número máximo de sesiones de datos que pueden enviar datos a un servidor de destino. Este parámetro es opcional cuando repara datos de un servidor de réplica.

El valor que se especifique puede estar en el rango de 1 a 20. El valor predeterminado es 1. Si aumenta el número de sesiones, puede reparar más rápidamente la agrupación de almacenamiento.

Cuando establezca un valor para el parámetro MAXSESSIONS, asegúrese de que el ancho de banda disponible y la capacidad del procesador de los servidores de origen y de destino sean suficientes.

#### Consejos:

- Si emite un mandato QUERY SESSION, el número total de sesiones puede superar el número de sesiones de datos.
- El número de sesiones que se utilizan para reparar agrupaciones de almacenamiento depende de la cantidad de datos que se reparan. Si está reparando solamente una cantidad pequeña de datos, no conseguirá ninguna ventaja si aumenta el número de sesiones.

### Preview

Especifica si se van a previsualizar los datos o si se van a reparar. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

#### No

Especifica que los datos se reparan en la agrupación de almacenamiento pero que no se previsualizan.

#### Yes

Especifica que los datos se previsualizan pero que no se reparan.

### Wait

Especifica si se debe esperar a que el servidor termine el proceso de reparación de la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar este parámetro solamente desde una línea de mandatos administrativa. Puede especificar uno de los siguientes valores:

#### No

Especifica que el mandato se procesa en segundo plano. Para supervisar el proceso en segundo plano del mandato REPAIR STGPOOL, emita el mandato QUERY PROCESS.

Yes

Especifica que el comando se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del mandato.

## Ejemplo: reparar una agrupación de almacenamiento y obtener una vista previa de los datos

Reparar una agrupación de almacenamiento que se denomina POOL1 y previsualizar los datos.

```
repair stgpool pool1 preview=yes
```

## Ejemplo: Reparar una agrupación de almacenamiento y especificar un número máximo de sesiones

Reparar una agrupación de almacenamiento que se denomina POOL1 y especificar un máximo de 10 sesiones.

```
repair stgpool pool1 maxsessions=10
```

## Ejemplo: reparar una agrupación de almacenamiento desde cinta

Reparar una agrupación de almacenamiento llamada POOL1 y especificar local para la ubicación de origen.

```
repair stgpool pool1 SRCLOcation=local
```

Tabla 1. Mandatos relacionados con REPAIR STGPOOL

Comando	Descripción
DEFINE (contenedor de directorios)	Definir una agrupación de almacenamientos de contenedores de nube.
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.

## REPLICATE NODE (Replicar los datos de los espacios de archivos que pertenecen a un nodo de cliente)

Utilice este comando para replicar los datos de los espacios de archivos que pertenecen a uno o varios nodos de cliente, o a grupos definidos de nodos de clientes.

Cuando emite este mandato, se inicia un proceso en el que los datos que pertenecen a los nodos de cliente especificados se replican según las reglas de réplica. Los archivos que ya no se almacenan en el servidor de réplica de origen pero que existen en el servidor de réplica de destino se suprimen durante este proceso.

Si se está ejecutando un proceso de réplica de nodos para un nodo de cliente especificado por este mandato, el nodo se omite y se inicia la réplica para otros nodos que estén activados para la réplica.

Una vez que se haya completado el proceso de réplica de nodo, se puede iniciar un proceso de recuperación en el servidor de réplica de destino. Los archivos sólo se recuperan si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores a la recuperación de archivos dañados y replicados.







Especifica el nombre del nodo de cliente y del grupo definido de nodos de cliente cuyos datos van a replicarse. También puede especificar una combinación de nombres de nodos de cliente y nombres de grupos de nodos de cliente. Para especificar varios nombres de nodos de cliente o nombres de grupos de nodos de cliente, sepárelos con comas sin espacios intercalados. Puede utilizar caracteres comodín con los nombres de nodos de cliente pero no con los nombres de grupos de nodos de cliente. Se comprueban las reglas de réplica de todos los espacios de archivos en los nodos de cliente especificados.

nombre\_espacio\_archivos o FSID

Especifica el nombre del espacio de archivos o el identificador del espacio de archivos (FSID) que se ha de replicar. Un nombre o FSID es opcional. Si no especifica un nombre o un FSID, todos los datos de todos los espacios de archivos de los nodos de cliente especificados son candidatos para la réplica.

nombre\_espacio\_de\_archivos

Especifica el nombre del espacio de archivos que tiene datos que se van a replicar. Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos, emita el comando QUERY FILESPACE. Cuando existan varios nombres, separe éstos mediante comas, sin espacios intercalados. Cuando especifique el nombre, puede utilizar caracteres comodín.

Es posible que un servidor que tiene clientes con espacios de archivos que están habilitados para Unicode tenga que convertir el nombre de espacio de archivos. Por ejemplo, puede que el servidor deba convertir un nombre de la página de códigos del servidor a Unicode. Para obtener información adicional, consulte el parámetro NAMETYPE. Si no especifica ningún nombre de espacio de archivos o si especifica un único carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a los espacios de archivos que no son Unicode.

FSID

Especifica el identificador del espacio de archivos que se va a replicar. El servidor utiliza los FSID para encontrar los espacios de archivos que se deben replicar. Para determinar el FSID de un espacio de archivos, emita el comando QUERY FILESPACE. Cuando existan varios FSID, sepárelos mediante comas, sin espacios intercalados. Si especifica un FSID, el valor del parámetro NAMETYPE debe ser FSID.

NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y que tienen sistemas operativos Windows, Macintosh OS X o NetWare.

Utilice este parámetro sólo cuando especifique un nombre de espacio de archivos parcialmente o totalmente cualificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende de los caracteres que contiene el nombre y de la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema.

FSID

El servidor interpreta los nombres de espacio de archivos utilizando los identificadores de espacios de archivos.

CODETYPE

Especifica el tipo de espacios de archivos que se van a incluir en el proceso de réplica de nodos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. El valor predeterminado es BOTH, que especifica que los espacios de archivos se incluyen independientemente del tipo de página de códigos. Puede especificar uno de los siguientes valores:

UNICODE

Incluir espacios de archivos que solo están en Unicode.

NONUNICODE

Especifica espacios de archivos que no están en Unicode.

BOTH

Especifica todos los espacios de archivos independientemente del tipo de página de códigos.

DATATYPE

Especifica el tipo de datos que se van a replicar. Los datos se replican según la regla de réplica que se aplica al tipo de datos. Este parámetro es opcional. Puede especificar uno o varios tipos de datos. Si no especifica un tipo de datos, se replican todos los datos de copia de seguridad, archivado y gestionados por espacio. Cuando existan varios tipos de datos, sepárelos mediante comas, sin espacios intercalados. No puede utilizar caracteres comodín. Puede especificar uno de los siguientes valores:

ALL

Replica todos los datos de copia de seguridad, archivado y gestionados por espacio en un espacio de archivos según la regla asignada al tipo de datos. Por ejemplo, suponga que NODE1 tiene un único espacio de archivos. Se aplican las siguientes reglas de réplica:

- Las reglas de espacio de archivos de los datos de copia de seguridad y archivado en el espacio de archivos se establecen en ALL\_DATA.
- La regla de espacio de archivos de los datos gestionados por espacio se establece en DEFAULT.
- La regla de nodo de cliente de los datos gestionados por espacio se establece en NONE.

Si emite `REPLICATE NODE NODE1 DATATYPE=ALL`, sólo se replican los datos de copia de seguridad y los datos de archivado.

#### BACKUP

Replica los datos de seguridad activos e inactivos en un espacio de archivos si la regla de réplica que se aplica es ALL\_DATA, ACTIVE\_DATA, ALL\_DATA\_HIGH\_PRIORITY o ACTIVE\_DATA\_HIGH\_PRIORITY.

#### BACKUPActive

Replica sólo los datos de copia de seguridad activos en un espacio de archivos si la regla de réplica que se aplica es ACTIVE\_DATA o ACTIVE\_DATA\_HIGH\_PRIORITY.

#### ARCHive

Replica los datos de archivado solo en un espacio de archivos si la regla de réplica de control es ALL\_DATA o ALL\_DATA\_HIGH\_PRIORITY.

#### SPACEManaged

Replica sólo los datos gestionados por espacio en un espacio de archivos si la regla de réplica que se aplica es ALL\_DATA o ALL\_DATA\_HIGH\_PRIORITY.

#### PRIority

Especifica los datos que se replican basándose en la prioridad de la regla de réplica. Puede especificar uno de los siguientes valores:

##### All

Replica todos los datos en un espacio de archivos si la regla de réplica que se aplica es ALL\_DATA, ACTIVE\_DATA, ALL\_DATA\_HIGH\_PRIORITY o ACTIVE\_DATA\_HIGH\_PRIORITY.

##### High

Replica sólo los datos en un espacio de archivos que tienen una regla de réplica aplicada igual a ALL\_DATA\_HIGH\_PRIORITY o ACTIVE\_DATA\_HIGH\_PRIORITY.

##### Normal

Replica sólo los datos en un espacio de archivos que tienen una regla de réplica aplicada igual a ALL\_DATA o ACTIVE\_DATA.

#### MAXSESSions

Especifica el número máximo permitido de sesiones de datos que se utilizan para enviar datos a un servidor de réplica de destino. Este parámetro es opcional. El rango de valores es de 1 a 99. El valor predeterminado es 10.

El aumento del número de sesiones puede mejorar el rendimiento de la réplica de nodos.

Cuando establece este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas al proceso de réplica. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de los siguientes factores:

- Otra actividad del sistema y IBM Spectrum Protect
- Los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan

Asegúrese de que están disponibles los puntos y las unidades de montaje suficientes para que los procesos de réplica de nodo se puedan completar. Cada sesión de réplica necesitará un punto de montaje en los servidores de réplica de origen y destino para los volúmenes de agrupación de almacenamiento. Si el tipo de dispositivo no es FILE, cada sesión necesitará también una unidad en los servidores de réplica de origen y destino.

Cuando establezca un valor para MAXSESSIONS, tenga en cuenta también el ancho de banda disponible y la capacidad del procesador de los servidores de réplica de origen y destino.

Consejo:

- El valor que especifica el parámetro MAXSESSIONS sólo se aplica a las sesiones de datos. Las sesiones de datos son sesiones en las que los datos se envían a un servidor de réplica de destino. No obstante, si emite un comando QUERY SESSION, el número total de sesiones puede exceder el número de sesiones de datos. La diferencia se debe a las sesiones de control breves que se utilizan para consultar y configurar operaciones de réplica.

- El valor del parámetro MAXSESSIONS representa el número máximo permitido de sesiones. El número de sesiones que se utilizan para réplica depende de la cantidad de datos que se deben duplicar. Si sólo va a replicar una pequeña cantidad de datos, no conseguirá ninguna ventaja si aumenta el número de sesiones. El número total de sesiones podría ser menor que el valor especificado por el parámetro MAXSESSIONS.

#### Preview

Especifica si se obtiene una vista previa de los datos. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que los datos se replican en el servidor de destino, pero no se obtiene una vista previa de los datos.

Yes

Especifica que se obtiene una vista previa de los datos, pero no se replican. Si especifica PREVIEW=YES, solo se mostrarán los volúmenes que se deben montar físicamente, como los volúmenes de cinta. No se mostrarán los volúmenes asignados a agrupaciones de almacenamiento que tienen una clase de dispositivo de FILE.

Se muestra la siguiente información en la salida:

- Los nombres de los nodos de cliente cuyos datos se replicarán.
- El número de archivos que se replicarán o suprimirán.
- La cantidad estimada de tiempo que se necesitará para completar el proceso de réplica de nodo.
- Una lista de los volúmenes que se van a montar.
- Un resumen de la información sobre los datos replicados y dañados. El resumen lista el número de nodos, los espacios de archivos, archivos y bytes que se pueden recuperar durante un proceso de recuperación de réplica. El resumen se visualiza solo si se especifica RECOVERDAMAGED=YES o RECOVERDAMAGED=ONLY.

Si los datos de nodo de cliente especificados por el mandato REPLICATE NODE no se han duplicado nunca y se especifica PREVIEW=YES, el nodo y los espacios de archivo se definen automáticamente en el servidor de réplica de destino.

#### LISTfiles

Especifica si se listan los nombres de los archivos que se replicarán. Este parámetro es opcional. El valor predeterminado es NO. Si especifica este parámetro, significa que el parámetro WAIT se ha establecido en YES y no puede emitir el parámetro WAIT desde la consola de servidor.

Puede especificar uno de los siguientes valores:

No

Especifica que no se muestran los nombres de los archivos que se replicarán.

Yes

Especifica que se muestran los nombres de los archivos que se replicarán.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

Especifica que el comando se procesa de forma subordinada. Para supervisar el proceso en segundo plano del comando REPLICATE NODE, emita el comando QUERY PROCESS.

Yes

Especifica que el comando se procesa en primer plano. Los mensajes no se visualizan hasta que se termina el proceso del comando. No se puede especificar WAIT=YES desde la consola del servidor.

#### RECOVERDamaged

Especifica si un proceso de recuperación se ha iniciado en un servidor de réplica de destino después de completar el proceso de réplica de nodo. Este parámetro es opcional y sustituye a cualquier valor que haya especificado para el parámetro RECOVERDamaged cuando haya definido o actualizado un nodo. Puede especificar uno de los siguientes valores:

Yes

Especifica se ha iniciado un proceso de réplica para recuperar archivos dañados, pero sólo si el valor para el parámetro del sistema REPLRECOVERDAMAGED es ON. Si el valor es OFF, no se han recuperado archivos dañados.

No

Especifica que los archivos dañados no se recuperan.

Only

Especifica que se ha iniciado un proceso de réplica para el único fin de recuperar archivos dañados, pero sólo si el valor del parámetro REPLRECOVERDAMAGED del sistema está en ON. Si el valor es OFF, no se han recuperado archivos dañados y recibe una notificación de que la recuperación no se ha iniciado.

Restricción: Si especifica una combinación no válida de valores y parámetros para la recuperación de archivos, la réplica se detiene y aparece un mensaje de error.

#### FORCEREconcile

Especifica si se deben comparar todos los archivos en el servidor de réplica de origen con los archivos en el servidor de réplica de destino y sincronizar las diferencias entre ellos. Antes de la V7.1.1, este comportamiento era el valor predeterminado para el proceso de réplica. Cuando está instalado IBM® Tivoli Storage Manager V7.1.1 o posterior en los servidores de réplica de origen y destino, se ejecuta automáticamente una reconciliación durante la réplica inicial. Después de la réplica inicial, puede utilizar este parámetro por los motivos siguientes:

- Para sincronizar los archivos en los servidores de réplica de origen y destino si son diferentes.
- Para sustituir archivos inactivos que se omitieron después de cambiar las reglas de réplica de ACTIVE\_DATA a ALL\_DATA.
- Para suprimir archivos inactivos del servidor de réplica de destino cuando cambia las reglas de réplica ACTIVE\_DATA a ALL\_DATA.
- Para asegurarse de que sólo replica datos activos cuando se utiliza la regla de réplica ACTIVE\_DATA de forma que el servidor de réplica de destino sólo tiene archivos activos.
- Para resincronizar los archivos para que el servidor de réplica de destino tenga los mismos archivos que el servidor de réplica de origen si anteriormente ha utilizado o está utilizando actualmente las políticas en el servidor de réplica de destino para gestionar los archivos replicados.
- Para volver a sincronizar los archivos en los servidores de réplica de origen y destino, si la base de datos ha regresado a un momento anterior utilizando un método distinto al mandato DSMSERV RESTORE DB.
- Para volver a enlazar los archivos a la nueva clase de gestión en el servidor de réplica de destino si esta clase de gestión no existía cuando se replicaron los archivos. Debe utilizar las políticas que están definidas en el servidor de réplica de destino para gestionar los archivos replicados.

Recuerde: Cuando se asigna la regla ALL\_DATA, solo se completa una reconciliación para archivos activos en el servidor de réplica de origen.

Este parámetro es opcional. Puede especificar uno de los siguientes valores:


No

Especifica que el proceso de réplica no fuerza una reconciliación para comparar todos los archivos en el servidor de réplica de origen con archivos en el servidor de réplica de destino. En su lugar, el proceso de réplica realiza un seguimiento de los cambios de archivos en el servidor de réplica de origen desde la última réplica y sincroniza estos cambios en el servidor de réplica de destino. NO es el valor predeterminado.

Yes

Especifica que el proceso de réplica fuerza una reconciliación para comparar todos los archivos en el servidor de réplica de origen con archivos en el servidor de réplica de destino y sincroniza los archivos en el servidor de réplica de destino con el servidor de réplica de origen.

#### Sistemas operativos LinuxTRANSFERMethod

 Sistemas operativos LinuxEspecifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN). Si especifica TRANSFERMETHOD=FASP, altera temporalmente cualquier parámetro TRANSFERMETHOD que haya especificado en los mandatos DEFINE SERVER o UPDATE SERVER.

Restricciones:

- Solo los datos almacenados en una agrupación de almacenamiento de contenedores de directorio se pueden transferir utilizando tecnología Aspera FASP. Los datos que no se almacenan en una agrupación de almacenamiento de contenedores de directorio se transfieren utilizando TCP/IP.
- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, la réplica de nodo falla.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.

## Ejemplo: replicar los datos por tipo de datos y prioridad

Replique los datos de copia de seguridad activos de prioridad alta y los datos de archivado de prioridad alta que pertenecen a todos los nodos de cliente en el grupo PAYROLL.

```
replicate node payroll datatype=backupactive,archive priority=high
```

## Ejemplo: replicar todos los datos que pertenecen a un nodo según las reglas de réplica asignadas

NODE1 tiene un único espacio de archivos. Se aplican las siguientes reglas de réplica:

- Reglas de espacio de archivos:
  - Datos de copia de seguridad: ACTIVE\_DATA
  - Datos de archivado: DEFAULT
  - Datos gestionados por espacio: DEFAULT
- Reglas de nodos cliente
  - Datos de copia de seguridad: DEFAULT
  - Datos de archivado: ALL\_DATA\_HIGH\_PRIORITY
  - Datos gestionados por espacio: DEFAULT
- Reglas de servidor:
  - Datos de copia de seguridad: ALL\_DATA
  - Datos de archivado: ALL\_DATA
  - Datos gestionados por espacio: NONE

```
replicate node node1 priority=all
```

Los datos de copia de seguridad activos en el espacio de archivos se replican con una prioridad normal. Los datos de archivado se replican con una prioridad alta. Los datos gestionados por espacio no se replican.

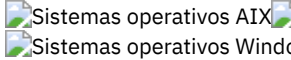
## Ejemplo: Recuperar archivos dañados sin iniciar el proceso de réplica completo

Sin iniciar el proceso de réplica completo, recupere los archivos dañados en los nodos cliente del grupo PAYROLL. Asegúrese de que el valor del parámetro del sistema REPLRECOVERDAMAGED está encendido. Después, emita el siguiente mandato:

```
replicate node payroll recoverdamaged=only
```

## Comandos relacionados

Tabla 2. Comandos relacionados con REPLICATE NODE

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
CANCEL REPLICATION	Cancela los procesos de réplica de nodo.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE REPLNODE	Elimina un nodo de la réplica.
 Sistemas operativos AIX, Linux, Windows PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

Comando	Descripción
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## REPLY (Permitir una petición para continuar el proceso)

Utilice este comando y un número de identificación para informar al servidor de que ha finalizado una operación solicitada. No todas las peticiones de servidor requieren una respuesta. Este comando sólo es necesario si el mensaje de petición indica específicamente que se necesita una respuesta.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

### Sintaxis

```
>>-REPLY--número_solicitud--+-----+----->>
      '-LABEL--==-etiqueta_volumen-'
```

### Parámetros

*número\_solicitud* (**Necesario**)

Especifica el número de identificación de la petición.

LABEL

Especifica la etiqueta que se grabará en un volumen al responder a un mensaje originado por el proceso de un mandato LABEL LIBVOLUME. Este parámetro es opcional.

### Ejemplo: responder a una petición

Responder a una petición de respuesta utilizando 3 como el número de petición.

```
reply 3
```

### Comandos relacionados

Tabla 1. Comandos relacionados con REPLY

Comando	Descripción
CANCEL REQUEST	Cancela las peticiones pendientes de montaje de volúmenes.
QUERY REQUEST	Muestra información acerca de todas las peticiones de montaje pendientes.

## RESET PASSEXP (restablecer caducidad de contraseña)

Utilice el mandato RESET PASSEXP para restablecer el período de caducidad de las contraseñas en el período de caducidad común para las contraseñas de administrador y de nodo de cliente. El mandato RESET PASSEXP no se aplica a las contraseñas que se almacenan en un servidor de directorios LDAP.

Restricción: No puede restablecer el período de caducidad de contraseña en el período de caducidad común con el mandato SET PASSEXP.

Utilice el mandato QUERY STATUS para visualizar el período de caducidad común de las contraseñas.

Restricción: Si no especifica el parámetro NODE o el parámetro ADMIN, se restablecerán los períodos de caducidad de contraseña para todos los nodos cliente y los administradores.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.









```
FILELIST="/path/to/nombre de archivo1 con espacios",/path/to/
nombre_archivo2_sin_espacios
```

En el caso de nombres de archivo que contengan comas, debe entrecorillarse todo el argumento con comillas dobles y simples ("argumento con comas").

```
FILELIST="'"/path/to/nombreachivo1, con, comas"', /path/to/nombreachivo_sin_comas
```

Para restaurar un directorio completo, especifique un nombre de directorio en lugar de un nombre de archivo. Se restauran todos los archivos del directorio y los subdirectorios. No se necesita una barra inclinada (/) de cierre al final del nombre de directorio:

```
FILELIST=/path/to/mydir
```

#### nombre\_archivo

Especifica uno o más nombres de archivos o directorios que han de restaurarse. Los nombres que especifique no pueden contener caracteres comodín. Los nombres deben separarse por comas y sin espacios intercalados. Los nombres de archivo son sensibles a las mayúsculas/minúsculas.

#### FILE:lista\_archivos

Especifica el nombre de un archivo que contiene una lista de los nombres de archivos o directorios que han de restaurarse. En el archivo especificado, cada nombre de archivo o de directorio debe aparecer en una línea por separado. Se hace caso omiso de las líneas en blanco y de las líneas de comentarios que comienzan por un asterisco. Por ejemplo:

Para restaurar los archivos FILE01, FILE02 y FILE03, cree un archivo llamado RESTORELIST que contenga una línea para cada archivo:

```
FILE01
FILE02
FILE03
```

Con el comando, puede especificar los archivos que han de restaurarse de la forma siguiente:

```
FILELIST=FILE:RESTORELIST
```

#### NAMETYPE

Especifica cómo desea que el servidor interprete los nombres que ha especificado como FILELIST=nombre\_archivo o los nombres que ha indicado en la lista del archivo que se ha especificado con FILELIST=lista\_archivos. Este parámetro es útil cuando los nombres podrían contener caracteres Unicode. No tiene ningún efecto si no se ha especificado el parámetro FILELIST. El valor predeterminado es SERVER. Los valores posibles son:

#### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres.

#### HEXadecimal

El servidor interpretará los nombres que se especifiquen como la representación hexadecimal de un nombre en Unicode. Para ver la representación hexadecimal de un nombre de archivo o de directorio, puede utilizar el comando QUERY TOC con FORMAT=DETAILED.

#### UNICODE

El servidor interpretará los nombres como nombres con codificación UTF-8. Esta opción sólo se aplica cuando se ha especificado una lista con FILELIST=FILE:lista\_archivos.

Restricción: El protocolo de gestión de datos de red (NDMP) tiene limitaciones que impiden que IBM Spectrum Protect informe acerca de si los archivos y directorios individuales se han restaurado correctamente o no.

#### PITDate

Especifica la fecha de instante específico. Cuando se utiliza con el parámetro PITTIME, PITDATE establece el instante específico a partir del cual desea seleccionar los datos que desea restaurar. Se restaurarán los datos más recientes de los que se ha hecho copia de seguridad hasta la fecha y hora especificadas. Este parámetro es opcional. El valor predeterminado es TODAY.

Puede especificar la fecha con uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	06/25/2001
TODAY	La fecha actual	TODAY
TODAY-días o bien -días	La fecha actual menos los días especificados	TODAY-7 o -7.  Para restaurar datos de los que se ha hecho copia de seguridad hace una semana, especifique PITDATE=TODAY-7 o PITDATE=-7.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM

Valor	Descripción	Ejemplo
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1  Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9  Incluir los archivos que estaban activos el día 10 del mes actual.

#### PITTime

Especifica la hora de instante específico. Cuando se utiliza con el parámetro PITDATE, PITTIME establece el instante específico a partir del cual desea seleccionar los datos que desea restaurar. Se restaurarán los datos más recientes de los que se ha hecho copia de seguridad hasta la fecha y hora especificadas. Este parámetro es opcional. El valor predeterminado es la hora actual. Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta en la fecha especificada	12:33:28
NOW	La hora actual en la fecha especificada	NOW
NOW-HH:MM o bien -HH:MM	La hora actual menos las horas y minutos en la fecha inicial especificada	NOW-03:30 o -03:30.  Si emite este comando a las 9:00 con PITTIME=NOW-03:30 o PITTIME=-03:30, el servidor restaurará registros de copia de seguridad cuya hora sea las 5:30 o posterior de la fecha de instante específico.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. El valor predeterminado es NO. Los valores posibles son:

##### No

Especifica que el servidor procesa este comando en un proceso subordinado. Utilice el comando QUERY PROCESS para supervisar el proceso subordinado de este comando.

##### Yes

Especifica que el servidor procesa este comando en primer plano. Debe esperar a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

#### TYPE

Especifica el tipo de imagen que se ha de restaurar. El valor predeterminado para este parámetro es BACKUPIIMAGE y se utiliza para restaurar datos de copias de seguridad diferenciales o básicas NDMP estándares. Otros tipos de imágenes representan métodos de copia de seguridad que pueden ser específicos para un servidor de archivos determinado. Los valores posibles son:

##### BACKUPIImage

Especifica que debe restaurarse el sistema de archivos a partir de las imágenes de las copias de seguridad estándares NDMP apropiadas. Es el método predeterminado para realizar una operación de restauración NDMP. Si utiliza el tipo BACKUPIIMAGE puede restaurar datos de copias de seguridad diferenciales y básicas, y datos en el nivel de archivo.

##### SNAPMirror

Especifica que debe restaurarse el sistema de archivos a partir de una imagen de NetApp SnapMirror. Las imágenes SnapMirror son imágenes de copia de seguridad completa de nivel de bloqueo de un sistema de archivos NetApp. Una imagen SnapMirror solo puede restaurarse en un sistema de archivos que se haya preparado como volumen de destino SnapMirror. Consulte la documentación que ha recibido con el servidor de archivos NetApp para obtener más detalles.

Después de recuperar una imagen SnapMirror y copiarla en un sistema de archivos de destino, IBM Spectrum Protect rompe la relación de SnapMirror creada por el servidor de archivos durante la operación. Una vez finalizada la restauración, el sistema de archivos de destino recupera el mismo estado que el del sistema de archivos original en el instante específico de la copia de seguridad.

Cuando defina el parámetro TYPE como SNAPMirror, tenga en cuenta las siguientes restricciones:

Restricciones:

- No puede especificar el parámetro FILELIST.

- Ni el *nombre\_sistema\_archivos\_origen* ni el *nombre\_sistema\_archivos\_destino* pueden ser un nombre de espacio de archivos virtual.
- Este parámetro es válido únicamente para los servidores de archivos NetApp e IBM® N-Series.

## Ejemplo: restaurar un directorio completo

Restaura todos los archivos y los subdirectorios del directorio `/mydir`.

```
restore node nasnode /myfs /dest filelist=/path/to/mydir
```

## Ejemplo: restaurar datos de un sistema de archivos

Restaurar datos del sistema de archivos `/vol/vol10` en el nodo NAS `NAS1`.

```
restore node nas1 /vol/vol10
```

## Ejemplo: restaurar una copia de seguridad de nivel de directorio en la misma ubicación

Restaura la copia de seguridad del nivel del directorio a su ubicación original. El origen es el nombre de espacio de archivos virtual `/MIKESDIR` y no se ha especificado ningún destino.

```
restore node nas1 /mikesdir
```

Para este ejemplo y el siguiente ejemplo, se da por supuesto que las siguientes definiciones de espacio de archivos virtual existen en el servidor para el nodo `NAS1`.

VFS Name	Filesystem	Path
<code>/mikesdir</code>	<code>/vol/vol2</code>	<code>/mikes</code>
<code>/TargetDirVol2</code>	<code>/vol/vol2</code>	<code>/tmp</code>
<code>/TargetDirVol1</code>	<code>/vol/vol1</code>	<code>/tmp</code>

## Ejemplo: restaurar una copia de seguridad de nivel de directorio en un sistema de archivos distinto

Restaurar la copia de seguridad del nivel de directorio a un sistema de archivos distinto conservando la ruta.

```
restore node nas1 /mikesdir /vol/vol0
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RESTORE NODE

Comando	Descripción
BACKUP NODE	Hace una copia de seguridad de un nodo de almacenamiento conectado a red (NAS).
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
QUERY NASBACKUP	Visualiza información sobre imágenes de copia de seguridad de NAS.
QUERY TOC	Visualiza detalles sobre la tabla de contenido para una imagen de copia de seguridad especificada.

## RESTORE STGPOOL (Restaurar datos de agrupación de almacenamiento desde una agrupación de copia o una agrupación de datos activos)

Utilice este comando para restaurar archivos desde una o varias agrupaciones de almacenamiento de copia o agrupaciones de datos activos hasta una agrupación de almacenamiento primaria.

IBM Spectrum Protect restaura todos los archivos de agrupaciones de almacenamiento primarias que:

- Se han identificado como teniendo errores
- Residen en un volumen con modalidad de acceso DESTROYED

Restricción: No puede utilizar este mandato para agrupaciones de almacenamiento de contenedor. Utilice el mandato REPLICATE STGPOOL para proteger datos de las agrupaciones de almacenamiento de contenedor.

También puede utilizar este comando para identificar los volúmenes que contienen archivos primarios dañados. Durante el proceso de restauración, se emite un mensaje para cada volumen de la agrupación de almacenamiento restaurada que contiene los archivos dañados que no están en caché. Utilice el comando QUERY CONTENT para identificar los archivos primarios dañados de un volumen específico.

No puede restaurar una agrupación de almacenamiento definida con una clase de dispositivo CENTERA.

Además de restaurar datos en las agrupaciones de almacenamiento primarias que tienen los formatos de datos NATIVE o NONBLOCK, este comando también le permite restaurar datos en las agrupaciones de almacenamiento primarias que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). La agrupación de almacenamiento primaria debe tener el mismo formato de datos que la agrupación de almacenamiento de copia desde la que se restaurarán datos. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

Consejo: Para restaurar datos de nodo cliente NAS en agrupaciones de almacenamiento NAS, debe cambiar manualmente la modalidad de acceso de los volúmenes por DESTROYED con el mandato UPDATE VOLUME. No obstante, si está usando el gestor de recuperación ante siniestro, el archivo del plan contendrá la información que necesita el servidor para marcar de forma automática los volúmenes como DESTROYED.

Puede que la restauración de archivos no sea completa si, durante el proceso de restauración, otros procesos de IBM Spectrum Protect han traspasado o suprimido datos activos o copias de archivos de copias de seguridad de agrupaciones de almacenamiento de copia. Para que no se produzca este problema, no emita los siguientes comandos para copiar volúmenes de agrupación de almacenamiento de copia o de agrupación de datos activos mientras el proceso de restauración está en progreso:

- MOVE DATA
- DELETE VOLUME (DISCARDDATA=YES)
- AUDIT VOLUME (FIX=YES)

Asimismo, puede impedir la ejecución del proceso de reclamación de las agrupaciones de almacenamiento de copia estableciendo el porcentaje de RECLAIM en 100 con el comando UPDATE STGPOOL.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento limitado a la agrupación de almacenamiento primaria para la que se han de restaurar los archivos. Si es usted un administrador con privilegio de almacenamiento con restricciones y desea restaurar archivos en una nueva agrupación de almacenamiento primaria, debe tener también autorización sobre la nueva agrupación de almacenamiento.

## Sintaxis

```
>>-RESTORE STGpool--nombre_agrupación_primaria----->
>--+-----+----->
  '-COPYstgpool----nombre_agrupación_copia-'
  .-ACTIVEDATAOnly----No-----.
>--+-----+----->
  '-ACTIVEDATAOnly----+No-----+'
                        '-Yes--| A |-'

>--+-----+----->
  '-NEWstgpool----nombre_nueva_agrupación_primaria-'
  .-MAXProcess----1-----.  .-Preview ----No-----.
>--+-----+----->
  '-MAXProcess----número-'  '-Preview----+No--+-'
                                '-Yes-'

  .-Wait----No-----.
>--+-----+-----<
  '-Wait----+No--+-'
                        '-Yes-'

A (Yes)

|--ACTIVEDATAPool----nombre_agrupación_datos-activos-----|
```

## Parámetros

---

nombre\_agrupación\_primaria (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento primaria que se está restaurando.

COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia desde la que se han de restaurar los archivos. Este parámetro es opcional. Si no se especifica este parámetro, se restaurarán los archivos desde cualquier agrupación de copia en la que se puedan ubicar copias. No utilice este parámetro con los parámetros ACTIVEONLY o ACTIVEPOOL.

ACTIVEONLY

Especifica que las versiones activas de archivos de copias de seguridad deben restaurarse únicamente a partir de las agrupaciones de datos activos. Este parámetro es opcional. El valor predeterminado es NO. Si no se especifica este parámetro, los archivos se restaurarán desde las agrupaciones de almacenamiento de copia. No utilice este parámetro con el parámetro COPYSTGPOOL. Los valores posibles son:

No

Especifica que la agrupación de almacenamiento no se restaurará desde las agrupaciones de datos activos.

Yes

Especifica que la agrupación de almacenamiento se restaurará desde la agrupación o agrupaciones activas que se especifiquen con el parámetro ACTIVEPOOL. Si especifica el valor YES para ACTIVEONLY, pero no especifica un valor para ACTIVEPOOL, los archivos se restaurarán desde cualquier agrupación de datos activos en la que puedan localizarse versiones activas de los archivos de copia de seguridad.

Atención: La restauración de una agrupación de almacenamiento primaria desde una agrupación de datos activos podría dar lugar a que algunos o todos los archivos inactivos se supriman de la base de datos si el servidor determina que existe un archivo inactivo que debe sustituirse pero no puede encontrarlo en la agrupación de datos activos.

ACTIVEPOOL

Especifica el nombre de la agrupación de datos activos desde la que se deben restaurar las versiones activas de archivos de copias de seguridad. Este parámetro es opcional. Si no se especifica este parámetro, los archivos se restaurarán desde cualquier agrupación de datos activos en la que se puedan ubicar versiones activas de archivos de copias de seguridad.

NEWstgpool

Especifica el nombre de la nueva agrupación de copia en la que se restaurarán los archivos. Este parámetro es opcional. Si no se especifica este parámetro, se restaurarán los archivos en la agrupación de almacenamiento primaria original (la agrupación que está restaurándose).

MAXProcess

Especifica el número máximo de procesos paralelos que se utilizan para restaurar archivos. Al utilizar varios procesos paralelos, se puede mejorar el rendimiento de la operación de restauración. Este parámetro es opcional. Puede especificar un valor entre 1 y 999. El valor predeterminado es 1.

Al determinar este valor, tenga en cuenta el número de puntos de montaje (unidades lógicas) y de unidades físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la operación de restauración.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia y, si el tipo de dispositivo no es FILE, también necesita una unidad. Si efectúa la operación de restauración de archivos en una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si la clase de dispositivo no es FILE, una unidad adicional. Por ejemplo, imaginemos que especifica un máximo de 3 procesos para restaurar una agrupación de almacenamiento secuencial primaria desde una agrupación de almacenamiento de copia que tiene la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo 6 puntos de montaje y 6 unidades.

Para previsualizar una restauración, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

Preview

Especifica si se desea previsualizar la restauración sin hacerla. La función de previsualización permite identificar los volúmenes necesarios para restaurar la agrupación de almacenamiento. La función de previsualización muestra:

- Una lista de volúmenes de agrupación de almacenamiento primaria que contienen archivos dañados.
- El número de archivos y el número de bytes que se restaurarán, suponiendo que la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia necesarios es READWRITE o READONLY, cuando se realiza la operación de restauración.
- Una lista de los volúmenes de agrupación de almacenamiento de copia que contienen los archivos que se restaurarán. Estos volúmenes deben montarse si ejecuta la restauración.
- Una lista de todos los volúmenes que contienen archivos que no se pueden restaurar.

Nota: Para ver una lista de los volúmenes de agrupación de almacenamiento de copia fuera del local que se montarán durante una operación de restauración, cambie la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia a UNAVAILABLE. De este modo se evita el proceso de reclamación y de traspaso de datos de los volúmenes hasta que éstos se trasladan al local para efectuar la restauración.

Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que se realiza la operación de restauración.

Yes

Especifica que se desea previsualizar la restauración sin llevarla a cabo realmente.

Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el comando.

Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes. Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, pueden haberse restaurado ya algunos archivos antes de la cancelación.

Yes

Especifica que el servidor realiza esta operación en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando la operación finaliza.

Nota: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: restaurar archivos desde una agrupación de almacenamiento de copia hasta la agrupación de almacenamiento primaria

Restaurar archivos de cualquier agrupación de almacenamiento de copia en la agrupación de almacenamiento primaria, PRIMARY\_POOL.

```
restore stgpool primary_pool
```

## Ejemplo: restaurar archivos desde una agrupación de datos activos específica hasta la agrupación de almacenamiento primaria

Restaurar archivos desde la agrupación de datos activos ADP1 hasta la agrupación de almacenamiento primaria PRIMARY\_POOL.

```
restore stgpool primary_pool activedataonly=yes activedatapool=adp1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RESTORE STGPOOL

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.



Comando	Descripción
UPDATE VOLUME	Actualiza los atributos de volúmenes de agrupación de almacenamiento.

## RESTORE VOLUME (Restaurar datos de volumen primario desde una agrupación de copia o agrupación de datos activos)

Utilice este comando para restaurar todos los archivos que están en volúmenes dañados de una agrupación de almacenamiento primaria cuya copia de seguridad se ha realizado en una agrupación de almacenamiento de copia o en una agrupación de datos activos. IBM Spectrum Protect no restaura las copias en caché de los archivos y elimina de la base de datos esos archivos en caché durante el proceso de restauración.

Además de restaurar datos en los volúmenes de las agrupaciones de almacenamiento que tienen los formatos de datos NATIVE o NONBLOCK, este comando también le permite restaurar datos en los volúmenes de las agrupaciones de almacenamiento que tienen formatos de datos NDMP (NETAPPDUMP, CELERRADUMP o NDMPDUMP). Los volúmenes que se desean restaurar deben tener el mismo formato de datos que los volúmenes de la agrupación de almacenamiento de copia. IBM Spectrum Protect da soporte al traspaso de datos de fondo para las imágenes NDMP.

Este comando cambia la modalidad de acceso de los volúmenes especificados a DESTROYED. Cuando se han restaurado todos los archivos de los volúmenes en otras ubicaciones, el volumen destruido estará vacío y se suprimirá de la base de datos.

La operación de restauración puede quedar incompleta debido a una o más de las razones siguientes:

- Nunca se efectuó una copia de seguridad de los archivos o las copias de seguridad están marcadas como dañadas. Utilice el comando QUERY CONTENT para obtener más información acerca de los demás archivos del volumen.
- Se ha especificado una agrupación de almacenamiento de copia en el comando RESTORE, pero se ha realizado la copia de seguridad de los archivos en una agrupación de almacenamiento de copia distinta. Utilice el parámetro PREVIEW cuando vuelva a emitir el comando RESTORE para determinar si este es el problema.
- Los volúmenes de la agrupación de almacenamiento de copia que son necesarios para realizar una operación de restauración están fuera del local o no están disponibles. Compruebe en las anotaciones de actividades si se han producido mensajes durante el proceso de restauración.
- Otros procesos han traspasado o suprimido copias de seguridad de los archivos de agrupaciones de almacenamiento de copia durante el proceso de restauración. Consulte la nota 3.
- Se ha especificado una agrupación de datos activos para la restauración y no había archivos inactivos para realizar la copia.

Importante:

1. No puede restaurar volúmenes en agrupaciones de almacenamiento definidas con una clase de dispositivo CENTERA.
2. Para poder restaurar un volumen de acceso aleatorio, primero debe emitir el comando VARY para desactivar el volumen.
3. Para impedir que otros procesos traspasen o supriman archivos de agrupación de almacenamiento de copia, no emita los comandos siguientes para los volúmenes de agrupación de almacenamiento de copia durante una operación de restauración:
  - MOVE DATA
  - DELETE VOLUME (DISCARDATA=YES)
  - AUDIT VOLUME (FIX=YES)

Para impedir el proceso de reclamación de las agrupaciones de almacenamiento de copia, emita el comando UPDATE STGPOOL con el parámetro RECLAIM establecido en 100.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento restringido para la agrupación de almacenamiento primaria. Si es usted un administrador con privilegio restringido y desea restaurar archivos en una nueva agrupación de almacenamiento primaria, también debe tener autorización sobre la nueva agrupación de almacenamiento.

### Sintaxis

```

      .-|-----|
      v |
>>-RESTORE Volume----nombre_volumen+----->
>--+-----+----->
  '-COPYstgpool----nombre_agrupación_copia-'
.-ACTIVEDATAonly----No-----.
```

```

>----->
'-ACTIVEDATAOnly-----+No-----+'
          '-Yes--| A |- '

>----->
'-NEWstgpool-----nombre_nueva_agrupación_primaria-'

.-MAXPRocess-----1-----.-Preview -----No-----
>----->
'-MAXPRocess-----número-' '-Preview-----+No--+-'
          '-Yes-'

.-Wait-----No-----
>-----<
'-Wait-----+No--+-'
          '-Yes-'

A (Yes)

|--ACTIVEDATAPool-----nombre_agrupación_datos-activos-----|

```

## Parámetros

### nombre\_volumen (Necesario)

Especifica el nombre de la agrupación de almacenamiento primaria que se restaura. Para especificar una lista de volúmenes que pertenecen a la misma agrupación de almacenamiento primaria, debe separar los nombres con comas y sin espacios intercalados.

### COPYstgpool

Especifica el nombre de la agrupación de almacenamiento de copia desde la que se han de restaurar los archivos. Este parámetro es opcional. Si no especifica este parámetro, se restaurarán los archivos desde todas las agrupaciones de copia en las que se puedan ubicar copias. No utilice este parámetro con los parámetros `ACTIVEDATAONLY` o `ACTIVEDATAPOOL`.

### ACTIVEDATAOnly

Especifica que las versiones activas de archivos de copias de seguridad deben restaurarse únicamente a partir de las agrupaciones de datos activos. Este parámetro es opcional. El valor predeterminado es `NO`. Si no se especifica este parámetro, los archivos se restaurarán desde las agrupaciones de almacenamiento de copia. No utilice este parámetro con el parámetro `COPYSTGPOOL`. Los valores posibles son:

No

Especifica que la agrupación de almacenamiento no se restaurará desde las agrupaciones de datos activos.

Yes

Especifica que la agrupación de almacenamiento se restaurará desde la agrupación o agrupaciones activas que se especifiquen con el parámetro `ACTIVEDATAPOOL`. Si especifica el valor `YES` para `ACTIVEDATAONLY`, pero no especifica un valor para `ACTIVEDATAPOOL`, los archivos se restaurarán desde cualquier agrupación de datos activos en la que puedan localizarse versiones activas de los archivos de copia de seguridad.

Atención: La restauración de un volumen desde una agrupación de datos activos podría dar lugar a que algunos o todos los archivos inactivos se supriman de la base de datos si el servidor determina que existe un archivo inactivo que debe sustituirse pero no puede encontrarlo en la agrupación de datos activos.

### ACTIVEDATAPool

Especifica el nombre de la agrupación de datos activos desde la que se deben restaurar las versiones activas de archivos de copias de seguridad. Este parámetro es opcional. Si no se especifica este parámetro, los archivos se restaurarán desde cualquier agrupación de datos activos en la que se puedan ubicar versiones activas de archivos de copias de seguridad.

### NEWstgpool

Especifica el nombre de la nueva agrupación de copia en la que se restaurarán los archivos. Este parámetro es opcional. Si no especifica este parámetro, los archivos se restaurarán en la agrupación de almacenamiento primaria original.

### MAXPRocess

Especifica el número máximo de procesos paralelos que se utilizan para restaurar archivos. El rendimiento puede mejorar con el uso de procesos paralelos. Este parámetro es opcional. Puede especificar un valor entre 1 y 999. El valor predeterminado es 1.

Al determinar este valor, tenga en cuenta el número de puntos de montaje (unidades lógicas) y de unidades físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es `FILE`, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la operación de restauración.

Cada proceso necesita un punto de montaje para los volúmenes de agrupación de almacenamiento de copia. Si el tipo de dispositivo no es `FILE`, cada proceso necesita también una unidad. Si restaura una agrupación de almacenamiento secuencial, cada proceso necesita un punto de montaje adicional para los volúmenes de agrupación de almacenamiento primaria y, si la

clase de dispositivo no es FILE, una unidad adicional. Por ejemplo, suponga que especifica un máximo de tres procesos para hacer copia de seguridad de una agrupación de almacenamiento primaria secuencial en una agrupación de almacenamiento de copia de la misma clase de dispositivo. Cada uno de los procesos necesita dos puntos de montaje y dos unidades. Para ejecutar los tres procesos, la clase de dispositivo debe tener un límite de montaje como mínimo de 6, y debe haber disponibles como mínimo 6 puntos de montaje y 6 unidades.

Para previsualizar una copia de seguridad, sólo se utiliza un proceso y no se necesita ningún punto de montaje ni ninguna unidad.

#### Preview

Especifica si se desea previsualizar la restauración sin hacerla. Puede utilizar esta opción para identificar los volúmenes fuera del local necesarios para restaurar una agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que desea realizar la operación de restauración.

Yes

Especifica que desea previsualizar la operación de restauración, pero restaurando los datos.

Consejo: Si se va a previsualizar una operación de restauración para ver la lista de los volúmenes de agrupación de copia fuera del local que se han de montar, debe cambiar la modalidad de acceso de los volúmenes identificados a UNAVAILABLE. De este modo impedirá la reclamación y el proceso MOVE DATA de estos volúmenes hasta que se hayan transportado a la ubicación del local para su utilización en el proceso de restauración.

La función de previsualización muestra lo siguiente:

- El número de archivos y de bytes que se restaurarán, si la modalidad de acceso de los volúmenes de agrupación de almacenamiento de copia es READWRITE o READONLY, cuando se realiza la operación de restauración.
- Una lista de los volúmenes de agrupación de almacenamiento de copia que contienen los archivos que se restaurarán. Estos volúmenes deben montarse si ejecuta la restauración.
- Una lista de los volúmenes que contienen archivos que no se pueden restaurar.

#### Wait

Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

No

Especifica que el servidor procesa este comando en un proceso subordinado.

Puede continuar trabajando con otras tareas mientras se procesa el mandato. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, en función de dónde se anoten los mensajes.

Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, puede haberse hecho ya copia de seguridad de algunos archivos antes de la cancelación.

Yes

Especifica que el servidor procesa este comando en primer plano. La operación debe estar terminada para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración cuando el comando finaliza.

Recuerde: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: restaurar archivos de datos del volumen primario

Restaurar los archivos almacenados en el volumen PVOL2 de la agrupación de almacenamiento primaria PRIMARY\_POOL.

```
restore volume pvol2
```

## Ejemplo: restaurar los archivos de datos del volumen primario de una agrupación de datos activos

Restaurar los archivos almacenados en el volumen VOL001 de la agrupación primaria PRIMARY\_POOL desde la agrupación de datos activos ADP1.

```
restore volume vol001 activedataonly=yes activedatapool=adp1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con RESTORE VOLUME

Comando	Descripción
---------	-------------

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVEDATA	Copia los datos de copia de seguridad activos.
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.

## Comandos REVOKE

Utilice los comandos REVOKE para revocar el acceso o los privilegios.

- REVOKE AUTHORITY (revocar autorización de administrador)
- REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)

## REVOKE AUTHORITY (revocar autorización de administrador)

Utilice este mandato para revocar una o varias clases de privilegios de un administrador.

También puede utilizar este mandato para restringir el número de dominios de políticas para los que un administrador de política restringida dispone de autorización y el número de agrupaciones de almacenamiento para las que un administrador de almacenamiento restringido dispone de autorización.

Si utiliza el comando REVOKE AUTHORITY sin los parámetros CLASSES, DOMAINS y STGPools, revocará todos los privilegios del administrador especificado.

Como mínimo un administrador debe tener privilegio de sistema; por lo tanto, si el administrador es el único que tiene privilegio de sistema, no puede revocar la autorización.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-REVoKe AUTHority--nombre_admin----->
>+-----+
|          .-,------. |
|          V          | |
|'-Classes-----+System-----+-'
|                   +-Policy-----+
|                   +-Storage-----+
|                   +-Operator-----+
|'-Node--| A |-'
>+-----+
|          .-,------. |
|          V          | |
|'-Domains-----nombre_dominio+-'
>+-----+<
|          .-,------. |
|          V          | |
|'-STGpools-----nombre_agrupación+-'
A
.-AUTHority---Access-----
|+-----+
|'-AUTHority---+Access+-'
|'-Owner--'
```

```
>---+D0mains-----nombre_dominio+-----|
      '-N0de-----node_name-----'
```

Notas:

1. Si se omiten todos estos parámetros, se revocarán todos los privilegios de administrador de este administrador.

## Parámetros

---

nombre\_admin (Necesario)

Especifica el nombre del administrador cuyo privilegio de administración se va a revocar o reducir.

CLasses

Especifica una o más clases de privilegios de administración que se revocarán a un administrador. Puede especificar varias clases separando cada una con una coma.

SYstem

Indica que se ha de revocar la autorización del sistema para este administrador. Si se especifica CLASSES=SYSTEM, no pueden especificarse otras clases, ni tampoco pueden especificarse los parámetros DOMAINS y STGPOOLS.

Policy

Indica que se ha de revocar el privilegio de política de este administrador. Para revocar todos los privilegios de políticas, especifique CLASSES=POLICY y no especifique el parámetro DOMAINS.

STorage

Indica que se ha de revocar el privilegio de almacenamiento para este administrador. Para revocar todos los privilegios de almacenamiento, especifique CLASSES=STORAGE y no especifique el parámetro STGPOOLS.

Operator

Indica que se ha de revocar el privilegio de operador de este administrador.

Node

Indica que se ha de revocar el privilegio de nodo para este usuario.

AUTHority

Indica el nivel de autorización que se revoca para un usuario con privilegio de nodo. Este parámetro es opcional.

Si un administrador ya tiene privilegio de sistema o de políticas para el dominio de políticas al que pertenece el nodo, este comando no modificará el privilegio del administrador.

Los niveles de autorización posibles son:

Access

Indica que se revoca la autorización de acceso a cliente. Es el valor predeterminado si se ha especificado CLASSES=NODE.

Nota: Un nodo cliente puede establecer la opción REVOKEREMOTEACCESS para evitar que acceda un usuario con privilegio de nodo y autorización de acceso a cliente. Si un usuario con privilegio de nodo tiene autorización de propietario de cliente, o tiene privilegios de sistema o de políticas para el dominio de políticas al que pertenece el nodo, ese administrador podrá seguir accediendo al cliente de copia de seguridad/archivado de Web.

Owner

Indica que se revoca la autorización de propietario de cliente.

DOmains

Indica que desea revocar la autorización de acceso a cliente o de propietario de cliente de un administrador para todos los clientes del dominio de políticas especificado. Este parámetro no se puede utilizar con el parámetro NODE.

NOde

Indica que desea revocar la autorización de acceso a cliente o de propietario de cliente de un administrador para el nodo. Este parámetro no se puede utilizar con el parámetro DOMAIN.

DOmains

Cuando se utiliza con CLASSES=POLICY, especifica una lista de los dominios de política que un administrador de políticas con restricciones ya no puede gestionar. (El administrador tenía autorización para gestionar estos dominios hasta que se ha emitido el comando REVOKE.) Este parámetro es opcional. Los elementos de la lista se separan con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Se ha revocado la autorización para todos los dominios que coinciden. Si se especifica DOMAINS, el parámetro CLASSES=POLICY es opcional.

STGpools

Especifica una lista de agrupaciones de almacenamiento que ya no puede gestionar un administrador con privilegio de política con restricciones. (El administrador tenía autorización para gestionar estas agrupaciones de almacenamiento hasta que se ha

emitido el comando REVOKE). Este parámetro es opcional. Los elementos de la lista se separan con comas, sin espacios intercalados. Puede utilizar caracteres comodín para especificar un nombre. Se revocará la autorización para todas las agrupaciones de almacenamiento que coincidan. Si se especifica STGPOOLS, entonces el parámetro CLASSES=STORAGE es opcional.

## Notas de uso

1. Para que un administrador con privilegio de almacenamiento sin restricciones pase a tener privilegio de almacenamiento con restricciones, en primer lugar debe utilizar este mandato para revocar el privilegio sin restricciones. A continuación, ha de utilizar el comando GRANT AUTHORITY para otorgar al administrador privilegio de almacenamiento con restricciones y para identificar las agrupaciones de almacenamiento sobre las que el administrador tiene autorización.

Para revocar el privilegio de política sin restricciones de un administrador, especifique el parámetro CLASSES=STORAGE. No puede utilizar el parámetro STGPOOLS para revocar la autorización sobre las agrupaciones de almacenamiento seleccionadas de un administrador con privilegio de almacenamiento sin restricciones.

2. Para que un administrador con privilegio de política sin restricciones pase a tener privilegio de política con restricciones, en primer lugar debe utilizar este mandato para revocar el privilegio sin restricciones. A continuación, ha de utilizar el comando GRANT AUTHORITY para otorgar al administrador privilegio de política con restricciones y para identificar los dominios de políticas sobre los que el administrador tiene autorización.

Para revocar el privilegio de política sin restricciones de un administrador, especifique el parámetro CLASSES=POLICY. No puede utilizar el parámetro DOMAINS para revocar la autorización sobre los dominios seleccionados de un administrador con privilegio sin restricciones.

## Ejemplo: revocar determinados privilegios de administración

Revocar parte de los privilegios del administrador CLAUDIA. CLAUDIA tiene privilegio de política con restricciones para los dominios de políticas EMPLOYEE\_RECORDS y PROG1. Limitar los privilegios de políticas de CLAUDIA al dominio de políticas EMPLOYEE\_RECORDS.

```
revoke authority claudia classes=policy  
domains=employee_records
```

## Ejemplo: revocar todos los privilegios de administración

El administrador LARRY actualmente tiene privilegios de operador y de políticas con restricciones. Revocar todos los privilegios del administrador LARRY. Para revocar todos los privilegios de un administrador, identifique al administrador, pero no especifique CLASSES, DOMAINS o STGPOOLS. LARRY continúa siendo un administrador pero únicamente podrá utilizar los comandos que puede emitir cualquier administrador.

```
revoke authority larry
```

## Ejemplo: revocar privilegio de nodo

El usuario de personal del departamento de soporte CONNIE tiene actualmente privilegio de nodo con autorización de propietario de cliente para el nodo cliente WARD3. Revocar su privilegio de nodo con autorización de propietario de cliente.

```
revoke authority connie classes=node  
authority=owner node=ward3
```

## Comandos relacionados

Tabla 1. Comandos relacionados con REVOKE AUTHORITY

Comando	Descripción
GRANT AUTHORITY	Asigna clases de privilegios a un administrador.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.

## REVOKE PROXYNODE (revocar la autoridad proxy de un nodo cliente)

Utilice este comando para revocar la autoridad de un nodo cliente agente para realizar operaciones de copia de seguridad y restauración para un nodo de destino en el servidor de IBM Spectrum Protect.

## Clase de privilegio

Para emitir este comando, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones

## Sintaxis

---

```
>>-REVoke PROXynode TArget-----nombre_nodo_destino----->  
>--AGent-----nombre_nodo_agente-----><
```

## Parámetros

---

TArget (Obligatorio)

Especifica el nodo de destino al cual ha otorgado autorización de proxy el nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.

AGent (Obligatorio)

Especifica qué nodo tiene autorización para actuar como proxy respecto al nodo de destino. Se permiten los caracteres comodín y las listas separadas con comas de nombres de nodo.

## Ejemplo: revocar la autorización de proxy de un nodo

---

Para revocar la autorización del nodo de destino NASCLUSTER que actúa como proxy para todos los nodos agente que empiezan por la letra M, emita el comando siguiente.

```
revoke proxynode target=nascluster agent=m*
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con REVOKE PROXYNODE

Comando	Descripción
GRANT PROXYNODE	Concede autorización de proxy a un nodo agente.
QUERY PROXYNODE	Visualiza los nodos con autoridad para actuar como nodos proxy.

## ROLLBACK (Retrotraer cambios no validados en una macro)

---

Utilice este mandato en una macro para deshacer todos los cambios de proceso que han realizado los mandatos que el servidor ha ejecutado pero que todavía no se han validado en la base de datos. Un cambio validado es permanente y no se puede retrotraer. El mandato ROLLBACK es útil para probar las macros.

Asegúrese de que su sesión de cliente de administración no está ejecutándose con la opción ITEMCOMMIT cuando utilice este mandato.

Importante: Los comandos SETOPT en una macro no pueden retrotraerse.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

```
>>-ROLLBACK-----><
```

## Parámetros

---

Ninguno

## Ejemplo: retrotraer cambios en una macro

---

Ejecute la macro REGN con el mandato ROLLBACK para verificar que la macro funciona sin validar ningún cambio. El contenido de la macro es :

```
/* Macro para registrar administradores
de políticas y otorgar autorización */
REGister Admin sara hobby
GRant AUTHority sara CLasses=Policy
REGister Admin ken plane
GRant AUTHority ken CLasses=Policy
ROLLBACK /* impide que se validen los cambios */
```

## Comandos relacionados

Tabla 1. Comandos relacionados con ROLLBACK

Comando	Descripción
COMMIT	Hace que los cambios en la base de datos sean permanentes.
MACRO	Ejecuta un archivo de macro especificado.

### Conceptos relacionados:

Macros de cliente administrativo

## RUN (ejecutar un script de IBM Spectrum Protect)

Utilice este mandato para ejecutar un script de IBM Spectrum Protect. Para emitir este comando en otro servidor, el script que se ejecuta debe estar definido en ese servidor.

Puede incluir comandos RUN en los scripts siempre que éstos no creen bucles. Por ejemplo, debe evitar incluir comandos RUN donde SCRIPT\_A ejecuta SCRIPT\_B y SCRIPT\_B ejecuta SCRIPT\_A.

Importante: IBM Spectrum Protect no dispone de un comando que pueda cancelar un script después de haberse iniciado éste. Para detener un script, debe detener el servidor.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de operador, políticas, almacenamiento o sistema.

## Sintaxis

```
>>-RUn--nombre_script--+-----+----->
      | .,-----+-----+-----+-----|
      | V          | |          | |          |
      +---valor_sustitución+---'
      .-Preview ----No----- .  .-Verbose----No----- .
>+-----+-----+-----+-----<
  '-Preview----+No--+-'  '-Verbose----+No--+-'
      '-Yes-'          '-Yes-'
```

## Parámetros

nombre\_script (Obligatorio)

Especifica el nombre del script que desea procesar. El nombre que especifique no puede ser una variable de sustitución como, por ejemplo, \$1.

substitution\_value

Especifica uno o varios valores que se sustituirán por variables al ejecutarse el script. En un script, una variable de sustitución se compone de un carácter '\$' seguido de un número. Al ejecutar el script, IBM Spectrum Protect sustituye las variables de sustitución definidas en un script con los valores suministrados con este comando. Debe especificar valores para cada una de las variables de sustitución definidas en el script; de lo contrario, el script no se ejecutará. Este parámetro es opcional.

Preview

Especifica si se previsualizan las líneas de comandos del script sin ejecutar realmente el script. El valor predeterminado es NO. Los valores posibles son:

Yes

Especifica que se visualizan las líneas de comandos incluidas en un script, pero el script no se procesa.



No

Especifica que se visualizan las líneas de comandos incluidas en un script y el script se procesa.

Verbose

Especifica hay que visualizar las líneas de comandos, la sustitución de variables y el recorrido por la lógica condicional a medida que se procesa el script. Este parámetro se ignora si se especifica PREVIEW=YES. El valor predeterminado es NO.

Los valores posibles son:

Yes

Especifica que se visualicen las líneas de comandos, la sustitución de variables y el recorrido de la lógica condicional a medida que se procesa el script.

No

Especifica que no se visualicen las líneas de comandos, la sustitución de variables y el recorrido de la lógica condicional a medida que se procesa el script.

## Ejemplo: ver los comandos que ha generado un script con una variable de sustitución de nombre de tabla

---

Para ejecutar el siguiente script de ejemplo, denominado QSAMPLE, emita un comando RUN que especifique el nombre de tabla ACTLOG como valor para la variable de sustitución, \$1. Utilice la salida para obtener una previsualización de los comandos que genera el script antes de ejecutar los comandos.

```
001 /* Esta es una consulta SQL con formato amplio */
005 SET SQLDISPLAYMODE WIDE
010 SELECT colname FROM -
015 COLUMNS WHERE TABNAME='$1'

run qsample actlog preview=yes

ANR1461I RUN: Ejecutando el script de comandos QSAMPLE.
ANR1466I RUN: Script de comandos QSAMPLE, Línea 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Script de comandos QSAMPLE, Línea 15:
           select colname from columns where tabname='ACTLOG'.
ANR1470I RUN: Script de comandos QSAMPLE completado correctamente
           (modo PREVIEW)
```

## Ejemplo: ejecutar un script para que se visualicen y se ejecuten los comandos que genera el script

---

Ejecutar el mismo script como se mostraba en el ejemplo anterior para que se visualicen los comandos generados y los resultados de los comandos.

```
run qsample actlog verbose=yes

ANR1461I RUN: Ejecutando el script de comandos QSAMPLE.
ANR1466I RUN: Script de comandos QSAMPLE, Línea 5 :
           set sqldisplaymode wide.
ANR1466I RUN: Script de comandos QSAMPLE, Línea 5: RC=RC_OK
ANR1466I RUN: Script de comandos QSAMPLE, Línea 15:
           select colname from columns where tabname='ACTLOG'.

COLNAME
-----
DATE_TIME
MSGNO
SEVERITY
MESSAGE
ORIGINATOR
NODENAME
OWNERNAME
SCHEDNAME
DOMAINNAME
SESSID

ANR1462I RUN: Script de comandos QSAMPLE, Línea 15: RC=RC_OK
ANR1462I RUN: Script de comandos QSAMPLE completado correctamente.
```

## Ejemplo: ejecutar un script para que sólo se visualicen los resultados de los comandos del script

---

Ejecutar el script de ejemplo anterior, sin que se visualicen los comandos generados, sólo los resultados de los comandos generados en el script.

```
run qsample actlog verbose=no
```

```
COLNAME  
-----  
DATE_TIME  
MSGNO  
SEVERITY  
MESSAGE  
ORIGINATOR  
NODENAME  
OWNERNAME  
SCHEDNAME  
DOMAINNAME  
SESSID
```

```
ANR1462I RUN: Script de comandos QSAMPLE completado correctamente.
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con RUN

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
UPDATE SCRIPT	Cambia o añade líneas a un script.

**Tareas relacionadas:**

Ejecución de un script del servidor

## SELECT (Realizar una consulta SQL de la base de datos de IBM Spectrum Protect)

---

Utilice el mandato SELECT para crear y dar formato a una consulta personalizada de la base de datos de IBM Spectrum Protect .

IBM Spectrum Protect proporciona una interfaz SQL para un programa de DB2. DB2 maneja directamente las restricciones y las directrices para gestionar consultas SQL.

Como ayuda para encontrar la información que está disponible, IBM Spectrum Protect proporciona tres tablas de catálogos del sistema:

SYSCAT.TABLES

Contiene información acerca de todas las tablas que pueden consultarse con el mandato SELECT.

SYSCAT.COLUMNS

Describe las columnas de cada tabla.

Puede emitir el mandato SELECT para consultar estas tablas y determinar la ubicación de la información que desea obtener.

## Notas de uso

---

No puede emitir el mandato SELECT desde una consola de servidor.

Dado que el mandato SELECT no bloquea ni desbloquea registros, la contención de un registro puede provocar que el servidor emita por error el mensaje ANR2034E: `SELECT: No se ha encontrado ninguna entrada con este criterio`. Compruebe que sus criterios de selección sean correctos y ejecute el mandato de nuevo.

Para detener el proceso de un mandato SELECT después de haberse iniciado éste, cancele la sesión de administración desde la que se ha emitido el mandato. Puede cancelar la sesión desde la consola del servidor o desde otra sesión de administración.

Los espacios de tabla temporales se utilizan para procesar consultas SQL en DB2. Un espacio temporal inadecuado puede provocar errores de consulta SQL.

Para exportar la salida de un archivo separado por comas para su importación a una hoja de cálculo, utilice las opciones de línea de mandatos `-comma` y `>` las opciones de línea de mandatos en el mandato `dsmadm`.

## Clase de privilegio

---

Cualquier administrador puede emitir este comando.

## Sintaxis

---

Para obtener la sintaxis de la sentencia SELECT y las directrices, busque en Información sobre el producto DB2.

Importante: La sintaxis adecuada para la sentencia Select de la indicación de fecha y hora es:

```
SELECT * FROM SUMMARY WHERE ACTIVITY='EXPIRATION' AND START_TIME >'2009-05-10 00:00:00' AND START_TIME <'2009-05-11 23:23:23'
```

## Lista de ejemplos

---

El mandato SELECT se utiliza para personalizar gran diversidad de consultas. Para darle una idea de lo que puede hacer con el mandato, esta sección incluye muchos ejemplos. Sin embargo, existen muchas más posibilidades. La salida de la consulta se muestra únicamente para los comandos más complejos para poder ilustrar su formato.

En la lista siguiente se resumen los mandatos SELECT de ejemplo:

- Lista las contraseñas del ID de usuario administrador que se autentican con un servidor de directorios LDAP externo
- Obtener una lista de las tablas disponibles
- Obtener una lista de los nodos cliente y de los clientes de administración que actualmente tienen bloqueado el acceso al servidor
- Obtener una lista de los nodos cliente y de los clientes de administración que finalmente no han especificado la contraseña correcta
- Obtener una lista de los nodos del dominio de políticas estándar que no se han asociado a la planificación de copia de seguridad diaria DAILYBACKUP
- Obtener una lista de los administradores que disponen de autorización de política
- Obtener una lista de los mensajes de tipo E (ERROR) o W (WARNING) que se han emitido en el período de tiempo durante el cual han estado realizándose tareas de mantenimiento para los registros del registro de actividad
- Obtener una lista de las planificaciones de administración que ha definido o alterado el administrador JAKE
- Obtener una lista de las prioridades de planificación de administración relativas
- Obtener una lista de las clases de gestión que tienen un grupo de copias archivadas con un período de retención de más de 365 días
- Obtener una lista de los nodos cliente que se encuentran en cada dominio de políticas
- Contar el número de archivos que se han archivado de cada nodo
- Obtener una lista de los clientes que utilizan la gestión de espacio
- Determinar cuántos volúmenes deberían reclamarse si el umbral de reclamación se cambia al 50 para la agrupación de almacenamiento TAPE
- Determinar cuántos archivos de copia de seguridad se verían afectados en cada nodo si se cambiara o suprimiera la clase de gestión DAILY en el dominio de políticas STANDARD
- Para todas las sesiones de cliente activas, determinar durante cuánto tiempo han estado conectadas éstas y su rendimiento efectivo en bytes por segundo
- Determinar durante cuánto tiempo han estado ejecutándose los procesos en segundo plano actuales y determinar su rendimiento efectivo en términos de tiempo y de archivos por segundo
- Contar el número de nodos cliente que existen para cada tipo de plataforma
- Contar el número de espacios de archivos que tiene cada nodo y obtener una lista de los nodos cliente por orden ascendente
- Obtener información estadística para calcular el número de volúmenes fuera del local cuyo espacio se reclama durante la reclamación de una agrupación de almacenamiento.
- Obtener registros de detalle de estimaciones de PVU
- Obtener información sobre los roles del nodo
- Obtener información sobre el estado.

## Ejemplo: Lista los ID de usuario administrador que se autentican con el servidor IBM Spectrum Protect

---

Lista todos los ID de usuario administrador cuyas contraseñas se autentican con el servidor IBM Spectrum Protect :

```
select admin_name from admins where authentication=local
```

## Ejemplo: obtener una lista de las tablas disponibles

---

Obtener una lista de todas las tablas disponibles para consultar la base de datos de IBM Spectrum Protect.

```

select * from syscat.tables

      ABSHEMA: SERVER1
      TABNAME: ACTLOG
      CREATE_TIME: 1999-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: FALSE
      REMARKS: Server activity log

      TABSCHEMA: SERVER1
      TABNAME: ADMIN_SCHEDULES
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 14
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: TRUE
      REMARKS: Administrative command schedules

      TABSCHEMA: SERVER1
      TABNAME: ADMINS
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 15
INDEX_COLCOUNT: 1
      UNIQUE_INDEX: TRUE
      REMARKS: Server administrators

      TABSCHEMA: SERVER1
      TABNAME: ARCHIVES
      CREATE_TIME: 1995-05-01 07:39:06
      COLCOUNT: 10
INDEX_COLCOUNT: 5
      UNIQUE_INDEX: FALSE
      REMARKS: Copias archivadas cliente

```

### Ejemplo: obtener una lista de los nodos cliente y de los clientes de administración que actualmente tienen bloqueado el acceso al servidor

---

```

select node_name from nodes where locked='YES'

select admin_name from admins where locked='YES'

```

### Ejemplo: listar nodos de cliente, clientes administrativos y servidores que están utilizando la seguridad de sesión transicional

---

```

select node_name from nodes where session_security='Transitional'

select admin_name from admins where session_security='Transitional'

select server_name from servers where session_security='Transitional'

```

### Ejemplo: obtener una lista de los nodos cliente y de los clientes de administración que finalmente no han especificado la contraseña correcta

---

```

select node_name from nodes where invalid_pw_count <>0

select admin_name from admins where invalid_pw_count <>0

```

### Ejemplo: obtener una lista de los nodos del dominio de políticas estándar que no se han asociado a la planificación de copia de seguridad diaria DAILYBACKUP

---

```

select node_name from nodes where domain_name='STANDARD' and
node_name not in (select node_name from associations
where domain_name='STANDARD' and
schedule_name='DAILYBACKUP')

```

### Ejemplo: listar los administradores que disponen de autorización de política

---

```

select admin_name from admins where
upper(system_priv) <>'NO'
or upper(policy_priv) <>'NO'

```

## Ejemplo: obtener una lista de los mensajes de tipo E (ERROR) o W (WARNING) que se han emitido en el período de tiempo durante el cual han estado realizándose tareas de mantenimiento para los registros del registro de actividad

---

```
select date_time,msgno,message from actlog
where severity='E' or severity='W'
```

## Ejemplo: obtener una lista de las planificaciones de administración que ha definido o alterado el administrador JAKE

---

```
select schedule_name from admin_schedules
where chg_admin='JAKE'
```

## Ejemplo: obtener una lista de las prioridades de planificación de administración relativas

---

```
select schedule_name,priority from admin_schedules order
by priority
```

## Ejemplo: obtener una lista de las clases de gestión que tienen un grupo de copias archivadas con un período de retención de más de 365 días

---

```
select domain_name,set_name,class_name from ar_copygroups
where retver='NOLIMIT' or cast(retver as integer) >365
```

## Ejemplo: obtener una lista de las clases de gestión que especifican más de cinco versiones de copia de seguridad

---

```
select domain_name,set_name,class_name from bu_copygroups
where verexists = 'NOLIMIT' or
cast(verexists as integer)>5
```

## Ejemplo: obtener una lista de los nodos cliente que utilizan el conjunto de opciones de cliente denominado SECURE

---

```
select node_name from nodes where option_set='SECURE'
```

## Ejemplo: obtener una lista de los nodos cliente que se encuentran en cada dominio de políticas

---

```
select domain_name,num_nodes from domains
```

## Ejemplo: contar el número de archivos que se han archivado de cada nodo

---

Atención: Este mandato puede tardar mucho tiempo en finalizar.

```
select node_name,count(*) from archives
group by node_name
```

## Ejemplo: obtener una lista de los clientes que utilizan la gestión de espacio

---

```
select node_name from auditocc where spacemg_mb <>0
```

## Ejemplo: determinar cuántos volúmenes deberían reclamarse si el umbral de reclamación se cambia al 50 para la agrupación de almacenamiento TAPE

---

```
select count(*) from volumes where stgpool_name='TAPE'
and upper(status)='FULL' and pct_utilized < 50
```

## Ejemplo: determinar cuántos archivos de copia de seguridad se verían afectados en cada nodo si se cambiara o suprimiera la clase de gestión DAILY en el dominio de políticas STANDARD

---

Nota: Este mandato necesita una cantidad de tiempo y de recursos significativa para completarse.

```
select node_name, count(*) as "Files" from backups
where class_name='DAILY' and node_name in
```

```
(select node_name from nodes where domain_name='STANDARD')
group by node_name
```

## Ejemplo: para todas las sesiones de cliente activas, determinar durante cuánto tiempo han estado conectadas éstas y su rendimiento efectivo en bytes por segundo

---

```
select session_id as "Sesión",
client_name as "Cliente",
state as "Estado",
current_timestamp-start_time as "Tiempo transcurrido",
(cast(bytes_sent as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes enviados/segundo",
(cast(bytes_received as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes recibidos/segundo"
from sessions
```

```
Sesión: 24
Cliente: ALBERT
Estado: Run
Tiempo transcurrido: 0 01:14:05.000000
Bytes enviados/segundo: 564321,9302768451
Bytes recibidos/segundo: 0,0026748857944
```

```
Sesión: 26
Cliente: MILTON
Estado: Run
Tiempo transcurrido: 0 00:06:13.000000
Bytes enviados/segundo: 1638,5284210992221
Bytes recibidos/segundo: 675821,6888561849
```

## Ejemplo: determinar durante cuánto tiempo han estado ejecutándose los procesos en segundo plano actuales y determinar su rendimiento efectivo en términos de tiempo y de archivos por segundo

---

Nota: La caducidad no informa acerca del número de bytes procesados.

```
select process_num as "Número",
process,
current_timestamp-start_time as "Tiempo transcurrido",
(cast(files_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Archivos/segundo",
(cast(bytes_processed as decimal(18,0)) /
cast(second(current_timestamp-start_time) as decimal(18,0)))
as "Bytes/segundo"
from processes
```

```
Número: 1
PROCESS: Expiration
Tiempo transcurrido: 0 00:24:36,000000
Archivos/segundo: 6,3216755870092
Bytes/segundo: 0,00000000000000
```

## Ejemplo: contar el número de nodos cliente que existen para cada tipo de plataforma

---

```
select platform_name,count(*) as "Número de nodos"
from nodes group by platform_name
```

PLATFORM_NAME	Número de nodos
AIX	6
SunOS	27
Win32	14
Linux	20

## Ejemplo: contar el número de espacios de archivos que tiene cada nodo y obtener una lista de los nodos cliente por orden ascendente

---

```
select node_name, count(*) as "number of tablespaces"
from tablespaces group by node_name order by 2
```

NODE_NAME	número de espacios de archivos
ALBERT	2
MILTON	2
BARNEY	3
SEBASTIAN	3
MAILHOST	4
FALCON	4
WILBER	4
NEWTON	4
JEREMY	4
WATSON	5
RUSSELL	5

### Ejemplo: obtener información estadística para calcular el número de volúmenes fuera del local cuyo espacio se reclama durante la reclamación de una agrupación de almacenamiento.

---

```
select * from summary where activity='OFFSITE RECLAMATION'
```

```
START_TIME: 2004-06-16 13:47:31.000000
END_TIME: 2004-06-16 13:47:34.000000
ACTIVITY: OFFSITE RECLAMATION
NUMBER: 4
ENTITY: COPYPOOL
COMMMETH:
ADDRESS:
SCHEDULE_NAME:
EXAMINED: 170
AFFECTED: 170
FAILED: 0
BYTES: 17821251
IDLE: 0
MEDIWA: 0
PROCESSES: 2
SUCCESSFUL: YES
VOLUME_NAME:
DRIVE_NAME:
LIBRARY_NAME:
LAST_USE:
COMM_WAIT:
NUM_OFFSITE_VOLS: 2
```

### Ejemplo: identificar qué agrupaciones de almacenamiento contienen datos cuyos duplicados han eliminado los clientes

---

```
select stgpool_name,has_client_dedup_data from stgpools
```

STGPOOL_NAME	HAS_CLIENT_DEDUP_DATA
ADPOOL	NO
ARCHIVEPOOL	NO
BACKUPPOOL	NO
COPYDEDUP	NO
COPYNODEDUP	NO
FILEPOOL	YES
FILEPOOL2	NO
LANFREEFILEPOOL	YES
SPACEMGPOOL	NO

### Ejemplo: obtener información sobre la base de datos

---

```
select * from db
```

```
DATABASE_NAME: TSMDB1
TOT_FILE_SYSTEM_MB: 2048000
USED_DB_SPACE_MB: 12576
FREE_SPACE_MB: 1576871
TOTAL_PAGES: 983044
USABLE_PAGES: 982908
```

```

USED_PAGES: 977736
FREE_PAGES: 5172
BUFF_HIT_RATIO: 96.2
TOTAL_BUFF_REQ: 53967
SORT_OVERFLOW: 0
LOCK_ESCALATION: 0
PKG_HIT_RATIO: 70.0
LAST_REORG: 2010-07-15 17:32:55.000000
FULL_DEV_CLASS: OUTFILE
NUM_BACKUP_INCR: 0
LAST_BACKUP_DATE: 2010-01-21 10:37:59.000000
PHYSICAL_VOLUMES: 0
PAGE_SIZE:
NUM_BACKUP_STREAMS: 4

```

## Ejemplo: obtener registros de detalle de estimaciones de PVU

---

Genere la estimación de PVU para un nodo denominado ACCTSRECSRV, que se utiliza en el producto IBM Spectrum Protect Extended Edition.

```
select * from pvuestimate_details where node_name='ACCTSRECSRV'
```

```

PRODUCT: PRODEE
LICENSE_NAME: MGSYSLAN
NODE_NAME: ACCTSRECSRV
LAST_USED: 2008-01-20 16:12:24.000000
TRYBUY: FALSE
PROC_VENDOR: IBM
PROC_BRAND: POWER5+ QCM
PROC_TYPE: 4
PROC_MODEL:
PROC_COUNT: 2
ROLE: SERVER
ROLE_OVERRIDE: USERREPORTED
ROLE_EFFECTIVE: SERVER
VALUE_UNITS: 50
VALUE_FROM_TABLE: YES
PVU: 100
SCAN_ERROR : NO
API_CLIENT: NO
PVU_AGNOSTIC: NO
HYPERVISOR: VMWARE
GUID: 01.2e.1c.80.e5.04-
      .11.da.aa.ab.00.-
      15.58.0b.d9.47
VERSION: 6
RELEASE: 3
LEVEL: 1
VENDOR_D: IBM(R)
BRAND_D: POWER5(TM) QCM
TYPE_D: Quad-core Module
MODEL_D: All Existing
PRODUCT_D: IBM Spectrum Protect Extended Edition

```

## Descripciones de los campos

---

### PRODUCT

Compilación de tipos de licencia en productos al nivel presentado en el comando QUERY PVUESTIMATE. Los valores posibles son PRODEE, PROTBASIC, PRODDATARET, PRODMAIL, PRODDDB, PRODSYSB, PRODSpace, PRODSAN, PRODERP o en blanco.

### LICENSE\_NAME

La licencia asignada a este nodo.

### NODE\_NAME

El nombre de nodo.

### LAST\_USED

Fecha y hora en que se conectó por última vez el nodo identificado al sistema bajo esta licencia.

### TRYBUY

Indica si se ejecuta con la modalidad de prueba. Los valores posibles son TRUE o FALSE.

### PROC\_VENDOR

El nombre de proveedor de procesador que notifica el cliente.

### PROC\_BRAND

El nombre de marca de procesador que notifica el cliente.

### PROC\_TYPE



El tipo de procesador que notifica el cliente. Este valor refleja también el número de núcleos. Los valores de ejemplo son 1=SINGLE CORE, 2=DUO CORE y 4=QUAD CORE.

PROC\_MODEL

El modelo de procesador que notifica el cliente.

PROC\_COUNT

La cantidad de procesador.

ROLE

El rol del nodo. Los valores posibles son CLIENT, SERVER u OTHER.

ROLE\_OVERRIDE

Altera temporalmente el valor especificado en el comando UPDATE NODE.

ROLE\_EFFECTIVE

Rol real basado en los valores de los campos ROLE y ROLE\_OVERRIDE.

VALUE\_UNITS

La unidad de valor de procesador (PVU) asignada del procesador.

PVU

El valor de PVU calculado.

$$\text{PVU por nodo} = \text{número de procesadores por nodo} * \text{tipo de procesador} * \text{valor de pvu}$$

donde el tipo de procesador representa el número de núcleos y el valor de pvu es el valor definido para el tipo de procesador en la tabla de PVU de IBM®.

VALUE\_FROM\_TABLE

Distintivo que indica si la PVU se ha calculado basándose en la tabla de PVU de IBM. Los valores posibles son YES o NO. Si es NO, se aplica un valor 100 para cada nodo definido como un servidor. Si no hay ningún rol definido para un nodo, se utiliza el rol del servidor a efectos de cálculo de PVU.

SCAN\_ERROR

Distintivo que indica si el cliente ha notificado información sobre licencias. Los valores posibles son YES o NO.

API\_CLIENT

Distintivo que indica una aplicación de API. Los valores posibles son YES o NO.

PVU\_AGNOSTIC

Distintivo que indica que el nivel de release de la versión del cliente es anterior a IBM Spectrum Protect V6.3. Si la versión es anterior a 6.3, no se esperan mediciones de PVU válidas. Los valores posibles son YES o NO.

HYPERVISOR

Nombre del software de máquina virtual que notifica el cliente.

GUID

Identificador exclusivo global (GUID) del sistema donde se ubica el nodo. El GUID se obtiene de la tabla de nodo.

VERSION

La versión del cliente.

RELEASE

El release del cliente.

LEVEL

El nivel del cliente.

VENDOR\_D

Valor de visualización del proveedor del procesador de la tabla de PVU.

BRAND\_D

Valor de visualización de la marca de procesador de la tabla de PVU.

TYPE\_D

Valor de visualización del tipo de procesador de la tabla de PVU.

MODEL\_D

Valor de visualización del modelo de procesador de la tabla de PVU.

PRODUCT\_D

Valor de visualización del producto de la tabla de PVU. Son posibles los siguientes valores:

- IBM Spectrum Protect
- IBM Spectrum Protect Extended Edition
- IBM Spectrum Protect para retención de datos
- IBM Spectrum Protect for SAN
- IBM Spectrum Protect for Space Management
- IBM Spectrum Protect for Mail
- IBM Spectrum Protect para bases de datos
- IBM Spectrum Protect for Enterprise Resource Planning
- IBM Spectrum Protect for System Backup and Recovery
- Blanco

## Ejemplo: obtener información de rol e información relacionada con PVU

En el ejemplo siguiente se muestran los resultados parciales de un nodo seleccionado, incluida la información de rol y la información relacionada con PVU. Los roles posibles son CLIENT, SERVER u OTHER. La PVU sólo se calcula para los nodos definidos como servidores.


```
select * from nodes
```

```
ROLE: CLIENT
ROLE_O: USEREPORTED
PVENDOR: INTEL
PBRAND: INTEL
PTYPE: 4
PMODEL:
PCOUNT: 1
HYPERVISOR:
PAPI: NO
SCANERROR: NO
```

## Comandos SET

---

Utilice los comandos SET para especificar valores que afectan a varias operaciones de IBM Spectrum Protect.

- SET ACCOUNTING (activar o desactivar registros de contabilidad)
- SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)
- SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)
- SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)
- SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)
- SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)
- SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)
- SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)
- SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)
- SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)
- SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)
- SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)
- SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)
- SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)
- SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)
- SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)
- SET CONFIGMANAGER (Especificar un gestor de configuración)
- SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)
- SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)
- SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)
- SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)
- SET DBRECOVERY (Establece la clase de dispositivo para copias de seguridad automáticas)
- SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)
- SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)
- DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)
- SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)
- SET DRMCHECKLABEL (Especificar comprobación de etiquetas)
- SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener comandos)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)
- SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)
- SET DRMCOURIERNAME (Especificar el nombre del transportista)
- SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)
- SET DRMFILEPROCESS (Especificar el proceso de archivos)
- SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)
- SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)
- SET DRMPPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)
- SET DRMPPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)
- SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)
- SET DRMRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)
- SET DRMVAULTNAME (Especificar el nombre de la cámara de seguridad)
- SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)
- SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)



- SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)
- SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)
- SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)
- SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)
- SET MAXCMDRETRIES (Establecer el número máximo de reintentos de comando)
- SET MAXSCHEDESESSIONS (Establecer número máximo de sesiones planificadas)
- SET MINPWLENGTH (Establecer longitud mínima de contraseña)
- SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)
- SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)
- SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)
- SET PASSEXP (Establecer fecha de caducidad de contraseña)
- SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)
- SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)
- SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)
- SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)
- SET REPLRETENTION (Establecer el período de retención de los registros de réplica)
- SET REPLSERVER (Establecer el servidor de réplica de destino)
- SET RETRYPERIOD (Establecer período de tiempo entre reintentos)
- SET SCHEDMODES (seleccionar modalidad de planificación central)
- SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)
- SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)
- SET SERVERNAME (Especificar el nombre del servidor)
- SET SERVERPASSWORD (Establecer contraseña de servidor)
- SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)
- SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)
- SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)
- SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)
- SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)
- SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)
- SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)
- SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)
- SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)
- SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)

## SET ACCOUNTING (activar o desactivar registros de contabilidad)

Utilice este comando para determinar si se crea un registro de contabilidad cada vez que finaliza una sesión de nodo cliente. Un registro de contabilidad realiza un seguimiento de la cantidad de almacenamiento que ha utilizado una sesión de nodo cliente.

Utilice el mandato QUERY STATUS para determinar si se han de generar registros de contabilidad. Durante la instalación, este valor se establece en OFF.

Los registros de contabilidad se guardan en un archivo de contabilidad llamado dsmacct.log.

 Sistemas operativos AIX  Sistemas operativos Linux La variable de entorno, DSMSERV\_ACCOUNTING\_DIR, especifica el directorio en el que se encuentra el archivo de contabilidad.

 Sistemas operativos Windows Una entrada de registro controla la ubicación del registro de contabilidad.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set ACCounting---+ON---+-----<<
      '-OFF-'
```

### Parámetros

ON

Especifica que el servidor crea un registro de contabilidad cada vez que finaliza una sesión de nodo cliente.

OFF

Especifica que el servidor no crea registros de contabilidad.

## Ejemplo: crear registros de contabilidad

Para crear un registro de contabilidad al final de cada sesión de nodo cliente, emita el comando siguiente:

```
set accounting on
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET ACCOUNTING

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET ACTLOGRETENTION (Establecer el período de retención o el tamaño de las anotaciones de actividades)

Utilice este mandato para gestionar los registros de las anotaciones de actividad por fecha o tamaño. Las anotaciones de actividades contienen los mensajes de actividad normales que genera el servidor. Estos mensajes contienen información relativa a las operaciones del servidor y de los clientes, como por ejemplo, la hora de inicio de las sesiones o errores de E/S de dispositivos.

La información de las anotaciones de actividades incluye mensajes, como por ejemplo:

- La sesión cliente se inicia y finaliza
- La migración se inicia y finaliza
- Mensajes de error de diagnóstico
- Salida de mandatos de administración planificados

Durante a instalación del servidor, la gestión de las anotaciones de actividad está basada en la retención y el período de retención es de 30 días.

Puede ajustar el período de tiempo durante el que las anotaciones de actividad mantienen los mensajes para evitar datos insuficientes o caducados. El servidor elimina automáticamente los mensajes de las anotaciones de actividad una vez expirado el período de retención.

También puede optar por limitar el tamaño total de las anotaciones de actividad para controlar la cantidad de espacio que ocupan. El servidor eliminará periódicamente los registros de anotaciones de actividad más antiguos hasta que el tamaño de las anotaciones deje de superar el máximo permitido configurado.

Puede ejecutar el mandato QUERY STATUS para que se visualice el número actual de registros de las anotaciones de actividad y el tamaño (en megabytes) que ocupan actualmente las anotaciones de actividades.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set ACTlogretention--número--'-Mgmtstyle-----Date-----'.
                                     +-----+-----+-----+-----><
                                     '-Mgmtstyle-----Date+-'
                                     '-Size-'
```

## Parámetros

número (Obligatorio)

Especifica el número de días que se retienen los mensajes en las anotaciones de actividades cuando se gestionan por fecha, o especifica el tamaño máximo de las anotaciones de actividades cuando se gestionan por tamaño. En el caso de la gestión basada en la retención, un valor de 1 especifica que se han de retener los registros de las anotaciones de actividades durante el día de hoy. En el caso de la gestión basada en el tamaño, un valor de 1 especifica un tamaño máximo de 1 MB para las anotaciones.

Puede especificar un número comprendido entre 0 y 9999. Un valor de 0 desactiva la retención de las anotaciones de actividades.

#### Mgmtstyle

Especifica si la gestión de las anotaciones de actividad se basa en la retención o el tamaño. Este parámetro es opcional. El valor predeterminado es DATE. Los valores posibles son:

#### Date

Especifica que la gestión de las anotaciones de actividad se basa en la retención.

#### Size

Especifica que la gestión de las anotaciones de actividad se basa en el tamaño.

## Ejemplo: establecer el período de retención de las anotaciones de actividades

Establezca el servidor de modo que retenga los registros de anotaciones de actividades durante 60 días. Emita el comando:

```
set actlogretention 60
```

## Ejemplo: establecer el tamaño de las anotaciones de actividades

Establecer el servidor para que limite el tamaño de las anotaciones de actividad a 300 MB. Emita el mandato:

```
set actlogretention 300 mgmtstyle=size
```

## Comandos relacionados

Tabla 1. Comando relacionado con SET ACTLOGRETENTION

Comando	Descripción
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)

Utilice este mandato para especificar durante cuánto tiempo permanece activa una alerta antes de quedar inactiva. Si se desencadena de nuevo una alerta activa, se reinicia el tiempo de duración.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set ALERTACTiveduration -número_mins-----<<
```

## Parámetros

#### número\_mins (Necesario)

Especifica el número de minutos durante los cuales una alerta permanece activa antes de queda inactiva. Especifique un valor de 1 a 20160. El valor predeterminado inicial de servidor es 480 minutos.

## Establecer la duración de una alerta activa a un día

Emita el siguiente mandato para especificar que las alertas permanezcan activas durante 1440 minutos antes de cambiar al estado inactivo:

```
set alertactiveduration 1440
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTACTIVEDURATION

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

## SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)

Utilice este mandato para especificar durante cuánto tiempo permanece cerrada una alerta antes de que se suprima.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set ALERTClosedduration -numero_mins-----<<
```

### Parámetros

numero\_mins (Necesario)

Especifica el número de minutos durante los cuales una alerta permanece cerrada antes de suprimirse. Si establece el valor en 0, las alertas se suprimen inmediatamente después de cerrarse. Especifique un valor de 0 a 99999. El valor predeterminado se establece en 60 minutos cuando se formatea inicialmente la base de datos de servidor de IBM Spectrum Protect.

### Suprimir alertas dos horas después de que se hayan cerrado

Especifique que las alertas permanezcan cerradas durante 120 minutos antes de que se supriman:

```
set alertclosedduration 120
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTCLOSEDDURATION

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

## SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)

Utilice este mandato para permitir que las alertas se envíen por correo electrónico a los administradores especificados.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set ALERTEMail---ON---+-----><
      '-Off-'
```

## Parámetros

---

ON

Especifica que las alertas se pueden enviar por correo electrónico a los administradores especificados.

Off

Especifica que las alertas no se pueden enviar por correo electrónico a los administradores especificados. Cuando se formatea inicialmente la base de datos del servidor, el valor ALERTEMAIL se establece en OFF.

## Habilitar alertas que se enviarán al administrador cuando se produzcan

---

Habilitar que se envíen las alertas por correo electrónico emitiendo el mandato siguiente:

```
SET ALERTEMAIL ON
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con SET ALERTEMAIL

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

## SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)

---

Utilice este mandato para especificar la dirección de correo electrónico del remitente de la alerta.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set ALERTEMAILFroMaddr -dirección_correo_electrónico-----><
```

## Parámetros

---

dirección\_correo\_electrónico (Necesario)

Especifica la dirección de correo electrónico del remitente. Las direcciones de correo electrónico tienen el formato de *nombre@dominio*. Los nombres de correo electrónico, incluida la dirección, no puede tener más de 64 caracteres de longitud y el nombre de dominio no puede tener más de 255 caracteres de longitud.

## Especificar la dirección de correo electrónico del remitente de alerta

Especifique la dirección de correo electrónico del remitente emitiendo el mandato siguiente:

```
set alertemailfromaddr djadmin@mydomain.com
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILFROMADDR

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

## SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)

Utilice este mandato para especificar el nombre de host de servidor de correo de SMTP (Protocolo simple de transferencia de correo) que se utiliza para enviar el correo electrónico de alerta.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set ALERTEMAILSMTPHost--nombre_host-----<<
```

## Parámetros

nombre\_host (Necesario)

Especifica el nombre de host de servidor de correo SMTP.

## Especifique el nombre de host del servidor de correo SMTP como mail.domain.com

Especifique `mail.domain.com` como el servidor de correo SMTP, emitiendo el siguiente mandato:

```
set alertemailsmtp host mail.domain.com
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILSMTPHOST

Comando	Descripción
---------	-------------



Comando	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

## SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)

Utilice este mandato para especificar el número de puerto para el servidor de correo SMTP. Este servidor de correo se utiliza para enviar las alertas por correo electrónico.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set ALERTEMAILSMTPPort--puerto_tcp-----<<
```

### Parámetros

puerto\_tcp (Obligatorio)  
Especifica el número de puerto del servidor de correo SMTP. Especifique un valor de 1 a 32767. El número de puerto predeterminado es 25.

### Especificar el número de puerto del servidor de correo SMTP

Especifique el número de puerto 450 como servidor de correo SMTP emitiendo el siguiente mandato:

```
set alertemailsmtpport 450
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTEMAILSMTPPORT

Comando	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)	Especifica los administradores que desean recibir resúmenes de alerta por correo electrónico.

## SET ALERTSUMMARYTOADMINS (Establecer la lista de administradores que deben recibir resúmenes de alertas por correo electrónico)

Utilice este mandato para especificar los administradores que desean recibir resúmenes de alerta por correo electrónico, cada hora.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set ALERTSUMMARYToadmins--+-nombre_admin-+----->>  
      ',-----'
```

## Parámetros

---

nombre\_admin (Necesario)

Especifica el nombre del administrador que desea recibir resúmenes de alerta por correo electrónico. Puede especificar un máximo de tres nombres de administrador separándolos con comas sin espacios intercalados.

## Especificar dos administradores para que reciban resúmenes de alerta

---

Especifique que los administradores HARRY y COLIN desean recibir resúmenes de alertas, emitiendo el siguiente mandato:

```
set alertsummarytoadmins HARRY,COLIN
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con SET ALERTSUMMARYTOADMINS

Comando	Descripción
SET ALERTEMAIL (Establecer el supervisor de alertas para que envíe por correo electrónico las alertas a los administradores)	Permite enviar alertas por correo electrónico a los administradores especificados.
SET ALERTEMAILFROMADDR (Establecer la dirección de correo electrónico del remitente)	Especifica la dirección de correo electrónico del remitente de la alerta.
SET ALERTEMAILSMTPHOST (Establecer el nombre de host de servidor de correo SMTP)	Especifica el nombre de host de servidor de correo SMTP que se utiliza para enviar alertas por correo electrónico.
SET ALERTEMAILSMTPPORT (Establecer el puerto de host de servidor de correo SMTP)	Especifica el servidor de correo SMTP que se utilizará para enviar las alertas.

## SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)

---

Utilice este mandato para especificar durante cuánto tiempo permanece inactiva una alerta. Una vez que ha transcurrido el periodo de duración de inactividad, la alerta se cierra.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set ALERTINactiveduration -numero_mins----->>
```

## Parámetros

---

numero\_mins (Necesario)

Especifica el número de minutos que una alerta permanece inactiva antes de que se cierre. Puede especificar un valor comprendido entre 1 – 20160. El valor predeterminado inicial de servidor es 480 minutos.

## Cambiar el estado de alerta de inactivo a cerrado después de 60 minutos

---

Emita el siguiente mandato para especificar que una alerta permanezca en estado inactivo durante 60 minutos antes de cambiar al estado cerrado:

```
set alertinactiveduration 60
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTINACTIVEDURATION

Comando	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

## SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)

Utilice este mandato para activar o desactivar el supervisor de alertas.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set ALERTMONITOR .-OFF- . --ON-------<<
```

### Parámetros

ON

Especifica que el servidor de IBM Spectrum Protect supervise las alertas.

OFF

Especifica que el servidor de IBM Spectrum Protect no supervise las alertas. Cuando se formatea inicialmente la base de datos de servidor de IBM Spectrum Protect, el valor de supervisión de alertas está establecido en OFF.

### Activar la supervisión de alertas

Active la supervisión de alertas emitiendo el mandato siguiente:

```
set alertmonitor on
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTMONITOR

Comando	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.

Comando	Descripción
SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)	Especifica la frecuencia con la que el supervisor de alertas actualiza y borra las alertas de la base de datos.

## SET ALERTUPDATEINTERVAL (Establecer con qué frecuencia el supervisor de alertas actualiza y borra las alertas)

Utilice este mandato para especificar la frecuencia con la que el supervisor de alertas actualiza y borra las alertas que se almacenan en la base de datos de servidor de IBM Spectrum Protect.

Durante este intervalo de comprobación, el supervisor de alertas examina cada alerta en el servidor y realiza las acciones siguientes:

- El supervisor de alertas determina si han transcurrido los tiempos de duración de actividad o inactividad. Si transcurre el tiempo de duración especificada, el estado de alerta se actualiza al estado siguiente. Por ejemplo:
  - Activo a inactivo
  - Inactivo a cerrado
- En caso de que se cierre una alerta durante el tiempo especificado por el mandato SET ALERTCLOSEDDURATION, la alerta se suprime.

Puede utilizar el mandato QUERY MONITORSETTINGS para determinar si la supervisión de alertas está activa. Utilice el mandato SET ALERTMONITOR para activar la supervisión de alertas.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set ALERTUPDateinterval -número_mins----->>
```

### Parámetros

número\_mins (Necesario)

Especifica el periodo de tiempo, en minutos, que el supervisor espera antes de que se actualicen y borren las alertas en el servidor. Especifique un valor de 1 a 9999. El servidor tiene un valor predeterminado inicial de 10 minutos.

### Establecer intervalo de actualización de alertas en 60 minutos

Especifique que las alertas se actualicen cada hora emitiendo el mandato siguiente:

```
set alertupdateinterval 60
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con SET ALERTUPDATEINTERVAL

Comando	Descripción
SET ALERTACTIVEDURATION (Establecer la duración de una alerta activa)	Especifica cuánto tiempo se queda activa la alerta hasta que se desactiva.
SET ALERTINACTIVEDURATION (Establecer la duración de una alerta inactiva)	Especifica cuánto tiempo se queda una alerta inactiva hasta que se cierra.
SET ALERTCLOSEDDURATION (Establecer la duración de una alerta cerrada)	Especifica cuánto tiempo la alerta se queda cerrada antes de suprimirse.
SET ALERTMONITOR (Establecer el supervisor de alertas en activado o desactivado)	Especifica si la supervisión de alerta está establecida en activada o desactivada.

## SET ARCHIVERETENTIONPROTECTION (activar la protección de retención de datos)

Utilice este mandato para activar y desactivar la protección de retención de datos de copia archivada. Para que este mandato funcione, el servidor no debe contener datos. Durante la instalación este valor se establece en OFF.

Si la protección de retención de datos de copia archivada está activa:

- Sólo se pueden almacenar copias archivadas en el servidor.
- No se puede suprimir la copia archivada hasta que el parámetro RETVER en el mandato DEFINE COPYGROUP (archivo) esté satisfecho.

Sólo los servidores con protección de retención de datos habilitada soportan la definición de agrupaciones de almacenamiento del tipo RECLAMATIONTYPE=SNAPLOCK.

Utilice el comando QUERY STATUS para que se visualice el estado de la protección de retención de datos de copia archivada.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-Set ARCHIVERETENTIONPROTECTion +-Off+-----<<  
      '-ON--'
```

## Parámetros

OFF

Especifica que la protección de retención de datos de copia archivada no está activa.

ON

Especifica que la protección de retención de datos de copia archivada sí está activa.

## Ejemplo: activar la protección de retención de datos

Activar la protección de retención de datos de copia archivada con el comando siguiente:

```
set archiveretentionprotection on
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET ARCHIVERETENTIONPROTECTION

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
AUDIT VOLUME	Compara la información de base de datos y de la agrupación de almacenamiento y, opcionalmente, resuelve las incoherencias.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

## SET ARREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de archivado)

Utilice este mandato para establecer la regla de réplica del servidor de los datos de archivado.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos de archivado se establecen en DEFAULT.

Emita este comando en el servidor que actúe como origen para los datos replicados.

Puede especificar una regla de réplica de prioridad normal o una regla de réplica de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y prioridad alta, se replican primero los datos de prioridad alta. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos de archivado y datos de copia de seguridad. La réplica de los datos de archivado tiene una prioridad más alta que los datos de copia de seguridad. Para dar prioridad a los datos de archivado, emita el mandato SET ARREPLRULEDEFAULT y especifique la regla de réplica ALL\_DATA\_HIGH\_PRIORITY. Para priorizar los datos de copia de seguridad, emita el comando SET BKREPLRULEDEFAULT y especifique la regla de réplica ALL\_DATA para los datos de copia de seguridad. La regla ALL\_DATA para los datos de copia de seguridad replica los datos de copia de seguridad con una prioridad normal.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set ARREPLRuledefault--+-ALL_DATA-----+-----><
                               +-ALL_DATA_HIGH_PRIORITY--+
                               '-NONE-----'
```

## Parámetros

ALL\_DATA  
Hace una réplica de los datos de archivado con una prioridad normal.

ALL\_DATA\_HIGH\_PRIORITY  
Hace una réplica de los datos de archivado con una prioridad alta.

NONE  
Los datos de archivado no se replican.

## Ejemplo: establecer la regla de réplica del servidor para los datos de archivado

Configure la regla predeterminada para que los datos de archivado se repliquen con una prioridad alta.

```
set arreplruledefault all_data_high_priority
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET ARREPLRULEDEFAULT

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.

Comando	Descripción
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## SET BKREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos de copia de seguridad)

Utilice este mandato para establecer la regla de réplica del servidor de los datos de copia de seguridad.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos de copia de seguridad se establecen en DEFAULT.

Emita este comando en el servidor que actúe como origen para los datos replicados.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a los datos de copia de seguridad, emita el mandato SET BKREPLRULEDEFAULT y especifique la regla de réplica ACTIVE\_DATA\_HIGH\_PRIORITY. Para priorizar los datos de archivado, emita el mandato SET ARREPLRULEDEFAULT y especifique la regla de réplica ALL\_DATA para los datos de archivado. La regla ALL\_DATA para los datos de archivado replica los datos de archivado con una prioridad normal.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set BKREPLRuledefault--+-ALL_DATA-----+-----><
      +-ACTIVE_DATA-----+
      +-ALL_DATA_HIGH_PRIORITY----+
      +-ACTIVE_DATA_HIGH_PRIORITY-+
      '-NONE-----'
```

### Parámetros

#### ALL\_DATA

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad normal.

#### ACTIVE\_DATA

Replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal.

Atención: Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro FORCERECONCILE=YES.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caduquen.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de copia de seguridad activos e inactivos. Los datos se replican con una prioridad alta.

#### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta.

NONE

Los datos de copia de seguridad no se replican.

## Ejemplo: establecer la regla de réplica del servidor para los datos de copia de seguridad

Configure la regla predeterminada para que los datos de seguridad repliquen solo los datos activos y para que se repliquen los datos con una prioridad alta.

```
set bkreplruledefault active_data_high_priority
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET BKREPLRULEDEFAULT

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET REPLRETENTION	Especifica el periodo de retención de los registros de historial de réplicas.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## SET CLIENTACTDURATION (Establecer el período de duración de la acción del cliente)

Utilice este comando para especificar la duración de la planificación que se ha definido con el comando DEFINE CLIENTACTION. Una acción del cliente define una planificación que se ejecuta una vez en un cliente.

El programa suprime estos registros de eventos independientemente de si el cliente ha procesado la planificación. Sin embargo, estas planificaciones no se suprimen hasta que se suprime el primer registro de eventos. El período de retención de eventos se establece de forma predeterminada en 10 días a partir de la instalación.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-SET CLIENTACTDuration--dias-----<<
```



## Parámetros

días (Obligatorio)

Especifica el número de días durante el cual estará activa la planificación de la acción del cliente. Puede especificar un entero de 0 a 999. El valor predeterminado son 5 días.

El número de días que especifique determina durante cuánto tiempo la base de datos retiene la planificación antes de suprimirla. El valor 0 indica que la duración de la planificación es indefinida y que la planificación y las asociaciones no se suprimen de la base de datos.

### Ejemplo: establecer un período de duración de 15 días para la acción del cliente.

Para especificar que la planificación de la acción del cliente esté activa durante 15 días, emita el comando siguiente:

```
set clientactduration 15
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET CLIENTACTDURATION

Comando	Descripción
DEFINE CLIENTACTION	Define un comando que se ha de realizar en un nodo cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET CONFIGMANAGER (Especificar un gestor de configuración)

Utilice este comando para especificar si un servidor es un gestor de configuración. En un gestor de configuración, puede definir perfiles de configuración a los que otros servidores pueden suscribirse.

No se puede designar un servidor como gestor de configuración si el servidor se suscribe a uno o más perfiles de otro gestor de configuración.

Si un servidor es un gestor de configuración, no puede cambiar esta designación hasta que suprima todos los perfiles, incluyendo el perfil predeterminado.

Emita el comando QUERY STATUS para determinar si un servidor es un gestor de configuración. Cuando se instala un servidor, no se designa como gestor de configuración.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set CONFIGManager--+-OFF-+-----><
                        '-ON--'
```

## Parámetros

ON

Especifica que el servidor es un gestor de configuración.

Al designar un servidor como gestor de configuración, IBM Spectrum Protect crea un perfil predeterminado denominado DEFAULT\_PROFILE y asocia al perfil todos los servidores y grupos de servidores definidos en el gestor de configuración. Puede modificar o suprimir el perfil predeterminado.

OFF

Especifica que el servidor no es un gestor de configuración.

### Ejemplo: especificar un gestor de configuración

Designar un servidor como gestor de configuración.

```
set configmanager on
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET CONFIGMANAGER

Comando	Descripción
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET CONFIGREFRESH	Especifica un intervalo de tiempo para que los servidores gestionados entren en contacto con los gestores de configuración.

## SET CONFIGREFRESH (Establecer renovación de configuración de servidores gestionados)

Utilice este comando en un servidor gestionado para especificar la frecuencia con la que ese servidor establece contacto con su gestor de configuración para obtener información de configuración actualizada.

Para que se visualice el valor actual, emita el comando QUERY STATUS. En la instalación, el intervalo se establece en 60 minutos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set CONFIGRefresh--minutos-----<<
```

### Parámetros

minutos (Obligatorio)

Especifica el intervalo, en minutos, antes de que un servidor gestionado se ponga en contacto con su servidor de configuración para obtener las actualizaciones de configuración. Especifique un entero de 0 a 10000.

- Si el valor es mayor que 0, el servidor gestionado establece contacto con el gestor de configuración inmediatamente. El siguiente contacto se produce al alcanzar el intervalo especificar.
- Si el valor es 0, el servidor gestionado no establece contacto con el gestor de configuración.

Se prescinde de este valor si el servidor no se inscribe como mínimo en un perfil de un gestor de configuración.

### Ejemplo: establecer un intervalo de renovación de 45 minutos

Especificar que un servidor gestionado contacte con su gestor de configuración cada 45 minutos.

```
set configrefresh 45
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET CONFIGREFRESH

Comando	Descripción
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.

Comando	Descripción
NOTIFY SUBSCRIBERS	Notifica a los servidores que deben renovar la información de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UPDATE PROFILE	Cambia la descripción de un perfil.

## SET CONTEXTMESSAGING (activar o desactivar el informe de contexto de mensajes)

Utilice este comando para obtener información adicional cuando aparezcan mensajes ANR9999D. IBM Spectrum Protect sondea los componentes del servidor en busca de información como el nombre de proceso, el nombre de la hebra, el identificador de sesión, los datos de transacción, los bloqueos mantenidos y las tablas de base de datos que se están utilizando.

Nota: Cuando un subproceso emite mensajes consecutivos de la misma área de código, sólo el primer mensaje proporciona información de contexto.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set CONTEXTmessaging--+-ON-----<<
      '-OFF-'
```

### Parámetros

- ON  
Especifica que se activa el informe de contexto de mensajes.
- OFF  
Especifica que se desactiva el informe de contexto de mensajes.

### Ejemplo: activar o desactivar el informe de contexto de mensajes

Activar el envío de mensajes de contexto para recibir información adicional que puede ayudar a determinar la causa de los mensajes ANR9999D.

```
set contextmessaging on
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET CONTEXTMESSAGING

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET CPUINFOREFRESH (Intervalo de renovación de la exploración de información de la estación de trabajo de cliente)

Utilice este comando para especificar el número de días entre exploraciones de cliente de la información de estación de trabajo que se utiliza para calcular la unidad de valor de procesador (PVU).

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set CPUINFOREFRESH--días-----<<
```

## Parámetros

días (Obligatorio)

Especifica el número de días entre exploraciones de dispositivos de cliente. Para recuperar el valor actual, emita el comando QUERY STATUS. Los valores posibles son de 1 a 9999. El valor predeterminado es 180.

## Ejemplo: Establecer la cantidad de tiempo antes de la siguiente renovación en 90 días

```
SET CPUINFOREFRESH 90
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET CPUINFOREFRESH

Comando	Descripción
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.

## SET CROSSDEFINE (Especificar si los servidores se definen el uno en el otro)

Utilice este comando para especificar si un servidor se define automáticamente en otro servidor.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set CROSSDefine---ON---<<
      '-Off-'
```

## Parámetros

ON

Especifica que un servidor se puede definir en otro servidor. Para definir automáticamente un servidor en otro, también debe permitir la definición cruzada de un servidor en la definición del otro servidor.

OFF

Especifica que un servidor no se puede definir en otro servidor.

## Ejemplo: especificar si los servidores se definen el uno en el otro

Establecer una definición cruzada que permita que la definición de un servidor esté en otro servidor.

```
set crossdefine on
```

## Comandos relacionados

Tabla 1. Comando relacionado con SET CROSSDEFINE

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.



Restricciones:

- Tenga cuidado al especificar el parámetro COMPRESS. La utilización de compresión durante las copias de seguridad de la base de datos puede reducir el tamaño de los archivos de copia de seguridad. Sin embargo, la compresión puede aumentar el tiempo necesario para completar el proceso de copia de seguridad de base de datos.
- No realice copias de seguridad de datos comprimidos en una cinta. Si el entorno del sistema almacena copias de seguridad de bases de datos en la cinta, establezca el parámetro COMPRESS en No en los mandatos SET DBRECOVERY y BACKUP DB.

#### PROTECTKeys

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es Yes (sí). Puede especificar uno de los valores siguientes:

No

Especifica que las copias de seguridad de base de datos no incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=NO, debe hacer copia de seguridad de la clave de cifrado maestra manualmente para el servidor y hacer que la clave está disponible cuando implementa la recuperación tras desastre.

Yes

Especifica que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra de servidor. Atención: Si especifica PROTECTKEYS=YES, también debe especificar el parámetro PASSWORD.

#### PASSword

Especifica la contraseña que se utiliza para proteger las copias de seguridad de base de datos. El valor predeterminado es proteger las copias de seguridad de base de datos.

Importante: Asegúrese de que recuerda esta contraseña. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos.

## Ejemplo: especificar una clase de dispositivo para copias de seguridad de bases de datos




Especificar la clase de dispositivo DBBACK para copias de seguridad de bases de datos. Ejecute el mandato siguiente:

```
set dbrecovery dbback
```

## Ejemplo: especificar una clase de dispositivo y el número de corrientes para copias de seguridad de bases de datos

Especifique la clase de dispositivo DBBACK para las copias de seguridad de bases de datos y especifique que la copia de seguridad utilice dos corrientes de movimiento de datos. Ejecute el mandato siguiente:

```
set dbrecovery dbback numstreams=2
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Ejemplo: Proteger las claves de cifrado de la agrupación de almacenamiento en copias de seguridad de base de datos

Cifrar los datos de agrupación de almacenamiento especificando que las copias de seguridad de base de datos incluyen una copia de la clave de cifrado maestra del servidor. Ejecute el mandato siguiente:

```
set dbrecovery dbback protectkeys=yes password=password_name
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DBRECOVERY

Comando	Descripción
BACKUP DB	Efectúa una copia de seguridad de la base de datos de IBM Spectrum Protect en volúmenes de acceso secuencial.
QUERY DB	Visualiza información de asignación acerca de la base de datos.
QUERY DBSPACE	Visualiza información acerca del espacio de almacenamiento definido para la base de datos.

## SET DEDUPVERIFICATIONLEVEL (Definir el porcentaje de extensiones que se deben verificar)

Utilice este comando para verificar las extensiones enviadas al servidor durante la eliminación de datos duplicados del lado del cliente.

Una aplicación invasora que reside en un sistema cliente y que imita al cliente, la API o la GUI y puede iniciar un ataque en el servidor. Para proteger al servidor a tales ataques, puede especificar un porcentaje de extensiones de cliente para que las verifique el servidor.

Si el servidor detecta que hay un ataque de seguridad en curso, se cancela la sesión actual. Además se cambia el valor del parámetro DEDUPLICATION del mandato REGISTER NODE. El valor cambia de CLIENTORSERVER a SERVERONLY. El valor SERVERONLY inhabilita la eliminación de datos duplicados del lado del cliente en ese nodo.

El servidor también emite un mensaje avisando de que se ha detectado un ataque potencial contra la seguridad y que la eliminación de datos duplicados del lado del cliente se ha inhabilitado en ese nodo. Si se inhabilita la eliminación de datos duplicados del lado del cliente, todas las demás operaciones del cliente (por ejemplo, las operaciones de copia de seguridad) continúan. Sólo se inhabilita la eliminación de datos duplicados del lado del cliente. Si se inhabilita la eliminación de datos duplicados del lado del cliente en un nodo porque se ha detectado un ataque potencial, el servidor elimina los duplicados de los datos elegibles para la eliminación de datos duplicados del lado del cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
.-0-----  
>>-Set DEDUPVERificationlevel--+-+-----<<  
'-valor_porcentaje-'
```

### Parámetros

valor\_porcentaje (Obligatorio)

Especifique un valor entero entre 0 y 100 para indicar el porcentaje de extensiones del cliente que se deben verificar. El valor 0 indica que no se verifica ninguna extensión del cliente. El valor predeterminado para este comando es 0.

Consejos:

- La verificación de extensiones consume potencia de procesamiento y perjudica el rendimiento del servidor. Para obtener un rendimiento óptimo, no especifique valores superiores a 10 en este mandato.
- Para visualizar el valor actual de SET DEDUPVERIFICATIONLEVEL, emita el comando QUERY STATUS.

### Ejemplo: especificar un nivel mínimo de verificación de eliminación de datos duplicados

Para especificar que se verifique el 1% de las extensiones creadas durante la eliminación de datos duplicados del lado del cliente, emita el siguiente mandato:

```
set dedupverificationlevel 1
```

### Ejemplo: desactivar la verificación de la eliminación de datos duplicados

Para especificar que no se verifique ninguna de las extensiones creadas durante la eliminación de datos duplicados del lado del cliente, emita el siguiente mandato:

```
set dedupverificationlevel 0
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET DEDUPVERIFICATIONLEVEL

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.

Comando	Descripción
QUERY CONTENT	Visualiza información sobre archivos de un volumen de agrupación de almacenamiento.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## SET DEFAULTAUTHENTICATION (Establecer el método de autenticación predeterminado para los mandatos REGISTER NODE y REGISTER ADMIN)

Utilice este mandato para configurar el método de autenticación de contraseña predeterminada para nodos y administradores que son resultado de los mandatos REGISTER NODE o REGISTER ADMIN .

Si especifica LDAP, establece el valor predeterminado para autenticarse en un directorio externo para cualquier mandato REGISTER NODE o REGISTER ADMIN nuevo. Este mandato facilita el registro de los nodos o administradores cuando se utiliza un servidor de directorios LDAP.

Consejo: El valor de autenticación predeterminado se puede sobrescribir cuando se especifica el método de autenticación en un REGISTER NODE o REGISTER ADMIN.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

### Sintaxis

```
>>-SET DEFAULTAUTHentication---Local-----<<
                        '-Ldap--'
```

### Parámetros

#### Local

Especifica que cualquier mandato REGISTER NODE o REGISTER ADMIN que emita en el futuro utilizará LOCAL como valor del parámetro de autenticación predeterminado. Las contraseñas autenticadas localmente son las que se almacenan en el servidor de IBM Spectrum Protect. Las contraseñas autenticadas a nivel local no distinguen entre mayúsculas y minúsculas.

#### LDap

Especifica que cualquier mandato REGISTER NODE o REGISTER ADMIN que emita en el futuro utilizará LDAP como valor del parámetro de autenticación predeterminado. Las contraseñas autenticadas mediante LDAP son aquellas que se almacenan en el servidor de directorios LDAP y distinguen entre mayúsculas y minúsculas.

### Ejemplo: establecer el valor de autenticación de contraseña predeterminada en LDAP

Especifique que cualquier mandato REGISTER NODE o REGISTER ADMIN que emite autentica contraseñas con un servidor de directorios LDAP.

```
set defaultauthentication ldap
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con SET DEFAULTAUTHENTICATION

Comando	Descripción
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.



Comando	Descripción
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.

## DISSIMILARPOLICIES SET (Habilitar las políticas en el servidor de réplica de destino para gestionar datos replicados)

Utilice el mandato SET DISSIMILARPOLICIES para habilitar las políticas que están definidas en el servidor de réplica de destino para gestionar datos del nodo cliente replicados. Si no utiliza las políticas en el servidor de réplica de destino, los datos del nodo cliente replicados se gestionan mediante políticas en el servidor de réplica de origen.

Asegúrese de que esté instalado IBM Spectrum Protect versión 7.1.1 o posterior en los servidores de réplica de origen y destino antes de emitir este mandato. Emita este mandato en el servidor de réplica de origen.

Antes de utilizar las políticas que están definidas en un servidor de réplica de destino, debe emitir el mandato VALIDATE REPLPOLICY para ese servidor de réplica de destino. Este mandato muestra las diferencias entre las políticas para los nodos cliente en el servidor de réplica de origen y las políticas en el servidor de réplica de destino. Puede modificar las políticas en el servidor de réplica de destino antes de habilitar estas políticas para gestionar datos de nodo cliente replicados.

Para obtener el nombre del servidor de réplica de destino para el que desea gestionar datos y para comprobar si las políticas en el servidor de réplica de destino se establecen en ON, utilice el mandato QUERY REPLSERVER. Durante la instalación este valor se establece en OFF.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set DISSIMILARPolicies--nombre_servidor_destino--+++++---->>
                                     .-OFF-.
                                     +-OFF-+
                                     '-ON--'
```

### Parámetros

nombre\_servidor\_destino (Obligatorio)

Especifica el nombre del servidor de réplica de destino para el que desea habilitar las políticas.

ON

Especifica que los datos del nodo cliente replicados los gestionan políticas que están definidas en el servidor de réplica de destino.

OFF

Especifica que los datos del nodo cliente replicados los gestionan políticas que están definidas en el servidor de réplica de origen. El valor predeterminado es desactivado (Off).

### Ejemplo: utilice las políticas en un servidor de réplica de destino

Para datos de nodo cliente replicados del servidor de réplica de destino, CVTCVS\_LXS\_SRV2, emita el mandato siguiente en el servidor de réplica de origen:

```
set dissimilarpolicies CVTCVS_LXS_SRV2 on
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con DISSIMILARPOLICIES SET

Comando	Descripción
---------	-------------

Comando	Descripción
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
VALIDATE REPLPOLICY	Verifica las políticas en el servidor de réplica de destino.

## SET DRMACTIVEDATASTGPOOL (especificar las agrupaciones de datos activos que gestionará DRM)

Utilice este comando para especificar los nombres de las agrupaciones de datos activos que han de recuperarse tras haberse producido un siniestro. IBM Spectrum Protect utiliza estos nombres si el comando PREPARE , MOVE DRMEDIA o QUERY DRMEDIA no incluye el parámetro ACTIVEDESTGPOOL.

De manera predeterminada, los volúmenes de las agrupaciones de datos activos no pueden seleccionarse para que el gestor de recuperación ante siniestro los procese. Para procesar volúmenes de agrupación de datos activos, debe emitir el comando SET DRMACTIVEDATASTGPOOL o debe utilizar el parámetro de línea de comandos ACTIVEDESTGPOOL en el comando MOVE DRMEDIA, QUERY DRMEDIA o PREPARE.

Utilice el comando QUERY DRMSTATUS para que se visualicen los valores actuales.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set DRMACTIVEDatastgpool----->
      .-,-----
      v |
>----nombre_agrupación_datos_activos+-----<
```

### Parámetros

nombre\_agrupación\_datos\_activos (Necesario)

Especifica los nombres de agrupación de datos activos. Cuando existan varios nombres, separe éstos mediante comas, sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados alterarán temporalmente los valores anteriores. Si especifica una serie nula (""), se eliminarán todos los nombres actuales y no se procesará ningún volumen de agrupación de datos activos cuyo estado sea MOUNTABLE si no se han especificado explícitamente como parámetros del comando MOVE DRMEDIA, QUERY DRMEDIA o PREPARE.

### Ejemplo: establecer una agrupación de datos activos como agrupación que puede seleccionarse

Establecer ACTIVEDESTGPOOL1 como agrupación de datos activos que puede seleccionarse.

```
set drmactivedatapool activedatastgpool1
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMACTIVEDATASTGPOOL

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.

Comando	Descripción
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.

## SET DRMCHECKLABEL (Especificar comprobación de etiquetas)

Utilice este comando para especificar si IBM Spectrum Protect ha de leer las etiquetas de los medios secuenciales a los que se ha dado de baja mediante el comando MOVE DRMEDIA. En la instalación, el valor de DRMCHECKLABEL se establece en YES.

Utilice el comando QUERY DRMSTATUS para comprobar los valores actuales.

 Sistemas operativos AIX  Sistemas operativos Linux Este comando no se utiliza con los tipos de dispositivo 349X.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

>>-Set DRMCHECKLabel-----><
      .-Yes-.
      +-Yes-+
      '-No--'

```

### Parámetros

Yes

Especifica que IBM Spectrum Protect ha de leer las etiquetas de los medios secuenciales a los que se ha dado de baja mediante el comando MOVE DRMEDIA.

No

Especifica que IBM Spectrum Protect no lee las etiquetas de los medios secuenciales que ha dado de baja el comando MOVE DRMEDIA.

### Ejemplo: Especificar que no se realice la comprobación de etiquetas

Especifique que no se realizado ninguna comprobación de etiquetas.

```
set drmchecklabel no
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMCHECKLABEL

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMCMDFILENAME (Especificar el nombre de un archivo que ha de contener comandos)

Utilice este comando para especificar el nombre del archivo que puede contener los comandos que se crean al emitir los comandos MOVE DRMEDIA o QUERY DRMEDIA. Si no se emite SET DRMCMDFILENAME, los comandos MOVE DRMEDIA o QUERY DRMEDIA generan un nombre de archivo.

Utilice el comando QUERY DRMSTATUS para que se muestre el nombre de archivo de comandos actual.

### Clase de privilegio

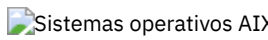
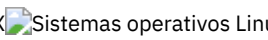
Para emitir este comando, debe tener privilegio de sistema.

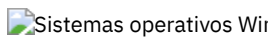
## Sintaxis

```
>>-Set DRMCMDfilename--nombre_archivo-----<<
```

## Parámetros

nombre\_archivo (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el nombre de la ruta completa del archivo que ha de contener los comandos que se han creado mediante los comandos MOVE DRMEDIA o QUERY DRMEDIA.

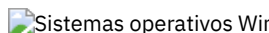
 Sistemas operativos Windows Especifica el nombre de la ruta completa del archivo que ha de contener los comandos que se han creado mediante los comandos MOVE DRMEDIA o QUERY DRMEDIA. El nombre del archivo puede contener un máximo de 259 caracteres.

Atención: Si ya existe un archivo con el mismo nombre, los comandos MOVE DRMEDIA o QUERY DRMEDIA intentan utilizarlo, y se graba encima de los datos existentes.

## Ejemplo: especificar el nombre del archivo que ha de contener los comandos DRMEDIA

 Sistemas operativos AIX  Sistemas operativos Linux Especificar el nombre de archivo /adsm/drm/orm/exec.cmds.

```
set drmcmdfilename /adsm/drm/orm/exec.cmds
```

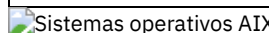
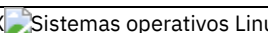
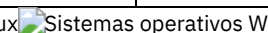
 Sistemas operativos Windows Especificar el nombre de archivo c:\drm\orm\exec.cmd.

```
set drmcmdfilename c:\drm\orm\exec.cmd
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMCMDFILENAME

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## SET DRMCOPYCONTAINERSTGPOOL (Especificar las agrupaciones de copia de contenedor que han de procesar los mandatos DRM)

Utilice este mandato para especificar las agrupaciones de almacenamiento de copia de contenedor que ha de procesar el mandato MOVE DRMEDIA o QUERY DRMEDIA cuando ese mandato no incluye el parámetro COPYCONTAINERSTGPOOL.

De forma predeterminada, los mandatos MOVE DRMEDIA y QUERY DRMEDIA no procesan los volúmenes de las agrupaciones de almacenamiento de copia de contenedor. Debe emitir el mandato SET DRMCOPYCONTAINERSTGPOOL o utilizar el parámetro COPYCONTAINERSTGPOOL en el mandato MOVE DRMEDIA o QUERY DRMEDIA.

Consejo: Para visualizar los valores actuales, utilice el mandato QUERY DRMSTATUS.

## Clase de privilegio

Para emitir este mandato, debe tener privilegios del sistema.

## Sintaxis

```
          .-,-----  
          |  
          v          |  
>>-Set DRMCOPYContainerstgpool----nombre_agrupación+-----<<
```

## Parámetros

nombre\_agrupación (Obligatorio)

Especifica los nombres de las agrupaciones de almacenamiento de copia de contenedor. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados sustituyen a todos los valores anteriores. Si especifica una serie nula (""), se eliminan todos los nombres actuales.

## Ejemplo: especifique las agrupaciones de almacenamiento que han de procesar los mandatos MOVE DRMEDIA y QUERY DRMEDIA

Establezca CONTCOPY1 y CONTCOPY2 como las agrupaciones de almacenamiento de copia de contenedor a procesar.

```
set drmcopystgpool contcopy1,contcopy2
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET DRMCOPYCONTAINERSTGPOOL

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMCOPYSTGPOOL (Especificar las agrupaciones de almacenamiento de copia que gestionará DRM)

Utilice este comando para especificar los nombres de las agrupaciones de almacenamiento de copia que se recuperarán a continuación de un siniestro. IBM Spectrum Protect utiliza estos nombres si el comando PREPARE no incluye el parámetro COPYSTGPOOL.

Si el comando MOVE DRMEDIA o QUERY DRMEDIA no incluye el parámetro COPYSTGPOOL, el comando procesa los volúmenes cuyo estado es MOUNTABLE y que se encuentran en la agrupación de almacenamiento de copia que indica el comando SET DRMCOPYSTGPOOL. En la instalación, todas las agrupaciones de almacenamiento de copia se pueden seleccionar para el proceso de DRM.

Utilice el comando QUERY DRMSTATUS para que se visualicen los valores actuales.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
set drmcopystgpool <nombre_agrupación_copia>
```

## Parámetros

nombre\_agrupación\_copia (Obligatorio)

Especifica los nombres de agrupación de almacenamiento de copia. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín. Los nombres especificados sustituyen a todos los valores anteriores. Si especifica una serie nula (""), se eliminan todos los nombres actuales y se pueden seleccionar todas las agrupaciones de almacenamiento de copia para el proceso.

## Ejemplo: establecer una agrupación de almacenamiento de copia como agrupación que puede seleccionarse

Establecer COPYSTGPOOL1 como la agrupación de almacenamiento de copia seleccionable.

```
set drmcopystgpool copystgpool1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMCOPYSTGPOOL

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMPRIMSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento primario.

## SET DRMCOURIERNAME (Especificar el nombre del transportista)

Utilice este comando para especificar el nombre del transportista. En la instalación, este nombre se establece en COURIER. El comando MOVE DRMEDIA utiliza el nombre del transportista para establecer la ubicación de los volúmenes que se establecen en el estado COURIER.

Puede utilizar QUERY DRMSTATUS para ver el nombre del transportista.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set DRMCOURiername--courier_name-----<<
```

## Parámetros

nombre\_transportista (Obligatorio)

Especifica el nombre del transportista. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

## Ejemplo: establecer el nombre del transportista

Establecer el nombre del transportista en Joe's Courier Service.

```
set drmcouriername "Joe's Courier Service"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMCOURIERNAME

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

Utilice este mandato para especificar cuándo una serie de copia de seguridad de base de datos es seleccionable para caducarla.

El valor que establece este mandato se aplica tanto a una serie de copia de seguridad de instantánea de base de datos como a una serie de copia de seguridad de base de datos completa e incremental. Cualquier tipo de serie de copia de seguridad de base de datos se considera seleccionable para caducidad si se cumplen todas las condiciones siguientes:

- La antigüedad del último volumen de la serie supera el valor de caducidad establece con el mandato SET DRMDBBACKUPEXPIREDAYS y el valor especificado para el parámetro DELgraceperiod con el mandato DEFINE SERVER. El parámetro DELgraceperiod solo se aplica a las copias de seguridad de base de datos remotas. El valor predeterminado para el parámetro DELgraceperiod es de 5 días. Por ejemplo, si establece el valor para el mandato SET DRMDBBACKUPEXPIREDAYS en 7 días y establece el valor para el parámetro DELgraceperiod en 6 días, la serie de copia de seguridad de base de datos remota no caduca hasta que han transcurrido 13 días.
- En el caso de los volúmenes que no son volúmenes virtuales, todos los volúmenes de la serie se encuentran en el estado VAULT.
- El volumen no forma parte de la serie de copia de seguridad de base de datos más reciente.

Recuerde: La serie de copia de seguridad más reciente de cualquiera de los dos tipos no se suprime. Consulte el mandato MOVE DRMEDIA para obtener más información acerca de la caducidad de los volúmenes de copia de seguridad de la base de datos que no son volúmenes virtuales. Consulte el mandato EXPIRE INVENTORY para obtener más información acerca de la caducidad de los volúmenes de copia de seguridad de la base de datos que son volúmenes virtuales.

Utilice el mandato QUERY DRMSTATUS para ver el número de días especificado.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set DRMDBBackupexpiredays--días-----<<
```

## Parámetros

días (Obligatorio)

Especifica el número de días que debe transcurrir desde la creación de una serie de base de datos hasta que sea seleccionable para caducidad. El número de días debe coincidir con el período de retardo de reutilización de volúmenes para las agrupaciones de almacenamiento de copia que gestiona el gestor de recuperación ante siniestro. Especifique un valor entero de 0 a 9999.

## Ejemplo: establecer la caducidad de la serie de copia de seguridad de la base de datos

Establecer el valor de caducidad de serie de copia de seguridad de base de datos en 60.

```
set drmdbbackupexpiredays 60
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMDBBACKUPEXPIREDAYS

Comando	Descripción
DSMSERV RESTORE DB	Restaura una base de datos de IBM Spectrum Protect.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

## SET DRMFILPROCESS (Especificar el proceso de archivos)

Utilice este comando para especificar si los comandos MOVE DRMEDIA o QUERY DRMEDIA deben procesar los volúmenes de copia de seguridad de base de datos y los volúmenes de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE. Durante la instalación este valor se establece en NO. Utilice el mandato QUERY DRMSTATUS para determinar el valor actual.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set DRMFILEProcess--+-No-- .-----<<
                               +-No--+
                               '-Yes-'
```

### Parámetros

No

Especifica que los comandos MOVE DRMEDIA y QUERY DRMEDIA no procesan los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE. Este es el valor predeterminado.

Yes

Especifica que los comandos MOVE DRMEDIA y QUERY DRMEDIA procesan los volúmenes de copia de seguridad de base de datos y de agrupación de almacenamiento de copia que se asocian a una clase de dispositivo FILE.

### Ejemplo: especificar que los comandos DRMEDIA no incluyan clases de dispositivo de tipo FILE

Establecer el valor del proceso de archivos en no.

```
set drmfileprocess no
```

### Comandos relacionados



Tabla 1. Comandos relacionados con SET DRMFILEPROCESS


Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMINSTRPREFIX (Especificar el prefijo de los nombres de archivos de instrucciones de recuperación)

Utilice este comando para especificar un prefijo para el nombre de archivo de instrucciones de recuperación. Si emite este comando, IBM Spectrum Protect utilizará el prefijo especificado si el comando PREPARE se ha emitido sin el prefijo INSTRPREFIX.

Utilice el comando QUERY DRMSTATUS para visualizar el valor actual del prefijo.

 Sistemas operativos AIX  Sistemas operativos Linux El prefijo es el directorio de trabajo actual del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Si no se establece ningún prefijo, el prefijo se establece en el directorio que representa la instancia del servidor, que generalmente es el directorio desde donde se ha instalado el servidor originalmente.

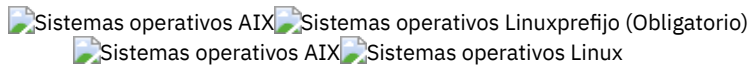
## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set DRMINSTRPrefix--prefijo-----<<
```





Especifica un prefijo de nombre de ruta para los archivos que contienen las instrucciones de recuperación. Al procesar el comando PREPARE, IBM Spectrum Protect añade el nombre de la sección del archivo de plan de recuperación adecuado para buscar el archivo. La longitud máxima es de 250 caracteres.

El prefijo puede ser uno de los siguientes:

- **Ruta del directorio:** Finalice el prefijo con una barra inclinada (/). Por ejemplo:

```
/admsrv/recinstr/
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/admsrv/recinstr/RECOVERY.INSTRUCTIONS.GENERAL
```

- **Ruta del directorio seguida de una serie:** IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
/admsrv/recinstr/accounts
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

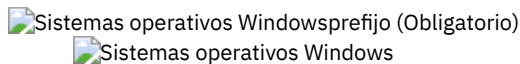
```
/admsrv/recinstr/accounts.RECOVERY.INSTRUCTIONS.GENERAL
```

- **Sólo serie:** IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado.
  - IBM Spectrum Protect utiliza el nombre del directorio de trabajo actual. Por ejemplo, el directorio de trabajo actual es /opt/tivoli/tsm/server/bin. Especifique lo siguiente:

```
shipping
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
/opt/tivoli/tsm/server/bin/shipping.RECOVERY.INSTRUCTIONS.GENERAL
```



Especifica un prefijo de nombre de ruta para los archivos que contienen las instrucciones de recuperación. Al procesar el comando PREPARE, IBM Spectrum Protect añade el nombre de la sección del archivo de plan de recuperación adecuado para buscar el archivo. La longitud máxima son 200 caracteres.

El prefijo puede ser uno de los siguientes:

- **Ruta del directorio:** Finalice el prefijo con una barra inclinada invertida (\). Por ejemplo:

```
c:\admsrv\recinstr\
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
c:\admsrv\recinstr\RECOVERY.INSTRUCTIONS.GENERAL
```

- **Ruta del directorio seguida de una serie:** IBM Spectrum Protect trata la serie como parte del nombre de archivo. Por ejemplo:

```
c:\admsrv\recinstr\accounts
```

En el caso del archivo RECOVERY.INSTRUCTIONS.GENERAL, el nombre de archivo resultante sería:

```
c:\admsrv\recinstr\accounts.RECOVERY.INSTRUCTIONS.GENERAL
```



- **Sólo serie:** IBM Spectrum Protect especifica la ruta del directorio y agrega el nombre de sección del archivo del plan de recuperación adecuado. La ruta del directorio es el directorio que representa a esta instancia del servidor de IBM Spectrum Protect (normalmente, el directorio de instalación original del servidor de IBM Spectrum Protect). Por ejemplo, el directorio que representa a esta instancia del servidor es c:\Archivos de programa\Tivoli\TSM;\server2 y se especifica el prefijo siguiente:

```
shipping
```


El nombre del archivo del plan de recuperación resultante es:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.19971115.051421
```

## Ejemplo: especificar el prefijo del plan de recuperación

 Sistemas operativos AIX  Sistemas operativos Linux Especificar la lectura de las instrucciones del plan de recuperación del directorio /drmpln/primesrv.

```
set drminstrprefix /drmpln/primesrv/
```

 Sistemas operativos Windows Especificar la lectura de las instrucciones del plan de recuperación del directorio c:\win32app\ibm\adsm\server2\.

```
set drminstrprefix c:\win32app\ibm\adsm\server2\
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMINSTRPREFIX

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMNOTMOUNTABLENAME (Especificar el nombre de la ubicación no montable)

Utilice este comando para especificar el nombre de la ubicación en el local para almacenar los medios. En la instalación, el nombre se establece en NOTMOUNTABLE. Utilice el comando QUERY DRMSTATUS para ver el nombre de la ubicación.

El comando MOVE DRMEDIA utiliza el nombre de la ubicación para establecer la ubicación de los volúmenes que se traspan al estado NOTMOUNTABLE.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set DRMNOTMOUNTABLENAME--ubicación-----<<
```

## Parámetros

ubicación (Obligatorio)

Especifica el nombre de la ubicación en el local para almacenar los medios. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

## Ejemplo: especificar el nombre de la ubicación en el local

Establecer el nombre de la ubicación en room 123/31.

```
set drmnotmountable "room 123/31"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMNOTMOUNTABLENAME

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.

Comando	Descripción
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMPLANPREFIX (Especificar un prefijo para nombres de archivos del plan de recuperación)

Utilice este comando para especificar un prefijo para un nombre de archivo del plan.

Si emite este comando, IBM Spectrum Protect utilizará el prefijo especificado si el comando PREPARE no incluye el parámetro PLANPREFIX.

Utilice el comando QUERY DRMSTATUS para visualizar el valor actual del prefijo del plan de recuperación.



### Clase de privilegio



Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set DRMPLANPrefix--prefijo-----<<
```

### Parámetros

 Sistemas operativos AIX  Sistemas operativos Linux prefijo (Obligatorio)

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el prefijo de un nombre de archivo de plan de recuperación. La longitud máxima del prefijo son 250 caracteres. Si especifica una serie nula (""), el prefijo actual se elimina y el servidor utiliza el algoritmo que se describe en el parámetro PLANPREFIX del comando PREPARE.

Para el prefijo, puede especificar:

- **Una ruta de directorio seguida de una barra inclinada (/):** IBM Spectrum Protect añade al prefijo la fecha y la hora en formato `aaaammdd.hhmmss`. Por ejemplo, SET DRMPLANPREFIX se ha establecido en lo siguiente:

```
/admsrv/recplans/
```

El nombre del archivo del plan de recuperación resultante es:

```
/admsrv/recplans/19971115.051421
```

- **Una ruta del directorio seguida de una serie:** IBM Spectrum Protect utiliza la serie como parte del nombre del archivo. IBM Spectrum Protect agrega al prefijo la fecha y la hora con el formato `.aaaammdd.hhmmss` (observe el punto inicial). Por ejemplo, SET DRMPLANPREFIX está establecido del modo siguiente:

```
/admsrv/recplans/accounting
```

El nombre de archivo del plan de recuperación resultante será:

```
/admsrv/recplans/accounting.19971115.051421
```

- **Una serie que no tiene antepuesta una ruta del directorio:** IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato `.aaaammdd.hhmmss` (observe el punto inicial). IBM Spectrum Protect determina la ruta del directorio del modo siguiente:


- IBM Spectrum Protect utiliza el nombre de ruta del directorio de trabajo actual del servidor de IBM Spectrum Protect. Por ejemplo, el directorio de trabajo actual de IBM Spectrum Protect es `/opt/tivoli/tsm/server/bin`. El comando SET DRMPLANPREFIX está establecido del modo siguiente:

```
shipping
```

El nombre del archivo del plan de recuperación resultante es:

```
/opt/tivoli/tsm/server/bin/shipping.19971115.051421
```

 Sistemas operativos Windows prefijo (Obligatorio)

 Sistemas operativos Windows Especifica el prefijo del nombre de ruta que se utiliza para generar el nombre del archivo del plan de recuperación. El prefijo puede tener hasta 200 caracteres. IBM Spectrum Protect utiliza el prefijo si el mandato PREPARE se emite sin el parámetro PLANPREFIX. IBM Spectrum Protect crea un nombre de archivo de plan de recuperación exclusivo

añadiendo al prefijo el formato de la fecha y la hora: `aaaaamddd.hhmmss` (por ejemplo, 19951115.051421). Si especifica una serie nula (""), el prefijo actual se elimina y el servidor utiliza el algoritmo que se describe en el parámetro `PLANPREFIX` del mandato `PREPARE`.

Para el prefijo, puede especificar:

1. Una ruta de directorio
2. Una ruta de directorio seguida por una serie
3. Una serie

A continuación se describen las reglas de las especificaciones de prefijos posibles:

1. Para especificar una ruta de directorio para el prefijo, finalice el prefijo con una barra inclinada invertida (`\`). IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato `aaaaamddd.hhmmss`. Por ejemplo, el mandato `SET DRMPLANPREFIX` se ha establecido de este modo:

```
c:\admsrv\recplans\  
c:\admsrv\recplans\19951115.051421
```

El nombre del archivo del plan de recuperación resultante es:

```
c:\admsrv\recplans\19951115.051421
```

Importante: Si emite el comando `SET DRMPLANPREFIX` desde un cliente de línea de comandos y el último carácter de la línea de comandos es una barra inclinada invertida, IBM Spectrum Protect interpretará que se trata de un carácter de continuación. Para evitar esto, delimite el prefijo con comillas. Por ejemplo: `"c:\admsrv\recplans\"`

2. Si el prefijo es una ruta del directorio seguida de una serie, IBM Spectrum Protect utiliza la serie como parte del nombre de archivo. IBM Spectrum Protect agrega al prefijo la fecha y la hora con el formato `.aaaaamddd.hhmmss` (observe el punto inicial). Por ejemplo, el mandato `SET DRMPLANPREFIX` se ha establecido de este modo:

```
c:\admsrv\recplans\accounting  
c:\admsrv\recplans\accounting.19951115.051421
```

El nombre de archivo del plan de recuperación resultante será el siguiente:

```
c:\admsrv\recplans\accounting.19951115.051421
```

3. Si el prefijo es una serie que no tiene delante una ruta, IBM Spectrum Protect agrega al prefijo la información de fecha y hora con el formato `.aaaaamddd.hhmmss` (observe el punto inicial). La ruta que IBM Spectrum Protect utiliza es la que representa a esta instancia del servidor de IBM Spectrum Protect (normalmente, el directorio desde donde se ha instalado originalmente el servidor de IBM Spectrum Protect). Por ejemplo, el directorio que representa esta instancia del servidor es `c:\Archivos de programa\Tivoli\TSM;\server2`, y decide establecer el prefijo en:




```
shipping  
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.19951115.051421
```



El nombre de archivo del plan de recuperación resultante será:

```
c:\Archivos de programa\Tivoli\TSM;\server2\shipping.19951115.051421
```

## Ejemplo: especificar un prefijo para los nombres de archivo de plan de recuperación

Especificar un prefijo de modo que los archivos de plan de recuperación generados se almacenen en el directorio siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux/drmplan/primsrv
-  Sistemas operativos Windows:c:\drmtest\prepare\

Emita el comando:  Sistemas operativos AIX  Sistemas operativos Linux

```
set drmprefix /drmplan/primsrv/
```

 Sistemas operativos Windows

```
set drmprefix c:\drmtest\prepare\
```

## Comandos relacionados

Tabla 1. Comandos relacionados con `SET DRMPLANPREFIX`

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMPLANVPOSTFIX (Especificar la sustitución de los nombres de volúmenes)

Utilice este comando para especificar el carácter que se ha de agregar a los nombres de volúmenes de sustitución del archivo del plan de recuperación. El carácter puede ayudarle a localizar o generar los nombres de volúmenes de sustitución cuando utiliza el archivo del plan de recuperación.

Durante la instalación, el carácter se establece en @. IBM Spectrum Protect genera nombres de sustitución para los volúmenes de agrupación de almacenamiento primaria que el comando DEFINE VOLUME ha añadido. Utilice el carácter agregado para:

- Localizar los nombres de volúmenes de sustitución en las secciones del plan de recuperación para poder cambiar los nombres en el momento de la recuperación. Por ejemplo, puede desconocer los nombres de los volúmenes de cinta disponibles en el local de recuperación.
- Generar los nombres de volúmenes de sustitución. Necesita un convenio de denominación que funcione para todos los tipos de dispositivo de las agrupaciones de almacenamiento primarias. Tenga en cuenta lo siguiente:
  - La longitud generada del nombre de volumen de sustitución
  - Los caracteres legales del nombre del volumen de sustitución
  - Los conflictos con nombres de volúmenes existentes
  - Los nombres de volumen de sustitución deben ser distintos de todos los nombres de volúmenes destruidos, existentes o nuevos.

Utilice el comando QUERY DRMSTATUS para ver el carácter que se ha añadido al final de los nombres de los volúmenes de sustitución.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis


```
>>-Set DRMPLANVpostfix--carácter-----<<
```


### Parámetros

carácter (Obligatorio)

Especifica el carácter que se agrega a los nombres de volúmenes de sustitución en el archivo de plan de recuperación.

Especifique un carácter alfanumérico o especial.

 Sistemas operativos AIX Atención: Un carácter especial puede ocasionar resultados imprevisibles en el shell o en el entorno de línea de comandos de AIX.

 Sistemas operativos Windows Atención: Un carácter especial puede ocasionar resultados imprevisibles en el proceso por lotes o en el entorno de línea de comandos de Windows.

### Ejemplo: especificar el carácter que ha de añadirse a los nombres de los volúmenes de sustitución

Establecer el carácter a agregar a los nombres de volumen de sustitución en R.

```
set drmplnvpostfix R
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMPLANVPOSTFIX

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET DRMPRIMSTGPOOL (Especificar las agrupaciones de almacenamiento primarias que ha de gestionar DRM)

Utilice este comando para especificar los nombres de las agrupaciones de almacenamiento primarias que desea recuperar. Si el comando PREPARE no incluye el parámetro PRIMSTGPOOL, DRM procesará los nombres especificados en este comando.

Utilice el comando QUERY DRMSTATUS para que se visualicen los valores actuales. Durante la instalación, todas las agrupaciones de almacenamiento primarias definidas en el servidor se pueden seleccionar para el proceso de DRM.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
      .-.,-----  
      v                                     |  
>>-Set DRMPRIMstgpool----nombre_agrupación_primaria+-----><
```

## Parámetros

nombre\_agrupación\_primaria (Obligatorio)

Especifica los nombres de las agrupaciones de almacenamiento primarias que desea recuperar. Puede separar varios nombres con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres. Los nombres especificados sustituirán a los valores anteriores. Si especifica una serie nula (""), se eliminan todos los nombres actuales y se pueden seleccionar todas las agrupaciones de almacenamiento primarias para el proceso de DRM.

## Ejemplo: establecer una agrupación de almacenamiento primaria que DRM ha de gestionar

Establecer en PRIMSTGPOOL1 la agrupación de almacenamiento primaria que ha de gestionar DRM.

```
set drmpriestgpool primstgpool1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMPRIMSTGPOOL

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
SET DRMCOPYSTGPOOL	Especifica que DRM gestiona las agrupaciones de almacenamiento.

## SET DRMRPFEXPIREDAYS (Establecer los criterios de caducidad del archivo del plan de recuperación)

Utilice este mandato para especificar cuándo los archivos de planes de recuperación son seleccionables para caducarlos. Este mandato y el proceso de caducidad sólo se aplican a los archivos de plan de recuperación que se han creado con el parámetro DEVCLASS especificado en el mandato PREPARE (es decir, volúmenes virtuales de tipo RPFILe y RPSNAPSHOT). El proceso de caducidad del servidor de origen caduca los archivos de planes almacenados en el servidor de destino. Los archivos de planes de recuperación creados localmente no caducan.

Un archivo RPFILe está asociado con una serie de copia de seguridad de base de datos completa más las incrementales. Un archivo RPFsnapshot está asociado con una serie de copia de seguridad de instantánea de base de datos.

Atención: Los últimos archivos RPFILe y RPFsnapshot no se suprimen nunca.

Un archivo del plan recuperación es seleccionable para caducarlo si se cumplen las dos condiciones siguientes:

- El último archivo del plan de recuperación de la serie supera el valor de caducidad especificado con el mandato SET DRMRPFEXPIREDAYS y el valor que se ha especificado para el parámetro DELgraceperiod en el mandato DEFINE SERVER. El valor predeterminado para el parámetro DELgraceperiod es de 5 días. Por ejemplo, si establece el valor para el mandato SET DRMRPFEXPIREDAYS en 80 días y establece el valor para el parámetro DELgraceperiod en 6 días, el archivo de plan de recuperación no caduca hasta que han transcurrido 86 días.
- El último archivo del plan de recuperación no está asociado con la serie de copia de seguridad de base de datos más reciente.

Para obtener información acerca del proceso de caducidad, consulte el mandato EXPIRE INVENTORY.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set DRMRPFExpiredays--días-----<<
```

## Parámetros

---

días (Obligatorio)

Especifica el número de días que deben transcurrir para que caduque un archivo del plan de recuperación. Puede especificar un número de 0 a 9999. Durante la instalación, este valor se establece en 60.

## Ejemplo: establecer la caducidad del plan de recuperación

---

Establecer el valor de caducidad del archivo del plan de recuperación en 30.

```
set drmrpexpiredays 30
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con SET DRMRPFEXPIREDDAYS

Comando	Descripción
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.
QUERY RPFCONTENT	Muestra el contenido de un archivo del plan de recuperación.
QUERY RPFFILE	Muestra información sobre archivos del plan de recuperación.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.

## SET DRMVaultName (Especificar el nombre de la cámara de seguridad)

---

Utilice este comando para especificar el nombre de la cámara de seguridad. En la instalación, el nombre se establece en VAULT. Utilice el comando QUERY DRMSTATUS para ver el nombre de la cámara de seguridad.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-SET DRMVaultname--vault_name-----<<
```

## Parámetros

---

nombre\_cámara\_seguridad (Obligatorio)

Especifica el nombre de la cámara de seguridad. El nombre puede tener hasta 255 caracteres. El nombre debe estar delimitado por comillas si contiene algún carácter en blanco.

## Ejemplo: especificar un nombre de cámara de seguridad

---

Especificar `ironmountain` como nombre de la cámara de seguridad.

## Comandos relacionados

Tabla 1. Comandos relacionados con SET DRMVAULTNAME

Comando	Descripción
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY DRMSTATUS	Visualiza los parámetros del sistema de DRM.

## SET EVENTRETENTION (Establecer el período de retención de los registros de eventos)

Utilice este comando para establecer el período de retención de los registros de eventos de la base de datos del servidor que le permitirá supervisar las planificaciones completadas. Se crea un registro de eventos cuando se arranca o falla el proceso de un comando planificado.

Puede ajustar el período de tiempo durante el que el servidor mantiene la información de eventos para evitar datos insuficientes o caducados. El servidor elimina automáticamente de la base de datos los registros de eventos una vez transcurrido el período de retención y el margen de puesta en marcha del evento.

Puede emitir el comando QUERY EVENT para que se visualice información acerca de los eventos planificados y que se han completado.

Puede emitir el comando DELETE EVENT para suprimir registros de eventos, con independencia de si ha transcurrido o no el período de retención de éstos.

Puede emitir el comando QUERY STATUS para que se visualice el valor del período de retención de eventos. Durante la instalación, este valor se establece en 10 días.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set EVentretention--días-----<<
```

### Parámetros

días (Obligatorio)

El número de días que la base de datos retiene los registros de eventos. Puede especificar un entero de 0 a 9999. El valor 0 indica que sólo se retienen los registros de eventos del día actual.

### Ejemplo: establecer el período de retención de los registros de eventos

Establecer el período de retención en 15 días.

```
set eventretention 15
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET EVENTRETENTION

Comando	Descripción
DELETE EVENT	Elimina los registros de eventos antes de una fecha y hora especificadas.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.



Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET FAILOVERHLADDRESS (Establecer una dirección de alto nivel de migración tras error)

Utilice este mandato para especificar la dirección IP que un cliente utiliza para conectarse a este servidor como el servidor de réplica secundario durante la migración tras error, si la dirección es diferente a la dirección IP que se ha especificado para el proceso de réplica.

Debe especificar la dirección del servidor que se utiliza si la dirección de alto nivel (HLA) es diferente. Este mandato solamente es necesario si se utilizan redes dedicadas para la comunicación entre servidores y el acceso de cliente.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema.

### Sintaxis

```
>>-SET FAILOVERHLaddress--dirección_alto_nivel-----<<
```

### Parámetros

dirección\_alto\_nivel (Obligatorio)

Especifica una dirección de alto nivel (HLA) de servidor como nombre decimal con puntos o nombre de host para utilizar durante la recuperación de errores. Si especifica un nombre de host, debe estar disponible un servidor que pueda resolver el nombre al formato decimal con puntos.

Para eliminar la dirección IP de migración tras error, emita el comando sin especificar ningún valor.

### Ejemplo: Establecer una dirección de alto nivel para la recuperación de errores

El nombre de la dirección de alto nivel que desea establecer para las operaciones de migración tras error en este servidor.

```
set failoverhladdress server1
```

### Ejemplo: eliminar una dirección de alto nivel

Para eliminar una dirección de alto nivel de un servidor de migración tras error, emita el mandato siguiente:

```
set failoverhladdress
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con QUERY REPLSERVER

Comando	Descripción
QUERY REPLSERVER (Consultar un servidor de réplica)	Muestra información sobre servidores de réplica.
REMOVE REPLSERVER (Eliminar un servidor de réplica)	Elimina un servidor de la réplica.

## SET INVALIDPWLIMIT (Establecer número de intentos de conexión no válidos)

Utilice este mandato para establecer el número de intentos de conexión no válidos que se pueden realizar antes de bloquear un nodo.

El mandato SET INVALIDPWLIMIT también se aplica a los servidores de directorios LDAP que almacenan contraseñas complejas de nodos. Los servidores de directorios LDAP pueden limitar el número de intentos de contraseña no válidos independientemente del

servidor de IBM Spectrum Protect. Es posible que no desee configurar el servidor de directorios LDAP para intentos no válidos para el espacio de nombres de IBM Spectrum Protect si utiliza el mandato SET INVALIDPWLIMIT.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set--INVALIDPwlimit--number-----<<
```

## Parámetros

---

número (Obligatorio)

Especifica el número de intentos no válidos permitidos antes de bloquear un nodo.

Puede especificar un entero de 0 a 9999. El valor 0 significa que no se comprueba el número de intentos de conexión no válidos. El valor 1 significa que si un usuario escribe una contraseña no válida una vez, el servidor bloquea el nodo. El valor predeterminado es 0.

Importante: Si la contraseña se almacena en un servidor de directorios LDAP, la puede gestionar el servidor LDAP y el servidor de IBM Spectrum Protect. No todos los mandatos del servidor de IBM Spectrum Protect afectan a las contraseñas que se autentican con un servidor LDAP. Por ejemplo, los mandatos SET PASSEXP y RESET PASSEXP no afectan a las contraseñas que se autentican con un servidor de directorios LDAP. Puede gestionar las características de contraseñas mediante el servidor de IBM Spectrum Protect. Si ha emitido el comando SET INVALIDPWLIMIT, todas las contraseñas de IBM Spectrum Protect se controlan mediante el límite que establezca. Si configura el servidor de directorios LDAP para limitar el número de intentos de contraseña no válidos, puede producirse un conflicto.

## Ejemplo: definir el número de intentos de conexión no válidos permitidos

---

Establecer el número de intentos de conexión no válidos permitidos.

```
set invalidpwlimit 6
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con SET INVALIDPWLIMIT

Comando	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET MINPWLENGTH	Establece la longitud mínima de las contraseñas de cliente.

## SET LDAPPASSWORD (Establecer contraseña de LDAP para el servidor)

---

Utilice este mandato para definir una contraseña para el ID de usuario o cuenta especificado en el mandato SET LDAPUSER.

Requisito: Se debe definir la opción LDAPURL y emitir el mandato SET LDAPUSER antes de ejecutar el mandato SET LDAPPASSWORD. Si no está definida la opción LDAPURL cuando establece la contraseña de usuario para el servidor LDAP (Lightweight Directory Access Protocol), debe reiniciar el servidor de IBM Spectrum Protect después de definir la opción LDAPURL.

## Clase de privilegio

---

Para emitir este mandato, debe tener privilegios del sistema.

## Sintaxis

---

```
>>-Set LDAPPassword--ldap_user_password-----<<
```

## Parámetros

### ldap\_user\_password

Especifica la contraseña que utiliza el servidor de IBM Spectrum Protect cuando se autentica con el servidor LDAP. La longitud máxima de la contraseña es de 64 caracteres. Si tiene signos de igual en su contraseña, la contraseña debe estar encerrada entre comillas. Se pueden utilizar los caracteres siguientes:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

## Ejemplo: Establecer una contraseña LDAP

```
set ldappassword LdAp20&12PaSsWoRd
```

## Ejemplo: establecer una contraseña LDAP que incluya un signo igual

```
set ldappassword "LdAp=LastWoRd"
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET LDAPPASSWORD

Comando	Descripción
AUDIT LDAPDIRECTORY	Auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de directorios LDAP.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET LDAPUSER	Establece el usuario que supervisa las contraseñas y los administradores en el servidor de directorios LDAP.

## SET LDAPUSER (Especificar un ID para el servidor de directorios LDAP)

Utilice este mandato para especificar el ID de un usuario o cuenta que puede acceder a un servidor LDAP (Lightweight Directory Access Protocol).

El ID especificado debe tener acceso de lectura a las cuentas del servidor LDAP que se utilizan para la autenticación. Para modificar los ID o restaurar las contraseñas de los ID de LDAP, el ID de usuario o de cuenta especificado debe tener autorización para las cuentas del servidor LDAP.

Consejo: La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set LDAPUser--ldap_user_dn-----<<
```

## Parámetros

### ldap\_user\_dn

Especifica el ID de un usuario o cuenta que puede acceder a un servidor LDAP.

## Ejemplo: Especifique un ID de usuario administrativo para realizar operaciones en un servidor LDAP.

Para especificar un administrador con un ID de usuario JACKSPRATT, que representa a una empresa de EE.UU, con el nombre EXAMPLE, emita el mandato siguiente:

```
set ldapuser JackSpratt@us.example.com
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET LDAPUSER

Comando	Descripción
AUDIT LDAPDIRECTORY	Auditar un espacio de nombres controlado por IBM Spectrum Protect en un servidor de directorios LDAP.
SET DEFAULTAUTHENTICATION	Especifica el método de autenticación de contraseñas predeterminado para cualquier comando REGISTER NODE o REGISTER ADMIN.
SET LDAPPASSWORD	Establece la contraseña para LDAPUSER.

## SET LICENSEAUDITPERIOD (Establecer período de auditoría de licencias)

Utilice este comando para especificar el período, en días, entre las auditorías automáticas de licencias que realiza IBM Spectrum Protect.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>Set--LIcenseauditperiod--+-30---.-----+-----<<  
                              '-días-'
```

## Parámetros

días

Especifica el número de días entre auditorías automáticas de licencias. Este parámetro es opcional. El valor predeterminado es 30. Puede especificar un entero de 1 a 30, inclusive.

## Ejemplo: especificar una auditoría de licencia de servidor de 14 días

Especificar que el servidor hace la auditoría de licencias cada 14 días.

```
set licenseauditperiod 14
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET LICENSEAUDITPERIOD

Comando	Descripción
AUDIT LICENSES	Comprueba que se cumplan las licencias definidas.
QUERY AUDITOCCUPANCY	Visualiza la utilización del almacenamiento del servidor de un nodo cliente.
QUERY LICENSE	Visualiza información sobre licencias y auditorías.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER LICENSE	Registra una licencia con el servidor de IBM Spectrum Protect.

## SET MAXCMDRETRIES (Establecer el número máximo de reintentos de comando)

Utilice este comando para establecer el número máximo de veces que un planificador de un nodo cliente puede reintentar un comando planificado que no se ha podido ejecutar.

Puede utilizar el comando para modificar temporalmente el número máximo de reintentos que ha especificado el nodo cliente. El valor de un cliente se modifica temporalmente sólo si el cliente puede conectarse con el servidor.

Este comando se utiliza con el comando SET RETRYPERIOD para regular el período de tiempo y el número de reintentos que han de aplicarse a la reejecución de un comando que no se ha realizado correctamente.

Puede emitir el comando QUERY STATUS para visualizar el valor de reintentos actual. En la instalación, IBM Spectrum Protect se configura de modo que cada cliente determina su propio valor de reintentos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set MAXCMDRetries--+-----+----->><
                        '-number-'
```

### Parámetros

número

Especifica el número máximo de veces que el planificador de un nodo cliente puede reintentar un comando planificado que no se ha podido ejecutar. Este parámetro es opcional.

El valor predeterminado es que cada cliente determina su propio valor para este parámetro. Puede especificar un entero de 0 a 9999. Consulte la documentación correspondiente al cliente para obtener más información sobre cómo establecer el número máximo de reintentos de comandos del cliente.

### Ejemplo: establecer el número máximo de reintentos de un comando en 2

Reintentar, sólo dos veces, el intento fracasado de procesar un comando planificado.

```
set maxcmdretries 2
```

### Comandos relacionados

Tabla 1. Comando relacionado con SET MAXCMDRETRIES

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

## SET MAXSCHEDESESSIONS (Establecer número máximo de sesiones planificadas)

Utilice este mandato para establecer el número de sesiones que el servidor puede utilizar para procesar operaciones planificadas. Este mandato especifica el número máximo de sesiones planificadas como porcentaje del número total de sesiones del servidor disponibles.

Al limitar el número de sesiones, se asegura que algunas de ellas estén disponibles para operaciones no planificadas, por ejemplo copia de seguridad o archivado. Puede aumentar el número total de sesiones (con el parámetro MAXSESSIONS) o el porcentaje máximo de sesiones planificadas. Sin embargo, si se aumenta el número total de sesiones disponibles, el rendimiento del servidor puede resultar

afectado. Si se aumenta el porcentaje máximo de sesiones planificadas, se pueden reducir las sesiones disponibles para las operaciones sin planificar.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set MAXSchedsessions--porcentaje-----<<
```

## Parámetros

---

porcentaje (Obligatorio)

Especifica el porcentaje de sesiones totales del servidor que se puede utilizar para las operaciones planificadas. Puede especificar un entero de 0 a 100. El parámetro MAXSESSIONS del archivo de opciones de servidor determina el número máximo de sesiones de servidor totales disponibles.

Si establece el porcentaje máximo de sesiones planificadas en 0, no se pueden iniciar eventos planificados. Si establece el porcentaje máximo de sesiones planificadas en 100, el número máximo de sesiones planificadas es el valor de la opción MAXSESSIONS.

Consejo: Si el número máximo de sesiones planificadas no coincide con el porcentaje establecido en el mandato SET MAXSCHEDSESSIONS, ejecute el mandato SET MAXSCHEDSESSIONS otra vez. Compruebe la opción MAXSESSIONS y determine el número que se especifica. Si el número de la opción MAXSESSIONS ha cambiado y no ha emitido el mandato SET MAXSCHEDSESSIONS desde que se produjo el cambio, la cantidad máxima de sesiones planificadas puede cambiar.

## Establecer un máximo de 20 sesiones para actividades planificadas

---

La opción MAXSESSIONS tiene el valor 80. Si desea que no haya más de 20 sesiones disponibles para la actividad planificada, establezca el porcentaje en 25.

```
set maxschedsessions 25
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con SET MAXSCHEDSESSIONS

Comando	Descripción
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET MINPWLENGTH (Establecer longitud mínima de contraseña)

---

Utilice este comando para establecer la longitud mínima de una contraseña.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set--MINPwlength--longitud-----<<
```

## Parámetros

---

longitud (Obligatorio)

Especifica la longitud mínima de una contraseña. Puede especificar un entero de 0 a 64. El valor 0 significa que la longitud de la contraseña no se comprueba. El valor predeterminado para la longitud mínima de contraseña se establece en 0.

## Ejemplo: establecer la longitud mínima de la contraseña

Establecer la longitud mínima de la contraseña en 5 caracteres.

```
set minpwlenth 5
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET MINPWLENGTH

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET INVALIDPWLIMIT	Establece el número de intentos de conexión no válidos antes de que se bloquee un nodo.

## SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)

Utilice este mandato para establecer el grupo de servidores en los que se están supervisando las alertas y el estado. También puede utilizar este mandato para cambiar o eliminar el grupo de servidores supervisados.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set MONITOREDSEVERGroup--+-+-----+-----><  
                               '-nombre_grupo-'
```

### Parámetros

nombre\_grupo

Especifica el nombre de grupo de servidores de IBM Spectrum Protect que contiene todos los servidores supervisados. Puede eliminar un nombre de grupo de servidores supervisados emitiendo el mandato sin especificar un valor o especificando un valor vacío (""). Finaliza cualquier supervisión existente de alertas y estado de los servidores remotos.

## Establecer el nombre de un grupo de servidores supervisados

Establezca el nombre de un grupo de servidores supervisados SUBS, emitiendo el siguiente mandato:

```
set monitoredservergroup subs
```

## Eliminar el nombre de un grupo de servidores supervisados

Elimine el grupo de servidores supervisados, emitiendo el mandato siguiente:

```
set monitoredservergroup
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET MONITOREDSEVERGROUP

Comando	Descripción
DEFINE SERVERGROUP (Definir un grupo de nodo)	Define un nuevo grupo de servidores.
DEFINE GRPMEMBER (Agregar un servidor a un grupo de servidores)	Define un servidor como miembro de un grupo de servidores.
DELETE GRPMEMBER (Suprimir un servidor de un grupo de servidores)	Suprime un servidor de un grupo de servidores.

Comando	Descripción
QUERY SERVERGROUP (Consultar un grupo de servidores)	Muestra información sobre grupos de servidores.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)	Establece el nombre del administrador de supervisión.

## SET MONITORINGADMIN (Establecer el nombre del administrador de supervisión)

Utilice este mandato para establecer el nombre del administrador de supervisión que se utiliza para conectarse a los servidores del grupo de servidores supervisados.

Para visualizar el nombre del grupo de servidores supervisados, emita el mandato QUERY MONITORSETTINGS.

El nombre de administrador que especifique debe coincidir con el nombre de un administrador existente, de lo contrario, el mandato fallará.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set MONITORINGADMIN--+-+-----+-----><
                        '-nombre_admin-'
```

### Parámetros

nombre\_admin

Especifica el nombre de administrador. Puede eliminar nombres emitiendo el mandato sin especificar un valor o especificando un valor vacío ("").

### Establecer el nombre de administrador de supervisión

Establezca el nombre del administrador de supervisión MONADMIN, emitiendo el siguiente mandato:

```
set monitoringadmin monadmin
```

### Eliminar el nombre de administrador de supervisión

Elimine el administrador de supervisión, emitiendo el mandato siguiente:

```
set monitoringadmin ""
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con SET MONITORINGADMIN

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET MONITOREDSEVERGROUP (Establecer el grupo de servidores supervisados)	Establece el grupo de servidores supervisados.

## SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)



Utilice este comando para ajustar la modalidad de evaluación de riesgo de uno nodo individual.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el domino al que está asignado el nodo o bien autorización de propietario de cliente en el nodo.

## Sintaxis

```
>>---Set NODEATRISKINTERVAL--nombre_nodo----->
>--TYPE-----+--DEFAULT-----+-----<
      +-BYPASSED-----+
      '-CUSTOM--Interval--==--valor-'
```

## Parámetros

nombre\_nodo (necesario)

Especifica el nombre del nodo cliente que desea actualizar..

TYPE (necesario)

Especifica el tipo de evaluación de riesgo. Especifique uno de los siguientes valores:

DEFAULT

Especifica que el nodo se evalúa con el mismo intervalo que se ha especificado para la clasificación de nodos con el comando SET STATUSATRISKINTERVAL. El valor es cualquier sistema o aplicación, o VM y está determinado por el supervisor de estado.

Por ejemplo, puede especificar `TYPE = DEFAULT`, que permite que el supervisor de estado continúe y clasifique el nodo automáticamente. Entonces, el intervalo que se utiliza es el intervalo que se ha definido para dicha clasificación mediante el comando SET STATUSATRISKINTERVAL.

BYPASSED

Especifica que el nodo no se evalúa para el estado de MV en riesgo por el supervisor de estado.. Se ha informado de que el estado de riesgo también es eludido en Centro de operaciones.

CUSTOM

Especifica que el nodo se evalúa con el intervalo que se ha especificado para el comando SET STATUSATRISKINTERVAL.

Intervalo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. Debe especificar este parámetro cuando `TYPE = CUSTOM`. No especifique este parámetro cuando `TYPE = BYPASSED` o `TYPE = DEFAULT`. El valor de intervalo para todos los tipos de cliente se establece en 24 en la instalación del servidor.

## Establecer nombre de nodo para utilizar un intervalo de riesgo personaliad de 90 días

Establecer el intervalo de riesgo para un nodo denominado *fred* en 90 días.

```
set nodeatriskinterval fred type=custom interval=2160
```

## Eludir la evaluación del intervalo de riesgo

Eluda la comprobación del intervalo de riesgo para un nodo denominado *bob*.

```
set nodeatriskinterval bob type=bypassed
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con set nodeatriskinterval

Comando	Descripción
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)	Establece la modalidad de riesgo de un espacio de archivos de MV

Comando	Descripción
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
QUERY NODE (Consultar nodos)	Visualiza información parcial o completa sobre uno o más clientes.
QUERY FILESPACE (Consultar uno o más espacios de archivos)	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.

## SET PASSEXP (Establecer fecha de caducidad de contraseña)

Utilice este comando para establecer el período de caducidad para las contraseñas de administrador y de nodo cliente. Puede establecer un período de caducidad común de contraseña para todos las contraseñas de administradores o de nodos de cliente, o bien puede establecer períodos de caducidad de contraseñas de forma selectiva.

Restricción: El mandato SET PASSEXP no se aplica a contraseñas que se autentican con un servidor de directorio LDAP.

Puede alterar temporalmente el valor SET PASSEXP para uno o varios nodos mediante el comando REGISTER NODE o el comando UPDATE NODE con el parámetro PASSEXP.

Los parámetros NODE o ADMIN deben especificarse para cambiar el período de caducidad de contraseñas de los nodos de cliente y los administradores con períodos de caducidad de contraseñas establecido de forma selectiva. Si no especifica los parámetros NODE o ADMIN, *todas* las contraseñas de nodos cliente y administradores utilizarán el nuevo período de caducidad de contraseña. Si de forma selectiva establece una caducidad de contraseña para un nodo o administrador que todavía no tiene establecido un período de caducidad de contraseña, no se modificará si posteriormente se establece la caducidad de contraseña para todos los usuarios.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set PASSExp--días--+-----+----->
|           .-,------. |
|           v             | |
|'-Node-----nombre_nodo+--'|

>+-----+-----><
|           .-,------. |
|           v             | |
|'-Admin-----nombre_admin+--'|
```

### Parámetros

días (Obligatorio)

Especifica el número de días que será válida una contraseña.

Puede especificar un número entre 1 y 9999 si no especifica el parámetro NODE o ADMIN. Si especifica el parámetro NODE o el parámetro ADMIN, puede especificar un número del 0 al 9999. El valor 0 significa que la contraseña no caduca nunca. Si caduca una contraseña, el servidor solicita una nueva contraseña cuando el administrador o el nodo de cliente se pone en contacto con el servidor.

Node

Especifica el nombre del nodo para el que desea establecer el período de caducidad de contraseña. Para especificar una lista de nodos, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

Admin

Especifica el nombre del administrador cuyo período de caducidad de contraseña quiere establecer. Para especificar una lista de administradores, debe separar los nombres con comas y sin espacios intercalados. Este parámetro es opcional.

## Ejemplo: establecer la caducidad de la contraseña del administrador y del nodo de cliente

Establecer el período de caducidad de la contraseña de administrador o de nodo de cliente en 45 días.

```
set passexp 45
```

## Ejemplo: establecer la caducidad de contraseña de un administrador

Establecer el período de caducidad de la contraseña del administrador LARRY en 120 días.

```
set passexp 120 admin=larry
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET PASSEXP

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## SET PRODUCTOFFERING (Establecer la oferta de producto que tiene licencia para su empresa)

Utilice el comando SET PRODUCTOFFERING para definir la oferta de producto de IBM Spectrum Protect que tiene licencia para su empresa.

La definición se utiliza para determinar si IBM® License Metric Tool (ILMT) requiere cálculos de medida de capacidad de almacenamiento automático y si los tiene disponibles para su uso. Ejecute este comando sólo si está utilizando ILMT para determinar el consumo de licencia.

Para las ofertas de productos donde ILMT tiene disponibles para su uso cálculos de medida de capacidad de almacenamiento automático, el parámetro también define qué enfoque de medida de capacidad se utiliza para esos cálculos.

El método de medición de capacidad se define en los términos de licencia de su oferta de producto específica. Para determinar la capacidad de almacenamiento calculada actualmente para su oferta de producto, consulte Verificación del cumplimiento de la licencia.

La misma información de capacidad de almacenamiento está disponible para ILMT semanalmente. Después de definir una oferta de producto aplicable utilizando este comando, IBM Spectrum Protect realiza el cálculo de capacidad actual para esa oferta que está disponible para ILMT. Cuando se determina el cálculo de capacidad inicial que está disponible para ILMT, IBM Spectrum Protect actualiza el valor semanalmente.

## Clase de privilegio

Para ejecutar este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-SET PRODUCTOFFERING--oferta_producto-----<<
```

## Parámetros

---

### oferta\_producto (Obligatorio)

Especifica una oferta de producto. La longitud máxima de la serie de texto es de 255 caracteres. Las opciones siguientes están disponibles:

#### ENTry

Especifica que la oferta del producto con licencia en su empresa es IBM Spectrum Protect Entry. Esta oferta de producto utiliza una medida de licencia de tipo Per Managed Server. Las medidas de capacidad de esta oferta de producto no son aplicables.

#### DATARet

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect para retención de datos. Las medidas de capacidad para esta oferta de producto no se calculan automáticamente ni están disponibles para su uso en ILMT.

#### BASIC

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect. Esta oferta de producto utiliza una medida de licencia de processor value unit (PVU). Las medidas de capacidad de esta oferta de producto no son aplicables.

#### EE

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Extended Edition. Esta oferta de producto utiliza una medida de licencia de PVU. Las medidas de capacidad de esta oferta de producto no son aplicables.

#### SUIte

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### SUITEEntry

Especifica que la oferta del producto con licencia en su empresa es IBM Spectrum Protect Suite Entry. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### SUITEArchive

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - Archive. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### SUITEProtectier

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - ProtecTier. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### SUITEFrontend

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite - FrontEnd. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### SUITEENTRYFrontend

Especifica que la oferta de producto con licencia en su empresa es IBM Spectrum Protect Suite Entry - FrontEnd. Las medidas de capacidad para esta oferta de producto se calculan automáticamente y están disponibles para su uso en ILMT.

#### CLEAR

No se ha especificado ninguna oferta de producto.

## Ejemplo: establecer la oferta de producto en IBM Spectrum Protect (BASIC)

---

```
set productoffering BASIC
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con SET PRODUCTOFFERING

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET QUERYSCHEDPERIOD (Establecer período de consulta para sondeo de nodos clientes)

Utilice este comando para regular la frecuencia con que los nodos cliente se ponen en contacto con el servidor para obtener el trabajo planificado cuando se ejecuta en la modalidad de planificación por sondeo de cliente.

Cada cliente puede establecer su propio período de reintentos en el momento en que se inicia su programa planificador. Puede utilizar este comando para modificar temporalmente el valor que especifican todos los clientes que pueden conectarse con el servidor.

Si los nodos cliente sondean con mayor frecuencia para ver si hay planificaciones, los nodos reciben los cambios efectuados en las planificaciones con mayor rapidez. Sin embargo, si los nodos clientes aumentan el sondeo se aumenta también el tráfico de la red.

Puede emitir el comando QUERY STATUS para que se visualice el valor del período establecido entre consultas de planificación. En la instalación, IBM Spectrum Protect se configura de modo que cada cliente determina su propio valor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set QUERYSChedperiod--+-+-----+-----><
                               '-horas-'
```

### Parámetros

horas

Especifica el número máximo de horas que el planificador de un nodo cliente espera entre intentos de ponerse en contacto con el servidor para obtener una planificación. Este parámetro es opcional. Puede especificar un entero de 1 a 9999. Si no especifica un valor para este parámetro, cada cliente determina su propio valor para este parámetro.

### Ejemplo: establecer el período de sondeo para todos los nodos cliente

Hacer que todos los clientes que utilicen la modalidad de planificación por sondeo se pongan en contacto con el servidor cada 24 horas.

```
set querieschedperiod 24
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SET QUERYSCHEDPERIOD

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.

## SET RANDOMIZE (Establecer la aleatorización de las horas de inicio planificadas)

Utilice este comando para establecer las horas de inicio aleatorias en el margen de puesta en marcha de cada planificación para los clientes utilizando la modalidad de planificación por sondeo de cliente. El margen de puesta en marcha es la hora de inicio y la duración durante la que debe iniciarse la planificación. La modalidad de planificación por sondeo de cliente es una técnica de comunicaciones de cliente/servidor donde el cliente consulta el trabajo que hay al servidor.

Cada planificación cuenta con un margen de tiempo que indica durante qué período de tiempo puede llevarse a cabo su ejecución. Para equilibrar la carga de la red y del servidor, las horas de inicio para los clientes se pueden distribuir en dicho margen. Utilice este comando para especificar la fracción del margen por la cual se distribuyen las horas de inicio para los clientes.

La aleatorización se produce al principio del margen para dejar tiempo para reintentos, si es necesario. Cuando la modalidad de planificación no se establece en sondeo, la aleatorización no se produce si el primer contacto del cliente con el servidor tiene lugar

después de la hora de inicio del evento.

Puede emitir el mandato QUERY STATUS para que se visualice el valor del porcentaje de aleatorización de la planificación. En la instalación, el valor se establece en el 25 por ciento.

Establezca el porcentaje de aleatorización en un valor mayor que 0 para impedir errores de comunicaciones. Los errores de comunicaciones pueden producirse porque un gran grupo de clientes entra en contacto con el servidor simultáneamente. Si sufre errores de comunicaciones, puede aumentar el porcentaje de aleatorización, de modo que el contacto del cliente se distribuya. Con esto disminuyen las posibilidades de sobrecargas y errores en las comunicaciones.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set RANDomize--porcentaje-----<<
```

## Parámetros

---

porcentaje (Obligatorio)

Especifica el porcentaje del margen de puesta en marcha sobre el que se distribuyen las horas de inicio de los clientes individuales. Puede especificar un entero de 0 a 50.

El valor 0 indica que no se produce ninguna aleatorización y que todos los clientes ejecutan las planificaciones al principio de los márgenes de tiempo de puesta en marcha.

El valor 50 indica que a los clientes se les asigna horas de inicio que se distribuyen aleatoriamente por la primera mitad de cada margen de puesta en marcha.

Durante la instalación, este valor es 25, lo cual indica que el primer 25 por ciento del margen de puesta en marcha se utiliza para la aleatorización.

Si ha especificado DURUNITS=INDEFINITE en el comando DEFINE SCHEDULE, el porcentaje se aplica a un período de 24 horas. Por ejemplo, el valor 25% produciría un margen de 6 horas.

## Ejemplo: establecer la aleatorización de las horas de inicio planificadas

---

Establecer la aleatorización en el 50 por cien.

```
set randomize 50
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con SET RANDOMIZE

Comando	Descripción
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET SCHEDMODES	Especifica la modalidad de planificación central del servidor.

## SET REPLRECOVERDAMAGED (Especificar si los archivos dañados se recuperan de un servidor de réplica)

---

Utilice este mandato para habilitar la recuperación en todo el sistema de archivos dañados a partir de un servidor de réplica de destino. Si este valor está activado, el proceso de réplica del nodo se puede configurar para detectar archivos dañados en el servidor de réplica de origen y sustituirlo por archivos sin dañar del servidor de réplica de destino.

El parámetro del sistema REPLRECOVERDAMAGED afecta a todos los procesos de recuperación de archivos en todos los procesos de réplica para todos los nodos y espacios de archivos. La recuperación de archivos sólo es posible si está instalado el software del



ON

Especifica que la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.

OFF

Especifica que la réplica de nodo no está habilitada para recuperar archivos dañados a partir de un servidor de réplica de destino.

## Ejemplo: Habilitar recuperación de archivos dañados

Para especificar un valor para todo el sistema que permita que el servidor recupere los archivos dañados a partir de un servidor de réplica de destino, emita el mandato siguiente:

```
set replrecoverdamaged on
```

## Comandos relacionados

Tabla 2. Mandatos relacionados con SET REPLRECOVERDAMAGED

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## SET REPLRETENTION (Establecer el período de retención de los registros de réplica)

Para mantener la información adecuada sobre los procesos de réplica, puede utilizar este comando para ajustar el periodo de tiempo durante el cual el servidor de réplica de origen retiene los registros de réplica en la base de datos. El comando SET REPLRETENTION especifica el periodo de retención de los registros de réplica de nodo de cliente en la base de datos de servidor de réplica de origen. Puede utilizar los registros de réplica de nodo de cliente para supervisar los procesos en ejecución y completados.

Se crea un registro de réplica cuando se inicia el proceso del comando REPLICATE NODE. De forma predeterminada, IBM Spectrum Protect retiene los registros de réplica de nodo de cliente durante 30 días naturales. Un día natural consta de 24 horas, de medianoche a medianoche. Por ejemplo, suponga que el periodo de retención es de dos días naturales. Si un proceso de réplica se completa a las 11:00 p.m. del día  $n$ , se retiene un registro de dicho proceso durante 25 horas hasta la medianoche del día  $n+1$ . Para visualizar el periodo de retención para los registros de réplica, emita el comando QUERY STATUS en el servidor de réplica de origen.

Emita el comando SET REPLRETENTION en el servidor que actúe como origen para los datos replicados.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set REPLREtention--+-30-----+----->>  
'-número_de_días-'
```

## Parámetros

número\_de\_días (Obligatorio)

El número de días que el servidor de réplica de origen retiene los registros de réplica. Puede especificar un entero de 0 a 9999. El valor predeterminado es 30.

## Ejemplo: establecer un período de retención para los registros de réplica de nodo de cliente



Desea retener los registros de réplica de nodo de cliente durante 10 días.

```
set replretention 10
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET REPLRETENTION

Comando	Descripción
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET REPLSERVER (Establecer el servidor de réplica de destino)

Utilice este comando para establecer el nombre de un servidor de réplica de destino. También puede utilizar este comando para cambiar o eliminar un servidor de réplica de destino.

Emita este comando en el servidor que actúe como origen para los datos replicados.

Para visualizar el nombre de un servidor de réplica de destino, emita el comando QUERY STATUS en un servidor de réplica de origen.

Importante:

- El nombre de servidor que especifique con este comando debe coincidir con el nombre de una definición de servidor existente. También debe ser el nombre del servidor que se utilizará como servidor de réplica de destino. Si el nombre de servidor especificado por este mandato no coincide con el nombre de servidor de una definición de servidor existente, el mandato falla.
- Tenga cuidado cuando cambie o elimine un servidor de réplica de destino. Si cambia un servidor de réplica de destino, los datos del nodo de cliente replicados se envían a un servidor de réplica de destino diferente. Si elimina un servidor de réplica de destino, los datos del nodo de cliente no se replican.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set REPLSERVER--+-----+-----<<  
                    '-nombre_servidor_destino-'
```

## Parámetros

nombre\_servidor\_destino

Especifica el nombre del servidor de réplica de destino. El nombre que especifique debe coincidir con el nombre de un servidor existente. La longitud máxima de un nombre es de 64 caracteres.

Para eliminar un servidor de réplica de destino, emita el comando sin especificar ningún valor.

Nota: Si no desea continuar replicando datos, puede eliminar la configuración de réplica de nodo después de eliminar el servidor de réplica de destino.

## Ejemplo: establecer un servidor de réplica de destino

El nombre del servidor que desea establecer como servidor de réplica de destino es SERVER1.

```
set replserver server1
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET REPLSERVER

Comando	Descripción
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
UPDATE SERVER	Actualiza la información sobre un servidor.
REMOVE REPLNODE	Elimina un nodo de la réplica.
REMOVE REPLSERVER	Elimina un servidor de la réplica.

## SET RETRYPERIOD (Establecer período de tiempo entre reintentos)

Utilice este comando para establecer el número de minutos que el planificador de un nodo cliente espera entre reintentos después de que haya fracasado un intento de ponerse en contacto con el servidor o de que un comando planificado no se haya podido procesar.

Cada cliente puede establecer su propio período de reintentos en el momento en que se inicia su programa planificador. Puede utilizar este comando para modificar temporalmente los valores que especifican todos los clientes que pueden conectarse con el servidor.

Este comando se utiliza junto con el comando SET MAXCMDRETRIES para regular el período de tiempo y el número de reintentos que han de aplicarse a la ejecución de un comando que no se ha completado correctamente.

Puede emitir el comando QUERY STATUS para que se visualice el valor del período establecido entre reintentos. En la instalación, IBM Spectrum Protect permite que cada cliente determine su propio período entre reintentos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set RETRYPeriod--+-+-----+-----<<
                        '-minutos-'
```

### Parámetros

minutos

Especifica el número de minutos que el planificador de un nodo cliente espera entre reintentos después de que haya fracasado un intento de contactar al servidor o de que un comando planificado no se haya podido procesar. Al establecer el período entre reintentos, establezca un período de tiempo que permita más de un reintento en un margen de puesta en marcha normal. Puede especificar un entero de 1 a 9999.

### Ejemplo: establecer un período de tiempo de quince minutos entre reintentos

Establecer que el planificador cliente vuelva a intentar cada quince minutos el establecimiento de contacto con el servidor o el proceso de los comandos planificados que no se han ejecutado correctamente.

```
set retryperiod 15
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET RETRYPERIOD

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

Comando	Descripción
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un comando planificado.

## SET SCHEDMODES (seleccionar modalidad de planificación central)

Utilice este comando para determinar cómo se comunican los clientes con el servidor para comenzar el trabajo planificado. Cada cliente debe configurarse para seleccionar la modalidad de planificación en la que opera.

Utilice este comando con el comando SET RETRYPERIOD para regular el período de tiempo y el número de reintentos de proceso que han de aplicarse a un comando que no se ha ejecutado correctamente.

Puede emitir el comando QUERY STATUS para que se visualice el valor de la modalidad de planificación que recibe soporte. En la instalación, este valor es ANY.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set SCHEDMODEs---ANY-----+-----><
      +-Polling--+
      '-PROMPTed-'
```

### Parámetros

ANY

Especifica que los clientes pueden ejecutar la modalidad de planificación por sondeo de cliente o por petición de servidor.

POLLing

Especifica que únicamente puede utilizarse la modalidad de planificación por sondeo de cliente. Los nodos de cliente sondean el servidor en intervalos de tiempo especificados para obtener el trabajo planificado.

PROMPTed

Especifica que únicamente puede utilizarse la modalidad de planificación por petición de servidor. Esta modalidad únicamente está disponible para los clientes que se comunican a través de TCP/IP. Los nodos de cliente esperan a que el servidor se ponga en contacto con ellos cuando se ha de realizar el trabajo planificado y hay una sesión disponible.

### Ejemplo: limitar las operaciones planificadas para los clientes con el sondeo por cliente

Los clientes pueden ejecutar la planificación central por petición de servidor y por sondeo de cliente. Suponga que se desea limitar temporalmente las operaciones planificadas a los clientes que utilicen la modalidad de planificación por sondeo de cliente. Si establece la modalidad de planificación en POLLING, el servidor dejará de solicitar a los clientes que ejecuten los comandos planificados. Esto significa que cualquier planificador cliente que utilice la modalidad de planificación por petición de servidor esperará hasta que establezca la modalidad de planificación en ANY o PROMPTED.

```
set schedmodes polling
```

### Comandos relacionados

Tabla 1. Comando relacionado con SET SCHEDMODES

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

## SET SCRATCHPADRETENTION (Establecer hora de retención de registro)

Utilice este mandato para establecer la cantidad de tiempo para la que se retienen entradas de registro.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-SET SCRATCHPADRETENTION--días-----<<
```

## Parámetros

---

días (Obligatorio)

Especifica el número de días que una entrada de registro se retiene después de la última actualización en la entrada de registro. Puede especificar un entero en el rango 1 – 9999.

## Ejemplo: retener entradas de registro para 367 días después de que se actualicen

---

```
set scratchpadretention 367
```

## Comandos relacionados

---

Tabla 1. Mandatos relacionados con SET SCRATCHPADRETENTION

Comando	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
UPDATE SCRATCHPADENTRY	Actualiza datos en una línea en la anotación.

## SET SERVERHLADDRESS (Establecer la dirección de alto nivel de un servidor)

---

Utilice este comando para establecer la dirección de alto nivel (IP) de un servidor. IBM Spectrum Protect utiliza la dirección cuando se emite un comando DEFINE SERVER con CROSSDEFINE=YES. Es necesario utilizar el mandato SET SERVERHLADDRESS para todos los despliegues automáticos de cliente.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set SERVERHladdress--dirección_ip-----<<
```

## Parámetros

---

dirección\_ip (Obligatorio)

Especifica la dirección de alto nivel como un nombre numérico decimal con puntos o como un nombre de host. Si se especifica un nombre de host, debe haber disponible un servidor que pueda resolver el nombre con el formato decimal con puntos.

## Ejemplo: establecer la dirección de alto nivel de un servidor

---

Establecer la dirección de alto nivel de HQ\_SERVER en 9.230.99.66.

```
set serverhladdress 9.230.99.66
```

## Comandos relacionados

---

Tabla 1. Comando relacionado con SET SERVERHLADDRESS

Comando	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.

## SET SERVERLLADDRESS (Establecer la dirección de bajo nivel de un servidor)

Utilice este comando para establecer la dirección de bajo nivel de un servidor. IBM Spectrum Protect utiliza la dirección cuando se emite un comando DEFINE SERVER con CROSSDEFINE=YES.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set SERVERLladdress--puerto_tcp-----><
```

### Parámetros

puerto\_tcp (Obligatorio)

Especifica la dirección de bajo nivel del servidor. Por lo general, esta dirección es idéntica a la de la opción TCPPOINT del archivo de opciones del servidor.

### Ejemplo: establecer la dirección de bajo nivel de un servidor

Establecer la dirección de bajo nivel de HQ\_SERVER en 1500.

```
set serverlladdress 1500
```

### Comandos relacionados

Tabla 1. Comando relacionado con SET SERVERLLADDRESS

Comando	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERPASSWORD	Especifica la contraseña del servidor.

## SET SERVERNAME (Especificar el nombre del servidor)

Utilice este comando para cambiar el nombre del servidor. Cuando instala el servidor de IBM Spectrum Protect, el nombre se establece durante la instalación en SERVER1.

Utilice el comando QUERY STATUS para que se visualice el nombre del servidor.

Si migra desde ADSM hasta IBM Spectrum Protect, el nombre se establece en ADSM o en el último nombre que se ha especificado para ADSM con el comando SET SERVERNAME.

Importante:

- Si es un servidor origen para una operación de volúmenes virtuales, el cambio del nombre puede afectar a la capacidad del servidor origen de acceder a los datos almacenados en el servidor destino correspondiente y gestionarlos.
- Para evitar que se produzcan problemas relacionados con la propiedad de los volúmenes, no cambie el nombre de un servidor si es un cliente de biblioteca.

Al cambiar el nombre de un servidor, tenga en cuenta las restricciones adicionales siguientes:

- Los clientes de Windows utilizan el nombre del servidor para identificar qué contraseñas pertenecen a qué servidores. El cambio del nombre del servidor después de que los clientes se hayan conectado dará lugar a que los clientes deban volver a especificar forzosamente las contraseñas.
- Debe establecer nombres exclusivos en los servidores que se comunican entre sí. En una red donde los clientes se conectan a múltiples servidores, es recomendable que todos ellos tengan nombres exclusivos.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set SERVERname--nombre_servidor-----<<
```

## Parámetros

---

nombre\_servidor (Obligatorio)

Especifica el nuevo nombre del servidor. El nombre debe ser exclusivo en toda la red de servidores para la anotación de eventos de empresa, la configuración de empresa, el direccionamiento de comandos o los volúmenes virtuales. La longitud máxima del nombre es de 64 caracteres.

## Ejemplo: especificar el nombre de un servidor

---

Dar al servidor el nombre WELLS\_DESIGN\_DEPT.

```
set servername wells_design_dept
```

## Comandos relacionados

---

Tabla 1. Comando relacionado con SET SERVERNAME

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET SERVERPASSWORD (Establecer contraseña de servidor)

---

Utilice este mandato para establecer la contraseña de las comunicaciones entre servidores para dar soporte a la administración de empresa y a el registro de eventos y supervisión de empresa.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set SERVERPAssword--contraseña-----<<
```

## Parámetros

---

contraseña (Obligatorio)

Especifica la contraseña del servidor. Los demás servidores deben tener la misma contraseña en las definiciones de este servidor.

## Ejemplo: establecer la contraseña de un servidor

---

Establecer la contraseña de HQ\_SERVER en agave.

```
set serverpassword agave
```

## Comandos relacionados

Tabla 1. Comando relacionado con SET SERVERPASSWORD

Comando	Descripción
SET CROSSDEFINE	Especifica si los servidores deben definirse unos en otros.
SET SERVERHLADDRESS	Especifica la dirección de alto nivel de un servidor.
SET SERVERLLADDRESS	Especifica la dirección de bajo nivel de un servidor.

## SET SPREPLRULEDEFAULT (Establecer la regla de réplica del servidor para los datos gestionados por espacio)

Utilice este mandato para establecer la regla de réplica del servidor de los datos gestionados por espacio.

Restricción: La regla de réplica que se establece con este mandato sólo se aplica si las reglas de espacio de archivos y las reglas de nodo de cliente de los datos gestionados por espacio se establecen en DEFAULT.

Emita este comando en el servidor que actúe como origen para los datos replicados.

Puede especificar una regla de réplica de prioridad normal o una regla de réplica de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que los nodos de cliente contienen datos gestionados por espacio y datos de copia de seguridad. La réplica de los datos gestionados por espacio tiene una prioridad más alta que los datos de copia de seguridad. Para dar prioridad a los datos gestionados por espacio, emita el mandato SET SPREPLRULEDEFAULT y especifique la regla de réplica ALL\_DATA\_HIGH\_PRIORITY. Para priorizar los datos de copia de seguridad, emita el mandato SET BKREPLRULEDEFAULT y especifique la regla de réplica ALL\_DATA para los datos de copia de seguridad. La regla ALL\_DATA para los datos de copia de seguridad replica los datos de copia de seguridad con una prioridad normal.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-Set SPREPLRuledefault--+-ALL_DATA-----+-----<<
      +-ALL_DATA_HIGH_PRIORITY--+
      '-NONE-----'
```

## Parámetros

ALL\_DATA

Hace una réplica de los datos gestionados por espacio con una prioridad normal.

ALL\_DATA\_HIGH\_PRIORITY

Hace una réplica de los datos gestionados por espacio con una prioridad alta.

NONE

Los datos gestionados por espacio no se replican.

## Ejemplo: establecer la regla de réplica del servidor para los datos gestionados por espacio

Configure la regla predeterminada para que los datos gestionados por espacio se repliquen con una prioridad alta.

```
set spreplruledefault all_data_high_priority
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET BKREPLRULEDEFAULT

Comando	Descripción
---------	-------------

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)

Utilice este mandato para ajustar el intervalo de actividad de copia de seguridad que se utiliza cuando el supervisor de estado valora si los clientes están en peligro.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>---Set STATUSATRISKINTERVAL--TYPE--=====+All-----+----->
                                     +-Applications-+
                                     +-VM-----+
                                     '-Systems-----'

>----Interval---valor-----<<
```

### Parámetros

#### TYPE (necesario)

Especifica el tipo de cliente que debe evaluarse. Especifique uno de los siguientes valores:

ALL

Especifique este valor para todos los tipos de cliente.

Applications

Especifique este valor sólo para tipos de cliente de aplicación.

VM

Especifique este valor para tipos de clientes de sistemas virtuales.

Systems

Especifique este valor para los tipos de cliente de sistemas.

#### Interval (Necesario)

Especifica la cantidad de tiempo, en horas, entre la actividad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. El valor de intervalo para todos los tipos de cliente se





almacenamiento primario se establecen automáticamente para visualizar un aviso cuando el valor de umbral alcance el 80%, y un error cuando el umbral de utilización alcance el 90%.

OFF

Especifica que se desactive la supervisión de estado. El valor predeterminado es desactivado (Off).

## Habilitar la supervisión de estado

Establezca la supervisión de estado en activada para habilitarla.

```
set statusmonitor on
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET STATUSMONITOR

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)

Utilice este mandato para especificar el número de minutos entre consultas de servidor de supervisión de estado.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set STATUSREFreshinterval--minutos-----<<
```

### Parámetros

minutos (Necesario)

Especifica el número aproximado de minutos entre consultas de servidor de supervisión. Puede especificar un entero en el rango 1 – 2440. El valor predeterminado es 5.

Restricciones:

- En un entorno de almacenamiento supervisado por el Centro de operaciones, establezca el mismo intervalo de renovación en los servidores de concentrador y spoke. Si utiliza intervalos diferentes, el Centro de operaciones puede mostrar

- información inexacta para los servidores spoke.
- Los intervalos cortos de renovación de estado utilizan más espacio en la base de datos de servidor y pueden necesitar más recursos de procesador y de disco. Por ejemplo, disminuir el intervalo por la mitad duplica el espacio necesario de base de datos y de registro de archivado. Los intervalos largos reducen la actualidad de los datos del Centro de operaciones, pero se ajustan mejor a una configuración de red de alta latencia.
- Un intervalo de renovación de estado de menos de 5 minutos puede producir los problemas siguientes:
  - Los datos del Centro de operaciones que se supone se han de renovar después del intervalo definido tardan mucho más tiempo en renovarse.
  - Los datos del Centro de operaciones que se supone se han de renovar casi inmediatamente después de que se produzca un cambio relacionado en el entorno de almacenamiento también tardan más tiempo en renovarse.

## Establecer el intervalo de renovación para la supervisión de estado

Especifique que el estado de servidor se consulte cada 6 minutos, emitiendo el mandato siguiente:

```
set statusrefreshinterval 6
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET STATUSREFRESHINTERVAL

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)

Utilice este mandato para hacer que el supervisor de estado considere a los clientes como en riesgo cuando evalúe el estado para cada cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set STATUSSKIPASFAILURE--+-Yes+----->
                               '-No--'

>--TYPE---+All-----+-----<
           +-Applications+
           +-VM-----+
```

## Parámetros

### State (Necesario)

Especifica si se habilitará la comprobación de los archivos omitidos durante la última copia de seguridad. Esta comprobación significa que el cliente está en riesgo si se ha omitido algún archivo. Los datos de cliente que se han omitido o de los que no se ha realizado una copia de seguridad correcta se consideran en riesgo.

Yes

Especifica que el servidor evalúa si un cliente está en riesgo.

No

Especifica que el servidor no evalúa si un cliente está en riesgo.

### TYPE (necesario)

Especifica el tipo de cliente que debe evaluarse. Especifique uno de los siguientes valores:

ALL

Especifique este valor para todos los tipos de cliente.

Applications

Especifique este valor sólo para tipos de cliente de aplicación.

VM

Especifique este valor para tipos de clientes de sistemas virtuales.

Systems

Especifique este valor para los tipos de cliente de sistemas.

## Inhabilitar la evaluación de en riesgo para los tipos de cliente de sistema virtual

Ejecute el siguiente mandato para inhabilitar la evaluación de en riesgo para los tipos de cliente de sistemas virtuales:

```
set statusskipasfailure off type=vm
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SET STATUSSKIPASFAILURE

Comando	Descripción
DEFINE STATUSTHRESHOLD (Definir un umbral de supervisión de estado)	Define un umbral de supervisión de estado.
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## SET SUBFILE (Establecer copia de seguridad de subarchivos para nodos cliente)

Utilice este comando para configurar el servidor para que los clientes puedan hacer copias de seguridad de subarchivos. En la estación de trabajo del cliente, las opciones SUBFILECACHEPATH y SUBFILECACHESIZE deben especificarse en el archivo de opciones del cliente (dsm.opt). Si utiliza un cliente Windows, también debe especificar la opción SUBFILEBACKUP.

Con las copias de seguridad de subarchivos, cuando anteriormente se ha realizado la copia de seguridad de un archivo del cliente, la realización de las copias de seguridad posteriores normalmente se aplica a la parte (un subarchivo) del archivo del cliente que ha cambiado, en lugar de aplicarse al archivo completo.

Utilice el comando QUERY STATUS para determinar si puede realizarse la copia de seguridad de los subarchivos en el servidor que ejecuta este comando.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set SUBFILE--+-Client-+-----><
                    '-No-----'
```

## Parámetros

---

Client

Especifica que el nodo cliente puede determinar si desea utilizar la copia de seguridad de subarchivos.

No

Especifica que las copias de seguridad de subarchivos no se utilizarán. Durante la instalación, este valor se establece en No.

## Ejemplo: establecer la realización de la copia de seguridad de los subarchivos para los nodos cliente

---

Permitir que el nodo cliente realice copias de seguridad de subarchivos en el servidor.

```
set subfile client
```

## Comandos relacionados

---

Tabla 1. Comando relacionado con SET SUBFILE

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET SUMMARYRETENTION (Establecer el número de días que han de conservarse los datos en la tabla resumen de actividades)

---

Utilice este comando para especificar el número de días que se debe mantener la información en la tabla resumen de actividades SQL.

La tabla resumen de actividades SQL contiene estadísticas sobre cada sesión de cliente y los procesos del servidor. Para obtener una descripción de la información que contiene la tabla resumen de actividades SQL, emita el siguiente comando:

```
select colname, remarks from columns where tablename='SUMMARY'
```

Emita el comando QUERY STATUS para visualizar el número de días que ha de conservarse la información. Durante la instalación, IBM Spectrum Protect permite que cada servidor determine su propio número de días que debe mantener la información en la tabla resumen de actividades SQL.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

---

```
>>-Set SUMmaryretention--+-----+----->><
      '-días-'
```

## Parámetros

días

Especifica el número de días que se debe mantener la información en la tabla resumen de actividades. Puede especificar un número comprendido entre 0 y 9999. El valor 0 significa que no se mantiene información en la tabla resumen de actividades. Un valor de 1 especifica que se debe mantener la tabla resumen de actividades durante el día de hoy.

## Ejemplo: especificar el número de días que ha de conservarse la información en la tabla resumen de actividades SQL

Establecer el servidor para que retenga la información de la tabla resumen de actividades durante 15 días.

```
set summaryretention 15
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET SUMMARYRETENTION

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
SET ACTLOGRETENTION	Especifica el número de días que se han de retener los registros de anotaciones en las anotaciones de actividades.
QUERY ACTLOG	Visualiza los mensajes de las anotaciones de actividades del servidor.
SELECT	Permite las consultas personalizadas de la base de datos de IBM Spectrum Protect.

## SET TAPEALERTMSG (Activar o desactivar los mensajes de alerta de cinta)

Utilice este comando para permitir al servidor de IBM Spectrum Protect anotar las notificaciones de la información de diagnóstico de los dispositivos de unidad y biblioteca. Durante la instalación, este valor se establece en OFF. Si se activan, el servidor puede recuperar información de diagnóstico de un dispositivo de cinta o biblioteca y visualizarla mediante mensajes ANR. Si se desactivan, el servidor no consultará ningún dispositivo para obtener esta información.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-Set TAPEAlertmsg--+ON--+----->><
      '-OFF-'
```

## Parámetros

ON

Especifica que la información de diagnóstico se reportará al servidor.

OFF

Especifica que la información de diagnóstico no se reportará al servidor.

## Ejemplo: activar los mensajes de alerta de cinta

Permitir que el servidor reciba mensajes de la información de diagnóstico.

```
set tapealertmsg on
```

## Comandos relacionados

Tabla 1. Comando relacionado con SET TAPEALERTMSG

Comando	Descripción
QUERY TAPEALERTMSG	Visualiza si el servidor anota la información de diagnóstico de hardware.

## SET TOCLOADRETENTION (Establecer período de retención de carga para la Tabla de contenido)

Utilice este comando para especificar el número de minutos aproximado que los datos de tabla de contenido sin referencia permanecerán cargados en la base de datos del servidor.

En las operaciones de copia de seguridad controladas por NDMP de los sistemas de archivos NAS, el servidor puede recopilar información sobre los archivos y directorios de la imagen y almacenar esta información en una tabla de contenido dentro de una agrupación de almacenamiento. Se puede emplear el cliente web para examinar los archivos y directorios de una o varias imágenes de sistema de archivos visualizando las entradas de los datos de la tabla de contenido. El servidor carga los datos necesarios de la tabla de contenido en una tabla de base de datos temporal.

Una vez cargados los datos, el usuario puede seleccionar los archivos y directorios que se restaurarán. Como esta tabla de base de datos es temporal, los datos sólo permanecerán cargados durante un período de tiempo específico desde la última referencia a esos datos. Durante la instalación, el tiempo de retención se establece en 120 minutos. Utilice el comando QUERY STATUS para ver el tiempo de retención de carga de la tabla de contenido.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-Set TOCLOADRetention--minutos-----<<
```

### Parámetros

minutos (Obligatorio)

Especifica el número de minutos aproximado que los datos de tabla de contenido sin referencia se conservan en la base de datos. Puede especificar un entero de 30 a 1000.

### Ejemplo: definir el período de retención de carga para la tabla de contenido

Utilizar el comando SET TOCLOADRETENTION para especificar que los datos de la tabla de contenido sin referencia deben conservarse en la base de datos durante 45 minutos.

```
set tocloadretention 45
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SET TOCLOADRETENTION

Comando	Descripción
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.

## SET VMATRISKINTERVAL (Especifica la modalidad de riesgo para un espacio de archivos de la máquina virtual individual)

Utilice este comando para ajustar la modalidad de evaluación de riesgo para un espacio de archivos de la máquina virtual individual.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas para el dominio al que está asignado el nodo o bien autorización de propietario de cliente en el nodo.

## Sintaxis

```
>>---Set VMATRISKINTERVAL--nombre_nodo--fsid----->
>--TYPE-----+---DEFAULT---+---+-----+-----<
      +-BYPASSED-+  '-Interval----valor-'
      '-CUSTOM---'
```

## Parámetros

nombre\_nodo (necesario)

Especifica el nombre del nodo de cliente que posee el espacio de archivo de máquina virtual que desea actualizar.

fsid (necesario)

Especifica el ID de espacio de archivos del nodo cliente que desea actualizar.

TYPE (necesario)

Especifica qué modalidad de evaluación de riesgo el supervisor de estado debe utilizar al evaluar la clasificación de riesgo del espacio de archivos de MV de los nodos especificados. Especifique uno de los siguientes valores:

DEFAULT

Especifica que el espacio de archivos de la máquina virtual se evalúa con el mismo intervalo que se ha especificado para el mandato SET STATUSATRISKINTERVAL.

BYPASSED

Especifica que el espacio de archivos no se evalúa para el estado de MV en riesgo por el supervisor de estado. Se ha informado de que el estado de riesgo también es eludido en Centro de operaciones.

CUSTOM

Especifica que el espacio de archivos de la máquina virtual se evalúa con el intervalo que se ha especificado para el comando SET STATUSATRISKINTERVAL.

Intervalo

Especifica la cantidad de tiempo, en horas, entre la actividad de copia de seguridad del cliente antes de que el supervisor de estado considere que el cliente está en riesgo. Puede especificar un entero en el rango 6 – 8808. Debe especificar este parámetro cuando TYPE = CUSTOM. No especifique este parámetro cuando TYPE = BYPASSED o TYPE = DEFAULT. El valor de intervalo para todos los tipos de cliente se establece en 24 en la instalación del servidor.

## Establecer nombre de nodo para utilizar un intervalo de riesgo personalizado de 90 días

Definir el intervalo de riesgo de uno nodo denominado *charlievm* (ID de espacio de archivos 50) en un nodo de centro de datos denominado *alice* para utilizar un intervalo de riesgo de 90 días. Puede emitir el mandato QUERY FILESPACE para determinar el ID de espacio de archivos de la MV.

```
set vmatriskinterval alice 50 type=custom interval=2160
```

## Eludir la evaluación del intervalo de riesgo

Excluir la MV llamada *davevm* (ID de espacio de archivos 213) en el nodo de datos denominado *erin* de la comprobación de intervalo de peligro. Puede emitir el mandato QUERY FILESPACE para determinar el ID de espacio de archivos de la MV denominada *davevm*. A continuación, establezca la comprobación del intervalo de riesgo para la MV en eludido.

```
set vmatriskinterval erin 213 type=bypassed
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con set vmatriskinterval

Comando	Descripción
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.



Comando	Descripción
SET NODEATRISKINTERVAL (Especifica la modalidad de riesgo de un nodo individual)	Establece la modalidad y el intervalo de riesgo de un nodo
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
QUERY NODE (Consultar nodos)	Visualiza información parcial o completa sobre uno o más clientes.
QUERY FILESPACE (Consultar uno o más espacios de archivos)	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.

## SETOPT (Establecer una opción de servidor para actualización dinámica)

Puede utilizar el mandato SETOPT para actualizar la mayoría de las opciones de servidor dinámicamente sin detener y reiniciar el servidor. Para la opción DBDIAGLOGSIZE, debe detener e iniciar el servidor. Un mandato SETOPT que esté en una macro o en un script no se puede retrotraer.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.


### Sintaxis







```
>>-SETOPT--nombre_opción--valor_opción-----<<
```

### Parámetros

nombre\_opción (Obligatorio)

Especifica un texto informativo que identifica la opción del servidor que se actualiza. La longitud máxima de la serie de texto es de 255 caracteres. Las opciones siguientes están disponibles:

- ADMINCOMMTimeout
- ADMINIDLETIMEOUT
- ALLOWREORGINDEX
- ALLOWREORGTABLE
- ARCHLOGCOMPRESS
- BACKUPINITIATIONROOT
- CHECKTAPEPOS
- CLIENTDEDUPTXNlimit
- COMMTimeout
-  Sistemas operativos WindowsDATEFORMAT
- DBDIAGLOGSize
- DBDIAGPATHFSTHreshold
- DEDUPTIER2FILESIZE
- DEDUPTIER3FILESIZE
- DEDUPREQUIRESBACKUP
- DNSLOOKUP
- EXPInterval
- EXPQuiet
- FSUSEDTHreshold

- IDLETimeout
- LDAPCACHEDURATION
- MAXSessions
- MOVEBatchsize
- MOVESizethresh
- NDMPPREFDATAINTERFACE
-  Sistemas operativos WindowsNUMBERFORMAT
- NUMOPENVOLsallowed
- RECLAIMDELAY
- RECLAIMPERIOD
- REORGBEGINTime
- REORGDuration
- RESOURCETimeout
- RESTOREINTERVAL
- RETENTIONEXTENSION
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsSANDISCOVERY
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsSANREFRESHTIME
- SERVERDEDUPTXNlimit
- SHREDding
-  Sistemas operativos WindowsTCPPOPT
- THROUGHPUTDatathreshold
- THROUGHPUTTimethreshold
-  Sistemas operativos WindowsTIMEFORMAT
- TXNGroupmax

valor\_opción (Obligatorio)  
Especifica el valor de la opción del servidor.

## Ejemplo: establecer el número máximo de sesiones de cliente

Actualice a 40 la opción del servidor para el número máximo de sesiones de clientes.

```
setopt maxsessions 40
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SETOPT

Comando	Descripción
QUERY OPTION	Muestra información sobre opciones de servidor.
QUERY SYSTEM	Muestra detalles sobre el sistema servidor de IBM Spectrum Protect.

## SHRED DATA (destruir datos)

Utilice este comando para iniciar manualmente el proceso de destrucción de los datos confidenciales suprimidos. La destrucción manual de datos es posible únicamente si la destrucción automática está inhabilitada.

Puede controlar el proceso de destrucción automática mediante la opción del servidor SHREDDING.

Este mandato crea un proceso en segundo plano que puede cancelarse con el mandato CANCEL PROCESS. Para que se visualice información acerca de los procesos en segundo plano, utilice el mandato QUERY PROCESS.

Si se suprimen datos de una agrupación de almacenamiento que impone la destrucción de datos mientras un proceso de destrucción automática está activo, se añadirá al proceso en ejecución.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
.-Wait-----No-----.
```

```

>>-SHRED DATA-----+-----+-----+-----+----->
      '-Duration---minutos-' '-Wait---+No--+'
                                   '-Yes-'

.-IOERROR----SHREDFailure----.
>-----+-----+-----+-----+-----<
      '-IOERROR----+SHREDFailure-+-'
                                   '-SHREDSuccess-'

```

## Parámetros

### DURATION

Especifica el número máximo de minutos durante los que el proceso de destrucción de datos se ejecuta antes de cancelarse automáticamente. Al transcurrir el número de minutos especificado, el servidor cancelará el proceso de destrucción. Tan pronto como el proceso reconoce la cancelación, finaliza. Como consecuencia, es posible que el proceso se ejecute durante más tiempo que el valor que especifique para este parámetro. Puede especificar un número del 1 al 9999. Este parámetro es opcional. Si no se especifica, el servidor se detendrá únicamente después de que todos los datos confidenciales suprimidos se hayan destruido.

### Wait



Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es No. Los valores posibles son:

#### No

Especifica que el servidor procesa este comando en un proceso subordinado. Puede continuar trabajando con otras tareas mientras se procesa el comando. Los mensajes creados a partir del proceso subordinado se visualizan en las anotaciones de actividades o en la consola del servidor, o en ambos, en función de dónde se anoten los mensajes. Para cancelar un proceso subordinado, utilice el comando CANCEL PROCESS. Si cancela este proceso, es posible que se hayan destruido algunos archivos antes de la cancelación. Este es el valor predeterminado.

#### Yes

Especifica que el servidor procesa este comando en primer plano. Debe esperar a que la operación finalice para poder continuar con otras tareas. El servidor muestra los mensajes de salida en el cliente de administración al terminarse la operación. Los mensajes también se visualizan en las anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

 Sistemas operativos AIX  Sistemas operativos LinuxNota: No se puede especificar WAIT=YES desde la consola del servidor.

### IOERROR

Especifica si un error de E/S detectado durante la destrucción de datos debe considerarse como una destrucción satisfactoria. Este parámetro es opcional. El valor predeterminado es SHREDFAILURE. Los valores posibles son:

#### SHREDFailure

Especifica que si el servidor detecta un error de E/S durante la destrucción de datos, se considerará que los datos no se han destruido satisfactoriamente y el archivo propietario se marcará como dañado. El servidor intentará destruir los datos la próxima vez que se ejecute el proceso de destrucción, de modo que tendrá una oportunidad para corregir el error y asegurarse de que los datos se han destruido correctamente.

#### SHREDSuccess

Especifica que si el servidor detecta un error de E/S durante la destrucción de datos y el archivo propietario se ha marcado previamente como dañado, se considerará que los datos se han destruido satisfactoriamente. Debería utilizar esta opción únicamente después de que el servidor haya notificado errores de E/S durante la destrucción de datos y no pueda corregir el error.

## Ejemplo: destruir datos

Iniciar manualmente la destrucción de todos los datos confidenciales suprimidos. Permitir que la ejecución del proceso continúe durante seis horas como máximo antes de que tenga lugar la cancelación automática de éste.

```
shred data duration=360
```

## Comandos relacionados

Tabla 1. Comandos relacionados con SHRED DATA

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
QUERY PROCESS	Muestra información sobre procesos subordinados.

Comando	Descripción
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.

## SUSPEND EXPORT (Suspender una operación de exportación actualmente en ejecución)

Utilice este comando para suspender una operación de exportación de servidor a servidor que tiene un valor de FILEDATA que no es NONE. La operación de exportación que desea suspender debe haber pasado la fase de inicialización para poder considerarse seleccionable para la suspensión. El estado de la operación de exportación se guarda. La operación puede reiniciarse mediante la emisión del comando RESTART EXPORT.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-SUSPend EXPORT .-*-----
+-----+-----<
'---identificador_exportación---'
```

### Parámetros

#### EXPORTIdentifier

Este parámetro opcional especifica el nombre de la operación de exportación. Puede buscar un nombre emitiendo el comando QUERY EXPORT para que se muestren todas las operaciones de exportación de servidor a servidor que se están ejecutando en ese momento y se pueden suspender. También puede utilizar el carácter comodín para especificar el nombre.

### Ejemplo: suspender una operación de exportación específica

Suspender la operación de exportación en EXPORTALLACCTNODES en ejecución. Cuando se emite el comando SUSPEND EXPORT, no se genera ninguna salida. Debe emitir el comando QUERY EXPORT para verificar que la operación EXPORTALLACCTNODES se ha suspendido.

```
suspend export exportallacctnodes
```

### Ejemplo: suspender todas las operaciones de exportación en ejecución

Suspender todas las operaciones de exportación con el estado RUNNING.

```
suspend export *
```

### Comandos relacionados

Tabla 1. Comandos relacionados con SUSPEND EXPORT

Comando	Descripción
CANCEL EXPORT	Suprime una operación de exportación suspendida.
EXPORT NODE	Copia información de nodos cliente en un medio externo o directamente en otro servidor.
EXPORT SERVER	Copia todo o una parte del servidor en un medio externo o directamente en otro servidor.
QUERY EXPORT	Visualiza las operaciones de exportación que actualmente están en ejecución o que se han suspendido.
RESTART EXPORT	Reinicia una operación de exportación suspendida.

## Mandatos UNLOCK

Utilice los comandos UNLOCK para restablecer el acceso después de que se haya bloqueado un objeto.

- UNLOCK ADMIN (Desbloquear un administrador)
- UNLOCK NODE (Desbloquear un nodo cliente)
- UNLOCK PROFILE (Desbloquear un perfil)

## UNLOCK ADMIN (Desbloquear un administrador)

Utilice el mandato UNLOCK ADMIN para permitir que un administrador bloqueado acceda de nuevo al servidor. También puede desbloquear varios administradores que se autentican con el mismo método.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UNLOCK Admin--+-*-----+--+-----+>><
                '-nombre_admin-' '-AUTHentication--==--+Local-+-'
                                     '-LDap--'
```

### Parámetros

nombre\_admin (Necesario)

Especifica el nombre del administrador que se desbloquea. Puede utilizar caracteres comodín para especificar el nombre del administrador. No tiene que especificar un nombre de administrador, si desea desbloquear a todos los administradores de acuerdo con su método de autenticación. Utilice el carácter comodín con un método de autenticación para desbloquear múltiples administradores. El parámetro es necesario (no hay un comodín predeterminado).

AUTHentication

Especifica el método de autenticación de contraseñas que necesita el administrador para iniciar la sesión.

Local

Especifica que desea bloquear los ID de usuario administrado que autentican las contraseñas con el servidor de IBM Spectrum Protect.

LDap

Especifica que desea desbloquear los ID de usuario administrador que autentican las contraseñas con el servidor de directorio LDAP.

### Ejemplo: desbloquear un ID de usuario administrador

El ID de usuario administrador JOE tiene bloqueado el acceso a IBM Spectrum Protect. Permitir que JOE acceda al servidor. Emita el comando siguiente:

```
unlock admin joe
```

### Ejemplo: desbloquear todos los ID de usuario administrador que autentican contraseñas con un servidor de directorios LDAP

El ID de usuario administrador que utiliza contraseñas para autenticarse con un servidor de directorios LDAP debe estar bloqueado para que los ID puedan comunicarse con el servidor de IBM Spectrum Protect .

```
unlock admin * authentication=ldap
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UNLOCK ADMIN

Comando	Descripción
LOCK ADMIN	Impide que un administrador acceda a IBM Spectrum Protect.
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.

## UNLOCK NODE (Desbloquear un nodo cliente)

Utilice este comando para permitir que un nodo bloqueado tenga acceso al servidor. También puede desbloquear varios nodos que utilizan el mismo método de autenticación.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

### Sintaxis

```
>>-UNLOCK Node--+-*-----+-----+-----+-----+><
                '-nombre_nodo-' '-AUTHentication---+Lcal+-'
                                     '-LDap--'
```

### Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se desbloquea. Puede utilizar caracteres comodín para especificar el nombre de nodo. No tiene que especificar un nombre de nodo, si desea desbloquear todos los nodos de acuerdo con su método de autenticación. Utilice el comodín con un método de autenticación para desbloquear grupos de nodos. Este parámetro es obligatorio. No hay ningún carácter comodín de forma predeterminada.

AUTHentication

Especifica el método de autenticación de contraseña del nodo. Este parámetro es opcional.

Lcal

Especifica que desea bloquear los nodos que autentican las contraseñas con el servidor de IBM Spectrum Protect.

LDap

Especifica que desea desbloquear los nodos que autentican las contraseñas con el servidor de directorio LDAP.

### Ejemplo: desbloquear un nodo

El nodo de cliente SMITH tiene bloqueado el acceso a IBM Spectrum Protect. Permitir que SMITH acceda al servidor.

```
unlock node smith
```

### Ejemplo: Desbloquear todos los nodos que se autentican con el servidor de IBM Spectrum Protect

Los nodos que no autentican las contraseñas con servidores de directorio LDAP deben estar desbloqueado.

```
unlock node * authentication=local
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UNLOCK NODE

Comando	Descripción
LOCK NODE	Impide que un cliente acceda al servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.

## UNLOCK PROFILE (Desbloquear un perfil)

Utilice este comando en un gestor de configuración para desbloquear un perfil de configuración para que pueda distribuirse a los servidores gestionados que se inscriben.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
>>-UNLOCK PROFILE--nombre_perfil-----<<
```

## Parámetros

nombre\_perfil (Obligatorio)

Especifica el perfil que se desbloquea. Puede utilizar caracteres comodín para especificar varios nombres.

## Ejemplo: desbloquear un perfil

Desbloquear un perfil denominado TOM.

```
desbloquear el perfil tom
```

## Comandos relacionados




Tabla 1. Comandos relacionados con UNLOCK PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UPDATE PROFILE	Cambia la descripción de un perfil.

## Comandos UPDATE

Utilice el comando UPDATE para modificar uno o más atributos de un objeto IBM Spectrum Protect existente.

- UPDATE ADMIN (Actualizar un administrador)
- UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)
- UPDATE ALERTSTATUS (actualizar el estado de una alerta)
- UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)
- UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)
- UPDATE CLOPTSET (Actualizar la descripción de un conjunto de opciones de cliente)
- UPDATE COLLOGGROUP (Actualizar un grupo de proximidad)
- UPDATE COPYGROUP (Actualizar un grupo de copia)
- UPDATE DATAMOVER (Actualizar un transportador de datos)
- UPDATE DEVCLASS (Actualizar los atributos de una clase de dispositivo)
- UPDATE DOMAIN (Actualizar un dominio de políticas)
- UPDATE DRIVE (Actualizar una unidad)
- UPDATE FILESPACE (Actualizar reglas de réplica de nodos de espacio de archivos)
- UPDATE LIBRARY (Actualizar una biblioteca)
- UPDATE LIBVOLUME (Cambiar el estado de un volumen de almacenamiento)
- UPDATE MACHINE (Actualizar información de máquina)
- UPDATE MGMTCLASS (Actualizar una clase de gestión)
- UPDATE NODE (Actualizar atributos del nodo)
- UPDATE NODEGROUP (Actualizar un grupo de nodos)
- UPDATE PATH (cambiar una ruta)
- UPDATE POLICYSET (Actualizar la descripción de un juego de políticas)
- UPDATE PROFILE (Actualizar una descripción de perfil)
- UPDATE RECOVERYMEDIA (Actualizar medio de recuperación)

- UPDATE REPLRULE (Actualizar reglas de réplica)
- UPDATE SCHEDULE (Actualizar una planificación)
- UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)
- UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)
- UPDATE SERVERGROUP (Actualizar una descripción de grupo de servidores)
- UPDATE SPACETRIGGER (Actualizar los desencadenantes de espacio)
- UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows UPDATE STGPOOLDIRECTORY (Actualización de un directorio de agrupaciones de almacenamiento)
- UPDATE VIRTUALFSMAPPING (Actualizar una correlación de espacios de archivos virtuales)
- UPDATE VOLHISTORY (Actualizar información histórica de volúmenes secuenciales)
- UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

## UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)

Utilice este mandato para actualizar los atributos de uno o varios desencadenantes de alertas.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

      .-n-----
      v              |
>>-UPDate ALERTRTrigger-----+---+---+----->
      .-CAtegory-----SErver-----
>-----+-----+-----+----->
      '-CAtegory-----+APplication+-'
              +-INventory---+
              +-CLient-----+
              +-DEvice-----+
              +-SErver-----+
              +-STorage-----+
              +-SYstem-----+
              '-VMclient---'

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
      |           .-,------. | | |           .-,------. | | |
      |           v              | | |           v              | | |
      '-ADDadmin-----+nombre_admin+-' '-DELadmin-----+nombre_admin+-'
  
```

### Parámetros

**número\_mensaje** (Obligatorio)

Especifica el número de mensaje que desea asociar con el desencadenante de la alerta. Especifique varios números de mensajes, separados por comas, sin espacios intercalados. Los números de mensajes tienen una longitud máxima de ocho caracteres.

**CATegory**

Especifica el tipo de categoría de la alerta, que está determinado por los tipos de mensajes. El valor predeterminado es SERVER. Nota: Si se cambia la categoría de un desencadenante de alerta, no se cambia la categoría de las alertas existentes en el servidor. Las nuevas alertas se clasifican dentro de la nueva categoría.

Especifique uno de los siguientes valores:

**APplication**

La alerta se clasifica como una categoría de aplicación. Por ejemplo, puede especificar esta categoría para los mensajes asociados con los clientes de aplicación (TDP).

**INventory**

La alerta se clasifica como categoría de inventario. Por ejemplo, puede especificar esta categoría para mensajes que están asociados con la base de datos, el archivo de registro activo o el archivo de registro de archivado.

**CLient**

La alerta se clasifica como una categoría de cliente. Por ejemplo, puede especificar esta categoría para los mensajes asociados con actividades de cliente generales.



#### DDevice

La alerta se clasifica como una categoría de dispositivo. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados a las clases de dispositivos, bibliotecas, unidades o vías de acceso.

#### SERver

La alerta se clasifica como una categoría de servidor general. Por ejemplo, puede especificar esta categoría para los mensajes asociados a las actividades del servidor generales o a sucesos.

#### STorage

La alerta se clasifica como una categoría de almacenamiento. Por ejemplo, puede especificar esta categoría para los mensajes asociados con las agrupaciones de almacenamiento.

#### SYstems

La alerta se clasifica como una categoría de clientes del sistema. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con los clientes de archivado y copia de seguridad del sistema o archivado y copia de seguridad de gestión de almacenamiento jerárquico (HSM).

#### VMclient

La alerta se clasifica bajo la categoría VMclient. Por ejemplo, puede especificar esta categoría para los mensajes que están asociados con clientes de máquina virtual.

#### ADmin

Este parámetro opcional especifica el nombre del administrador que recibe el correo electrónico de notificación de esta alerta. El desencadenante de alerta se ha definido satisfactoriamente aunque no se ha especificado ningún nombre de administrador.

#### ADDadmin

Especifica el nombre de administrador que desea agregar a la lista de administradores que reciben alertas por correo electrónico. Especifique varios nombres de administrador, separados por comas y sin espacios intercalados.

#### DELadmin

Especifica el nombre del administrador que desea suprimir de la lista de administradores que reciben alertas por correo electrónico. Especifique varios nombres de administrador, separados por comas y sin espacios intercalados.

## Actualizar desencadenante de alerta

Añada los nombres de los administradores que desea que reciban la notificación cuando se produzca una alerta ANR1073E, ANR1074E, y suprima el nombre de un administrador que ya no desee que reciba la notificación, emitiendo el siguiente mandato:

```
update alerttrigger ANR1073E,ANR1074E ADDadmin=djee,cdawson,mhaye deladmin=harryh
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con UPDATE ALERTTRIGGER

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTSTATUS (actualizar el estado de una alerta)	Actualiza el estado de una alerta notificada.

## UPDATE ALERTSTATUS (actualizar el estado de una alerta)

Utilice este mandato para actualizar el estado de una alerta sobre la que se ha informado.

## Clase de privilegio

Cualquier administrador puede emitir este mandato.

## Sintaxis

```

      .-,-----,
      v          |
>>-UPDate ALERTStatus-----+--ID_alerta-+----->
>+-----+-----+-----+-----+----->
  '-Status-----+Inactive-+-'  '-ASSigned-----texto-'
      '-Closed---'
>+-----+-----+-----+-----+-----><
  '-RESolvedby----text-'  '-REMark----text-'

```

## Parámetros

### id\_alerta (Necesario)

Especifica la alerta que desea actualizar. Puede especificar varios números de mensaje separándolos con comas y sin espacios intercalados.

### Status

Especifica el tipo de estado que desea actualizar. El estado de las alertas se puede cambiar a partir de activo a inactivo o cerrado, o de inactivo a cerrado. Los valores posibles son:

#### Inactivo

Las alertas activas pueden cambiar al estado inactivo.

#### Cerrado

Las alertas activas e inactivas pueden cambiar al estado cerrado.

### ASSigned

Especifica el nombre del administrador que se asigna a la alerta que desea consultar.

### RESolvedby

Especifica el nombre de administrador que ha resuelto la alerta que desea consultar.

### REMark

Este parámetro especifica el texto de comentario. El texto de comentario no puede tener más de 255 caracteres. Si la descripción contiene espacios en blanco, escriba el texto entero entre comillas (""). Elimine el texto definido anteriormente especificando una serie nula ("") para este valor.

## Actualizar el texto de comentario de una alerta

Emita el mandato siguiente para actualizar el texto de comentario y el número de ID de alerta 25 e indicar que *DJADMIN* está trabajando en la alerta:

```
update alertstatus 25 assigned=DJADMIN
```

## Actualizar estado de alerta

Emita el mandato siguiente para cambiar el número de ID de alerta 72 al estado cerrado y agregar un comentario sobre cómo se ha resuelto la alerta:

```
update alertstatus 72 status=closed remark="Se ha aumentado el tamaño del sistema de
archivos para
el registro activo"
```

## Comandos relacionados



Tabla 1. Mandatos relacionados con UPDATE ALERTSTATUS

Comando	Descripción
DEFINE ALERTTRIGGER (Definir un desencadenante de alerta)	Asocia los mensajes especificados a un desencadenante de alerta.
DELETE ALERTTRIGGER (eliminar un mensaje de un desencadenante de alerta)	Elimina un número de mensaje que puede desencadenar una alerta.
QUERY ALERTSTATUS (Consultar el estado de una alerta)	Muestra información sobre alertas que se han emitido en el servidor.
QUERY ALERTTRIGGER (Consultar la lista de desencadenantes de alertas)	Visualiza números de mensaje que desencadenan una alerta.

Comando	Descripción
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
UPDATE ALERTTRIGGER (Actualizar un desencadenante de alerta definido)	Actualiza los atributos de uno o varios desencadenantes de alertas.

## UPDATE ADMIN (Actualizar un administrador)

Utilice este comando para cambiar la contraseña o la información de contacto de un administrador. Sin embargo, no puede actualizar el nombre de administrador SERVER\_CONSOLE.

 Sistemas operativos AIX  Sistemas operativos Linux Las contraseñas de los administradores deben cambiarse después de un periodo de tiempo que se determina mediante el mandato SET PASSEXP. El mandato SET PASSEXP no afecta a las contraseñas que se autentican con un servidor LDAP (Lightweight Directory Access Protocol).

Restricción: No puede actualizar el método de autenticación para su propio ID de usuario. Si es necesario, otro administrador debe hacer ese cambio. Asimismo, cuando actualiza una contraseña con el mandato UPDATE ADMIN, no puede utilizar un comodín con el parámetro `admin_name`.

Se pueden crear administradores con el mismo nombre como nodo durante un mandato REGISTER NODE . Para mantener el nodo y el administrador con el mismo nombre sincronizados, el método de autenticación y el valor de SSLREQUIRED del nodo se actualizan para coincidan con el del administrador. Si el método de autenticación de administrador se cambia de LOCAL a LDAP, y no se proporciona una contraseña, el nodo se coloca en estado "pendiente de LDAP". La contraseña se solicita en el siguiente inicio de sesión. Las contraseñas entre nodos y administradores con el mismo nombre se mantienen sincronizadas después de cualquier cambio de autenticación.

Debe utilizar el mandato RENAME ADMIN para cambiar el nombre de un administrador registrado.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Si un ID de usuario de administración coincide con un nombre de nodo, no actualice el método de autenticación a LDAP. Si lo hace, podría darse un comportamiento imprevisto, debido a los cambios automáticos de contraseña que actualizan la misma contraseña dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

## Clase de privilegio

Para emitir este mandato para cambiar la contraseña o la información de contacto de otro administrador, debe tener privilegio de sistema. Cualquier administrador puede emitir este mandato para actualizar su propia contraseña o información de contacto.

## Sintaxis

```

>>-UPDate Admin-----nombre_admin-----+-----+----->
                                     '-contraseña-'
>--+-----+-----+-----+-----+-----+----->
  '-PASSExp----días-'  '-CONTACT---texto-'
>--+-----+-----+-----+-----+-----+----->
  '-FORCEPwreset-----+No--+-'
                               '-Yes-'
>--+-----+-----+-----+-----+-----+----->
  '-EMAILAddress----ID_usuario@nodo-'
>--+-----+-----+-----+-----+-----+----->
|                                     (3) |
|                                     .-SYNCLdapdelete-----+No-- |
| '-AUTHentication-----+LOCAL+-----+-----+-----+-----+-----+----->
|                                     '-LDap--'  '-SYNCLdapdelete-----+Yes+-'
|                                     '-No--'

```

```

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
|          (4)          |
|'-SSLrequired-----+-Yes-----+-'|
|          +-No-----+|
|          '-DEFault-'|
|
|.-SESSIONSECurity----TRANSitional----.|
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
|'-SESSIONSECurity----+-STRict-----+-'|
|          '-TRANSitional-'|
|
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<
|'-ALert-----+-Yes-+-'|
|          '-No--'|

```

#### Notas:

1. Debe especificar como mínimo un parámetro opcional en este mandato.
2. Las contraseñas son opcionales para este mandato, excepto si se cambia el método de autenticación de LDAP local.
3. El parámetro SYNCDapdelete si un administrador que se autentica en un servidor de directorios LDAP regresa a la autenticación local.
4. El parámetro SSLREQUIRED está en desuso.

## Parámetros

### nombre\_admin (Necesario)

Especifica el nombre del administrador que se ha de actualizar.

### contraseña

Especifica la contraseña del administrador. Este parámetro es opcional en la mayoría de los casos. Si se cambia el método de autenticación del administrador de LDAP a LOCAL, se necesita una contraseña. Si se utiliza un servidor LDAP para la autenticación de administradores, no especifique una contraseña utilizando el mandato UPDATE ADMIN.

### PASSExp

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña en el rango de 0 – 9999. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, el período de caducidad de contraseña permanece igual. Este parámetro no se aplica a las contraseñas que se almacenan en un servidor de directorios LDAP.

### CONtact

Especifica una serie de texto que identifica al administrador. Este parámetro es opcional. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir la información de contacto definida, especifique una serie nula ("").

### FORCEPwreset

Especifica si el administrador tiene que cambiar o restablecer la contraseña. Este parámetro es opcional. Los valores posibles son:

#### No

Especifica que el administrador no necesita cambiar ni restablecer la contraseña al intentar conectarse al servidor. El período de caducidad de la contraseña se establece mediante el comando SET PASSEXP.

#### Yes

Especifica que la contraseña del administrador caducará durante la próxima conexión. El cliente debe cambiar o restaurar la contraseña entonces. Si no se especifica una contraseña, recibirá un error de sintaxis.

Restricciones:

- En el caso de los ID de usuarios administrativos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si tiene previsto especificar AUTHENTICATION=LDAP.
- Si tiene previsto actualizar un ID de usuario administrativo para la autenticación con un servidor LDAP y ha especificado FORCEPWRESET=YES, debe cambiar la contraseña para poder especificar FORCEPWRESET=NO y AUTHENTICATION=LDAP.

### EMAILAddress

Este parámetro se utiliza para información de contacto adicional. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

### AUTHentication

Este parámetro determina el método de autenticación de la contraseña que utiliza el ID de administrador, bien LDAP o LOCAL.

### Local

Especifica que el administrador utiliza la base de datos del servidor de IBM Spectrum Protect local para almacenar las contraseñas para la autenticación.

## LDap

Especifica que el administrador utiliza un servidor de directorios LDAP para la autenticación de contraseñas.

## SYNCldapdelete

Este parámetro solo se aplica si un administrador que se autentica en un servidor LDAP quiere volver a la autenticación local.

### Yes

Especifica que se ha de suprimir el administrador del servidor LDAP.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

### No

Especifica que no se ha de suprimir el administrador del servidor LDAP. Este es el valor predeterminado.

## SSLrequired (en desuso)

Especifica si el ID de usuario administrador debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect y el cliente de archivado y copia de seguridad. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red

Importante: A partir de IBM Spectrum Protect Versión 8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

## SESSIONSECurity

Especifica si el administrador debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

### STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el administrador. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el administrador. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el administrador pueda autenticarse en el servidor:

- Tanto el administrador como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el administrador para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el administrador.

Los administradores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

### TRANSitional

Especifica que se aplicarán los valores de seguridad existentes para el administrador. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el administrador no cumplen nunca los requisitos para el valor STRICT, el administrador continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un administrador cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el administrador ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el administrador se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un administrador que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como el direccionamiento de mandatos o la exportación entre servidores, cuando el administrador se autentica en el servidor IBM Spectrum Protect como administrador de otro servidor.

## ALert

Especifica si las alertas se envían a una dirección de correo electrónico de los administradores.

### Yes

Especifica que las alertas se envíen a la dirección de correo electrónico especificada de los administradores.

### No

Especifica que las alertas no se envíen a la dirección de correo electrónico especificada de los administradores. Este es el valor predeterminado.

Consejo: La supervisión de alertas debe estar habilitada y los valores de correo electrónico deben estar definidos correctamente para recibir las alertas por correo electrónico de forma satisfactoria. Para ver los valores actuales, emita el mandato QUERY MONITORSETTINGS.

## Ejemplo: Actualizar una contraseña y el período de caducidad de la contraseña

Actualizar el administrador LARRY de modo que tenga la contraseña SECRETWORD y el período de caducidad de contraseña de 120 días. El administrador de este ejemplo se autentica en el servidor de IBM Spectrum Protect.

```
update admin larry secretword passexp=120
```

## Ejemplo: Actualizar todos los administradores para comunicarse con un servidor utilizando la seguridad de sesión estricta.

Actualice todos los administradores para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
update admin * sessionsecurity=strict
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE ADMIN

Comando	Descripción
QUERY ADMIN	Muestra información sobre uno o varios administradores de IBM Spectrum Protect.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
RENAME ADMIN	Cambia el nombre de un administrador de IBM Spectrum Protect.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

### Tareas relacionadas:

Nombrar objetos de Tivoli Storage Manager

### Información relacionada:

Opción de cliente SSL

## UPDATE BACKUPSET (Actualizar un valor de retención asignado a un juego de copias de seguridad)

Utilice este mandato para actualizar el valor de retención asociado al juego de copias de seguridad de un cliente.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas para el dominio al que está asignado el nodo cliente.

## Sintaxis

```

      .-,------.
      v           |
>>-UPDate BACKUPSET-----+nombre_nodo-----+----->
      '-nombre_grupo_nodos-'
      .-,------.

```

```

V
|
>---nombre_juego_copias_seguridad+----->
>--REtention---+---días---+----->
      '-NOLimit-' '-BEGINDate----fecha-'
>+-----+-----+----->
      '-BEgINTime----hora-' '-ENDDate----fecha-'
>+-----+-----+----->
      '-ENDTime----hora-' '-WHEREREtention---+---días---+-'
                                   '-NOLimit-'
. -WHEREDATAType----ALL-----
>+-----+-----+----->
|                                     V | |
|                                     | | |
'-WHEREDATAType-----+FILE--+-----'
                                   '-IMAGE-'
>+-----+-----+----->
      '-WHEREDEScRiption----descripción-'
. -VERSiOn---Any-----
>+-----+-----+-----<
      '-Preview---+No--+-' '-VERSiOn---+Any---+-'
      '-Yes-'                '-Latest-'

```

## Parámetros

nombre\_nodo o nombre\_grupo\_nodos (Necesario)

Especifica los nombres de los nodos cliente o grupos de nodos cuyos datos se incluyen en el juego de copias de seguridad especificado que se ha de actualizar. Para especificar varios nombres de nodo y nombres de grupos de nodos, debe separarlos con comas y sin espacios intercalados. Los nombres de nodo que especifique pueden contener caracteres comodín, pero los nombres de grupos de nodos no pueden contener caracteres comodín.

nombre\_juego\_copias\_seguridad (Obligatorio)

Especifica el nombre del juego de copias de seguridad que se va a actualizar. El nombre de juego de copias de seguridad especificado puede contener caracteres comodín. Puede especificar varios nombres de juego de copias de seguridad separándolos con comas y sin espacios intercalados.

REtention (Obligatorio)

Especifica el número actualizado de días que se retiene el juego de copias de seguridad en el servidor. Puede especificar un entero entre el 0 y el 30000. Los valores son:

días

Especifica el número actualizado de días que se retiene el juego de copias de seguridad.

NOLimit

Especifica que el juego de copias de seguridad se retiene indefinidamente en el servidor. Si especifica NOLIMIT, el servidor retiene para siempre los volúmenes que contienen el juego de copias de seguridad, excepto si un usuario o un administrador suprime los volúmenes del almacenamiento del servidor.

Atención: la actualización del período de retención de un juego de copias de seguridad podría hacer que caducase a una hora diferente de otros juegos de copias de seguridad almacenados en el mismo medio de salida. En cualquier caso, el medio no estará disponible para otros usos hasta que todos sus juegos de copias de seguridad hayan caducado.

BEGINDate

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. El valor predeterminado es la fecha actual. Puede utilizar este parámetro con el parámetro BEGINTIME para especificar un rango para la fecha y la hora. Si especifica una fecha inicial sin una hora inicial, la hora será a las 12:00 de la noche de la fecha que especifique.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY-3 o -3.

Valor	Descripción	Ejemplo
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### BEGINTime

Especifica la fecha inicial en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. El valor predeterminado es la hora actual. Puede utilizar este parámetro con el parámetro BEGINDATE para especificar un rango para la hora y la fecha. Si especifica una hora inicial sin una fecha inicial, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos en la fecha final especificada	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos en la fecha final especificada	NOW-02:00 o -02:00.

#### ENDDate

Especifica la fecha final en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. Puede utilizar este parámetro con el parámetro ENDTIME para especificar un rango para la hora y la fecha. Si especifica una fecha final sin una hora final, la hora será a las 11:59:59 de la noche de la fecha final especificada.

Puede especificar la fecha utilizando uno de los valores siguientes:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1999
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados.	TODAY +3 o +3.
TODAY-días o -días	La fecha actual menos los días especificados.	TODAY -3 o -3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### ENDTime

Especifica la hora final en la que se creó el juego de copias de seguridad que se va a actualizar. Este parámetro es opcional.

Puede utilizar este parámetro con el parámetro ENDDATE para especificar un rango para la hora y la fecha. Si especifica una hora final sin una fecha final, la fecha será la fecha actual para la hora que especifique.

Puede especificar la hora con uno de los valores siguientes:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08



Valor	Descripción	Ejemplo
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00.

#### WHERERetention

Especifica, en días, el valor de retención asociado a los juegos de copias de seguridad que se van a actualizar. Los valores son:

días

Especifica que el juego de copias de seguridad que se va a retener el número de días especificado está actualizado.

NOLimit

Especifica que el juego de copias de seguridad retenido de forma indefinida está actualizado.

#### WHEREDescription

Especifica la descripción asociada al juego de copias de seguridad que se va a actualizar. Este parámetro es opcional. Puede especificar caracteres comodín en la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

#### WHEREDataType

Especifica que se van a actualizar los juegos de copias de seguridad que contienen los tipos especificados de datos. Este parámetro es opcional. El valor predeterminado es que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben actualizar. Para especificar varios tipos de datos, sepárelos con comas y sin espacios intercalados. Los valores posibles son:

ALL

Especifica que los juegos de copias de seguridad para todos los tipos de datos (nivel de archivo, imagen y aplicación) se deben actualizar. Este es el valor predeterminado.

FILE

Especifica que un juego de copias de seguridad de nivel de archivo se va a actualizar. Los juegos de copias de seguridad de nivel de archivo contienen copias de seguridad de archivos y directorios realizadas por el cliente de copia de seguridad/archivado.

IMAGE

Especifica que se va a actualizar un juego de copias de seguridad de imagen. Los juegos de copias de seguridad de imagen contienen las imágenes que ha creado el comando BACKUP IMAGE del cliente de copia de seguridad/archivado.

#### Preview

Especifica si se previsualiza la lista de los juegos de copias de seguridad que se van a actualizar, sin actualizar realmente los juegos de copias de seguridad. Este parámetro es opcional. El valor predeterminado es No. Los valores son:

No

Especifica que los juegos de copias de seguridad se actualizarán.

Yes

Especifica que el servidor visualiza la lista de los juegos de copias de seguridad que se van a actualizar, sin actualizarlos realmente.

#### VERSION

Especifica la versión del juego de copias de seguridad que se va a actualizar. Los juegos de copias de seguridad con el mismo nombre de prefijo se consideran versiones diferentes del mismo juego de copias de seguridad. Este parámetro es opcional. El valor predeterminado es actualizar cualquier versión que coincida con los criterios especificados en el comando. Los valores son:

Any

Especifica que cualquier versión que coincida con los criterios especificados en el comando debe actualizarse.

Latest

Especifica que únicamente debe actualizarse la versión más reciente del juego de copias de seguridad. Si otros criterios especificados en el comando (por ejemplo, ENDDATE o WHERERetention) excluyen la versión más reciente del juego de copias de seguridad, no se actualizará ningún juego de copias de seguridad.

## Ejemplo: actualizar un período de retención

Actualizar el periodo de retención donde la descripción es Healthy Computers. El periodo de retención se asigna al juego de copias de seguridad PERS\_DATA.3099 que contiene datos del nodo cliente JANE. Cambiar el periodo de retención a 70 días.

```
update backupset jane pers_data.3099
retention=70 wheredescription="healthy computers"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE BACKUPSET

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
GENERATE BACKUPSETTOC	Genera una tabla de contenido para un juego de copias de seguridad.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY BACKUPSETCONTENTS	Visualiza el contenido que hay en los juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE NODEGROUP	Actualiza la descripción de un grupo de nodos.

## UPDATE CLIENTOPT (Actualizar un número de secuencia de opción de cliente)

Utilice este comando para actualizar el número de secuencia de una opción de cliente en un conjunto de opciones de cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

### Sintaxis

```
>>-UPDate CLIENTOpt--nombre_conjunto_opciones--nombre_opción---->  
>--número_secuencia_actual--número_secuencia_nueva-----><
```

### Parámetros

nombre\_conjunto\_opciones (Obligatorio)  
Especifica el nombre del conjunto de opciones.

nombre\_opción (Obligatorio)  
Especifica una opción cliente válida.

número\_secuencia\_actual (Obligatorio)  
Especifica el número de secuencia actual de la opción.

nuevo\_número\_secuencia (Obligatorio)  
Especifica el nuevo número de secuencia de la opción.

### Ejemplo: actualizar un número de secuencia de opción de cliente

Para actualizar el número de secuencia de la opción de cliente actual, emita el comando siguiente:

```
update clientopt eng dateformat 0 9
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE CLIENTOPT

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.

## UPDATE CLOPTSET (Actualizar la descripción de un conjunto de opciones de cliente)

Utilice este comando para actualizar la descripción de un conjunto de opciones de cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que está asignado el nodo cliente.

### Sintaxis

```
>>-UPDate CLOptset--nombre_conjunto_opciones----->
>--DESCRiption--===descripción-----><
```

### Parámetros

nombre\_conjunto\_opciones (Obligatorio)

Especifica el nombre del conjunto de opciones.

DESCRiption (Obligatorio)

Especifica una descripción del conjunto de opciones de cliente. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

### Ejemplo: actualizar la descripción de un conjunto de opciones de cliente

Actualizar la descripción de un conjunto de opciones de cliente denominado ENG.

```
update cloptset eng description="unix"
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE CLOPTSET

Comando	Descripción
COPY CLOPTSET	Copia un juego de opciones de cliente.
DEFINE CLIENTOPT	Añade una opción de cliente a un conjunto de opciones de cliente.
DEFINE CLOPTSET	Define un juego de opciones de cliente
DELETE CLIENTOPT	Elimina una opción cliente de un conjunto de opciones de cliente.
DELETE CLOPTSET	Suprime un juego de opciones de cliente.
QUERY CLOPTSET	Visualiza información sobre un conjunto de opciones de cliente.
UPDATE CLIENTOPT	Actualiza el número de secuencia de una opción de cliente de un conjunto de opciones de cliente.

## UPDATE COLLOGROUP (Actualizar un grupo de proximidad)

Utilice este comando para modificar la descripción de un grupo de proximidad.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o de almacenamiento sin restricciones.

## Sintaxis

```
>>-UPDate COLLOCGroup--nombre_grupo----->  
>--DESCRiption----descripción-----<<
```

## Parámetros

nombre\_grupo

Especifica el nombre del grupo de proximidad cuya descripción desea actualizar.

DESCRiption (Obligatorio)

Especifica una descripción del grupo de proximidad. Este parámetro es necesario. La longitud máxima de la descripción es de 255 caracteres. Si la descripción contiene blancos, encierre toda la descripción entre comillas.

## Ejemplo: actualizar un grupo de proximidad

Actualizar el grupo de proximidad, GROUP1, con una nueva descripción.

```
update collogroup group1 "Human Resources"
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE COLLOGROUP

Comando	Descripción
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
MOVE NODEDATA	Traspasa datos de uno o varios nodos o de un único nodo con espacios de archivos seleccionados.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE STGPOOL	Cambia los atributos de una agrupación de almacenamiento.

## UPDATE COPYGROUP (Actualizar un grupo de copia)

Utilice este comando para actualizar un grupo de copia de seguridad o de copia archivada. Para que los clientes puedan utilizar el grupo de copia actualizado, debe activar el juego de políticas que contiene el grupo de copia.

Consejo: El comando UPDATE COPYGROUP no se ejecutará correctamente si especifica como destino una agrupación de almacenamiento de copia.

El comando UPDATE COPYGROUP ofrece dos posibilidades, en función de si la actualización se realiza para un grupo de copias de seguridad o para un grupo de copias archivadas. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con UPDATE COPYGROUP

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE COPYGROUP	Elimina un grupo de copia de seguridad o copia archivada de un dominio de políticas y juego de políticas.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
EXPIRE INVENTORY	Inicia manualmente el proceso de caducidad de inventario.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.

- UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)  
Utilice este comando para actualizar un grupo de copia de seguridad definido.
- UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)  
Utilice este comando para actualizar un grupo de copia archivada definido.

## UPDATE COPYGROUP (Actualizar un grupo de copias de seguridad)

Utilice este comando para actualizar un grupo de copia de seguridad definido.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

### Sintaxis

```
>>-UPDate COpYgroup----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+--+-----+----->
  '-STANDARD-'  '-Type----Backup-'
>--+-----+--+-----+----->
  '-DESTination----nombre_agrupación-'
>--+-----+--+-----+----->
  '-FREquency----días-'  '-VERExists----+número--+-'
                          '-NOLimit-'
>--+-----+--+-----+----->
  '-VERDeleted----+número--+-'
                          '-NOLimit-'
>--+-----+--+-----+----->
  '-RETEExtra----+días--+-'  '-RETOOnly----+días--+-'
                          '-NOLimit-'                          '-NOLimit-'
```

```

>-----+----->
'-MODE---+---MODified--+'
      '-ABSolute-'

>-----+----->
'-SERialization---+---SHRStatic---+'
      +-Static-----+
      +-SHRDynamic--+
      '-DYNAMIC---+'

>-----+-----<
'-TOCDestination---+---nombre_agrupación---+'

```

## Parámetros

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el grupo de copia.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas al que pertenece el grupo de copia. No puede actualizar un grupo de copia del juego de políticas ACTIVE.

nom\_clase (Necesario)

Especifica la clase de gestión a la que pertenece el grupo de copia.

STANDARD

Especifica el grupo de copia, que debe ser STANDARD. Este parámetro es opcional.

Type=Backup

Especifica que desea actualizar un grupo de copia de seguridad. Este parámetro es opcional.

DESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los datos de copia de seguridad. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency

Especifica la frecuencia con la que el servidor puede hacer copia de seguridad de un archivo. Este parámetro es opcional. El servidor sólo hace copia de seguridad de un archivo cuando ha transcurrido el número de días especificado desde la última copia de seguridad. El valor de FREQUENCY sólo se utiliza durante una operación de copia de seguridad incremental. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial. Puede especificar un entero de 0 a 9999. El valor 0 significa que el servidor puede hacer copia de seguridad de un archivo independientemente del momento en que se hizo la última copia de seguridad del archivo.

VERExists

Especifica el número máximo de versiones de copia de seguridad para retener los archivos que actualmente se encuentran en el sistema de archivos del cliente. Este parámetro es opcional.

Si una copia de seguridad incremental hace que se sobrepase el límite, el servidor hará que caduque la versión de copia de seguridad más antigua que existe en el almacenamiento del servidor. Los valores posibles son:

número

Especifica el número de versiones de copia de seguridad a retener para los archivos que actualmente se encuentran en el sistema de archivos del cliente. Puede especificar un entero de 1 a 9999.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad.

El número de versiones de copia de seguridad que se retienen se controla mediante este parámetro hasta que las versiones sobrepasen el tiempo de retención que especifica el parámetro RETEXTRA.

VERDeleted

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad utilizando el servidor. Este parámetro es opcional.

Si un usuario suprime un archivo del sistema de archivos del cliente, la siguiente copia de seguridad incremental hará que el servidor cambie la versión de copia de seguridad activa del archivo a inactiva y que caduque las versiones más antiguas que sobrepasen este número. La fecha de caducidad de las versiones restantes se determina mediante el tiempo de retención especificado en los parámetros RETEXTRA y RETONLY. Los valores posibles son:

número

Especifica el número máximo de versiones de copia de seguridad que se retienen de los archivos que se han suprimido del sistema de archivos del cliente una vez hecha la copia de seguridad. Puede especificar un valor de 0 a 9999.

NOLimit

Especifica que el servidor debe retener todas las versiones de copia de seguridad de los archivos que se han suprimido del sistema de archivos del cliente después de hacerse la copia de seguridad.

RETEExtra

Especifica el número de días que servidor retiene una versión de copia de seguridad una vez que esa versión se convierte en inactiva. Una versión de un archivo se convierte en inactiva cuando el cliente almacena otra copia de seguridad más reciente o cuando el cliente suprime el archivo de la estación de trabajo y luego ejecuta una copia de seguridad incremental completa. El servidor suprime las versiones inactivas basándose en el tiempo de retención aunque el número de versiones inactivas no sobrepase el número que permiten los parámetros VEREXISTS o VERDELETED. Este parámetro es opcional. Los valores posibles son:

días

Especifica el número de días que se retienen las versiones de copia de seguridad inactivas. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que las versiones de copia de seguridad inactivas se retienen de forma indefinida.

Si especifica NOLIMIT, el servidor suprime las versiones de copia de seguridad adicionales basándose en el parámetro VEREXISTS (si el archivo sigue existiendo en el sistema de archivos del cliente) o en el parámetro VERDELETED (si el archivo ya no existe en el sistema de archivos del cliente).

RETOOnly

Especifica el número de días que se retiene la última versión de copia de seguridad de un archivo que se ha suprimido del sistema de archivos del cliente. Este parámetro es opcional. Los valores posibles son:

días

Especifica el número de días que se han de retener la última copia de seguridad inactiva. Puede especificar un entero de 0 a 9999.

NOLimit

Especifica que se desea conservar la última versión inactiva restante de un archivo de forma indefinida.

Si especifica NOLIMIT, el servidor retiene la última versión de copia de seguridad restante para siempre, excepto si un usuario o un administrador suprime el archivo del almacenamiento del servidor.

MODE

Especifica si el servidor sólo hace copia de seguridad de un archivo si éste se ha modificado desde la última copia de seguridad o si la hace siempre que un cliente solicita una copia de seguridad. Este parámetro es opcional. Los valores posibles son:

MODified

Especifica que se realiza la copia de seguridad del archivo únicamente si se ha modificado desde la última copia de seguridad. Se considera que un archivo se ha modificado si se cumple algunas de las siguientes condiciones:

- La fecha de última modificación es diferente
- El tamaño del archivo es diferente
- El propietario del archivo es diferente
- Los permisos de los archivos son diferentes

ABSolute

Especifica que se realiza la copia de seguridad del archivo independientemente de si se ha modificado.

El valor de MODE sólo se utiliza en la copia de seguridad incremental completa. Se prescinde de este valor durante la copia de seguridad selectiva o la copia de seguridad incremental parcial.

SERialization

Especifica cómo debe procesar el servidor los archivos o directorios cuando éstos se modifican durante el proceso de realización de la copia de seguridad. Este parámetro es opcional. Los valores posibles son:

SHRStatic

Especifica que el servidor sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. El servidor intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo o directorio se modifica durante cada intento de copia de seguridad, el servidor no hace la copia de seguridad.

STatic

Especifica que el servidor sólo hace copia de seguridad de un archivo o directorio si no se ha modificado durante la copia de seguridad. El servidor intenta efectuar la copia de seguridad una sola vez.

Las plataformas que no admiten la opción STATIC establecen como valor predeterminado SHRSTATIC.

SHRDYnamic

Especifica que si se modifica un archivo o directorio durante un intento de copia de seguridad, el servidor hace copia de seguridad del archivo o directorio durante el último intento aunque el archivo o directorio se esté modificando. El servidor intenta realizar una copia de seguridad hasta cuatro veces, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

## DYNAMIC

Especifica que el servidor realiza la copia de seguridad de un archivo o directorio en el primer intento, independientemente de que el archivo o directorio esté modificándose durante el proceso de copia de seguridad.

Importante: Debe tener mucho cuidado al utilizar los valores SHRSDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar la copia de seguridad de un archivo o directorio mientras están produciéndose modificaciones. Como consecuencia, la versión de copia de seguridad puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se restaura un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una versión de copia de seguridad solo si el archivo o directorio no se está modificando.

## TOCDestination

Especifica la agrupación de almacenamiento primaria en la que inicialmente se almacenará una tabla de contenido (TOC) para cualquier operación de copia de seguridad NDMP u operación de juego de copias de seguridad para la que se genere una TOC. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino. La agrupación de almacenamiento que se especifique para el destino debe tener el formato de datos NATIVE o NONBLOCK. Para evitar que se produzcan retardos de montaje, se recomienda que la agrupación de almacenamiento tenga una clase de dispositivo DISK o DEVTYPE=FILE. La generación de la TOC es opcional en las operaciones de copia de seguridad NDMP, pero no está admitida en otras operaciones de copia de seguridad de imagen.

Para eliminar un destino de TOC existente del grupo de copias, especifique una serie nula ("") para este valor.

Si se solicita la creación de la TOC para una operación de copia de seguridad que utilice NDMP y la imagen está vinculada a una clase de gestión cuyo grupo de copia de seguridad no especifica un destino de TOC, el resultado de la operación dependerá del parámetro TOC de la operación de copia de seguridad.

- Si TOC=PREFERRED (el valor predeterminado), la copia de seguridad continuará sin crearse una TOC.
- Si TOC=YES, la copia de seguridad en su totalidad resultará anómala porque no puede crearse ninguna TOC.

## Ejemplo: actualizar un grupo de copias de seguridad

Actualizar el grupo de copia de seguridad STANDARD del dominio de políticas EMPLOYEE\_RECORDS, juego de políticas VACATION, clase de gestión ACTIVEFILES. El destino se cambiará a DISKPOOL, con un intervalo mínimo de siete días entre copias de seguridad, independientemente de si se han modificado los archivos. Se retendrán hasta tres versiones de copia de seguridad mientras exista un archivo en un sistema de archivos de cliente.

```
update copygroup employee_records vacation
activefiles type=backup destination=diskpool
frequency=7 verexists=3 mode=absolute
```

## UPDATE COPYGROUP (Actualizar un grupo de copias archivadas definido)

Utilice este comando para actualizar un grupo de copia archivada definido.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el grupo de copia.

## Sintaxis

```
>>-UPDate COpYgroup----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+--Type----Archive----->
  '-STANDARD-'
>--+-----+----->
  '-DESTINATION----nombre_agrupación-'
>--+-----+--+----->
  '-FREQUENCY----Cmd-' '-RETVer----dias----'
                                '-NOLimit-'
```



```

>--+-----+-----+-----+-----+----->
  '-MODE---ABSolute-' '-REtMin---días--'

>--+-----+-----+-----+-----+-----<
  '-SERialization---+SHRStatic--+-'
                        +-STatic-----+
                        +-SHRDYnamic--+
                        '-DYnamic----'

```

## Parámetros

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el grupo de copia.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas al que pertenece el grupo de copia. No puede actualizar un grupo de copia del juego de políticas ACTIVE.

nom\_clase (Necesario)

Especifica la clase de gestión a la que pertenece el grupo de copia.

STANDARD

Especifica el grupo de copias, que debe ser STANDARD. Este parámetro es opcional.

Type=Archive (Necesario)

Especifica que desea actualizar un grupo de copia archivada. Este parámetro es necesario.

DESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente la copia archivada. Este parámetro es opcional. No puede especificar una agrupación de almacenamiento de copia como destino.

FREQuency=Cmd

Especifica la frecuencia de copia, que debe ser CMD. Este parámetro es opcional.

RETVer

Especifica el número de días que se ha de mantener una copia archivada. Este parámetro es opcional. Los valores posibles son:

días

Especifica el número de días que se ha de mantener una copia archivada. Puede especificar un entero entre el 0 y el 30000.

NOLimit

Especifica que desea conservar una copia archivada de forma indefinida.

Si especifica NOLIMIT, el servidor retendrá las copias archivadas sin límite de tiempo, a menos que un usuario o un administrador suprima el archivo del almacenamiento del servidor.

El valor del parámetro RETVER puede afectar a la clase de gestión a la que el servidor vincula un directorio de copia archivada. Si el cliente no utiliza la opción ARCHMC, el servidor vincula los directorios de copia archivada con la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor vincula los directorios de copia archivada con la clase de gestión que presente el período de retención más reducido.

MODE=ABSolute

Especifica que siempre se archiva un archivo cuando el cliente lo solicita. El valor de MODE debe ser ABSOLUTE. Este parámetro es opcional.

REtMin

Especifica el número mínimo de días que se ha de mantener una copia archivada después de haberla archivado. Este parámetro es opcional. El valor predeterminado es 365.

SERialization

Especifica cómo debe procesar el servidor los archivos que se modifican durante la operación de archivado. Este parámetro es opcional. Los valores posibles son:

SHRStatic

Especifica que el servidor no guarda una copia archivada de un archivo que se está modificando. El servidor intenta efectuar una operación de archivado cuatro veces como máximo, en función del valor especificado en la opción del cliente CHANGINGRETRIES. Si el archivo se modifica durante el intento de archivado, el servidor no archivará el archivo.

STatic

Especifica que el servidor no guarda una copia archivada de un archivo que se está modificando. Si un archivo se modifica durante el intento de archivado, el servidor no archivará el archivo.

Las plataformas que no admiten la opción STATIC establecen como valor predeterminado SHRSTATIC.

SHRDYnamic

Especifica que si se modifica el archivo durante un intento de archivar, el servidor archivará el archivo en el último intento aunque se esté modificando. El servidor intenta la operación de archivado cuatro veces como máximo, en función del valor especificado en la opción del cliente CHANGINGRETRIES.

#### Dynamic

Especifica que el servidor realiza la copia archivada de un archivo en el primer intento, independientemente de si el archivo está modificándose durante el proceso de archivado.

Importante: Debe tener mucho cuidado al utilizar los valores SHRDYNAMIC y DYNAMIC. IBM Spectrum Protect utiliza estos valores para determinar si debe realizar una operación de archivado de un archivo mientras están produciéndose modificaciones. Como consecuencia, la copia archivada puede ser una copia de seguridad difusa. Una copia de seguridad difusa no refleja con exactitud lo que hay actualmente en el archivo o directorio, ya que contiene algunas de las modificaciones pero no todas. Si se recupera un archivo que contiene una copia de seguridad difusa, es posible que el archivo no sea utilizable, dependiendo de la aplicación que utiliza el archivo. Si una copia de seguridad difusa no es aceptable, defina de SERIALIZATION a SHRSTATIC o STATIC de manera que permita a IBM Spectrum Protect crear una copia de archivado solo si el archivo no se está modificando. Consejo: Proceda con precaución al seleccionar valores de retención para agrupaciones de almacenamiento primarias con el tipo CLAMATIONTYPE=SNAPLOCK. Los volúmenes con este tipo de agrupación de almacenamiento no se pueden suprimir hasta que no han sobrepasado sus fechas de retención.

## Ejemplo: actualizar varios elementos de un grupo de copias

Actualizar el grupo de copia archivada STANDARD del dominio de políticas EMPLOYEE\_RECORDS, juego de políticas VACATION, clase de gestión ACTIVEFILES. Se cambiará el destino a TAPEPOOL. Las copias archivadas se conservarán 190 días.

```
update copygroup employee_records vacation
activefiles standard type=archive
destination=tapepool retver=190
```

## UPDATE DATAMOVER (Actualizar un transportador de datos)

Utilice este comando para actualizar la definición de un transportador de datos o para poner fuera de línea un transportador de datos cuando se somete a mantenimiento el hardware.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate DATAMover--nombre_transportador_datos----->
>--+-----+--+-----+----->
  '-HLAddress---==dirección-' '-LLAddress---==puerto_tcp-'
>--+-----+--+-----+----->
  '-USERid----ID_usuario-' '-PASsword---==contraseña-'
>--+-----+--+-----+-----<
  '-ONLine---==+-Yes-+-'
  '-No--'
```

### Parámetros

nombre\_transportador\_datos (Obligatorio)

Especifica el nombre del transportador de datos.

HLAddress

Especifica la nueva dirección IP numérica o el nuevo nombre de dominio, que se utiliza para acceder al servidor de archivos NAS. Este parámetro es opcional.

LLAddress

Especifica el nuevo número de puerto TCP para acceder al servidor de archivos NAS para sesiones con el protocolo NDMP (Network Data Management Protocol). Este parámetro es opcional.

USERid

Especifica el ID de un usuario autorizado para iniciar una sesión con el servidor de archivos NAS. Por ejemplo, especifique el ID de administración de un servidor de archivos NetApp. Este parámetro es opcional.

PASsword

Especifica la nueva contraseña del ID de usuario para iniciar una sesión en el servidor de archivos NAS. Este parámetro es opcional.

ONLine

Especifica si el transportador de datos está disponible para utilizarlo. Este parámetro es opcional.

Yes

Especifica que el transportador de datos está disponible para utilizarlo.

No

Especifica que el transportador de datos no está disponible para utilizarlo.

Atención: Si se controla una biblioteca mediante una ruta desde un transportador de datos a la biblioteca y el transportador de datos está desactivado, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras el transportador de datos está desactivado, no se inicializará la biblioteca.

## Ejemplo: actualizar la dirección IP de un transportador de datos

Actualizar el transportador de datos para el nodo denominado NAS1. Cambiar la dirección IP numérica 9.67.97.103 por 9.67.97.109.

```
update datamover nas1 hladdress=9.67.97.109
```

## Ejemplo: actualizar el nombre de dominio de un transportador de datos

Actualizar el transportador de datos para el nodo denominado NAS1. Cambiar la dirección IP numérica 9.67.97.109 por el nombre de dominio NETAPP2.TUCSON.IBM.COM.

```
update datamover nas1 hladdress=netapp2.tucson.ibm.com
```

## Comandos relacionados



Tabla 1. Comandos relacionados con UPDATE DATAMOVER

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DATAMOVER	Suprimir un transportador de datos.
QUERY DATAMOVER	Visualiza definiciones de transportador de datos.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## UPDATE DEVCLASS (Actualizar los atributos de una clase de dispositivo)

Utilice este comando para actualizar una clase de dispositivo definida.

Nota: La clase de dispositivo DISK viene predefinida por IBM Spectrum Protect y no puede modificarse con el comando UPDATE DEVCLASS.

 Sistemas operativos AIX  Sistemas operativos Linux Si está actualizando una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS).

La sintaxis y las descripciones de los parámetros se proporcionan según el tipo de dispositivo. La información de sintaxis y parámetros se presenta en el orden siguiente.

- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 4MM)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 8MM)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo CENTERA)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo DLT)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE)





-  Sistemas operativos AIX  Sistemas operativos Windows UPDATE DEVCLASS (Actualizar una clase de dispositivo GENERICTAPE)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo LTO)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo NAS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo REMOVABLEFILE)
- UPDATE DEVCLASS Actualizar una clase de dispositivo SERVER)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo VOLSAFE)

Tabla 1. Comandos relacionados con UPDATE DEVCLASS

Comando	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DIRSPACE	Muestra información sobre los directorios FILE.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590)

Utilice la clase de dispositivo 3590 cuando utilice dispositivos de cinta 3590.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS).

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-+-----+-----+-----+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-+-----+-----+-----+-----+-----+----->
  '-FORMAT----+DRIVE---+' '-ESTCAPacity---tamaño-'
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'
>--+-+-----+-----+-----+-----+-----+----->
  '-PREFIX----+ADSM-----+-'
      '-prefijo_volumen_cinta-'
>--+-+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
>--+-+-----+-----+-----+-----+-----+----->
  '-MOUNTLimit----+DRIVES-+'
      +-numero+
      '-0-----'
```

### Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir.

**LIBRARY**

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

**FORMAT**

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En las tablas siguientes se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3590:

**Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para 3590**

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3590B	10 GB	Formato sin comprimir (básico)
3590C	Consulte la nota 20 GB	Formato comprimido
3590E-B	10 GB	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Consulte la nota 20 GB	Formato comprimido, similar al formato 3590C
3590H-B	30 GB (cartucho J, longitud estándar) 60 GB (cartucho K, longitud ampliada)	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Consulte la nota 60 GB (cartucho J, longitud estándar) 120 GB (cartucho K, longitud ampliada)	Formato comprimido, similar al formato 3590C

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

**Tabla 2. Selecciones de formato de grabación de dispositivos 3590**

Dispositivo	Formato					
	3590B	3590C	3590E-B	3590E-C	3590H-B	3590H-C
3590	–	–	–	–	–	–
Ultra-SCSI	Lectura/ Grabación	Lectura/ Grabación	–	–	–	–
3590E	Lectura/ Grabación	Lectura/ Grabación	Lectura/ Grabación	Lectura/ Grabación	–	–
3590H	Lectura Lectura	Lectura Lectura	Lectura	Lectura	Lectura/ Grabación	Lectura/ Grabación

**ESTCAPacity**

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.



número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592)

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS).

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-LBProtect----+READWrite+-'
                    +-WRITEOnly-+
                    '-No-----'
>--+-----+-----+----->
  '-SCALECapacity----+100--+'  '-FORMAT----+DRIVE---+'
                    +-90--+      +-3592----+
                    '-20--'      +-3592C---+
                                +-3592-2--+
                                +-3592-2C-+
                                +-3592-3--+
                                +-3592-3C-+
                                +-3592-4--+
                                '-3592-4C-'
>--+-----+----->
  '-ESTCapacity----tamaño-'
>--+-----+----->
  '-PREFIX----+ADSM-----+'
                    '-prefijo_volumen_cinta-'
>--+-----+-----+----->
  '-MOUNTRetention----minutos-'  '-MOUNTWait----minutos-'
>--+-----+----->
  '-MOUNTLimit----+DRIVES+-'
                    +-numero-+
                    '-0-----'
>--+-----+-----><
  | (1) (2) |
  |-----DRIVEEncryption----+ON-----|
                                +-ALLOW----+
                                +-EXTERNAL-+
                                '-OFF-----'
```

Notas:

1. No puede especificar WORM=Yes y DRIVEENCRYPTION=ON a la vez.
2. Se admite el cifrado de unidad solo para la segunda generación de unidades 3592 o posteriores.

## Parámetros

---

### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

### LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

### LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

#### READWRITE

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

#### WRITEONLY

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

#### No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades IBM® 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.

Consulte la nota técnica 1634851, Información adicional sobre la opción LBProtect de Tivoli Storage Manager, para ver una explicación sobre cuándo utilizar el parámetro LBProtect.

### SCALECAPacity

Especifica el porcentaje de la capacidad del medio que puede utilizarse para almacenar datos. Este parámetro es opcional. Los valores posibles son 20, 90 y 100.

Si se establece en 100 el porcentaje de la capacidad de escala, se proporciona la capacidad máxima de almacenamiento. Si se establece en 20 se obtiene el tiempo de acceso más rápido.

Nota: El valor de la capacidad de escala entra en vigor cuando se graban datos por primera vez en un volumen. Cualquier actualización de la clase de dispositivo de capacidad de escala no afecta a los volúmenes que ya tienen datos grabados hasta que el volumen se vuelve a poner en estado reutilizable.

### FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.



Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación, capacidades estimadas y opciones de formato de grabación de los dispositivos 3592:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para 3592

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
3592	300 GB	Formato sin comprimir (básico)
3592C	Consulte la nota 900 GB	Formato comprimido
3592-2	500 GB 700 GB	Cintas JA con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico)
3592-2C	1,5 TB 2,1 TB	Cintas JA con formato comprimido Cintas JB con formato comprimido
3592-3	640 GB 1 TB	Cintas JA con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico)
3592-3C	1,9 TB 3 TB	Cintas JA con formato comprimido Cintas JB con formato comprimido
3592-4	400 GB 1,5 TB 3,1 TB	Cintas JB con formato sin comprimir (básico) Cintas JB con formato sin comprimir (básico) Cintas JC con formato sin comprimir (básico)
3592-4C	1,2 TB 4,4 TB 9,4 TB	Cintas JK con formato comprimido Cintas JB con formato comprimido Cintas JC con formato comprimido

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

Importante: Para un rendimiento óptimo, evite combinar distintas generaciones de unidades en una única biblioteca SCSI.

También se necesitan configuraciones especiales para combinar distintas generaciones de unidades 3592 en bibliotecas 349x y ACSLS.

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional.

La actualización de este parámetro solamente afecta a los volúmenes vacíos. Si un volumen de llenado se ha cifrado anteriormente o no está cifrado, y actualiza el parámetro DRIVEENCRYPTION, el volumen mantiene su estado cifrado o no cifrado original. El volumen de llenado también mantiene su estado de gestión de claves original.

ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifrarán otros tipos de volúmenes, por ejemplo, juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos). Si especifica ON y activa el método de cifrado del sistema o de la biblioteca, no se permitirá el cifrado de unidades y las operaciones de copia de seguridad fallarán.

ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa el método de cifrado del sistema o de la biblioteca.

EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad.

Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado.

En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado del sistema o de la biblioteca, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo 4MM)

---

Utilice la clase de dispositivo 4MM cuando utilice dispositivos de cinta de 4 mm.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-FORMAT----+--DRIVE--'  '-ESTCAPacity----tamaño-'
      +-DDS1--+
      +-DDS1C+
      +-DDS2--+
      +-DDS2C+
      +-DDS3--+
      +-DDS3C+
      +-DDS4--+
      +-DDS4C+
      +-DDS5--+
      +-DDS5C+
      +-DDS6--+
      '-DDS6C-'
>--+-----+----->
  '-PREFIX----+--ADSM-----+'
      '-prefijo_volumen_cinta-'
>--+-----+----->
  '-MOUNTWait----minutos-'  '-MOUNTRetention----minutos-'
>--+-----+-----<
  '-MOUNTLimit----+--DRIVES--'
      +-numero+
      '-0-----'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 4 mm que ha utilizado esta clase de dispositivo. Este parámetro es opcional. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 4 mm:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para las cintas de 4 mm

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DDS1	1,3 GB (60 metros) 2,0 GB (90 metros)	Formato sin comprimir, sólo aplicable a cintas de 60 y 90 metros
DDS1C	Consulte la nota 1,3 GB (60 metros) 2,0 GB (90 metros)	Formato comprimido, sólo aplicable a cintas de 60 y 90 metros
DDS2	4 GB	Formato sin comprimir, sólo se aplica a cintas de 120 metros
DDS2C	Consulte la nota 8 GB	Formato comprimido, sólo se aplica a cintas de 120 metros
DDS3	12 GB	Formato sin comprimir, sólo se aplica a cintas de 125 metros
DDS3C	Consulte la nota 24 GB	Formato comprimido, sólo se aplica a cintas de 125 metros
DDS4	20 GB	Formato sin comprimir, sólo se aplica a cintas de 150 metros
DDS4C	Consulte la nota 40 GB	Formato comprimido, sólo se aplica a cintas de 150 metros
DDS5	36 GB	Formato sin comprimir cuando se utilizan medios DAT 72
DDS5C	Consulte la nota 72 GB	Formato comprimido cuando se utilizan medios DAT 72
DDS6	80 GB	Formato sin comprimir, cuando se utilizan medios DAT 160
DDS6C	Consulte la nota 160 GB	Formato comprimido, cuando se utilizan medios DAT 160

Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.

ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 4 mm, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del nombre de archivo en el que el servidor graba las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo 8MM)

---

Utilice la clase de dispositivo 8MM cuando utilice dispositivos de cinta de 8 mm.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY---nombre_biblioteca-'
>--+-----+----->
  '-FORMAT---+DRIVE--'  '-ESTCAPacity---tamaño-'
      +-8200--+
      +-8200C--+
      +-8500--+
      +-8500C--+
      +-8900--+
      +-AIT---+
      +-AITC--+
      +-M2----+
      +-M2C---+
      +-SAIT--+
      +-SAITC--+
      +-VXA2--+
      +-VXA2C--+
      +-VXA3--+
      '-VXA3C-'
>--+-----+----->
  '-PREFIX---+ADSM-----+'
      '-prefijo_volumen_cinta-'
>--+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>--+-----+-----<
  '-MOUNTLimit---+DRIVES--'
      +-número+
      '-0-----'
```

### Parámetros

---

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta de 8 mm que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente se muestra una lista de los formatos de grabación y de las capacidades estimadas para los dispositivos de 8 mm:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para cintas de 8 mm

<b>Formato</b>	<b>Capacidad estimada</b>	<b>Descripción</b>
<b>Tipo de medio</b>		
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
8200	2,3 GB	Formato sin comprimir (estándar) con cartuchos de cintas de 112 metros
8200C	Consulte la nota 3,5 GB 4,6 GB	Formato comprimido con cartuchos de cintas de 112 metros estándar
8500	Consulte la nota	Unidades (Lectura Grabación)
15 m	600 MB	Eliant 820 (RW)
15 m	600 MB	Exabyte 8500/8500C (RW)
15 m	600 MB	Exabyte 8505 (RW)
54 m	2,35 GB	Eliant 820 (RW)
54 m	2,35 GB	Exabyte 8500/8500C (RW)
54 m	2,35 GB	Exabyte 8505 (RW)
112 m	5 GB o 10 GB	Eliant 820 (RW)
112 m	5 GB o 10 GB	Exabyte 8500/8500C (RW)
112 m	5 GB o 10 GB	Exabyte 8505 (RW)
160 m XL	7 GB	Eliant 820 (RW)
8500C	Consulte la nota	Unidades (Lectura Grabación)
15 m	1,2 GB	Eliant 820 (RW)
15 m	1,2 GB	Exabyte 8500/8500C (RW)
15 m	1,2 GB	Exabyte 8505 (RW)
54 m	4,7 GB	Eliant 820 (RW)
54 m	4,7 GB	Exabyte 8500/8500C (RW)
54 m	4,7 GB	Exabyte 8505 (RW)
112 m	5 GB o 10 GB	Eliant 820 (RW)
112 m	5 GB o 10 GB	Exabyte 8500/8500C (RW)
112 m	5 GB o 10 GB	Exabyte 8505 (RW)
160 m XL	7 GB	Eliant 820 (RW)
8900	Consulte la nota	Unidad (Lectura Grabación)
15 m	–	Mammoth 8900 (R)
54 m	–	Mammoth 8900 (R)
112 m	–	Mammoth 8900 (R)
160 m XL	–	Mammoth 8900 (R)
22 m	2,5 GB	Mammoth 8900 (RW)
125 m	–	Mammoth 8900 (RW con actualización)
170 m	40 GB	Mammoth 8900 (RW)

<b>Formato</b>		<b>Descripción</b>
<b>Tipo de medio</b>	<b>Capacidad estimada</b>	
AIT	Consulte la nota	Unidad
SDX1-25C	25 GB	Unidades
SDX1-35C	35 GB	AIT, AIT2 y AIT3
SDX2-36C	36 GB	Unidades
SDX2-50C	50 GB	AIT, AIT2 y AIT3
SDX3-100C	100 GB	Unidades AIT2 y AIT3
SDX3X-150C	150 GB	Unidades AIT2 y AIT3
SDX4-200C	200 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	400 GB	Unidades AIT3-Ex, AIT4 y AIT5 Unidades AIT4 y AIT5 Unidad AIT5
AITC	Consulte la nota	Unidad
SDX1-25C	50 GB	Unidades
SDX1-35C	91 GB	AIT, AIT2 y AIT3
SDX2-36C	72 GB	Unidades
SDX2-50C	130 GB	AIT, AIT2 y AIT3
SDX3-100C	260 GB	Unidades AIT2 y AIT3
SDX3X-150C	390 GB	Unidades AIT2 y AIT3
SDX4-200C	520 GB	Unidades AIT3, AIT4 y AIT5
SDX5-400C	1040 GB	Unidades AIT3-Ex, AIT4 y AIT5 Unidades AIT4 y AIT5 Unidad AIT5
M2	Consulte la nota	Unidad (Lectura Grabación)
75 m	20 GB	Mammoth II (RW)
150 m	40 GB	Mammoth II (RW)
225 m	60 GB	Mammoth II (RW)
M2C	Consulte la nota	Unidad (Lectura Grabación)
75 m	50 GB	Mammoth II (RW)
150 m	100 GB	Mammoth II (RW)
225 m	150 GB	Mammoth II (RW)
SAIT	Consulte la nota	Unidad (Lectura Grabación)
	500 GB	Sony SAIT1-500(RW)
SAITC	Consulte la nota	Unidad (Lectura Grabación)
	1300 GB (1,3 TB)	Sony SAIT1-500(RW)
VXA2	Consulte la nota	Unidad (Lectura Grabación)
V6 (62 m)	20 GB	VXA-2
V10 (124 m)	40 GB	
V17 (170 m)	60 GB	
VXA2C	Consulte la nota	Unidad (Lectura Grabación)
V6 (62 m)	40 GB	VXA-2
V10 (124 m)	80 GB	
V17 (170 m)	120 GB	
VXA3	Consulte la nota	Unidad (Lectura Grabación)
X6 (62 m)	40 GB	VXA-3
X10 (124 m)	86 GB	
X23 (230 m)	160 GB	



Formato		Descripción
Tipo de medio	Capacidad estimada	
VXA3C  X6 (62 m) X10 (124 m) X23 (230 m)	Consulte la nota  80 GB 172 GB 320 GB	Unidad (Lectura Grabación)  VXA-3
<p>Nota: Las capacidades reales pueden variar en función de los cartuchos y las unidades que se utilicen.</p> <ul style="list-style-type: none"> <li>• Para los formatos AITC y SAITC, la proporción de compresión normal es de 2.6:1.</li> <li>• Para el formato M2C, la proporción de compresión normal es de 2,5:1.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de 8 mm, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## Ejemplo: actualizar el límite de montaje y la capacidad de una clase de dispositivo de 8 mm

---

Actualizar una clase de dispositivo denominada 8MMTAPE. Cambiar el límite de montaje por 3 y la capacidad estimada por 10 GB.

```
update devclass 8mmtape mountlimit=3 estcapacity=10G
```

## Ejemplo: actualizar el período de retención de montaje de una clase de dispositivo de 8 mm

---

Actualizar una clase de dispositivo de 8 mm que se denomina 8MMTAPE en una retención de montaje de 15 minutos.

```
update devclass 8mmtape mountretention=15
```

## UPDATE DEVCLASS (Actualizar una clase de dispositivo CENTERA)

---

Utilice la clase de dispositivo CENTERA cuando utilice dispositivos de almacenamiento EMC Centera. El tipo de dispositivo CENTERA utiliza los archivos como volúmenes para almacenar los datos de forma secuencial. Es similar a la clase de dispositivo FILE.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
                                     (1)
>--HLAddress-----dirección_ip?archivo_PEA----->
>>+-----+----->
```

```
'-MINCAPacity-----tamaño---'  
>+-----+-----<<  
'-MOUNTLimit-----número---'
```

#### Notas:

1. Para cada clase de dispositivo Centera, debe especificar una dirección IP. Sin embargo, la ruta y el nombre del archivo PEA (autorización de entrada de agrupación) son opcionales, y la especificación del archivo PEA debe indicarse después de la dirección IP. Utilice el carácter "?" para separar la ruta y el nombre de archivo PEA de la dirección IP.

## Parámetros

---


### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.


### HLAddress

Especifica una dirección IP para el dispositivo de almacenamiento Centera y, opcionalmente, el nombre y la ruta de un archivo PEA (autorización de entrada de agrupación). Especifique las direcciones IP en formato decimal con punto (por ejemplo, 9.10.111.222). Un dispositivo Centera puede tener varias direcciones IP. Sin embargo, solo es necesario especificar una como valor para este parámetro.

 Sistemas operativos AIX La ruta y el nombre del archivo PEA son sensibles a las mayúsculas y minúsculas.

Si agrega el nombre y la ruta de un archivo PEA, asegúrese de que el archivo se almacena en un directorio del sistema que ejecuta el servidor de IBM Spectrum Protect. Separe el nombre y la ruta del archivo PEA de la dirección o direcciones IP con "?" como por ejemplo:  Sistemas operativos Windows

```
HLADDRESS=9.10.111.222?c:\controlFiles\TSM.PEA
```

 Sistemas operativos AIX

```
HLADDRESS=9.10.111.222?/user/ControlFiles/TSM.PEA
```

Especifique sólo una ruta y nombre de archivo PEA para cada definición de clase de dispositivo. Si especifica dos clases de dispositivo Centera distintas que hagan referencia al mismo dispositivo de almacenamiento Centera y si las definiciones de clase de dispositivo contienen distintas rutas y nombres de archivo PEA, el servidor utiliza el archivo PEA especificado en el parámetro HLADDRESS de la clase de dispositivo que se haya utilizado en primer lugar para abrir el dispositivo de almacenamiento Centera.

#### Nota:

1. El servidor no incluye un archivo PEA durante la instalación. Si no crea ningún archivo PEA, el servidor utilizará el perfil predeterminado de Centera, que permite a las aplicaciones leer, escribir, suprimir, depurar y consultar datos de un dispositivo de almacenamiento Centera. Para conseguir un control más estricto, cree un archivo PEA utilizando la interfaz de línea de mandatos proporcionada por EMC Centera. Para obtener detalles sobre la autenticación y autorización de Centera, consulte la publicación *Programmer's Guide* de EMC Centera.
2. También puede especificar la ruta y el nombre del archivo PEA en una variable de entorno utilizando la sintaxis `CENTERA_PEA_LOCATION=rutaarchivo_nombrearchivo`. La ruta y el nombre del archivo PEA especificados en esta variable de entorno se aplicarán a todos los clústeres de Centera. Si utiliza esta variable, no es necesario que especifique la ruta y el nombre del archivo PEA utilizando el parámetro HLADDRESS.
3. Al actualizar la clase de dispositivo con un nombre y ubicación del archivo PEA nuevos o cambiados, es posible que se requiera reiniciar el servidor si ya se ha accedido al dispositivo Centera identificado por la dirección IP en la instancia actual del servidor.

### MINCAPacity

Especifica el nuevo tamaño mínimo para los volúmenes Centera que se asignan a una agrupación de almacenamiento de esta clase de dispositivo. Este valor representa la cantidad mínima de datos que se almacenan en un volumen Centera antes de que el servidor lo marque como lleno. Los volúmenes Centera seguirán aceptando datos hasta que se haya almacenado la cantidad mínima de datos. Este parámetro es opcional.

### tamaño

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor mínimo permitido es 1 MB (MINCAPACITY=1M). El valor máximo permitido es 128 GB (MINCAPacity=128G).

### MOUNTLimit

Especifica el número máximo nuevo de sesiones que acceden al dispositivo Centera. Este parámetro es opcional. Puede especificar un número a partir de 0 o mayor; no obstante, la suma de todos los valores de límite de montaje para todas las clases de dispositivo asignadas al mismo dispositivo Centera no debe superar el número máximo de sesiones que permite Centera.

# UPDATE DEVCLASS (Actualizar una clase de dispositivo DLT)

Utilice la clase de dispositivo DLT cuando utilice dispositivos de cinta DLT.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>+-----+----->
  '-LIBRARY---nombre_biblioteca-'
>+-----+----->
  '-FORMAT-----+DRIVE---+'  '-ESTCAPacity---tamaño-'
      +-DLT1-----+
      +-DLT1C----+
      +-DLT10----+
      +-DLT10C---+
      +-DLT15----+
      +-DLT15C---+
      +-DLT20----+
      +-DLT20C---+
      +-DLT35----+
      +-DLT35C---+
      +-DLT40----+
      +-DLT40C---+
      +-DLT2-----+
      +-DLT2C----+
      +-DLT4-----+
      +-DLT4C----+
      +-SDLT-----+
      +-SDLTC----+
      +-SDLT320--+
      +-SDLT320C-+
      +-SDLT600--+
      +-SDLT600C-+
      +-DLTS4----+
      '-DLTS4C---'
>+-----+----->
  '-PREFIX-----+ADSM-----+'
      '-prefijo_volumen_cinta-'
>+-----+----->
  '-MOUNTRetention---minutos-'  '-MOUNTWait---minutos-'
>+-----+-----<
  '-MOUNTLimit---+DRIVES--+'
      +-número+
      '-0-----'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas DLT que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos DLT:

Tabla 1. Formato de grabación y capacidad estimada predeterminada para DLT

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
DLT1	40 GB	Formato sin comprimir sólo con cartuchos CompacTape III o CompacTape IV
DLT1C	Consulte la nota 1. 80 GB	Formato comprimido sólo con cartuchos CompacTape III y CompacTape IV
DLT10	10 GB	Formato sin comprimir sólo con cartuchos CompacTape III o CompacTape IV
DLT10C	Consulte la nota 1. 20 GB	Formato comprimido sólo con cartuchos CompacTape III y CompacTape IV
DLT15	15 GB	Formato sin comprimir sólo con cartuchos CompacTape IIIxt o CompacTape IV (no CompacTape III) Nota: Válido con unidades DLT2000XT, DLT4000 y DLT7000
DLT15C	Consulte la nota 1. 30 GB	Formato comprimido sólo con cartuchos CompacTape IIIxt o CompacTape IV (no CompacTape III) Válido con unidades DLT2000XT, DLT4000 y DLT7000
DLT20	20 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT20C	Consulte la nota 1. 40 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT4000, DLT7000 y DLT8000
DLT35	35 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT35C	Consulte la nota 1. 70 GB	Formato comprimido sólo con cartuchos CompacTape IV Válido con unidades DLT7000 y DLT8000
DLT40	40 GB	Formato sin comprimir sólo con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT40C	Consulte la nota 1. 80 GB	Formato comprimido con cartuchos CompacTape IV Válido con una unidad DLT8000
DLT2	80 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLTtape VS1
DLT2C	Consulte la nota 1. 160 GB	Formato comprimido, cuando se utilizan medios Quantum DLTtape VS1
DLT4	160 GB	Formato sin comprimir, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
DLT4C	Consulte la nota 1. 320 GB	Formato comprimido, utilizando cartuchos Quantum DLTtape VS1. Válido con una unidad Quantum DLT-V4
SDLT	100 GB	Formato sin comprimir con cartuchos Super DLT Tape 1
Consulte la nota 2.		Válido con una unidad Super DLT

Formato	Capacidad estimada	Descripción
SDLTC	Consulte la nota 1.	Formato comprimido con cartuchos Super DLT Tape 1
Consulte la nota 2.	200 GB	Válido con una unidad Super DLT
SDLT320	160 GB	Formato sin comprimir, cuando se utilizan medios Quantum SDLT I
Consulte la nota 2.		Válido con una unidad Super DLT
SDLT320C	Consulte la nota 1.	Formato comprimido, cuando se utilizan medios Quantum SDLT I
Consulte la nota 2.	320 GB	Válido con una unidad Super DLT
SDLT600	300 GB	Formato sin comprimir, cuando se utilizan medios SuperDLTtape-II
		Válido con una unidad Super DLT
SDLT600C	Consulte la nota 1.	Formato comprimido, cuando se utilizan medios SuperDLTtape-II
	600 GB	Válido con una unidad Super DLT
DLTS4	800 GB	Formato sin comprimir, cuando se utilizan medios Quantum DLT S4.
		Válido con una unidad DLT-S4
DLTS4C	Consulte la nota 1.	Formato comprimido, cuando se utilizan medios Quantum DLT S4.
	1,6 TB	Válido con una unidad DLT-S4
<p>Nota:</p> <ol style="list-style-type: none"> <li>1. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>2. IBM Spectrum Protect no admite una biblioteca que contenga unidades SDLT BRC (Backward Read Compatible) y SDLT NBRC (Non-Backward Read Compatible).</li> </ol>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información sobre capacidades estimadas, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.



#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE)

---

Utilice la clase de dispositivo ECARTRIDGE cuando está utilizando unidades StorageTek tales como StorageTek T10000 o T9840.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS).

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
```

```

>----->
'-LBProtect---+--READWrite+-'
      +-WRITEOnly-+
      '-No-----'

>----->
'-FORMAT-----+--DRIVE-----+-' '-ESTCAPacity-----tamaño-'
      +-T9840C-----+
      +-T9840C-C--+
      +-T9840D-----+
      +-T9840D-C--+
      +-T10000A-----+
      +-T10000A-C-+
      +-T10000B-----+
      +-T10000B-C-+
      +-T10000C-----+
      +-T10000C-C-+
      +-T10000D-----+
      '-T10000D-C-'

>----->
'-PREFIX---+--ADSM-----+-'
      '-prefijo_volumen_cinta-'

>----->
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

>----->
'-MOUNTLimit---+--DRIVES+-'
      +-número-+
      '-0-----'

>-----<
| (1) (2) |
'------DRIVEEncryption---+--ON-----+'
      +-ALLOW-----+
      +-EXTERNAL-+
      '-OFF-----'

```

#### Notas:

1. Puede utilizar el cifrado de unidad solo en unidades Oracle StorageTek T10000B con un valor de formato de DRIVE, T10000B o T10000B-C, para unidades Oracle StorageTek T10000C con un valor de formato de DRIVE, T10000C o T10000C-C y para unidades Oracle StorageTek T10000D con un valor de formato de DRIVE, T10000D y T10000D-C.
2. No puede especificar WORM=YES y DRIVEENCRYPTION=ON a la vez.

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido con las unidades de cintas ECARTRIDGE que puede utilizar esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

READWrite

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección



contra daños en los datos.

#### WRITEOnly

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

#### No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: La protección de bloques lógicos sólo está soportada en unidades Oracle StorageTek T10000C y Oracle StorageTek T10000D.

#### FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

Importante: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos ECARTRIDGE:

Tabla 1. Formatos de grabación y capacidades calculadas predeterminadas para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2

Formato	Capacidad estimada	Descripción
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Notas:</p> <ul style="list-style-type: none"> <li>Algunos formatos utilizan la función de compresión por hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este

parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional.

Restricción:

1. Solo puede utilizar el cifrado de unidad en las siguientes unidades:
  - Las unidades Sun StorageTek T10000B con un valor de formato DRIVE, T10000B o T10000B-C
  - Las unidades Sun StorageTek T10000C con un valor de formato DRIVE, T10000C o T10000C-C
  - Unidades Oracle StorageTek T10000D con un valor de formato DRIVE, T10000D o T10000D-C
2. No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (No se admite especificar WORM=YES y DRIVEENCRYPTION=ON a la vez).
3. Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

#### ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

#### ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

#### EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.



#### OFF


Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.



## UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE)

---

Utilice la clase de dispositivo FILE si utiliza archivos en el almacenamiento de disco magnético como volúmenes que almacenan datos secuencialmente (como en una cinta).

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo FILE no admite bibliotecas EXTERNAL.

 Sistemas operativos AIX  Sistemas operativos Linux Si está definiendo una clase de dispositivo para los dispositivos a los que se va a acceder a través de un servidor de medios de z/OS, consulte UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS).

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>-+-----+-----+-----+-----+-----+----->
   '-MOUNTLimit---número-'   '-MAXCAPacity---tamaño-'
>-+-----+-----+-----+-----+-----+----->
   |                         .',-----'. |
   |                         v             | |
   '-DIRectory---nombre_directorio-+-'
>-+-----+-----+-----+-----+-----+----->
   '-SHARED---+-No--+-'
                   '-Yes-'
```


## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

MOUNTLimit

Especifica el número máximo de archivos que se pueden abrir simultáneamente para entrada y salida. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

 Sistemas operativos Windows Si desea compartir la clase de dispositivo con un agente de almacenamiento (mediante la especificación del parámetro SHARED=YES), se definirán o se suprimirán unidades en función del valor de MOUNTLIMIT.



Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

MAXCAPacity

Especifica el tamaño máximo de los archivos de almacenamiento de datos clasificados por esta clase de dispositivo. Este parámetro es opcional.

Especifique este valor como un entero seguido de **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). Si está definiendo una clase de dispositivo FILE para los volúmenes de copia de seguridad de base de datos, especifique un valor para MAXCAPACITY que sea adecuado para el tamaño de la base de datos y que minimice el número de volúmenes de base de datos.

Por ejemplo, MAXCAPACITY=5G especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 gigabytes. El valor especificado debe ser menor o igual que el tamaño máximo admitido de un archivo en el sistema de archivos destino.

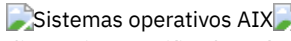
 Sistemas operativos AIX  Sistemas operativos Linux No defina un valor para MAXCAPACITY superior a 640M cuando este archivo se destine al soporte de CD REMOVABLEFILE. Un valor menor que un espacio utilizable del CD (650 MB) permite una coincidencia unívoca entre los archivos de la clase de dispositivo FILE y las copias que se encuentran en el CD.

DIRectory

Especifica las ubicaciones del directorio de los archivos utilizados en esta clase de dispositivo. Escriba comillas al principio y al final de la lista de directorios y utilice comas para separar los nombres de directorio individuales. Se permiten los caracteres

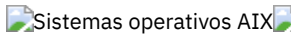
especiales (por ejemplo, espacios en blanco) en los nombres de directorio. Por ejemplo, la lista de directorios "abc def,xyz" contiene dos directorios: abc def y xyz. Este parámetro es opcional.

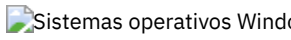
Al especificar un nombre o nombres de directorio, identifica las ubicaciones donde el servidor coloca los archivos que representan los volúmenes de almacenamiento para esta clase de dispositivo.

 Sistemas operativos AIX/Sistemas operativos Linux Al procesar el mandato, el servidor amplía el nombre o nombres de directorio especificados a forma completa, a partir del directorio raíz.

Importante: Si está utilizando agentes de almacenamiento para acceso compartido a volúmenes FILE, debe utilizar el mandato DEFINE PATH para definir una ruta para cada agente de almacenamiento. La definición de ruta incluye los nombres de directorio utilizados por el agente de almacenamiento para acceder a cada directorio.

Posteriormente, si el servidor necesita asignar un volumen reutilizable, crea un nuevo archivo en uno de estos directorios. (El servidor puede elegir cualquiera de los directorios para crear nuevos volúmenes reutilizables.) Para los volúmenes reutilizables que se utilizan para almacenar datos del cliente, el archivo que crea el servidor tiene la extensión de nombre de archivo .bfs. Para los volúmenes reutilizables que se utilizan para almacenar datos de exportación, se utiliza la extensión .exp.

 Sistemas operativos AIX/Sistemas operativos Linux Por ejemplo, si define una clase de dispositivo con un directorio de tsmstor y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine tsmstor\00566497.exp.

 Sistemas operativos Windows Por ejemplo, si define una clase de dispositivo con un directorio de c:\server y el servidor necesita un volumen reutilizable en esta clase de dispositivo para almacenar datos de exportación, puede que el archivo que crea el servidor se denomine c:\server\00566497.exp.

Consejo: Si especifica varios directorios para una clase de dispositivo, asegúrese de que los directorios están asociados con sistemas de archivos separados. Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio agregando valores que representan el espacio que queda en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar desactivado. Si un desencadenante se desactiva porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a activar el desencadenante con el siguiente mandato: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio. Restricción: Para modificar una lista de directorios debe sustituir la lista completa.

#### SHAREd

Especifica si esta clase de dispositivo FILE se compartirá entre el servidor y uno o más agentes de almacenamiento. Para prepararse para el compartimiento, se definirá de manera automática una biblioteca junto con un número de unidades correspondiente al valor de MOUNTLIMIT asociado con la clase de dispositivo. Si la biblioteca y las unidades ya existen y el valor de MOUNTLIMIT se modifica, se pueden crear unidades para alcanzar un nuevo valor de MOUNTLIMIT más elevado o suprimir para obtener un nuevo valor más bajo.

## Agentes de almacenamiento que utilizan volúmenes FILE

Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para acceder a los volúmenes FILE, los agentes de almacenamiento sustituyen los nombres de la lista de directorios en la definición de clase de dispositivo por los nombres de la lista de directorios de la definición de ruta asociada. A continuación, se muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:

 Sistemas operativos Windows

- c:\server
- d:\server
- e:\server

 Sistemas operativos AIX

- /usr/tivoli1
- /usr/tivoli2
- /usr/tivoli3

## Sistemas operativos Linux

- /opt/tivoli1
- /opt/tivoli2
- /opt/tivoli3

1. Utilice el siguiente comando para configurar una biblioteca FILE denominada CLASSA con una unidad denominada CLASSA1 en SERVER1:

### Sistemas operativos Windows

```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

### Sistemas operativos AIX

```
define devclass classa devtype=file
directory="/usr/tivoli1,/usr/tivoli2,/usr/tivoli3"
shared=yes mountlimit=1
```

### Sistemas operativos Linux


```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```

2. Quiere que el agente de almacenamiento STA1 pueda utilizar la biblioteca FILE, para poder definir la siguiente ruta para el agente de almacenamiento STA1:

- o  Sistemas operativos Windows


```
define path server1 stal srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio c:\server por el nombre de directorio \\192.168.1.10\c\server para poder acceder a los volúmenes FILE que se encuentran en el directorio c:\server del servidor.

- o  Sistemas operativos AIX

```
define path server1 stal srctype=server desttype=drive device=file
directory="/usr/ibm1,/usr/ibm2,/usr/ibm3" library=classa
```


En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio /usr/tivoli1 por el nombre de directorio /usr/ibm1 para poder acceder a los volúmenes FILE que se encuentran en el directorio /usr/tivoli1 del servidor.

- o  Sistemas operativos Linux

```
define path server1 stal srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```


En este caso, el agente de almacenamiento, STA1, sustituye el nombre de directorio /opt/tivoli1 por el nombre de directorio /opt/ibm1/ para poder acceder a los volúmenes FILE que se encuentran en el directorio /opt/tivoli1 del servidor.

Se producen los resultados siguientes:

-  Sistemas operativos Windows SERVER1 crea el volumen de archivo c:\server\file1.dsm. Si cambia más adelante el primer directorio de la clase de dispositivo con el mandato siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

SERVER1 todavía puede acceder al volumen de archivo c:\server\file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

-  Sistemas operativos AIX Si se crea el volumen de archivo /usr/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/usr/otherdir,/usr/tivoli2,
/usr/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /usr/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

-  Sistemas operativos Linux Si se crea el volumen de archivo /opt/tivoli1/file1.dsm en SERVER1 y se emite el siguiente mandato,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,  
/opt/tivoli3"
```

SERVER1 todavía puede acceder al volumen de archivo /opt/tivoli1/file1.dsm, pero el agente de almacenamiento STA1 no puede acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios PATH. Si no hay un nombre de directorio disponible en la lista de directorios asociado a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen FILE de ese directorio. Aunque todavía puede accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen FILE puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

## Ejemplo: actualizar una clase de dispositivo FILE para su compartimiento

---

Preparar una clase de dispositivo FILE (denominada PLAINFILES) para compartirla con un agente de almacenamiento de IBM Spectrum Protect.


```
update devclass plainfiles shared=yes
```

## Ejemplo: actualizar la capacidad de una clase de dispositivo FILE

---

Actualizar una clase de dispositivo FILE denominada STORFILES para establecer una capacidad máxima de 25 MB.

```
update devclass storfiles maxcap=25m
```

 Sistemas operativos AIX

## Ejemplo: añadir un directorio a una clase de dispositivo FILE

---

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, /usr/otherdir, a la lista de directorios. Los directorios /opt/tivoli2 y /opt/tivoli3 se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa  
directory="/opt/tivoli2,/opt/tivoli3,/usr/otherdir"
```

 Sistemas operativos Linux

## Ejemplo: añadir un directorio a una clase de dispositivo FILE

---

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, /usr/otherdir, a la lista de directorios. Los directorios /usr/tivoli2 y /usr/tivoli3 se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa  
directory="/usr/tivoli2,/usr/tivoli3,/usr/otherdir"
```

 Sistemas operativos Windows

## Ejemplo: añadir un directorio a una clase de dispositivo FILE

---

Actualizar la clase de dispositivo FILE, CLASSA, añadiendo un directorio, c:\otherdir, a la lista de directorios. Los directorios d:\server y e:\server se han especificado al definir por primera vez la clase de dispositivo.

```
update devclass classa  
directory="d:\server,e:\server,c:\otherdir"
```

 Sistemas operativos AIX  Sistemas operativos Windows

## UPDATE DEVCLASS (Actualizar una clase de dispositivo GENERICTAPE)

---

Utilice la clase de dispositivo GENERICTAPE para las unidades de cinta admitidas por los controladores de dispositivo del sistema operativo.

Cuando se utiliza este tipo de dispositivo, el servidor no reconoce ningún tipo de dispositivo ni el formato de grabación de cartuchos. Dado que el servidor no reconoce el tipo de dispositivo, si se produce un error de E/S, la información de error será menos detallada en comparación con la información de error que se generaría para un tipo de dispositivo específico (por ejemplo, 8MM). Cuando defina dispositivos en el servidor, no combine varios tipos de dispositivos en el mismo tipo de dispositivo.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

---

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-ESTCAPacity----tamaño-' '-MOUNTRetention----minutos-'
>--+-----+-----<
  '-MOUNTWait----minutos-' '-MOUNTLimit----+DRIVES+-'
                                     +-numero+
                                     '-0-----'
```

## Parámetros

---

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta que puede utilizar esta clase de dispositivo.

Este parámetro es opcional.

Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Especifique una capacidad adecuada a la unidad de cintas determinada que esté utilizándose.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento



óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo LTO)

Utilice la clase de dispositivo LTO cuando utilice dispositivos de cinta LTO.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-LBProtect----+READWrite+-'
                    +-WRITEOnly-+
                    '-No-----'
>--+-----+-----+----->
  '-FORMAT----+DRIVE-----+' '-ESTCAPacity----tamaño-'
                    +-ULTRIUM---+
                    +-ULTRIUMC---+
                    +-ULTRIUM2--+
                    +-ULTRIUM2C-+
                    +-ULTRIUM3--+
                    +-ULTRIUM3C-+
                    +-ULTRIUM4--+
                    +-ULTRIUM4C-+
                    +-ULTRIUM5--+
                    +-ULTRIUM5C-+
                    +-ULTRIUM6--+
                    '-ULTRIUM6C-'
>--+-----+----->
```

```

'-PREFIX-----+--ADSM-----+-'
      '-prefijo_volumen_cinta-'
>--+-----+--+-----+----->
      '-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
>--+-----+----->
      '-MOUNTLimit-----+--DRIVES--+-'
              +-numero+
              '-0-----'
>--+-----+-----><
      | (1) (2) |
      |-----DRIVEEncryption-----+--ON-----+|
              +-ALLOW-----+
              +-EXTERNAL-+
              '-OFF-----'

```

#### Notas:

1. No puede especificar DRIVEENCRYPTION=ON si las unidades van a utilizar un medio WORM (una sola grabación, varias lecturas).
2. El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

## Parámetros

#### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

#### LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas LTO que utiliza esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

#### LBProtect

Especifica si se utiliza la protección de bloque lógico para asegurar la integridad de los datos almacenados en la cinta. Cuando LBPROTECT se establece en READWRITE o en WRITEONLY, el servidor utiliza la característica de la unidad de cintas para la característica de protección de bloques lógicos y genera información de protección de CRC para cada bloque de datos que se graba en cinta. El servidor también valida la información de protección de CRC cuando los datos se vuelven a leer desde cinta.

Son posibles los siguientes valores:

#### READWRITE

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Los datos se almacenan con información de CRC en cada bloque. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect y la unidad de cintas a fin de calcular y comparar los valores de CRC. El valor READWRITE no afecta a los juegos de copias de seguridad ni a los datos generados por el BACKUP DB.

Cuando el parámetro LBPROTECT se establece en READWRITE, no es necesario especificar el parámetro CRCDATA en una definición de agrupación de almacenamiento ya que la protección de bloques lógicos proporciona una mejor protección contra daños en los datos.

#### WRITEONLY

Especifica que la protección de bloques lógicos está habilitada en el servidor y la unidad de cintas únicamente para operaciones de grabación. Los datos se almacenan con información de CRC en cada bloque. Para operaciones de lectura, el servidor y la unidad de cintas no validan CRC. Esta modalidad afecta al rendimiento, puesto que se requiere una utilización adicional del procesador para IBM Spectrum Protect a fin de generar CRC y para la unidad de cintas a fin de calcular y comparar los valores de CRC para operaciones de grabación. El valor WRITEONLY no afecta a los juegos de copias de seguridad ni a los datos generados por el mandato BACKUP DB.

#### No

Especifica que la protección de bloques lógicos no está habilitada en el servidor y la unidad de cintas para operaciones de lectura y grabación. Sin embargo, el servidor habilita la protección de bloques lógicos en operaciones de grabación para un volumen de llenado que ya contiene datos con protección de bloques lógicos.

Restricción: Se admite la protección de bloque lógico únicamente en IBM® LTO5 y unidades LTO6 soportadas.

#### FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades.

Cuando migre todas las unidades de dispositivos Ultrium a dispositivos Ultrium 2:

- Suprima todas las definiciones de unidades Ultrium existentes y las rutas asociadas a ellas.
- Defina las nuevas unidades y rutas Ultrium 2.

Si piensa en mezclar distintas generaciones de unidades y medios LTO, tenga en cuenta las siguientes restricciones.

Tabla 1. Posibilidades de lectura/grabación para diferentes generaciones de unidades LTO

Unidades	Soporte de primera generación	Soporte de segunda generación	Soporte de tercera generación	Soporte de cuarta generación	Soporte de quinta generación	Soporte de sexta generación
Primera generación	Lectura y grabación	n/d	n/d	n/d	n/d	n/d
Segunda generación	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d	n/d
Tercera generación <sup>1</sup>	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d	n/d
Cuarta generación <sup>2</sup>	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d	n/d
Quinta generación <sup>3</sup>	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación	n/d
Sexta generación <sup>4</sup>	n/d	n/d	n/d	Sólo lectura	Lectura y grabación	Lectura y grabación
<p><sup>1</sup> En una biblioteca con una unidad de tercera generación, es necesario dar de baja todos los volúmenes reutilizables de primera generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de primera generación a sólo lectura.</p> <p><sup>2</sup> En una biblioteca con una unidad de cuarta generación, es necesario dar de baja todos los volúmenes reutilizables de segunda generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de segunda generación a sólo lectura.</p> <p><sup>3</sup> En una biblioteca con una unidad de quinta generación, todos los volúmenes reutilizables de tercera generación se tienen que dar de baja y todos los volúmenes de agrupación de almacenamiento de tercera generación se tienen que actualizar a sólo lectura.</p> <p><sup>4</sup> En una biblioteca con una unidad de sexta generación, es necesario dar de baja todos los volúmenes reutilizables de cuarta generación y es necesario actualizar todos los volúmenes de agrupaciones de almacenamiento de cuarta generación a sólo lectura.</p>						

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades calculadas para los dispositivos LTO:

Tabla 2. Formato de grabación y capacidad estimada predeterminada para LTO

Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
ULTRIUM	100 GB	Formato sin comprimir, utilizando cartuchos Ultrium
ULTRIUMC	Consulte la nota 200 GB	Formato comprimido, utilizando cartuchos Ultrium
ULTRIUM2	200 GB	Formato sin comprimir (estándar) con cartuchos Ultrium 2
ULTRIUM2C	Consulte la nota 400 GB	Formato comprimido con cartuchos Ultrium 2

Formato	Capacidad estimada	Descripción
ULTRIUM3	400 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 3
ULTRIUM3C	Consulte la nota 800 GB	Formato comprimido, con cartuchos Ultrium 3
ULTRIUM4	800 GB	Formato sin comprimir (estándar), con cartuchos Ultrium 4
ULTRIUM4C	Consulte la nota 1,6 TB	Formato comprimido con cartuchos Ultrium 4
ULTRIUM5	1,5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 5
ULTRIUM5C	Consulte la nota 3.0 TB	Formato comprimido con cartuchos Ultrium 5
ULTRIUM6	2.5 TB	Formato sin comprimir (estándar) con cartuchos Ultrium 6
ULTRIUM6C	Consulte la nota 6.25 TB	Formato comprimido con cartuchos Ultrium 6
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser mayor que el valor que aparece en la lista.		

#### ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información sobre capacidades estimadas, consulte Tabla 2.

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL, si establece este parámetro en un valor inferior (por ejemplo, dos minutos), se aumenta la posibilidad de compartir dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### DRIVEEncryption

Especifica si se permite el cifrado de unidad. Este parámetro es opcional. El cifrado de unidad sólo se admite para medios y unidades Ultrium 4, Ultrium 5 y Ultrium 6.

Restricción: Si el cifrado está habilitado para una clase de dispositivo, y la clase de dispositivo está asociada a una agrupación de almacenamiento, la agrupación de almacenamiento no debe compartir una agrupación de reutilizables con las otras clases de dispositivos que no se pueden cifrar. Si una cinta está cifrada, y piensa utilizarla en una unidad que no se puede cifrar, debe volver a etiquetarla manualmente para poder utilizarla en esa unidad.

#### ON

Especifica que IBM Spectrum Protect es el gestor de claves para el cifrado de unidades y que permite el cifrado de unidades para los volúmenes de agrupación de almacenamiento vacíos sólo si está activado el método de aplicación. (No se cifran otros tipos de volúmenes. Por ejemplo, los juegos de copias de seguridad, volúmenes de exportación y volúmenes de copia de seguridad de bases de datos no se cifran). Si especifica ON y activa otro método de cifrado, no se permite el cifrado de unidad y las operaciones de copia de seguridad fallan.

Nota: No puede especificar IBM Spectrum Protect como gestor de claves para el cifrado de unidades de medios WORM (una sola grabación, varias lecturas). (Si va a utilizar un soporte WORM, no puede especificar DRIVEENCRYPTION=ON).

#### ALLOW

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Sin embargo, el cifrado de unidades para volúmenes vacíos está permitido si se activa otro método de cifrado.

#### EXTERNAL

Especifica que IBM Spectrum Protect no gestiona las claves para el cifrado de unidades. Utilice este valor con una metodología de cifrado que proporcione otro proveedor y que se utilice con el cifrado de método de aplicación (AME) habilitado en la unidad. Si se especifica EXTERNAL y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect no desactiva el cifrado. En cambio, si se especifica ALLOW y IBM Spectrum Protect detecta que el cifrado AME está activado, IBM Spectrum Protect desactiva el cifrado.

#### OFF

Especifica que el cifrado de unidad no está permitido. Si activa el método de cifrado, las copias de seguridad fallarán. Si activa el método de aplicación, IBM Spectrum Protect desactiva el cifrado y no se intenta llevar a cabo copias de seguridad.



## Ejemplo: actualizar el límite de montaje para una clase de dispositivo LTO

Actualizar una clase de dispositivo denominada LTOTAPE. Cambiar el límite de montaje a 2.

```
update devclass ltotape mountlimit=2
```

## UPDATE DEVCLASS (Actualizar una clase de dispositivo NAS)

Utilice la clase de dispositivo NAS cuando realice operaciones con el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad de servidores de archivos de almacenamiento conectado a red (NAS). La clase de dispositivo es para las unidades a las que da soporte el servidor de archivos NAS para copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

 Sistemas operativos Windows La clase de dispositivo NAS no admite las bibliotecas EXTERNAL.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRary----nombre_biblioteca-'
>--+-----+----->
  '-MOUNTRetention---0-' '-MOUNTWait---minutos-'
>--+-----+----->
  '-MOUNTLimit---+DRIVES++' '-ESTCAPacity---tamaño-'
                    +-numero+
                    '-0-----'
>--+-----+-----><
  '-PREFIX---prefijo_volumen_cinta-'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRary

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cinta SCSI utilizadas con esta clase de dispositivo. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el comando DEFINE LIBRARY.

MOUNTRetention=0

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Cero (0) es el único valor admitido para clases de dispositivo con DEVType=NAS.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: **K** (kilobytes), **M** (megabytes), **G** (gigabytes) o **T** (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

#### PREFIX

Especifica el calificador de alto nivel del archivo que el servidor graba en las etiquetas de los medios de acceso secuencial. Para todos los volúmenes de acceso secuencial asignados a esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de un nombre de conjunto de datos de volumen de cinta con el prefijo predeterminado es ADSM.BFS.

## Ejemplo: actualizar la capacidad estimada para una clase de dispositivo NAS.

---

Actualizar una clase de dispositivo denominada NASTAPE. Cambiar la capacidad estimada por 200 GB.

```
update devclass nastape library=naslib estcapacity=200G
```

## UPDATE DEVCLASS (Actualizar una clase de dispositivo REMOVABLEFILE)

---

Utilice la clase de dispositivo REMOVABLEFILE para los dispositivos de medios extraíbles que están conectados como sistemas de archivos locales y extraíbles.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

```
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+----->
  '-MAXCAPacity----tamaño-'  '-MOUNTRetention----minutos-'
>--+-----+----->
  '-MOUNTWait----minutos-'  '-MOUNTLimit----+DRIVES+-'
                               +-número+
                               '-0-----'
```

## Parámetros

nombre\_clase\_dispositivo (Necesario)



Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de medios extraíbles que puede utilizar esta clase de dispositivo. Este parámetro es opcional. Para obtener información acerca de cómo definir un objeto de biblioteca, consulte el mandato DEFINE LIBRARY.

MAXCAPacity

Especifica el tamaño máximo de los volúmenes definidos en una agrupación de almacenamiento clasificada por esta clase de dispositivo. Este parámetro es opcional.

 Sistemas operativos AIX  Sistemas operativos Windows Dado que el servidor abre únicamente un archivo por medio físico extraíble, especifique una capacidad que permita que un archivo pueda utilizar totalmente la capacidad de su medio.

Debe especificar este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes).

Por ejemplo, MAXCAPACITY=5M especifica que la capacidad máxima de un volumen de esta clase de dispositivo es de 5 MB. El valor más pequeño permitido es 1 MB (es decir, MAXCAPACITY=1M).

MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

DRIVES



Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

## UPDATE DEVCLASS Actualizar una clase de dispositivo SERVER)

Utilice la clase de dispositivo SERVER para utilizar los volúmenes de almacenamiento o los archivos archivados en otro servidor de IBM Spectrum Protect.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDdate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+-----+-----+-----+----->
  '-SERVERName--==--nombre_servidor-'
>--+-----+-----+-----+-----+-----+----->
  '-MAXCAPacity--===-tamaño-'
>--+-----+-----+-----+-----+-----+----->
  '-PREFIX--===+--ADSM-----+-----+-----+'
      '-prefijo_volumen_cinta-'
>--+-----+-----+-----+-----+-----+----->
  '-RETRYPeriod--===-minutos---'
>--+-----+-----+-----+-----+-----+----->
  '-RETRYInterval--===-seconds---'
>--+-----+-----+-----+-----+-----+----->
  '-MOUNTRetention--===-minutos-'
>--+-----+-----+-----+-----+-----+-----<
  '-MOUNTLimit--===+--número-+-'
      '-1-----'
```

### Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

SERVERName

Especifica el nombre del servidor. El parámetro SERVERNAME debe coincidir con un servidor definido.

Nota: Si cambia SERVERNAME de un servidor existente a un nombre nuevo, los datos en el volumen bajo SERVERNAME antiguo ya no es accesible con esta clase de dispositivo.

MAXCAPacity

Especifica el tamaño máximo que los objetos pueden crear en el servidor destino. Este parámetro es opcional.

Especifique este valor como un entero seguido de K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor mínimo permitido es 1 MB (MAXCAPACITY=1M).

PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es AD\$M.volume1.

#### RETRYPeriod

Especifica el período de reintento en minutos. El período de reintento es el intervalo de tiempo durante el cual el servidor debe intentar conectarse con un servidor destino, en caso de que se sospeche que existe un problema de comunicaciones. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

#### RETRYInterval

Especifica el intervalo de reintentos en segundos. El intervalo de reintentos es la frecuencia con la que se realizan los intentos dentro de un período de tiempo específico. Este parámetro es opcional. Puede especificar un número de 1 a 9999.

#### MOUNTRetention

Especifica el número de minutos que debe retenerse una conexión desocupada con el servidor de destino antes de que se cierre la conexión. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTLimit

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino. Los intentos de acceder a más sesiones de las que indica el límite de montaje harán que el emisor de la petición tenga que esperar. Este parámetro es opcional. Puede especificar un número de 1 a 4096.

Los siguientes son los valores posibles:

número

Especifica el número máximo de sesiones simultáneas entre el servidor de origen y el servidor de destino.

1

Especifica el número de sesiones simultáneas entre el servidor de origen y el servidor de destino.

## UPDATE DEVCLASS (Actualizar una clase de dispositivo VOLSAFE)

---

Utilice el tipo de dispositivo VOLSAFE para trabajar con medios y unidades de la marca StorageTek VolSafe. Esta tecnología utiliza medios que no se pueden sobregrabar. Por consiguiente, no emplee estos medios para copias de seguridad a corto plazo de archivos de cliente, la base de datos de servidor o cintas de exportación.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPdate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+-----+-----+----->
' -LIBRARY----nombre_biblioteca-'
>--+-----+-----+-----+-----+----->
' -FORMAT-----+--DRIVE-----+ ' ' -ESTCAPacity----tamaño-'
+--9840-----+
+--9840-C-----+
+--T9840C-----+
+--T9840C-C---+
```

```

+-T9840D----+
+-T9840D-C--+
+-T10000A---+
+-T10000A-C-+
+-T10000B---+
+-T10000B-C-+
+-T10000C---+
+-T10000C-C-+
+-T10000D---+
'-T10000D-C-'

>--+-----+
'-PREFIX----+ADSM-----+'
      '-prefijo_volumen_cinta-'

>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'

>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTLimit-----+DRIVES--+-'
      '+-numero-+'
      '-0-----+'

```

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre del objeto de biblioteca definido que contiene las unidades de cintas VolSafe que puede utilizar esta clase de dispositivo. Si alguna unidad de una biblioteca está activada para VOLSafe, todas las unidades de la biblioteca deben activarse para VOLSafe. Para obtener más información acerca del tipo de dispositivo VolSafe, consulte DEFINE DEVCLASS (Definir una clase de dispositivo VOLSAFE).

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Atención: Si especifica DRIVE para una clase de dispositivo que tenga dispositivos de acceso secuencial incompatibles, debe montar los volúmenes en dispositivos con capacidad de lectura o grabación en el formato que se ha establecido cuando se ha montado el volumen por primera vez. Esto puede ocasionar errores si ya está utilizándose el único dispositivo de acceso secuencial que puede acceder al volumen.

En la tabla siguiente aparece una lista de los formatos de grabación y las capacidades estimadas para los dispositivos VolSafe:

Tabla 1. Formatos de grabación y capacidades estimadas predeterminadas para cintas volsafe

Formato	Capacidad estimada	Descripción
DRIVE	–	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
9840	20 GB	Formato sin comprimir (estándar), cuando se utiliza un cartucho de 20 GB de 270 metros (885 pies) de cinta
9840-C	80 GB	Formato comprimido ampliado LZ-1 (4:1), cuando se utiliza un cartucho de 80 GB con 270 metros (885 pies) de cinta
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840

Formato	Capacidad estimada	Descripción
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos.

Debe especificar este valor como un entero seguido de uno de los indicadores de unidad siguientes: K (kilobytes), M (megabytes), G (gigabytes) o T (terabytes). El valor más pequeño que se acepta es 1 MB (ESTCAPACITY=1M).

Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G.

Para forzar el servidor de IBM Spectrum Protect a determinar la capacidad estimada de los volúmenes asignados a esta clase de dispositivo, especifique ESTCAPACITY="".

Para obtener más información acerca de la capacidad estimada predeterminada para cintas de cartuchos, consulte Tabla 1.

#### PREFIX

Especifica la parte inicial del nombre de archivo de alto nivel en el servidor de destino. Este parámetro es opcional. La longitud máxima de este prefijo es de 8 caracteres.

Si tiene un convenio de denominación para las etiquetas de medios que da soporte al sistema de gestión actual, utilice un prefijo de volumen que se ajuste a sus convenios de denominación.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

AB.CD2.E

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de archivo de archivado de alto nivel que utiliza el prefijo predeterminado es ADSM.volume1.

#### MOUNTRetention

Especifica el número de minutos que se mantiene un volumen de acceso secuencial desocupado antes de desmontarse. Este parámetro es opcional. Puede especificar un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

Sin embargo, para los tipos de biblioteca EXTERNAL (es decir, una biblioteca gestionada por un sistema de gestión de medios externo), establezca este parámetro en un valor inferior (por ejemplo, dos minutos) para mejorar el compartimiento de dispositivos entre aplicaciones.

Nota: Para entornos en los que los dispositivos se comparten entre aplicaciones de almacenamiento, el valor de MOUNTRETENTION debe sopesarse cuidadosamente. Este parámetro determina cuánto tiempo permanece un volumen desocupado en una unidad. Algunos gestores de medios no desmontan una unidad asignada para satisfacer las peticiones pendientes. Es posible que necesite ajustar este parámetro para satisfacer las peticiones de montaje y mantener el rendimiento óptimo del sistema. Normalmente, los problemas surgen con mayor frecuencia cuando el parámetro MOUNTRETENTION se ha establecido en un valor que es demasiado pequeño, por ejemplo, cero.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor espera a que un operador responda a una solicitud para montar un volumen en una unidad de una biblioteca manual o dar de alta un volumen para montarlo en una biblioteca automatizada. Este parámetro es opcional. Si la solicitud de montaje no se satisface dentro del espacio de tiempo especificado, se cancela la solicitud de montaje. Puede especificar un número de 0 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Puede especificar un número de 0 a 4096.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Los siguientes son los valores posibles:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

Nota: Para los tipos de biblioteca EXTERNAL, no especifique DRIVES como valor de MOUNTLIMIT. Debe especificar el número de unidades para la biblioteca como el valor de MOUNTLIMIT.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva. Todas las transacciones actuales continuarán hasta completarse pero las nuevas transacciones se interrumpirán.

 Sistemas operativos AIX  Sistemas operativos Linux

## UPDATE DEVCLASS - servidor de medios de z/OS (Actualizar clase de dispositivo para servidor de medios de z/OS)

Utilice este comando para actualizar una clase de dispositivo. Hay disponible un conjunto limitado de tipos de clase de dispositivo para los dispositivos a los que se accede mediante un servidor de medios de z/OS.

- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)
- UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS)

Tabla 1. Comandos relacionados con UPDATE DEVCLASS

Comando	Descripción
BACKUP DEVCONFIG	Efectúa una copia de seguridad de la información de dispositivos de IBM Spectrum Protect en un archivo.
DEFINE DEVCLASS (servidor de medios de z/OS)	Define una clase de dispositivo para utilizar el almacenamiento gestionado por un servidor de medios de z/OS.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DELETE DEVCLASS	Elimina una clase de dispositivo.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
UPDATE LIBRARY	Cambia los atributos de una biblioteca.

 Sistemas operativos AIX  Sistemas operativos Linux

# UPDATE DEVCLASS (Actualizar una clase de dispositivo 3590 para el servidor de medios de z/OS)

Utilice este comando para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a dispositivos 3590. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```

                                     (1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+----->
  '-LIBRARY----nombre_biblioteca-'
>--+-----+-----+----->
  '-FORMAT-----+DRIVE---+'  '-ESTCAPacity----tamaño-'
      +-3590B---+
      +-3590C---+
      +-3590E-B-+
      +-3590E-C-+
      +-3590H-B-+
      '-3590H-C-'
>--+-----+-----+----->
  '-COMpression----+Yes-+'
      '-No--'
>--+-----+-----+----->
  '-MOUNTRetention----minutos-'  '-MOUNTWait----minutos-'
>--+-----+-----+----->
  '-MOUNTLimit----+DRIVES-+'  '-EXPIration----yyyyddd-'
      +-número-+
      '-0-----'
>--+-----+-----+----->
  '-RETention----días-'  '-PROtection----+No-----+'
      +-Yes-----+
      '-Automatic-'
>--+-----+-----+-----<
  '-UNIT----nombre_unidad-'

```

### Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.
2. No puede actualizar el parámetro PREFIX con este comando. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

En la tabla siguiente se muestra una lista de las opciones de formato de grabación de los dispositivos 3590:

Tabla 1. Formatos de grabación para 3590

Formato	Descripción
3590B	Formato sin comprimir (básico)
3590C	Formato comprimido
3590E-B	Formato sin comprimir (básico), similar al formato 3590B
3590E-C	Formato comprimido, similar al formato 3590C
3590H-B	Formato sin comprimir (básico), similar al formato 3590B
3590H-C	Formato comprimido, similar al formato 3590C

Nota: Si el formato utiliza la función de compresión por hardware de la unidad de cintas, la capacidad real puede disminuir, dependiendo de la eficacia de la compresión.

#### ESTCAPacity

Especifica la capacidad estimada de los volúmenes de acceso secuencial clasificados por esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: **K** (KB), **M** (MB), **G** (GB) o **T** (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

#### COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

## DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

## EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

## RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto de cero para el parámetro RETENTION.

## PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

### No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

### Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

### Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.



No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

#### UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que dé soporte a la cinta 3590. Este parámetro es opcional. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

## UPDATE DEVCLASS (Actualizar una clase de dispositivo 3592 para el servidor de medios de z/OS)

Utilice este comando para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a dispositivos 3592. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
(1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+-----+----->
  '-LIBRARY---biblioteca_medio_zos-'
>--+-----+-----+----->
  '-FORMAT-----+DRIVE---+' '-ESTCAPacity---tamaño-'
      +-3592-----+
      +-3592C---+
      +-3592-2---+
      +-3592-2C-+
      +-3592-3---+
      +-3592-3C-+
      +-3592-4---+
      '-3592-4C-'
>--+-----+-----+----->
  '-COMPRESSION---+Yes-+-'
      '-No--'
>--+-----+-----+----->
  '-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
>--+-----+-----+----->
  '-MOUNTLimit---+DRIVES-+-' '-EXPIration---yyyddd-'
      +-número+
      '-0-----'
>--+-----+-----+----->
  '-RETention---días-' '-PROtection---+No-----+-'
      +-Yes-----+
      '-Automatic-'
>--+-----+-----+-----<
  '-UNIT---nombre_unidad-'
```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.
2. No puede actualizar el parámetro PREFIX con este comando. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

## Parámetros

nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional. El valor predeterminado es DRIVE.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para 3592

Formato	Descripción
3592	Formato sin comprimir (básico)
3592C	Formato comprimido
3592-2	Formato sin comprimir (básico), similar al formato 3592
3592-C	Formato comprimido, similar al formato 3592C
3592-3	Formato sin comprimir (básico), similar al formato 3592
3592-3C	Formato comprimido, similar al formato 3592C
3592-4	Formato sin comprimir (básico), similar al formato 3592
3592-4C	Formato comprimido, similar al formato 3592C
DRIVE	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
Nota: Si este formato utiliza la función de compresión por hardware de la unidad de cintas, dependiendo de la eficacia de la compresión, la capacidad real puede ser distinta del valor que aparece en la lista.	

Si las unidades están en una biblioteca que contiene unidades de distinta tecnología de cinta, no utilice el valor DRIVE. Utilice el formato específico que empleen las unidades. Para un resultado óptimo, no mezcle las generaciones de unidades en la misma biblioteca. Si una biblioteca contiene una mezcla de generaciones, pueden darse problemas en los medios. Por ejemplo, las unidades de primera generación y segunda generación no pueden leer medios de tercera generación. Si es posible, actualice todas las unidades a 3592 de tercera generación. Si no puede actualizar todas las unidades a 3592 de tercera generación, debe utilizar una configuración especial.

ESTCAPacity

Especifica la capacidad estimada para los volúmenes que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: K (KB), M (MB), G (GB) o T (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional. El valor predeterminado es YES.

Puede especificar uno de los siguientes valores:

Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

#### EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como 2014007 (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

#### RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto

de cero para el parámetro RETENTION.

#### PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

#### Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

#### UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cintas que dé soporte a la cinta 3592. Este parámetro es opcional. Este nombre puede tener un máximo de 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

## UPDATE DEVCLASS (Actualizar una clase de dispositivo ECARTRIDGE para el servidor de medios de z/OS)

---

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a unidades StorageTek como, por ejemplo, StorageTek T9840 o T10000. La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

```

(1) (2)
>>-UPDate DEVclass--nombre_clase_dispositivo----->
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-LIBRARY---biblioteca_medio_zos-'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-FORMAT---+DRIVE---+' '-ESTCAPacity---tamaño-'
      +-T9840C---+
      +-T9840C-C---+
      +-T9840D---+
      +-T9840D-C---+
      +-T1000A---+
      +-T1000A-C---+
      +-T1000B---+
      +-T1000B-C---+
      +-T1000C---+
      +-T1000C-C---+
      +-T1000D---+
      '-T1000D-C-'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTRetention---minutos-' '-MOUNTWait---minutos-'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-MOUNTLimit---+DRIVES---+' '-COMPRESSION---+Yes---+'
      +-numero+           '-No--'
      '-0-----'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-EXPIRATION---yyyddd-' '-RETENTION---dias-'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-PROTECTION---+No---+'
      +-Yes-----+
      '-Automatic-'
>+-----+-----+-----+-----+-----+-----+-----+-----+
'-UNIT---nombre_unidad-'

```

### Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.
2. No puede actualizar el parámetro PREFIX con este comando. Debe crear una clase de dispositivo con el valor que necesita para el parámetro PREFIX.

## Parámetros

### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de actualizar.

### LIBRARY

Especifica el nombre de una biblioteca que se ha definido con el parámetro LIBTYPE=ZOSMEDIA. La biblioteca y las unidades de cinta que puede utilizar esta clase de dispositivo están controladas por el servidor de medios de z/OS.

Este parámetro es opcional.

Para obtener información acerca de cómo definir una biblioteca, consulte el comando DEFINE LIBRARY.

### FORMAT

Especifica el formato de grabación que se ha de utilizar cuando se graban datos en medios de acceso secuencial. Este parámetro es opcional.

Consulte la siguiente tabla para ver los formatos de grabación.

Tabla 1. Formatos de grabación para cintas ECARTRIDGE

Formato	Capacidad estimada	Descripción
---------	--------------------	-------------

Formato	Capacidad estimada	Descripción
DRIVE	-	El servidor selecciona el formato más elevado que recibe soporte de la unidad en la que está montado un volumen. DRIVE es el valor predeterminado. Atención: Evite especificar DRIVE cuando se utilice una combinación de unidades diferentes en la misma biblioteca. Por ejemplo, no utilice esta opción para una biblioteca que contenga algunas unidades que soporten formatos de grabación superiores a los de otras unidades.
T9840C	40 GB	Formato T9840C sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840C-C	80 GB	Formato T9840C comprimido, cuando se utiliza un cartucho StorageTek 9840
T9840D	75 GB	Formato T9840D sin comprimir, cuando se utiliza un cartucho StorageTek 9840
T9840D-C	150 GB	Formato T9840D comprimido, cuando se utiliza un cartucho StorageTek 9840
T10000A	500 GB	Formato T10000A sin comprimir, cuando se utiliza un cartucho StorageTek T10000
T10000A-C	1 TB	Formato T10000A comprimido, cuando se utiliza un cartucho StorageTek T10000
T10000B	1 TB	Formato T10000B sin comprimir que utiliza un cartucho Oracle StorageTek T10000
T10000B-C	2 TB	Formato T10000B comprimido que utiliza un cartucho Oracle StorageTek T10000
T10000C	5 TB	Formato T10000C sin comprimir que utiliza un cartucho Oracle StorageTek T10000 T2
T10000C-C	10 TB	Formato T10000C comprimido que utiliza un cartucho Oracle StorageTek T10000 T2
T10000D	8 TB	Formato T10000D sin comprimir, cuando se utiliza un cartucho Oracle StorageTek T10000 T2
T10000D-C	15 TB	Formato T10000D comprimido, utilizando un cartucho Oracle StorageTek T10000 T2
<p>Nota:</p> <ul style="list-style-type: none"> <li>Algunos formatos utilizan una función de compresión del hardware de la unidad de cintas. Dependiendo de la eficacia de la compresión, la capacidad real puede ser superior al valor que aparece en la lista.</li> <li>Las unidades T10000A sólo pueden leer y grabar el formato T10000A. Las unidades T10000B pueden leer, pero no grabar, el formato T10000A. Las unidades T10000C pueden leer, pero no grabar, los formatos T10000A y T10000B. Las unidades T10000D pueden leer, pero no pueden escribir formatos T10000A, T10000B y T10000C.</li> </ul>		

#### ESTCAPacity

Especifica la capacidad estimada para los volúmenes de acceso secuencial que se asignan a esta clase de dispositivo. Este parámetro es opcional.

Puede especificar este parámetro si la capacidad estimada predeterminada para esta clase de dispositivo es imprecisa debido a la compresión de datos. El valor no determina la cantidad de datos almacenados en el volumen. El servidor utiliza el valor para determinar la utilización antes de que se llene el volumen. Una vez un volumen está completo, la cantidad real de datos almacenados en la cinta se utiliza para el cálculo de la utilización.

Especifique el valor como un entero con los siguientes indicadores de unidad: **K** (KB), **M** (MB), **G** (GB) o **T** (TB). Por ejemplo, especifique que la capacidad estimada es de 9 GB con el parámetro ESTCAPACITY=9G. El valor más pequeño que se acepta es 100 KB (ESTCAPACITY=100K).

#### MOUNTRetention

Especifica el número de minutos que se retiene un volumen de cinta desocupado antes de desmontarse. El intervalo de tiempo de retención de montaje comienza cuando caduca el periodo de tiempo de espera que el volumen ha estado desocupado. Este parámetro es opcional. Especifique un número de 0 a 9999.

Este parámetro puede mejorar el tiempo de respuesta de los montajes de medios de acceso secuencial ya que deja activados los volúmenes montados anteriormente.

#### MOUNTWait

Especifica el número máximo de minutos que el servidor de medios de z/OS espera un montaje de volumen. Si la petición de montaje no se cumple en el tiempo especificado, la petición de montaje falla. Si un dispositivo se asigna satisfactoriamente y la petición de abrir dispositivo no se realiza en el tiempo especificado, la petición de abrir dispositivo finaliza y la petición de montaje falla.

Este parámetro es opcional. Especifique un número de 1 a 9999.

Restricción: Si la biblioteca que está asociada con esta clase de dispositivo es externa (LIBTYPE=EXTERNAL), no especifique el parámetro MOUNTWAIT.

#### MOUNTLimit

Especifica el número máximo de volúmenes de acceso secuencial que se pueden montar simultáneamente para esta clase de dispositivo. Este parámetro es opcional.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

Puede especificar uno de los siguientes valores:

#### DRIVES

Especifica que cada vez que se asigna un punto de montaje, se utiliza el número de unidades que hay definidas y en línea en la biblioteca para calcular el valor verdadero.

#### número

Especifica el número máximo de unidades en esta clase de dispositivo que el servidor utiliza simultáneamente. Este valor nunca debe sobrepasar el número de unidades que están definidas y activadas en la biblioteca que da servicio a esta clase de dispositivo. Puede especificar un número de 0 a 4096.

#### 0 (zero)

Especifica que no puede conseguir acceder a la agrupación de almacenamiento ninguna transacción nueva.

#### COMPression

Especifica si se utiliza la compresión de archivos para esta clase de dispositivo. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

#### Yes

Especifica que los datos de cada volumen de cinta han de estar comprimidos.

#### No

Especifica que los datos de cada volumen de cinta no han de estar comprimidos.

#### EXPIration

Especifica la fecha de caducidad que se coloca en las etiquetas de cintas para esta clase de dispositivo. Este parámetro es opcional.

Especifique la fecha en que el servidor ya no necesite la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Especifique la fecha de caducidad utilizando el formato *aaaadd* (cuatro dígitos para el año y tres dígitos para el día). Por ejemplo, el 7 de enero de 2014 se especifica como *2014007* (el séptimo día del año 2014).

Si especifica el parámetro EXPIRATION, no puede especificar el parámetro RETENTION.

#### RETention

Especifica el número de días que se retendrá la cinta. Este parámetro es opcional.

Especifique el número de días (de 1 a 9999) que se espera que el servidor utilice la cinta. El servidor no utiliza esta información, aunque ésta pasa al servidor de medios de z/OS para que la utilicen los sistemas de gestión de cintas o z/OS.

Si especifica el parámetro RETENTION, no puede especificar el parámetro EXPIRATION.

Consejo: para este parámetro puede especificar el valor cero. Sin embargo, sólo puede hacerlo si también desea especificar un valor para el parámetro EXPIRATION. No puede especificar un valor para el parámetro EXPIRATION si especifica un valor distinto de cero para el parámetro RETENTION.

#### PROtection

Especifica si el programa RACF, en el caso de estar instalado, protege los volúmenes asignados a esta clase de dispositivo. Si se proporciona protección, se crean perfiles RACF cuando se utilizan los volúmenes por primera vez. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### No

Especifica que el programa RACF no protege los volúmenes asignados a esta clase de dispositivo.

#### Yes

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para volúmenes cuando el servidor utiliza por primera vez los volúmenes pero los perfiles no se suprimen cuando se suprimen volúmenes del servidor. Los perfiles deben suprimirse manualmente.

Consejo: Si hay datos confidenciales almacenados en los volúmenes asignados a esta clase de dispositivo, utilice PROTECTION=YES y suprima manualmente los perfiles RACF sólo una vez borrados los volúmenes de cinta.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

#### Automatic

Especifica que el programa RACF protege los volúmenes asignados a esta clase de dispositivo. Se crean perfiles RACF para los volúmenes cuando el servidor utiliza por primera vez los volúmenes. Se suprimen perfiles RACF cuando se suprimen volúmenes del servidor.

Los perfiles que se crean para los volúmenes dependen de los valores RACF del sistema. La protección suministrada es la misma que cuando se utiliza PROTECT=YES en JCL. Si el programa RACF está activo y TAPEVOL y TAPEDSN están inactivos, la asignación de cintas falla.

Importante: Si especifica PROTECTION=AUTOMATIC, cuando se suprime un volumen, se suprime su perfil RACF. Por lo tanto, el volumen ya no está protegido por el programa RACF. Otros usuarios pueden acceder a los datos que hay en estos volúmenes.

Si especifica PROTECTION=AUTOMATIC, el servidor de medios de z/OS emite comandos RACROUTE para suprimir perfiles cuando se suprime un volumen del servidor. Los comandos de supresión emitidos dependen de los valores actuales del sistema para TAPEVOL y TAPEDSN. Si la configuración del sistema ha cambiado, puede que el servidor de medios de z/OS no suprima los perfiles existentes.

No cambie el valor a PROTECTION=AUTOMATIC para una clase de dispositivo que se haya establecido en PROTECTION=NO. Puede que existan volúmenes sin perfiles y se generarán mensajes de error cuando se supriman estos volúmenes. Si es necesario un valor diferente para PROTECTION, defina una nueva clase de dispositivo.

La creación y supresión de archivos se produce según el valor de protección cuando se utiliza en primer lugar el volumen y cuando se suprime. El servidor no intenta crear perfiles para volúmenes que ya ha utilizado. Si la protección se establece en AUTOMATIC, el servidor intenta suprimir los perfiles cuando se supriman los volúmenes.

Consulte la documentación del programa RACF para obtener más información sobre los valores TAPEVOL y TAPEDSN, y los perfiles que se crean cuando estos valores están activos.

#### UNIT

Especifica un nombre de unidad esotérico para especificar un grupo de dispositivos de cinta que den soporte a las cintas ECARTRIDGE. Utilice el nombre de la unidad que representa el subconjunto de unidades de la biblioteca que están conectadas al sistema z/OS. Este parámetro es opcional. El nombre de unidad puede tener hasta 8 caracteres.

 Sistemas operativos AIX  Sistemas operativos Linux

## UPDATE DEVCLASS (Actualizar una clase de dispositivo FILE para el servidor de medios de z/OS)

---

Utilice este mandato para actualizar una clase de dispositivo que ha definido para utilizar un servidor de medios de z/OS para acceder a archivos en el almacenamiento de disco magnético como volúmenes de acceso secuencial (como en una cinta). La clase de dispositivo orientada al almacenamiento de un servidor de medios de z/OS requiere una definición de biblioteca de tipo ZOSMEDIA.

Un volumen en esta clase de dispositivo es un conjunto de datos lineal VSAM (Virtual Storage Access Method) al que accede el servidor de medios de z/OS. Se pueden utilizar los volúmenes reutilizables con una clase de dispositivo y el servidor de medios de z/OS asignará dinámicamente el conjunto de datos lineal VSAM. No es necesario definir volúmenes para que el servidor utilice la clase de dispositivo. Si define volúmenes, establezca el calificador de alto nivel (HLQ) para que SMS reconozca la solicitud de asignación del servidor de medios de z/OS. Si utiliza volúmenes definidos, la función formatear volúmenes no se admite para el servidor al utilizar esta clase de dispositivo. El servidor de medios de servidor de medios de z/OS z/OS utiliza una característica FormatWrite del gestor de medios DFSMS al llenar los volúmenes FILE.

Puede definir los volúmenes para la clase de dispositivo FILE utilizando el comando DEFINE VOLUME. No obstante, el servidor de medios de z/OS no asigna espacio para un volumen definido hasta que se abra el volumen para su primer uso.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---



```

>>-UPDate DEVclass--nombre_clase_dispositivo----->
>--+-----+--+-----+----->
  '-MAXCAPacity----tamaño-'  '-PRIMARYalloc----tamaño-'
>--+-----+----->
  '-SECONDARYalloc----tamaño-'
>--+-----+----->
  '-PREFIX----prefijo_volumen_archivo-'
>--+-----+-----<
  '-MOUNTLimit----número-'

```

## Parámetros

### nombre\_clase\_dispositivo (Necesario)

Especifica el nombre de la clase de dispositivo que se ha de definir. La longitud máxima del nombre de clase de dispositivo es de 30 caracteres.

### MAXCAPacity

Especifica el tamaño máximo de los volúmenes de archivos definidos en una agrupación de almacenamiento de esta clase de dispositivo. Este parámetro es opcional.

Especifique este valor como un entero seguido de **K** (KB), **M** (MB), **G** (GB) o **T** (TB). El tamaño mínimo es 1 MB (MAXCAPACITY=1M). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G).

### PRIMARYalloc

Especifica la cantidad de espacio inicial que se asigna dinámicamente cuando se abre un nuevo volumen. Debe haber disponible suficiente espacio para satisfacer la cantidad de asignación primaria. La política SMS (Storage Management Subsystem) determina si se pueden utilizar varios volúmenes físicos para satisfacer la petición de asignación primaria.

Este parámetro es opcional. Especifique este valor como un entero seguido de **K** (KB), **M** (MB), **G** (GB) o **T** (TB). El tamaño mínimo es 100 KB (PRIMARYALLOC=100K). El tamaño máximo es 16384 GB (MAXCAPACITY=16384G). Todos los valores se redondean al siguiente múltiple superior de 256 K.

Para evitar espacio desaprovechado, la operación de asignación dinámica utiliza el menor de los valores especificados en los dos parámetros PRIMARYALLOC y MAXCAPACITY.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

### SECONDARYalloc

Especifica la cantidad de espacio que se amplía un volumen de archivo cuando se utiliza todo el espacio que tiene asignado. El conjunto de datos de un volumen de archivos se amplía al tamaño establecido por el parámetro MAXCAPACITY y, a continuación, el volumen se marca como lleno.

Como la asignación secundaria de un conjunto de datos lineal no puede ocupar un volumen físico, tenga en cuenta el tamaño del volumen físico al seleccionar un tamaño de asignación secundaria. Por ejemplo, los volúmenes físicos de un modelo 3 de 3390 tienen aproximadamente 2,8 GB. Para garantizar que cada petición ocupe prácticamente un volumen físico completo, pero no más, utilice un tamaño de asignación secundario que sea un poco menor de 2,8 GB. Una cantidad de asignación secundaria de 2600 MB permite suficiente espacio para el conjunto de datos de volumen VSAM (VVDS), la etiqueta de volumen y la tabla de índice de volumen (VTOC).

Este parámetro es opcional. Especifique este valor como un entero seguido de **K** (KB), **M** (MB), **G** (GB) o **T** (TB). El valor mínimo es 0 KB (SECONDARYALLOC=0K). El valor máximo es 16384 GB. Excepto 0, todos los valores se redondean al siguiente múltiple superior de 256 K.

Si se especifica 0 (SECONDARYALLOC=0), el volumen de archivo no se puede ampliar más allá de la cantidad de asignación primaria.

Las rutinas de selección de clase automática (ACS) SMS puede determinar si se van a utilizar los valores PRIMARYALLOC y SECONDARYALLOC.

Si especifica un valor para el parámetro SECONDARYALLOCATION que no es 0, o si permite que el valor tome como valor predeterminado 2600M, la DATACLAS SMS asociada al identificador PREFIX (por ejemplo, calificador de alto nivel) debe tener especificado el atributo Extended Addressability (EA). Sin el atributo EA, la DATACLAS SMS limita la asignación del volumen FILE del conjunto de datos lineal VSAM a la ampliación primaria. (Consulte la descripción del parámetro PRIMARYALLOCATION). Con

el conjunto de datos limitado al tamaño de asignación primario, el servidor de medios de z/OS no puede ampliar el conjunto de datos y el volumen se marca como FULL antes de que se alcance la capacidad máxima.

Restricción: Asegúrese de que los valores especificados para los parámetros PRIMARYALLOC y SECONDARYALLOC entren en los límites prácticos del dispositivo de almacenamiento. El servidor no puede comprobar si los valores exceden los límites prácticos del dispositivo y tampoco comprueba si los dos valores exceden conjuntamente el valor de MAXCAPACITY actual.

Consejo: Para rellenar los volúmenes cuando especifica un valor elevado para el parámetro MAXCAPACITY, especifique valores elevados para los parámetros PRIMARYALLOC y SECONDARYALLOC. Utilice tamaños de volumen de MVS mayores para reducir la posibilidad de anomalías de ampliación.

#### PREFIX

Especifica el calificador de nivel superior del nombre del conjunto de datos que se utiliza para asignar conjuntos de datos de volúmenes reutilizables. Para todos los volúmenes de archivos reutilizables creados en esta clase de dispositivo, el servidor utiliza este prefijo para crear el nombre del conjunto de datos. Este parámetro es opcional. La longitud máxima del prefijo, incluidos los puntos, es de 32 caracteres.

Los valores que se han especificado para este parámetro deben reunir las condiciones siguientes:

- El valor ha de estar compuesto por calificadores, los cuales pueden tener un máximo de ocho caracteres, incluidos los puntos. Por ejemplo, el siguiente valor resulta aceptable:

```
AB.CD2.E
```

- Los calificadores deben estar separados por un punto.
- La primera letra de cada calificador debe ser alfabética o nacional (@,#,\$), seguida por caracteres alfabéticos, nacionales, guiones o numéricos.

Un ejemplo de nombre de conjunto de datos de volumen de archivo que utilice el prefijo predeterminado es

```
ADSM.B0000021.BFS.
```

Si tiene un convenio de denominación de conjunto de datos, utilice un prefijo que se ajuste a sus convenios de denominación. Por ejemplo, el siguiente valor es aceptable: `TSM.SERVER2.VSAMFILE`.

Si ejecuta varias instancias de servidor para IBM Spectrum Protect o Tivoli Storage Manager for z/OS Media, debe utilizar un valor exclusivo para el parámetro PREFIX para cada clase de dispositivo que actualice.

#### MOUNTLimit

Especifica el número máximo de volúmenes FILE que se pueden abrir simultáneamente para esta clase de dispositivo. Este parámetro es opcional. Para los dispositivos 3995 que emulan dispositivos 3390, el valor no debe establecerse en un número mayor que el número de corrientes de entrada y salida concurrentes que pueden existir en el medio que almacena los volúmenes.

El valor que especifique en este parámetro es importante si existe una importante penalización al conmutar de un volumen a otro. Por ejemplo, la conmutación puede llevarse a cabo cuando se utilizan dispositivos IBM® 3995 que emulan dispositivos 3390. El valor que especifique no puede ser mayor que el número de unidades físicas disponibles en el dispositivo.

Si tiene planificado utilizar la función de grabación simultánea, asegúrese de que haya suficientes unidades disponibles para la operación de grabación. Si el número de unidades necesarias para una operación de grabación simultánea es mayor que el valor del parámetro MOUNTLIMIT de una clase de dispositivo, la transacción fallará.

## UPDATE DOMAIN (Actualizar un dominio de políticas)

---

Utilice este comando para cambiar un dominio de políticas.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas especificado.

### Sintaxis

---

```
>>-UPDate Domain--nombre_dominio----->
>--+-----+----->
  '-DESCRiption----descripción-'
>--+-----+----->
  '-BACKREtention---días-'  '-ARCHREtention---días-'
```






Comando	Descripción
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE DOMAIN	Elimina un dominio de políticas junto con los objetos de políticas del dominio de políticas.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.

## UPDATE DRIVE (Actualizar una unidad)

Utilice este mandato para actualizar una unidad.

### Clase de privilegio

Si quiere obtener información detallada y actual sobre el soporte de unidades, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate DRive--nombre_biblioteca--nombre_unidad----->
>--+-----+-----+-----+-----+-----+-----+----->
  '-SERial-----+--número_serie--+'  '-ONLine-----+--Yes--+'
                    '-AUTODetect---'          '-No--'
>--+-----+-----+-----+-----+-----+-----+----->
  '-ELEment-----+--dirección--+'
                    '-AUTODetect-'
>--+-----+-----+-----+-----+-----+-----+----->
  |                                     (1) |
  '-ACSDRVID-----+--id_unidad-----+'
>--+-----+-----+-----+-----+-----+-----+-----><
  |                                     (2) |
  '-CLEANFREQuency-----+--NONE-----+--'
                    |                                     |
                    |                                     (3) |
                    +-ASNEEDED-----+
                    '-gigabytes----'
```

Notas:

1. El parámetro ACSDRVID sólo es válido para unidades de las bibliotecas ACSLS.
2. El parámetro CLEANFREQUENCY sólo es válido para unidades de las bibliotecas SCSI.
3. El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona para todas las unidades de cintas. Si desea obtener más información, consulte la descripción del parámetro.

### Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca a la que se asigna la unidad.

nombre\_unidad (Obligatorio)

Especifica el nombre asignado a la unidad.

SERial

Especifica el número de serie de las unidades que están actualizándose. Este parámetro sólo es válido para las unidades en una biblioteca de cintas virtual (VTL) o SCSI. Este parámetro es opcional. Los valores posibles son:

número\_serie

Especifica el número de serie de la unidad que está actualizándose.

Nota: Si ya se ha definido una ruta para esta unidad, el número que entra aquí se compara con el número detectado por IBM Spectrum Protect. Si los números no coinciden, el comando no se ejecuta correctamente.

#### AUTODETECT

Especifica que IBM Spectrum Protect detecta y utiliza automáticamente el número de serie si ya se ha definido una ruta a esta unidad.

Si no se ha definido una ruta a esta unidad, no se detecta el número de serie.

#### ONLine

Especifica si la unidad está disponible para utilizarla. Este parámetro especifica si las unidades se pueden poner fuera de línea y utilizarse para otra actividad, por ejemplo mantenimiento. Este parámetro es opcional.

Puede emitir este comando cuando la unidad esté relacionada en un proceso activo o sesión, pero no se recomienda. Si emite un mandato para que la unidad pase a un estado desactivado mientras está en uso, se emitirá un mensaje de error. El volumen montado completa su proceso actual. Si este volumen formaba parte de una serie de volúmenes para una transacción específica, la unidad no está disponible para finalizar el montaje de la serie. Si no hay ninguna otra unidad disponible, el proceso fallará.

Atención: Cuando se utilice una unidad, no especifique el parámetro ELEMENT con el parámetro ONLINE. La unidad no se actualiza y el mandato falla.

El estado de la unidad no cambiará aunque detenga y reinicie el servidor. Si una unidad está desactivada cuando se reinicia el servidor, se emite un mensaje de aviso que indica que la unidad debe activarse manualmente. Si todas las unidades de una biblioteca se actualizan para estar desactivadas, los procesos que necesitan un punto de montaje de biblioteca fallan, en lugar de hacer cola para obtener un punto de montaje.

#### YES

Especifica que la unidad está disponible para utilizarla (activada).

#### No

Especifica que la unidad no está disponible para utilizarla (desactivada).

#### ELEMent

Especifica la dirección del elemento de la unidad dentro de una biblioteca SCSI o VTL. El servidor utiliza la dirección de elemento para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Este parámetro solo es válido para una unidad de una biblioteca SCSI o VTL cuando se emite el mandato desde un servidor de gestor de bibliotecas de IBM Spectrum Protect. Los valores posibles son:

#### dirección

Especifica la dirección de elemento de la unidad que está actualizándose.

Para localizar la dirección del elemento para la configuración de la biblioteca, consulte la información del fabricante.

Recuerde: Si ya se ha definido una ruta a esta unidad, el número que entre aquí se comparará con el número detectado anteriormente por IBM Spectrum Protect. Si los números no coinciden, este comando no se ejecuta correctamente.

#### AUTODETECT

Especifica que IBM Spectrum Protect detecta y utiliza automáticamente el número de elemento si ya se ha definido una ruta a esta unidad.

Si no se ha definido una ruta a esta unidad, no se detecta el número de elemento.

Restricción: Si la biblioteca en la que se encuentra la unidad no admite el mandato SCSI Read Element Status, y ELEMENT=AUTODETECT, el mandato no se ejecuta correctamente y genera un mensaje de error de IBM Spectrum Protect.

#### ACSDRVID

Especifica el ID de la unidad a la que se accede en una biblioteca SCSI. El identificador de unidad es un conjunto de números que indica la ubicación física de una unidad dentro de una biblioteca ACSLS. Este identificador de unidad debe especificarse como *a,l,p,d*, siendo *a* el ACSID, *l* el LSM (módulo de almacenamiento de biblioteca), *p* el número de panel y *d* el ID de unidad. El servidor necesita el identificador de unidad para conectar la ubicación física de la unidad con la dirección SCSI de la unidad. Consulte la documentación de StorageTek para obtener más detalles.

#### CLEANFREQuency

Especifica la frecuencia con que el servidor activa la limpieza de la unidad. Este parámetro es opcional. Para conseguir el grado de automatización de limpieza más completo para una biblioteca automatizada, deberá tener un cartucho limpiador dado de alta en el inventario de volúmenes de la biblioteca. Si va a utilizar una limpieza en función de la biblioteca, se recomienda NONE cuando el tipo de biblioteca es compatible con esta función. Este parámetro sólo es válido para unidades en bibliotecas SCSI y no es válido para bibliotecas gestionadas externamente, por ejemplo bibliotecas 3494 o bibliotecas StorageTek que se gestionan bajo ACSLS.

Importante: Existen consideraciones especiales que debe tener en cuenta si tiene previsto utilizar la limpieza de unidades activada por el servidor con una biblioteca SCSI que proporcione soporte de limpieza automática de unidades en el hardware del dispositivo.

## NONE

Especifica que el servidor no hace el seguimiento de la limpieza de esta unidad. Utilice este parámetro para las bibliotecas que tengan su propia limpieza automática.

## ASNEEDED

Especifica que el servidor sólo carga la unidad con un cartucho limpiador dado de alta cuando una unidad notifica al controlador de dispositivo que es necesaria la limpieza.

El valor del parámetro CLEANFREQUENCY=ASNEEDED no funciona con todos los controladores de cinta. Visite el sitio web Dispositivos soportados correspondiente a su sistema operativo. Si ASNEEDED no está soportado, puede utilizar el valor gigabytes para la limpieza automática.

Con los controladores IBM 3592 e LTO, se recomienda la limpieza en función de la biblioteca. Si no es compatible la limpieza en función de la biblioteca, debe utilizarse ASNEEDED. Gigabytes no es recomendable.

Restricción: IBM Spectrum Protect no controla las unidades conectadas al servidor de archivos NAS. Si hay una unidad conectada sólo a un servidor de archivos NAS (no a un servidor o agente de almacenamiento), no especifique ASNEEDED como frecuencia de limpieza.

## gigabytes

Especifica, en gigabytes, la cantidad de datos procesada en la unidad antes de que el servidor cargue la unidad con un cartucho limpiador. El servidor restablece el contador de gigabytes procesados cada vez que carga un cartucho limpiador en la unidad.

Importante: Cuando CLEANFREQUENCY=gigabyte, se puede producir la limpieza de unidad antes de que se alcance el valor de gigabytes, si la unidad notifica al controlador de dispositivo que es necesaria una limpieza.

Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si la información ofrece las recomendaciones para la frecuencia de limpieza en términos de horas de uso, convierta el valor en gigabytes realizando lo siguiente:

1. Utilice el valor de bytes por segundo de la unidad para determinar el valor en gigabytes por hora.
2. Multiplique el valor en gigabytes por hora por las horas recomendadas de uso entre limpiezas.
3. Utilice el resultado como el valor de frecuencia de limpieza.

Consejo: En el caso de IBM 3590, especifique un valor para la frecuencia de limpieza con el fin de garantizar que las unidades reciben la limpieza adecuada. Consulte las recomendaciones para la limpieza en la información del fabricante de la unidad. Si utiliza la frecuencia de limpieza que recomienda IBM, las unidades no se limpian más de lo necesario.

## Ejemplo: actualizar la dirección de elemento de una unidad

Actualizar DRIVE3, en la biblioteca denominada AUTO, cambiando la dirección de elemento a 119.

```
update drive auto drive3 element=119
```

## Ejemplo: desactivar una unidad

Actualizar DRIVE3, en la biblioteca denominada MANLIB, para dejarla fuera de línea.

```
update drive manlib drive3 online=no
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE DRIVE

Comando	Descripción
CLEAN DRIVE	Marca una unidad para limpiarla.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
UPDATE PATH	Cambia los atributos asociados con una ruta.



## nombre\_espacio\_archivos (Necesario)

Especifica el nombre del espacio de archivos que se va a actualizar. Puede utilizar caracteres comodín o una lista delimitada por comas para especificar nombres.

Para un servidor que tenga clientes con espacios de archivos activados para Unicode, puede que deba hacer que el servidor convierta el nombre del espacio de archivos que especifique. Por ejemplo, es posible que deba hacer que el servidor convierta un nombre de la página de códigos del servidor a Unicode. Para obtener información adicional, consulte el parámetro NAMETYPE. Si sólo especifica un solo carácter comodín para el nombre, puede utilizar el parámetro CODETYPE para limitar la operación a los espacios de archivos Unicode o a espacios de archivos no Unicode.

Los nombres de espacios de archivos son sensibles a las mayúsculas/minúsculas. Para determinar la correcta especificación de mayúsculas/minúsculas para el espacio de archivos que se va a actualizar, utilice el comando QUERY FILESPACE.

## NAMETYPE

Especifica cómo desea que el servidor interprete los nombres de espacios de archivos especificados. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect que están habilitados para Unicode y tienen sistemas operativos de Windows, Macintosh OS X o NetWare.

Utilice este parámetro sólo si especifica un nombre de espacio de archivos parcial o totalmente calificado. El valor predeterminado es SERVER. Puede especificar uno de los siguientes valores:

### SERVER

El servidor utiliza la página de códigos del servidor para interpretar los nombres de espacios de archivos.

### UNICODE

El servidor convierte los nombres de espacios de archivos de la página de códigos del servidor a la página de códigos UTF-8. El éxito de la conversión depende del sistema operativo, los caracteres que contiene el nombre y la página de códigos del servidor. La conversión puede fallar si la serie incluye caracteres que no están disponibles en la página de códigos del servidor, o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión falla, el nombre puede contener signos de interrogación, espacios en blanco o puntos suspensivos (...).

### FSID

El servidor interpreta los nombres de los espacios de archivos como identificadores de espacios de archivos.

## CODETYPE

Especifica el tipo de espacios de archivos que se van a incluir en el proceso de réplica de nodos. El valor predeterminado es BOTH, lo que significa que se incluyen espacios de archivos independientemente del tipo de página de códigos. Utilice este parámetro sólo cuando especifique un único carácter comodín para el nombre de espacio de archivos. Puede especificar uno de los siguientes valores:

### UNICODE

Especifica sólo los espacios de archivos que están en Unicode.

### NONUNICODE

Especifica sólo los espacios de archivos que no están en Unicode.

### BOTH

Especifica todos los espacios de archivos independientemente del tipo de página de códigos.

## DATATYPE (obligatorio)

Especifica el tipo de datos al que se aplica una regla de réplica. Para especificar varios tipos de datos, separe los nombres con comas y sin espacios intercalados. Puede especificar los siguientes valores:

### BACKUP

Especifica el tipo de datos de copia de seguridad.

### ARCHIVE

Especifica el tipo de datos de archivado.

### SPACEMANAGED

Especifica el tipo de datos gestionados por espacio.

## REPLRULE

Especifica la regla de réplica que se aplica a un tipo de datos. No puede utilizar comodines. Si especifica varios tipos de datos, la regla de réplica se aplica a cada tipo de datos. Por ejemplo, si especifica `DATATYPE=BACKUP, ARCHIVE`, la regla de réplica se aplica a los datos de copia de seguridad y a los datos de archivado.

Restricción: El parámetro REPLRULE es opcional. No obstante, si no lo especifica, debe especificar el parámetro REPLSTATE.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.



Por ejemplo, supongamos que un espacio de archivos contiene datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a los datos de copia de seguridad activos, especifique `DATATYPE=BACKUP REPLRULE=ACTIVE_DATA_HIGH_PRIORITY`. Para asignar una prioridad normal a los datos de archivado, vuelva a emitir el comando `UPDATE FILESPACE` y especifique `DATATYPE=ARCHIVE REPLRULE=ALL_DATA`.

Puede especificar las reglas siguientes:

#### ALL\_DATA

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad normal.

#### ACTIVE\_DATA

Sólo replica datos de copia de seguridad activos en un espacio de archivos. Los datos se replican con una prioridad normal.

Atención: Si especifica `ACTIVE_DATA` y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando hay instalada una versión de servidor anterior a la 7.1.1 en los servidores de réplica de origen o destino.
- Cuando se utiliza el mandato `REPLICATE NODE` con el parámetro `FORCECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la réplica, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino desde una versión de servidor anterior a la 7.1.1.

Si no se cumplen las condiciones anteriores, se realiza la réplica de todos los archivos nuevos y modificados desde la última réplica, incluidos los archivos inactivos, y se suprimen los archivos cuando éstos caducan.

#### ALL\_DATA\_HIGH\_PRIORITY

Replica datos de copia de seguridad, de archivado o gestionados por espacio. Los datos se replican con una prioridad alta.

#### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica `ACTIVE_DATA` excepto que los datos se replican con una prioridad alta.

#### DEFAULT

Los datos se replican de acuerdo con la regla de nodo de cliente para el tipo de datos.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es especificar `DATATYPE=ARCHIVE REPLRULE=DEFAULT` para cada espacio de archivos. Asegúrese de que la regla de réplica del cliente de los datos de archivado esté establecida en `ALL_DATA_HIGH_PRIORITY` o en `DEFAULT`. Si la regla de réplica del cliente es `DEFAULT`, la regla de réplica del servidor para los datos de archivado debe establecerse en `ALL_DATA_HIGH_PRIORITY`.

#### NONE

No se replican datos. Por ejemplo, si no desea replicar los datos gestionados por espacio en un espacio de archivos, especifique `DATATYPE=SPACEMANAGED REPLRULE=NONE`.

#### REPLState

Especifica el estado de réplica de un tipo de datos. Si ha especificado varios tipos de datos, el estado se aplica a todos los tipos de datos. Por ejemplo, si ha especificado `DATATYPE=BACKUP, ARCHIVE`, el estado se aplica a los datos de copia de seguridad y a los datos de archivado.

El parámetro `REPLSTATE` es opcional. No obstante, si no lo especifica, debe especificar el parámetro `REPLRULE`. Puede especificar uno de los siguientes valores para el parámetro `REPLSTATE`:

#### ENabled

Especifica que el tipo de datos está preparado para la réplica.

#### DISabled

Especifica que la réplica no se realiza hasta que la activa.

#### PURGEdata

Especifica que los datos se suprime del servidor de réplica de destino. El tipo de datos suprimido es el tipo de datos especificado por el parámetro `DATATYPE`. Por ejemplo, si especifica `DATATYPE=BACKUP, ARCHIVE` y `REPLSTATE=PURGEDATA`, los datos de copia de seguridad y los datos de archivado se suprimen del espacio de archivos en el servidor de réplica de destino.

Una vez suprimidos los datos, el parámetro `REPLSTATE` se establece en `DISABLED`, lo que impide la réplica en el futuro del tipo o los tipos de datos. La regla de réplica del tipo de datos se establece en `DEFAULT`.

Recuerde: El proceso de `PURGEDATA` no suprime los espacios de archivos. Sólo se suprimen los datos. El espacio de archivos aparece como vacío en la salida del comando `QUERY OCCUPANCY`.

## Ejemplo: actualizar las reglas de réplica de dos tipos de datos

NODE1 tiene tres espacios de archivos: /a, /b y /c. Las reglas de réplica de todos los espacios de archivos se establecen en ALL\_DATA. No obstante, desea replicar los datos de copia de seguridad y archivado en el espacio de archivos /a antes de replicar los datos en los otros espacios de archivos.

```
update fileSPACE node1 /a datatype=backup,archive replrule=  
all_data_high_priority
```

## Ejemplo: actualizar las reglas de réplica de dos tipos de datos

NODE2 tiene dos espacios de archivos: /a y /b. Desea suspender temporalmente la réplica de todos los datos en el espacio de archivos /b.

```
update fileSPACE node2 /b datatype=backup,archive,spaceManaged  
replstate=disabled
```


## Comandos relacionados


Tabla 1. Comandos relacionados con UPDATE FILESPACE

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET REPLETENTION	Especifica el periodo de retención de los registros de historial de réplicas.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## UPDATE LIBRARY (Actualizar una biblioteca)

Utilice este comando para actualizar una definición de biblioteca.




 Sistemas operativos AIX  Sistemas operativos Windows Para actualizar el nombre de dispositivo, el número ACS o el nombre de ruta del gestor externo de una biblioteca, debe emplear el comando UPDATE PATH.

 Sistemas operativos Linux Para actualizar el nombre de dispositivo o el nombre de ruta del gestor externo de una biblioteca, debe emplear el comando UPDATE PATH.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de biblioteca.

- UPDATE LIBRARY (Actualizar una biblioteca 349X)
- UPDATE LIBRARY (Actualizar una biblioteca ACSLS)
- UPDATE LIBRARY (Actualizar una biblioteca EXTERNAL)
- UPDATE LIBRARY (Actualizar una biblioteca FILE)
- UPDATE LIBRARY (Actualizar una biblioteca manual)
- UPDATE LIBRARY (Actualizar una biblioteca SCSI)
- UPDATE LIBRARY (Actualizar una biblioteca compartida)
- UPDATE LIBRARY (Actualizar una biblioteca VTL)

Si quiere obtener información detallada y actual sobre soporte de bibliotecas, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

### Sistemas operativos Windows

Para etiquetar automáticamente volúmenes de cinta en bibliotecas de tipo SCSI, utilice el parámetro AUTOLABEL en los comandos DEFINE LIBRARY y UPDATE LIBRARY. Con este parámetro se evita tener que etiquetar previamente un conjunto de cintas. También es más eficaz que utilizar el comando LABEL LIBVOLUME, para lo que es necesario montar los volúmenes por separado. Si utiliza el parámetro AUTOLABEL, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

Una etiqueta no puede incluir espacios en blanco intercalados ni puntos y debe ser válida cuando se utilice como un nombre de archivo en el medio.

Debe etiquetar los volúmenes de CD-ROM, Zip o Jaz con los programas de utilidad del fabricante del dispositivo o de Windows porque IBM Spectrum Protect no proporciona programas de utilidad para formatear o etiquetar estos tipos de soporte. Los programas de utilidad del sistema operativo incluyen el programa de administración de discos (una interfaz gráfica de usuario) y el comando label.

## Comandos relacionados

Tabla 1. Mandatos relacionados con UPDATE LIBRARY

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE DRIVE	Suprime una unidad de una biblioteca.
DELETE LIBRARY	Suprime una biblioteca.
DELETE PATH	Suprime una ruta de un origen a un destino.
LABEL LIBVOLUME	Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DRIVE	Cambia los atributos de una unidad.
UPDATE LIBVOLUME	Cambia el estado de un volumen de almacenamiento.
UPDATE PATH	Cambia los atributos asociados con una ruta.

## UPDATE LIBRARY (Actualizar una biblioteca 349X)

Utilice esta sintaxis para actualizar una biblioteca 349X.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca--+-----+----->
                                     '-SHAREd-----Yes---'

>--+-----+-----+-----+-----+-----+----->
    '-RESETDrives-----+Yes-+-'
```

```

           '-No--'
>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
      '-AUTOLabel-----+-No-----+-'
                              +-Yes-----+
                        '-OVERWRITE-'
>--+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<<
      '-WORMSCRatchcategory-----número-'

```

## Parámetros

### nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

### SHAREd

Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este mandato desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

### AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

### No

Especifica que el servidor no intenta etiquetar ningún volumen.

### Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

### OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.


### WORMSCRatchcategory


Especifica el número de categoría que se ha de utilizar para los volúmenes reutilizables WORM en la biblioteca. Este parámetro es necesario si utiliza volúmenes WORM. Puede especificar un número de 1 a 65279. Este número debe ser exclusivo. No lo pueden compartir otras aplicaciones o bibliotecas definidas, y debe ser distinto de los demás números de categoría en esta biblioteca. Este parámetro sólo es válido cuando se utilizan volúmenes WORM 3592.

Restricción: Este parámetro sólo puede actualizarse si el parámetro WORM de la clase de dispositivo se establece en YES y WORMSCRATCHCATEGORY no tiene definido ningún valor actualmente.

### RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX/Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
---	---

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes



Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

## Ejemplo: añadir dispositivos nuevos a una biblioteca compartida

Actualizar una biblioteca 3494 compartida denominada 3494LIB2 con nuevos nombres de dispositivos.  Sistemas operativos AIX  
 Sistemas operativos Linux

```
update library 3494lib2 device=/dev/lmcp1,/dev/lmcp2,/dev/lmcp3
```

 Sistemas operativos Windows

```
update library 3494lib device=lb3.0.0.0,lb4.0.0.0,lb5.0.0.0
```

## UPDATE LIBRARY (Actualizar una biblioteca ACSLS)

Utilice esta sintaxis para actualizar una biblioteca ACSLS.

### Clase de privilegio

 Sistemas operativos Windows Para utilizar las funciones ACSLS, es obligatorio instalar el software StorageTek Library Attach.

Para emitir este mandato, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate LIBRary--nombre_biblioteca--+-+-----+----->
                                     '-SHARed-----Yes---'

>--+-+-----+----->
   '-RESEtDrives-----+-Yes-+-'
                                     '-No--'

>--+-+-----+-----<
   '-AUTOLabel--=-+-No-----+-'   '-ACSID-----núme-ro-'
                                     +-Yes-----+
                                     '-OVERWRITE-'
```

### Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

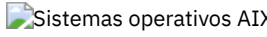
SHAREd


Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este comando desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHAREd=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX/Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX/Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHAREd=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

ACSID (Obligatorio)

Especifica el número de esta biblioteca StorageTek que ha asignado el ACSSA (Automatic Cartridge System System Administrator). Puede ser un número del 0 al 126. Emita QUERY ACS en el sistema para obtener el número del identificador de la biblioteca. Este parámetro es necesario.

Consulte la documentación de StorageTek para obtener más información.

## Ejemplo: actualizar un número de ID para una biblioteca ACSLS

---

Actualizar una biblioteca ACSLS denominada ACSLSLIB con un nuevo número de identificación.

```
update library acslslib acsid=1
```

## UPDATE LIBRARY (Actualizar una biblioteca EXTERNAL)

---

Utilice esta sintaxis para actualizar una biblioteca externa.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca----->
>--+-----+-----><
  '-AUTOLabel-----+No-----+'
      +-Yes-----+
      '-OVERWRITE-'
```

### Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.


OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

## Ejemplo: actualizar un nombre de ruta para una biblioteca externa

---

Actualizar una biblioteca externa denominada EXTLIB con un nuevo nombre de ruta para el gestor de medios.

 Sistemas operativos AIX  Sistemas operativos Linux

```
update library extlib externalmanager=/v/server/mediamanager
```

 Sistemas operativos Windows

```
update library extlib externalmanager=c:\server\mediamanager
```

## UPDATE LIBRARY (Actualizar una biblioteca FILE)

---

Utilice esta sintaxis para actualizar una biblioteca FILE.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca--+-----+---<<
                                     '-SHARed-----Yes---'
```

### Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

SHARed

Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este comando desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

### Ejemplo: actualizar una biblioteca FILE que se va a compartir

---

Actualice una biblioteca denominada FILE2 para que se pueda compartir:

```
update library file2 shared=yes
```

## UPDATE LIBRARY (Actualizar una biblioteca manual)

---

Utilice esta sintaxis para actualizar una biblioteca manual.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca----->
>--+-----+----->
   '-RESEtDrives-----+Yes-+-'
                       '-No--'
>--+-----+-----<<
   '-AUTOLabel-----+No-----+-'
                       +-Yes-----+
                       '-OVERWRITE-'
```

### Parámetros

---



nombre\_biblioteca (Necesario)


Especifica el nombre de la biblioteca que se ha de actualizar.

RESEtDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.



 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.


 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

## UPDATE LIBRARY (Actualizar una biblioteca SCSI)

---

Utilice esta sintaxis para actualizar una biblioteca SCSI.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca----->
>---LIBType-----+SCSI-+-----+----->
          '-VTL--'      '-SHARed-----Yes--'
>--+-----+----->
          '-RESETDrives-----+Yes-+-'
          '-No--'
```

```

>-----+----->
'-AUTOLabel--==--+-No-----+-'
          +-Yes-----+
          '-OVERWRITE-'

>-----+----->
'-RELABELSCRatch--==--+-No--+-'
          '-Yes-'

>-----+-----<----->
'-SERial---+-número_serie--+-'
          '-AUTODetect---'

```

## Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de actualizar.

LIBType (Obligatorio)

Especifica el tipo de biblioteca al que desea actualizar. Los valores posibles son:

VTL

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual SCSI.

Nota: Si selecciona la biblioteca VTL, se supone que se cumplen las siguientes condiciones:

- El entorno no incluye medios mixtos
- Hay rutas definidas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento, que utilizan la biblioteca

Si no se cumplen ambas condiciones, el rendimiento puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad cuando se utiliza la mayoría de unidades de forma simultánea.

SCSI

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual VTL.



SHARED


Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este comando desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

La tabla siguiente describe las tres configuraciones posibles para las unidades conectadas a dispositivos NAS.

Tabla 1. Configuraciones para las unidades conectadas a dispositivos NAS.

Configuración de dispositivos de biblioteca	El comportamiento de la reserva persistente
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y las unidades de cintas se comparten entre el servidor y el dispositivo NAS.	Se da soporte a la preferencia de unidad cuando el dispositivo NAS da soporte a la reserva persistente y ésta está habilitada. Para obtener más información sobre la definición de la reserva persistente, consulte la documentación para el dispositivo NAS.
El dispositivo de biblioteca está conectado al servidor de IBM Spectrum Protect, y a las unidades de cintas solo accede el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.
El dispositivo de biblioteca está conectado al dispositivo NAS, NDMP (protocolo de gestión de datos de red) accede indirectamente a él, y a las unidades de cintas solo se accede desde el dispositivo NAS.	La preferencia de reserva de unidad no está soportada. Si habilita la reserva persistente en el dispositivo NAS para estas unidades y el dispositivo NAS establece una reserva pero nunca la borra, debe utilizar otro método para borrar la reserva.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

SERial

Especifica el número de serie de la biblioteca que está actualizándose. Este parámetro es opcional. Los valores posibles son:

número\_serie

Especifica el número de serie de la biblioteca que está actualizándose.

Si ya se ha definido una ruta para esta biblioteca, el número que especifica aquí se compara con el número que IBM Spectrum Protect ha detectado. Si los números no coinciden, el comando no se ejecuta correctamente. Si no se ha definido una ruta, este número de serie se verifica cuando se defina una ruta.

AUTODetect

Especifica que, si ya se ha definido una ruta para esta biblioteca, IBM Spectrum Protect detecta y utiliza automáticamente el número de serie.

Si no se ha definido una ruta para esta biblioteca, el número de serie no se detecta.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando este parámetro se define con el valor SÍ, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta de volumen existente. Este parámetro es opcional y está pensado para utilizarse con una biblioteca de cintas virtual (VTL).

Nota: Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede afectar al rendimiento.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

## UPDATE LIBRARY (Actualizar una biblioteca compartida)

---

Utilice esta sintaxis para actualizar una biblioteca compartida.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca----->
>--PRIMarylibmanager---nombre_servidor-----<
```

### Parámetros

---

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

PRIMarylibmanager

Especifica el nombre del servidor responsable del control del acceso a los recursos de biblioteca. Debe definir este servidor con el mandato DEFINE SERVER para poder utilizarlo como gestor de bibliotecas.

### Ejemplo: cambiar el servidor del gestor de bibliotecas para una biblioteca

---

Para un servidor de clientes de bibliotecas, cambiar el nombre del servidor gestor de bibliotecas por CASTOR.

```
update library ltolib primarylibmanager=castor
```

## UPDATE LIBRARY (Actualizar una biblioteca VTL)

---

Utilice esta sintaxis para actualizar una biblioteca que está definida como VTL.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate LIBRary--nombre_biblioteca----->
>---LIBType---+VTL-+-----+----->
          '-SCSI-'      '-SHARED-----Yes---'
>+-----+----->
  '-RESETDrives-----+Yes-+-'
          '-No--'
>+-----+----->
  '-AUTOLabel-----+No-----+-'
          +-Yes-----+
          '-OVERWRITE-'
>+-----+----->
  '-RELABELSCRatch-----+No-+-'
          '-Yes-'
```

```
>-----<
'-SERial-----+--número_serie+-'
'-AUTODetect---'
```

## Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca que se ha de definir. La longitud máxima de este nombre es de 30 caracteres.

LIBType (Obligatorio)

Especifica el tipo de la biblioteca que está definiendo. Los valores posibles son:

SCSI

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual VTL.

VTL

Especifica que la biblioteca dispone de un dispositivo cambiador de medios controlado por SCSI que está representado por una biblioteca de cintas virtual. Para montar volúmenes en unidades en este tipo de biblioteca, IBM Spectrum Protect utiliza el dispositivo cambiador de medios. Este valor solo resulta efectivo si se especifica para las bibliotecas con un tipo de biblioteca actual SCSI.

Nota: Seleccione el tipo de biblioteca VTL solamente si se cumplen las condiciones siguientes:

- El entorno no incluye medios mixtos
- Hay rutas definidas entre todas las unidades de la biblioteca y todos los servidores definidos, incluidos los agentes de almacenamiento, que utilizan la biblioteca

Si no se cumplen ambas condiciones, el rendimiento puede disminuir a los mismos niveles que el tipo de biblioteca SCSI, especialmente en momentos de gran actividad cuando se utiliza la mayoría de unidades de forma simultánea.



SHARED


Especifica que esta biblioteca se comparte con otros servidores en una red de área de almacenamiento (SAN). Debe emitir este comando desde el servidor definido como el gestor principal de bibliotecas para la biblioteca compartida. Este parámetro es necesario para bibliotecas definidas en un gestor de bibliotecas y para bibliotecas utilizadas en operaciones NDMP. Especifique SHARED=YES para actualizar una biblioteca que no está compartida actualmente.

Importante: Si una biblioteca dispone de una ruta de un transportador de datos (como un servidor de archivos NAS) pero no dispone de conexión al servidor, la biblioteca no se puede compartir con otro servidor.

RESETDrives

Especifica si el servidor sustituye una reserva de unidad por una reserva persistente cuando se reinicia o cuando se establece un cliente de biblioteca o una reconexión de un agente de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Windows Si la reserva persistente no está soportada, el servidor realiza un restablecimiento de ruta al dispositivo de destino.

 Sistemas operativos Linux Si la reserva persistente no está soportada, el servidor no puede restablecer la vía de acceso al dispositivo de destino.

El soporte para la reserva persistente tiene las siguientes limitaciones:

- Si está utilizando el controlador de dispositivo IBM Spectrum Protect, la reserva persistente sólo se soporta en algunas de las unidades de cintas. Consulte Technote 1470319 para obtener más detalles.
- Si está utilizando el controlador de dispositivo de IBM®, la reserva persistente tiene que estar habilitada en el nivel de controlador de dispositivo. Para obtener información sobre la configuración del controlador, consulte la *Guía de instalación y uso de los controladores de dispositivo de cinta de IBM*.
- Si está utilizando una biblioteca de cintas virtual que está emulando una unidad soportada, es posible que no soporte la reserva persistente.

 Sistemas operativos AIX  Sistemas operativos Windows

Yes

Especifica que se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino.

No

Especifica que no se utilizan la preferencia de unidad a través de la reserva persistente o el restablecimiento de destino. El parámetro RESETDRIVES se debe establecer en YES en un entorno en clúster cuando SHARED=NO.

 Sistemas operativos Linux

Yes

Especifica que se utiliza la preferencia de unidad a través de la reserva persistente.

No

Especifica que no se utiliza la preferencia de unidad a través de la reserva persistente.

Nota: El gestor de biblioteca no podrá romper la reserva de unidad si el sistema que tiene la reserva de unidad no está configurado para utilizar la reserva persistente.

AUTOLabel

Especifica si el servidor intenta etiquetar automáticamente los volúmenes de cintas. Este parámetro es opcional.

Para utilizar esta opción, debe dar de alta las cintas especificando CHECKLABEL=BARCODE en el comando CHECKIN LIBVOLUME.

No

Especifica que el servidor no intenta etiquetar ningún volumen.

Yes

Especifica que el servidor sólo etiqueta los volúmenes que no tienen etiqueta.

OVERWRITE

Especifica que el servidor intenta grabar encima de una etiqueta existente. El servidor graba encima de las etiquetas existentes *sólo* si no se han definido aún ni la etiqueta ni la etiqueta ni la etiqueta de código de barra existentes en ninguna agrupación de almacenamiento del servidor o en la lista histórica de volúmenes.

RELABELSCRatch

Especifica si el servidor vuelve a etiquetar los volúmenes que se han suprimido y vuelven a ser reutilizables. Cuando se establece este parámetro en YES, se inicia una operación LABEL LIBVOLUME y se sobrescribe la etiqueta del volumen existente.

Nota: Si tiene volúmenes virtuales y reales en VTL, se vuelven a etiquetar ambos tipos cuando se activa este parámetro. Si la VTL incluye volúmenes reales, la especificación de esta opción puede afectar al rendimiento.

Yes

Especifica que el servidor vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

No

Especifica que el servidor no vuelve a etiquetar los volúmenes que se suprimen y se pueden reutilizar.

SERial

Especifica el número de serie de la biblioteca que está actualizándose. Este parámetro es opcional. Los valores posibles son:

número\_serie

Especifica el número de serie de la biblioteca que está actualizándose.

Si ya se ha definido una ruta para esta biblioteca, el número que especifica aquí se compara con el número que IBM Spectrum Protect ha detectado. Si los números no coinciden, el comando no se ejecuta correctamente. Si no se ha definido una ruta, este número de serie se verifica cuando se defina una ruta.

AUTODetect

Especifica que, si ya se ha definido una ruta para esta biblioteca, IBM Spectrum Protect detecta y utiliza automáticamente el número de serie.

Si no se ha definido una ruta para esta biblioteca, el número de serie no se detecta.

## UPDATE LIBVOLUME (Cambiar el estado de un volumen de almacenamiento)

Utilice este comando para cambiar el estado de un volumen de almacenamiento de acceso secuencial de una biblioteca.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate LIBVolume--nombre_biblioteca--nombre_volumen--STATus-----PRIVate-+++>
                                     '-SCRatch-'

>--+-----+-----<
   '-OWNer-----nombre_servidor-'
```

### Parámetros

nombre\_biblioteca (Necesario)

Especifica el nombre de la biblioteca.

nombre\_volumen (Necesario)

Especifica el nombre de volumen del volumen de almacenamiento.

STATus (Obligatorio)

Especifica un cambio del estado de un volumen de almacenamiento. Los valores posibles son los siguientes:




PRivate




Especifica que el servidor actualiza el volumen de almacenamiento a un volumen privado.

SCRatch

Especifica que el servidor actualiza el volumen de almacenamiento a un volumen reutilizable.

Restricción: No puede cambiar el estado de un volumen de privado a reutilizable si el volumen pertenece a una agrupación de almacenamiento o se define en el archivo histórico de volúmenes. Puede cambiar el estado si comete un error al dar de alta a los volúmenes en la biblioteca y asignar a los volúmenes el estado incorrecto.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows OWNER

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica qué servidor es el propietario de un volumen privado en una biblioteca compartida en una SAN. Puede cambiar el propietario de un volumen privado en una biblioteca compartida (SAN) si emite el mandato desde el servidor gestor de bibliotecas. Si no especifica este parámetro, el servidor gestor de bibliotecas será el propietario del volumen privado.

Importante: No utilice OWNER como valor para volúmenes reutilizables. Sin embargo, puede utilizar OWNER al cambiar un volumen reutilizable a privado.







## Ejemplo: actualizar el estado de un volumen

Actualice el volumen denominado WPDV00 de la biblioteca denominada AUTO de modo que refleje un estado de Privado (PRIVATE).

```
update libvolume auto wpdv00 status=private
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE LIBVOLUME

Comando	Descripción
AUDIT LIBRARY	Se asegura de que una biblioteca automatizada esté en un estado coherente.
CHECKIN LIBVOLUME	Da de alta un volumen de almacenamiento en una biblioteca automatizada.
CHECKOUT LIBVOLUME	Da de baja un volumen de almacenamiento en una biblioteca automatizada.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows LABEL LIBVOLUME	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Etiqueta volúmenes en bibliotecas manuales o automatizadas.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY LIBVOLUME	Visualiza información sobre un volumen de biblioteca.

## UPDATE MACHINE (Actualizar información de máquina)

Utilice este comando para actualizar la información de la máquina. Esta información se incluirá en el archivo del plan para ayudarle a recuperar las máquinas cliente.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UPDate MACHine--machine_name----->
```

```

>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DESCRiption-----descripci3n-' '-BUilding-----edificio-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-FLoor-----planta-' '-ROom-----sala-'
>-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<
'-PRIority-----n3mero-' '-ADSMServer-----+Yes+-'
                                          '-No--'

```

## Parámetros

nombre\_máquina (Obligatorio)

Especifica el nombre de la máquina que se ha de actualizar.

DESCRiption

Especifica la descripción de la máquina. Este parámetro es opcional. El texto puede tener hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

BUilding

Especifica el nombre o número del edificio donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

FLoor

Especifica el nombre o número de la planta donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

ROom

Especifica el nombre o número de la sala donde está esta máquina. Este parámetro es opcional. El texto puede tener hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un texto existente, especifique una serie nula ("").

PRIority

Especifica la prioridad de restauración de la máquina en forma de un entero del 1 al 99. La prioridad más alta es 1. Este parámetro es opcional. Utilice este valor para determinar la prioridad de la recuperación de la máquina de cliente.

ADSMServer

Especifica si la máquina contiene un servidor de IBM Spectrum Protect. Este parámetro es opcional. Los valores posibles son:

No

Esta máquina no contiene un servidor de IBM Spectrum Protect.

Yes

Esta máquina contiene un servidor de IBM Spectrum Protect. Solo puede definirse una máquina que contenga un servidor de IBM Spectrum Protect.

## Ejemplo: actualizar la información de una máquina específica

Actualizar la información de la máquina DISTRICT5 de modo que refleje que contiene el servidor.

```
update machine district5 admsserver=yes
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE MACHINE

Comando	Descripción
DEFINE MACHINE	Define una máquina para DRM.
DELETE MACHINE	Suprime una máquina.
INSERT MACHINE	Inserta características de la máquina o instrucciones de recuperación en la base de datos de IBM Spectrum Protect.
QUERY MACHINE	Muestra información sobre máquinas.

## UPDATE MGMTCLASS (Actualizar una clase de gestión)



Utilice este comando para cambiar una clase de gestión. Para que los clientes puedan utilizar la clase de gestión actualizada, debe activar el juego de políticas que contiene la clase de gestión.

Importante: El mandato UPDATE MGMTCLASS no se ejecutará correctamente si se especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

## Sintaxis

---

```
>>-UPDate MGMTclass----->
>--nombre_dominio--nombre_conjunto_políticas--nombre_clase----->
>--+-----+----->
  '-SPACEMGTEchnique-----+AUTOMATIC-+'
                        +-SElective-+
                        '-NONE-----'
>--+-----+----->
  '-AUTOMIGNonuse-----días-'
>--+-----+----->
  '-MIGREQUIRESBkup-----+Yes-+-'
                        '-No--'
>--+-----+----->
  '-MIGDESTination-----nombre_agrupación-'
>--+-----+-----><
  '-DESCRiption-----descripción-'
```

## Parámetros

---

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece la clase de gestión.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas al que pertenece la clase de gestión. No puede actualizar una clase de gestión que pertenezca al juego de políticas ACTIVE.

nom\_clase (Necesario)

Especifica la clase de gestión que se actualiza.

SPACEMGTEchnique

Especifica si un archivo que utiliza esta clase de gestión se puede seleccionar para una operación de migración. Este parámetro es opcional. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

AUTOMATIC

Especifica que se puede seleccionar el archivo para la migración automática y para la migración selectiva.

SElective

Especifica que el archivo se puede seleccionar únicamente para la migración selectiva.

NONE

Especifica que el archivo no se puede seleccionar para la operación de migración.

AUTOMIGNonuse

Especifica el número de días que deben transcurrir desde que se utilizó por última vez un archivo hasta que pueda seleccionarse para la migración automática. Este parámetro es opcional. Si SPACEMGTECHNIQUE no es AUTOMATIC, el servidor no tiene en cuenta este atributo. Puede especificar un entero de 0 a 9999.

Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

MIGREQUIRESBkup

Especifica si debe existir una versión de copia de seguridad de un archivo antes de que pueda migrarse un archivo. Este parámetro es opcional. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no

en los clientes de aplicación ni en los clientes de copia de seguridad/archivado. Los valores posibles son:

- Yes  
Especifica que debe existir una versión de copia de seguridad.
- No  
Especifica que la versión de copia de seguridad es opcional.

#### MIGDESTination

Especifica la agrupación de almacenamiento primaria donde el servidor almacena inicialmente los archivos migrados mediante clientes IBM Spectrum Protect for Space Management. Este parámetro únicamente tiene efecto en los clientes IBM Spectrum Protect for Space Management, no en los clientes de aplicación ni en los clientes de copia de seguridad/archivado.

El comando no se ejecutará si especifica una agrupación de almacenamiento de copia como destino.

#### DESCRiption

Especifica una descripción de la clase de gestión. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("").

## Ejemplo: actualizar el dominio de políticas y la agrupación de almacenamiento para una clase de gestión específica

Para la clase de gestión ACTIVEFILES, del juego de políticas VACATION del dominio de políticas EMPLOYEE\_RECORDS, cambiar la agrupación de almacenamiento donde se almacenan los archivos migrados.

```
update mgmtclass employee_records vacation  
activefiles migdestination=diskpool2
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE MGMTCLASS

Comando	Descripción
ASSIGN DEFMGMTCLASS	Asigna una clase de gestión como valor predeterminado para un juego de políticas especificado.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE MGMTCLASS	Elimina una clase de gestión de un dominio de políticas y juego de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.

## UPDATE NODE (Actualizar atributos del nodo)

Utilice este comando para modificar los atributos de un nodo inscrito.

Debe utilizar el comando RENAME NODE para cambiar el nombre de un nodo registrado.

Si actualiza el método de autenticación del nodo o el valor SSLREQUIRED del nodo y hay un administrador con el mismo nombre, cambie esos valores del ID de administrador.

Debe tener autorización de nivel de sistema para actualizar el método de autenticación del nodo o el valor SSLREQUIRED del nodo y también actualizar un ID de administrador con el mismo nombre. Si el administrador con el mismo nombre tiene la autorización de propietario de cliente sobre el nodo que se está actualizando, entonces no es necesaria la autorización de nivel de sistema. Debe tener

privilegio de política sin restricciones o privilegio de política con restricciones para el dominio de políticas al que pertenece el nodo cliente.

Para usuarios de servidores LDAP (Lightweight Directory Access Protocol):

- La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.
- Si cambia el modo de autenticación a LDAP y el nombre de nodo coincide con un ID de usuario de administración, podría darse un comportamiento imprevisto si se produce un cambio automático de contraseñas, ya que es posible que la contraseña se actualice dos veces. A consecuencia de esto, la contraseña podría acabar siendo desconocida para el ID de usuario de administración. También podría fallar la operación de actualización de contraseñas.

Cuando se registra o actualiza un nodo, puede especificar si los archivos dañados en el nodo pueden recuperarse de un servidor de réplica de destino. Los archivos sólo se pueden recuperar si se cumplen todas las condiciones siguientes:

- La versión 7.1.1 o superior está instalada en los servidores de réplica de origen y destino.
- El parámetro del sistema REPLRECOVERDAMAGED está establecido en ON. El parámetro del sistema se puede establecer utilizando el mandato SET REPLRECOVERDAMAGED.
- El servidor de origen incluye al menos un archivo que se marca como dañado en el nodo que se replica.
- Los datos del nodo se han replicado antes de que se produjera el daño.

La tabla siguiente describe cómo afectan los valores de los parámetros a la recuperación de archivos dañados y replicados.

Tabla 1. Valores que afectan a la recuperación de archivos dañados

Valor para el parámetro del sistema REPLRECOVERDAMAGED	Valor del parámetro RECOVERDAMAGED en el mandato REPLICATE NODE	Valor del parámetro RECOVERDAMAGED en el mandato REGISTER NODE y UPDATE NODE	Resultado
OFF	YES, NO, o sin especificar	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
OFF	ONLY	YES o NO	Aparece un mensaje de error porque los archivos no se pueden recuperar cuando el parámetro de sistema REPLRECOVERDAMAGED se establece en OFF.
ON	YES	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	NO	YES o NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.
ON	ONLY	YES o NO	Los archivos dañados se recuperan del servidor de réplica de destino, pero no se produce la réplica de nodo estándar.
ON	No especificado	YES	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados se recuperan del servidor de réplica de destino.
ON	No especificado	NO	Durante la réplica de nodo, se produce la réplica estándar y los archivos dañados no se han recuperado del servidor de réplica de destino.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de política sin restricciones, o privilegio de política limitado al dominio de políticas al que pertenece el nodo cliente.

## Sintaxis

(1)  
 >>-UPDate Node-----nombre\_nodo----->

```

>----->
| (2) |
+-----password-----+
| |
| '-FORCEPwreset-----+No--+-' |
| |
| '-FORCEPwreset-----Yes-----' |
| |
>----->
'-PASSExp-----días-' '-CLOptset-----option_set_name-'
>----->
'-CONTACT-----texto-' '-DOMAIN-----domain_name-'
>----->
'-COMPRESSION-----+Client+-' '-ARCHDELETE-----+Yes+-'
| |
| '+Yes-----+' '-No--' |
| '-No-----+' |
>----->
'-BACKDELETE-----+No--+-'
| |
| '-Yes-' |
>----->
'-WHEREDOMAIN-----domain_name-'
>----->
'-WHEREPLATFORM-----nombre_plataforma_cliente-'
>----->
'-MAXNUMMP-----number-' '-KEEPMP-----+No--+-'
| |
| '-Yes-' |
>----->
'-URL-----dirección_url-' '-UTILITYUrl-----utility_url-'
| |
| (3) |
>----->
'-AUTOFSRename-----+Yes-----+'
| |
| '+No-----+' |
| '-Client-' |
>----->
'-VALIDATEPROTOCOL-----+No-----+'
| |
| '+Dataonly-+' |
| '-All-----+' |
>----->
'-TXNGROUPMAX-----+0-----+'
| |
| '-número-' |
| |
| .-DATAWRITEPATH-----ANY----- |
>----->
'-DATAWRITEPATH-----+ANY-----+'
| |
| '+LAN-----+' |
| '-LANFree-' |
| |
| .-DATAREADPATH-----ANY----- |
>----->
'-DATAREADPATH-----+ANY-----+'
| |
| '+LAN-----+' |
| '-LANFree-' |
>----->
'-TARGETLevel-----V.R.M.F-'
| |
| .-SESSIONINITIATION-----Clientorserver----- |
>----->
'-SESSIONINITIATION-----+Clientorserver-----+ |
| |
| '-SERVEROnly--HLAddress-----dirección_ip--LAddress-----puerto_tcp-----' (4) |
>----->
'-HLAddress-----ip_address-'
>----->
| (4) |

```



1. Debe especificar como mínimo un parámetro opcional en este mandato.
2. Las contraseñas son opcionales para este mandato, excepto si se cambia el método de autenticación de LDAP a LOCAL.
3. El parámetro VALIDATEPROTOCOL está en desuso.
4. HLADDRESS y LLADDRESS se deben establecer o especificar previamente en el mandato UPDATE NODE o REGISTER NODE para utilizar SESSIONINITIATION=SERVERONLY.
5. El parámetro BACKUPINITIATION se ignora si el sistema operativo del nodo cliente no está soportado.
6. Si especifica el parámetro REPLSTATE y no especifica el parámetro REPLMODE, la modalidad de réplica del nodo se establece en SEND.
7. Si especifica el parámetro REPLMODE, también debe especificar el parámetro REPLSTATE.
8. El parámetro SYNCLDAPDELETE se aplica solamente si un nodo que se autentica en un servidor Lightweight Directory Access Protocol (LDAP) vuelve a la autenticación local.
9. El parámetro SSLREQUIRED está en desuso.

## Parámetros

### nombre\_nodo (Obligatorio)

Especifica el nombre del nodo cliente que se ha de actualizar. Puede utilizar caracteres comodín para especificar este nombre.

Restricción: Al actualizar una contraseña con el mandato UPDATE NODE, no puede utilizar un carácter comodín con el parámetro `node_name`.

### contraseña

Especifica la nueva contraseña del nodo cliente. Este parámetro es opcional en la mayoría de los casos. Si se cambia el método de autenticación de LDAP a local, es necesaria una contraseña. Si el método de autenticación de nodos es LDAP, no especifique ninguna contraseña utilizando el mandato UPDATE NODE. La longitud máxima de la contraseña es de 64 caracteres. Las contraseñas continúan siendo actuales durante un período de tiempo que queda determinado por el período de caducidad de contraseñas.

### FORCEPwreset

Especifica si se forzará que un cliente cambie o restablezca la contraseña. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### No

Especifica que el período de caducidad de contraseña se establece mediante el mandato SET PASSEXP. No se fuerza que un cliente cambie o restablezca la contraseña mientras se intenta iniciar la sesión en el servidor.

#### Yes

Especifica que la contraseña del administrador o del nodo de cliente caducará durante la próxima conexión. El cliente debe cambiar o restaurar la contraseña en el próximo inicio de sesión.

Restricciones:

- En el caso de los nodos que se autentican con un servidor LDAP, la caducidad de la contraseña se establece utilizando los programas de utilidad del servidor LDAP. Por este motivo, no especifique FORCEPWRESET=YES si tiene previsto especificar AUTHENTICATION=LDAP.
- Si tiene previsto actualizar un nodo para la autenticación con un servidor LDAP y ha especificado FORCEPWRESET=YES, debe cambiar la contraseña para poder especificar FORCEPWRESET=NO y AUTHENTICATION=LDAP.

### PASSExp

Especifica el número de días que será válida la contraseña. Puede establecer el período de caducidad de la contraseña en el rango de 0 – 9999 días. El valor 0 significa que la contraseña no caduca nunca. Este parámetro es opcional. Si no especifica este parámetro, el período de caducidad de contraseña permanece igual.

Puede cambiar el período de caducidad de la contraseña mediante los mandatos UPDATE NODE o SET PASSEXP. Para establecer un período de caducidad común para todos los administradores y nodos cliente, emita el mandato SET PASSEXP. También puede utilizar el mandato SET PASSEXP para establecer períodos de caducidad de contraseña de forma selectiva. Si establece un período de caducidad de la contraseña de forma selectiva mediante el mandato REGISTER NODE, el mandato UPDATE NODE o el mandato SET PASSEXP, el período de caducidad se excluirá de los períodos de caducidad de contraseñas comunes que se han creado mediante el mandato SET PASSEXP.

Puede utilizar el mandato RESET PASSEXP para restablecer el período de caducidad de contraseñas en un período de caducidad común. Este parámetro no se aplica a las contraseñas que se autentican con un servidor de directorios LDAP.

### CLOptset

Especifica el nombre del conjunto de opciones que ha de utilizar el cliente. Este parámetro es opcional. Para eliminar el conjunto de opciones de cliente, especifique el parámetro CLOPTSET con una serie vacía ("").

### CONtact

Especifica una serie de texto de información que identifica el nodo de cliente. Este parámetro es opcional. La longitud máxima de la serie de texto es de 255 caracteres. La información de contacto debe estar delimitada por comillas si contiene algún carácter

en blanco. Para suprimir la información de contacto definida, especifique una serie nula ("").

#### DOmain

Especifica el nombre del dominio de políticas en el que desea registrar el nodo cliente. Este parámetro es opcional.

Restricción: en el caso de los servidores que tienen la protección de retención de datos activada, un nodo inscrito archivado no se puede reasignar a un dominio de políticas diferente.

#### COMPression

Especifica si el nodo de cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada. Este parámetro es opcional.

Restricción: Este parámetro no se puede especificar para un nodo NAS.

Puede especificar uno de los siguientes valores:

#### Client

Especifica que el cliente determina si se comprimirán los archivos.

#### Yes

Especifica si el nodo de cliente comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada.

#### No

Especifica que el nodo de cliente no comprime sus archivos antes de enviarlos al servidor para copia de seguridad y copia archivada.

#### ARCHDElete

Especifica si el nodo cliente puede suprimir sus propias copias archivadas del servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### Yes

Especifica que el nodo cliente puede suprimir sus propias copias archivadas del servidor.

#### No

Especifica que el nodo cliente no puede suprimir sus propias copias archivadas del servidor.

#### BACKDElete

Especifica si el nodo cliente puede suprimir sus propias copias de seguridad del servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

#### No

Especifica que el nodo cliente no puede suprimir sus propias copias de seguridad del servidor.

#### Yes

Especifica que el nodo cliente puede suprimir sus propias copias de seguridad del servidor.

#### WHEREDomain

Especifica el nombre del dominio de políticas que se ha de utilizar como filtro junto con el nombre de nodo para seleccionar los nodos que se actualizan. Este parámetro es opcional.

#### WHEREPlatform

Especifica el nombre de la plataforma de cliente que se ha de utilizar como filtro junto con el nombre de nodo para seleccionar los nodos que se actualizan. Este parámetro es opcional.

#### MAXNUMMP

Especifica el número máximo de puntos de montaje que puede utilizar un nodo en el servidor o en el agente de almacenamiento sólo para operaciones como la copia de seguridad, el archivado y la migración IBM Spectrum Protect for Space Management. El parámetro es opcional y no se aplica a los nodos con un tipo NAS o SERVER. El valor predeterminado es 1. Puede especificar un entero en el rango de 0 a 999. Un valor de 0 especifica que un nodo no puede adquirir ningún punto de montaje para una operación de almacenamiento de datos de cliente. El valor MAXNUMMP no se evalúa ni se aplica durante las operaciones de lectura de datos de cliente como la restauración, la recuperación y la reclamación de IBM Spectrum Protect for Space Management. Sin embargo, los puntos de montaje utilizados en operaciones de lectura de datos se evalúan contrastándolos con los intentos las operaciones de almacenamiento de datos simultáneas del mismo nodo cliente, y puede que impidan que las operaciones de almacenamiento de datos obtengan puntos de montaje.

En el caso de los volúmenes de una agrupación de almacenamiento asociada al tipo de dispositivo FILE o CENTERA, el servidor puede disponer, simultáneamente, de varias sesiones que lean y de un único proceso que grabe en el mismo volumen. Para aumentar la concurrencia y proporcionar un acceso eficiente para nodos que tienen datos en agrupaciones de almacenamiento FILE o CENTERA, incremente el valor del parámetro MAXNUMMP.

En nodos que almacenan datos en agrupaciones de almacenamiento primarias con la función de grabación simultánea activada, deberá ajustar el valor del parámetro MAXNUMMP para especificar el número correcto de puntos de montaje de cada sesión de cliente. Una sesión de cliente requiere un punto de montaje para la agrupación de almacenamiento primario y un punto de montaje para cada agrupación de almacenamiento de copias y cada agrupación de datos activos.

#### URL

Especifica el URL del cliente web de IBM Spectrum Protect que se ha configurado en el sistema cliente. Puede utilizar el URL en un navegador web y en el Centro de operaciones para gestionar de forma remota el nodo cliente.

Este parámetro es opcional. El URL debe incluir el nombre DNS o la dirección IP del sistema cliente y el número de puerto que está definido en el sistema cliente para el cliente web de IBM Spectrum Protect. Por ejemplo, `http://client.mycorp.com:1581`

Si desea eliminar el valor de este parámetro, especifique comillas simples vacías o bien comillas dobles vacías, sin espacios (" para comillas simples o "" para comillas dobles).

#### UTILITYUrl

Especifica la dirección de los servicios de gestión del cliente de IBM Spectrum Protect configurados en el sistema cliente. Este URL lo utiliza Centro de operaciones para acceder a los archivos de registro del cliente para que pueda diagnosticar problemas del cliente remotamente desde Centro de operaciones.

Este parámetro es opcional. Puede especificar un URL de hasta 200 caracteres de longitud. El URL debe empezar por `https`. Incluye el nombre DNS o la dirección IP del sistema cliente y el número de puerto que se ha definido en el sistema cliente para los servicios de gestión de cliente de IBM Spectrum Protect. Por ejemplo, `https://client.mycorp.com:9028`

Si se omite el número de puerto, el Centro de operaciones utiliza el número de puerto 9028, que es el número de puerto predeterminado cuando se instalan los servicios de gestión del cliente en el sistema cliente.

#### KEEPMP

Especifica si el nodo cliente mantiene el punto de montaje durante toda la sesión. El parámetro es opcional. Puede especificar uno de los siguientes valores:

##### No

Especifica que el nodo de cliente libera el punto de montaje durante la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se publicarán los puntos de montaje que mantenga la sesión.

##### Yes

Especifica que el nodo cliente debe retener el punto de montaje durante toda la sesión. Si las definiciones de políticas hacen que los datos se almacenen en una agrupación de almacenamiento en disco después de almacenar los datos en una agrupación de almacenamiento de acceso secuencial, se retendrán los puntos de montaje que mantenga la sesión.

#### AUTOFSRename

Especifica si se solicita al cliente que redetermine los espacios de archivos cuando el sistema cliente se actualiza a un cliente que tiene soporte para Unicode. La solicitud y la redeterminación, si están permitidas, sólo se producen cuando el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. La redeterminación cambia los nombres de los espacios de archivos de los que se ha hecho una copia de seguridad que no están en Unicode en el almacenamiento del servidor. A continuación, se realiza una copia de seguridad de los espacios de archivos en Unicode. Puede utilizar este parámetro para los clientes de IBM Spectrum Protect activados para Unicode que utilizan los sistemas operativos Windows, Macintosh OS X y NetWare. Importante: Una vez que se ha instalado el cliente que admite Unicode, los nuevos espacios de archivos de los que el cliente hace una copia de seguridad se almacenan en el almacenamiento del servidor utilizando la página de códigos UTF-8. UTF-8 es un formato de codificación orientado a bytes que especifica el estándar de Unicode.

Puede especificar uno de los siguientes valores:

##### Yes

El servidor redetermina automáticamente los espacios de archivos existentes cuando el sistema cliente se actualiza en un cliente que tiene soporte para Unicode, y el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial. La redeterminación se produce si el cliente utiliza una interfaz gráfica de usuario, la línea de comandos o el planificador cliente.

Por ejemplo, el servidor redetermina una unidad del siguiente modo:

- Nombre original: D\_DRIVE
- Nombre nuevo: D\_DRIVE\_OLD

El nombre nuevo indica que el espacio de archivos se almacena en el servidor en un formato que no es Unicode.

##### No

El servidor no redetermina automáticamente los espacios de archivos cuando el sistema cliente se actualiza en un cliente que tiene soporte para Unicode, y el cliente ejecuta una de las operaciones siguientes: archivado, copia de seguridad selectiva, copia de seguridad incremental completa o copia de seguridad incremental parcial.

##### Client

La opción AUTOFSRENAME en el archivo de opciones del cliente determina si los espacios de archivos están redeterminados.



De forma predeterminada, la opción de cliente se define en PROMPT. Cuando el sistema cliente se actualiza en un cliente compatible con Unicode y el cliente realiza una operación de IBM Spectrum Protect con la interfaz gráfica de usuario o la línea de mandatos, el programa pregunta una vez al usuario si desea cambiar el nombre los espacios de archivos.

Cuando el planificador cliente realiza una operación, el programa no ofrece ninguna solicitud sobre red denominación y no red denomina los espacios de archivos. Las copias de seguridad de los espacios de archivos existentes se envían como antes (no en Unicode).

#### VALIDateprotocol (en desuso)

Especifica si IBM Spectrum Protect realiza una comprobación de redundancia cíclica para validar los datos enviados entre el cliente y el servidor. El parámetro es opcional.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

#### TXNGroupmax

Especifica el número máximo de archivos que se transferirán como un grupo entre un cliente y un servidor entres puntos de validación de transacciones. El rendimiento del cliente se puede mejorar empleando un valor mayor para esta opción.

Al especificar 0 se indica que el nodo utiliza el valor global del servidor establecido en el archivo de opciones del servidor. Si desea emplear un valor distinto del valor global del servidor, especifique un valor entre 4 y 65.000 para este parámetro. El valor del nodo prevalece sobre el valor del servidor.

Consejo: Si aumenta el valor de TXNGROUPMAX, aumenta la utilización de las anotaciones de recuperación. Una mayor utilización de las anotaciones de recuperación puede incrementar el riesgo de quedarse sin espacio de anotaciones. Evalúe el rendimiento de cada uno de los nodos antes de cambiar este parámetro.

#### DATAWritepath

Especifica la ruta de transferencia empleada cuando el cliente envía datos al servidor, agente de almacenamiento o ambos durante las operaciones de almacenamiento tales como copia de seguridad o archivado. El parámetro es opcional.

Recuerde: Si no hay disponible una ruta, el nodo no puede enviar ningún dato. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará.

Puede especificar uno de los siguientes valores:

##### ANY

Especifica que los datos se envían al servidor, agente de almacenamiento o a ambos mediante cualquier ruta disponible. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se mueven a través de la LAN.

##### LAN

Especifica que los datos se envían a través de la LAN.

##### LANFree

Especifica que los datos se envían a través de una ruta fuera de la LAN.

#### DATAReadpath

Especifica la ruta de transferencia empleada cuando el servidor, agente de almacenamiento, o ambos, leen datos para un cliente durante operaciones tales como restauración o recuperación. El parámetro es opcional.

Recuerde: Si no hay disponible una ruta, no es posible leer datos. Por ejemplo, si selecciona la opción de fuera de la LAN pero no se ha definido una ruta fuera de la LAN, la operación no funcionará. El valor de la vía de acceso de transferencia también se aplica a las conexiones de migración tras error. Si el valor se establece en LANFree, puede producirse la migración tras error para el nodo en el servidor secundario.

Puede especificar uno de los siguientes valores:

##### ANY

Especifica que el servidor, agente de almacenamiento o ambos utilizan cualquier ruta disponible para leer datos. Se utiliza una ruta fuera de la LAN si hay alguna disponible. Si no hay ninguna ruta fuera de la LAN disponible, los datos se leen a través de la LAN.

##### LAN

Especifica que los datos se leen a través de la LAN.

##### LANFree

Especifica que los datos se leen utilizando una ruta fuera de la LAN.

#### SESSIONINITiation

Controla si el servidor o el cliente ha de iniciar las sesiones. El parámetro es opcional.

#### Clientorserver

Especifica que el cliente puede iniciar sesiones con el servidor comunicándose en el puerto TCP/IP que se ha definido con la opción TCPPOINT. También puede utilizarse la planificación por petición de servidor para solicitar al cliente que se conecte con el servidor.

#### SERVEROnly

Especifica que el servidor no acepta peticiones de sesiones del cliente. Todas las sesiones deberá iniciarlas la planificación por petición de servidor en el puerto que se ha definido para el cliente con los mandatos REGISTER o UPDATE NODE. No se puede utilizar Client Acceptor, dsmdcad, para iniciar el planificador si SESSIONINITIATION está establecido en SERVERONLY.

#### HLAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

#### LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro debe utilizarse cuando SESSIONINITIATION está establecido en SERVERONLY, independientemente de las direcciones utilizadas anteriormente por el cliente para contactar con el servidor.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

#### HLAddress

Especifica la dirección IP del cliente que el servidor utiliza para iniciar los eventos planificados. Este parámetro opcional sólo se utiliza cuando se define SESSIONINITIATION con el valor SERVERONLY, independientemente de las direcciones que el cliente haya utilizado anteriormente para contactar con el servidor. Si SESSIONINITIATION SERVERONLY no está en uso, la opción no tendrá ningún efecto.

La dirección puede especificarse en formato numérico o en formato de nombres de host. Si se utiliza una dirección con formato numérico, ésta se guarda sin que el servidor de nombres de dominios la verifique. Si la dirección no es correcta, puede dar lugar a que se produzcan anomalías cuando el servidor intente establecer contacto con el cliente. Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. Los nombres verificados se guardan y se resuelven con los Servicios de nombres de dominios cuando el servidor establece el contacto con el cliente.

#### LLAddress

Especifica el número de puerto en el que el cliente está a la escucha de las sesiones del servidor. Este parámetro opcional sólo se utiliza cuando se define SESSIONINITIATION con el valor SERVERONLY, independientemente de las direcciones que el cliente haya utilizado anteriormente para contactar con el servidor. Si SESSIONINITIATION SERVERONLY no está en uso, la opción no tendrá ningún efecto.

El valor de este parámetro debe coincidir con el valor de la opción de cliente TCPCLIENTPORT. El valor predeterminado es 1501.

#### EMAILAddress

Este parámetro se utiliza para obtener más información de contacto. IBM Spectrum Protect no actúa en la información especificada por este parámetro.

#### DEDUPLICATION

Especifica dónde puede producirse la eliminación de datos duplicados para este nodo. Puede especificar uno de los siguientes valores:

##### SERVEROnly

Especifica que los datos almacenados por este nodo sólo se pueden deduplicar en el servidor.

##### Clientserver

Indica que los datos almacenados por este nodo se pueden deduplicar en el cliente o en el servidor. Para realizar la eliminación de datos duplicados en el cliente, debe especificar el valor YES en la opción de cliente

DEDUPLICATION. Puede especificar esta opción en el archivo de opciones del cliente o en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

#### TARGETLevel

Especifica el paquete de despliegue del cliente que se utiliza este nodo. Puede sustituir por un paquete de release aplicable V.R.M.F (Version.Release.Modification.Fix) Level. Por ejemplo: `TARGETLevel=6.2.0.0`.

Debe especificar cada segmento con un número aplicable a un paquete de despliegue. No se puede utilizar el asterisco en ningún campo como sustituto de un número válido. Para suprimir un valor existente, especifique una serie nula (" "). El parámetro es opcional.

Restricción: El parámetro TARGETLEVEL no se aplica a los nodos con un tipo NAS o SERVER.

#### BACKUPINITiation

Especifica si el ID de usuario no root en el nodo de cliente puede realizar una copia de seguridad de los archivos en el servidor. El parámetro es opcional. El valor predeterminado es ALL, que indica que los ID de usuario no root pueden realizar una copia de seguridad de los datos en el servidor. Puede seleccionar uno de los siguientes valores:

##### All

Especifica que los ID de usuario no root pueden realizar una copia de seguridad de los archivos en el servidor. ALL es el valor predeterminado si no se especifica BACKUPINITIATION.

##### ROOT

Especifica que sólo el ID de usuario root puede realizar una copia de seguridad de los archivos en el servidor.

Restricción: El servidor ignora el atributo si el cliente de archivado y copia de seguridad se conecta desde un sistema operativo distinto de AIX, Linux, Solaris o Mac OS.

#### BKREPLRuledefault, ARREPLRuledefault, y SPREPLRuledefault

Especifica la regla de réplica que se aplica a un tipo de datos si las reglas del espacio de archivos del tipo de datos se establecen en DEFAULT:

##### BKREPLRuledefault

Especifica la regla de réplica de los datos de copia de seguridad.

##### ARREPLRuledefault

Especifica la regla de réplica de los datos de archivado.

##### SPREPLRuledefault

Especifica la regla de réplica de los datos gestionados por espacio.

Puede especificar reglas de réplica de prioridad normal o de prioridad alta. En un proceso de réplica que incluye datos de prioridad normal y alta, los datos de prioridad alta se replican primero. Antes de especificar una regla, tenga en cuenta el orden en el que desea que se repliquen los datos.

Por ejemplo, supongamos que un nodo cliente contiene datos de archivado y datos de copia de seguridad activos. La réplica de los datos de copia de seguridad activos tiene una prioridad más alta que los datos de archivado. Para dar prioridad a ambos tipos de datos, especifique `BKREPLRULEDEFAULT=ACTIVE_DATA_HIGH_PRIORITY` `ARREPLRULEDEFAULT=ALL_DATA`.

Puede especificar las siguientes reglas:

##### ALL\_DATA

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio.

Los datos se replican con una prioridad normal.

##### ACTIVE\_DATA

Sólo replica datos de copia de seguridad activos. Los datos se replican con una prioridad normal. Esta regla sólo es válida para BKREPLRULEDEFAULT.

Atención:

Si especifica ACTIVE\_DATA y se cumplen una o más de las condiciones siguientes, los datos de copia de seguridad inactivos en el servidor de réplica de destino se suprimen y no se replican los datos de copia de seguridad inactivos en el servidor de réplica de origen.

- Cuando se instala una versión anterior a la Versión 7.1.1 en los servidores de réplica de origen o de destino.
- Cuando se utiliza el mandato REPLICATE NODE con el parámetro `FORCERECONCILE=YES`.
- Cuando se ejecuta la réplica inicial de un espacio de archivos después de configurar la duplicación, restaurar la base de datos, o actualizar los servidores de réplica de origen y destino de una versión anterior a V7.1.1.

Si las condiciones anteriores no son verdaderas, se duplican todos los archivos nuevos y cambiados desde la última réplica, incluidos los archivos inactivos, y los archivos se suprimen cuando caducan.

##### ALL\_DATA\_HIGH\_PRIORITY

Replica los datos de copia de seguridad activos e inactivos, los datos de archivado o los datos gestionados por espacio. Los datos se replican con una prioridad alta.

#### ACTIVE\_DATA\_HIGH\_PRIORITY

Esta regla es la misma que la regla de réplica ACTIVE\_DATA excepto que los datos se replican con una prioridad alta. Esta regla sólo es válida para BKREPLRULEDEFAULT.

#### DEFAULT

Replica los datos según la regla de réplica del servidor para los datos de copia de seguridad.

Por ejemplo, supongamos que desea replicar los datos de archivado en todos los espacios de archivo que pertenecen a un nodo de cliente. La réplica de los datos de archivado tiene una prioridad alta. Un método para realizar esta tarea es especificar `ARREPLRULEDEFAULT=DEFAULT`. Asegúrese de que las reglas de espacio de archivos de los datos de archivado también se establezcan en DEFAULT y que la regla del servidor de los datos de archivado se establezca en `ALL_DATA_HIGH_PRIORITY`.

Restricción: Si se configura un nodo para la réplica, las reglas de espacio de archivos se establecen en DEFAULT después de que el nodo almacene datos en el servidor de réplica de origen.

#### NONE

Los datos del tipo especificado no se replican.

Por ejemplo, si no desea replicar los datos gestionados por espacio que pertenecen a un nodo de cliente, especifique `SREPLRULEDEFAULT=NONE`

#### REPLState

Especifica si los datos que pertenecen al nodo de cliente están preparados para replicarse. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### Enabled

Especifica que el nodo de cliente está preparado para la réplica.

##### Disabled

Especifica que la réplica no se realiza hasta que la activa.

La respuesta del sistema a estos valores depende de los siguientes factores:

Si la definición de nodo de cliente existe sólo en el servidor de réplica de origen y está configurando el nodo de cliente para la réplica por primera vez

Si establece el estado de réplica en ENABLED o DISABLED, la modalidad de réplica del nodo en el servidor de réplica de origen se establece automáticamente en SEND después de que se emita el mandato UPDATE NODE. Cuando se realiza la réplica por primera vez, se crea automáticamente una definición de nodo de cliente en el servidor de destino. El estado de réplica del nodo de cliente en el servidor de destino se establece automáticamente en ENABLED. La modalidad de réplica se establece en RECEIVE.

Si la definición de nodo de cliente existe en los servidores de réplica de origen y destino, y los datos del nodo se han replicado previamente.

Para que se produzca la réplica, el estado de réplica del nodo de cliente en los servidores de origen y destino debe establecerse en ENABLED. Por ejemplo, si el estado de réplica de un nodo de cliente en el servidor de origen es ENABLED y el estado de réplica en el servidor de destino es DISABLED, la réplica no se realiza.

Si la definición de nodo de cliente existe en los servidores de réplica de origen y destino, y los datos del nodo se han exportado previamente desde el servidor de réplica de origen y se han importado al servidor de réplica de destino.

En este caso, está configurando los nodos de cliente para sincronizar los datos entre los dos servidores. Cuando se realiza la réplica por primera vez, el estado de réplica del nodo de cliente en el servidor de destino se establece automáticamente en ENABLED. Los datos en los servidores de origen y destino se sincronizan.

Restricción: Para sincronizar los datos, debe especificar el parámetro REPLMODE además del parámetro REPLSTATE.

Puede especificar el parámetro REPLMODE solo si nunca se ha replicado el nodo de cliente:

- Si la definición de nodo de cliente sólo existe en el servidor de réplica de origen, la modalidad de réplica del nodo en el servidor de réplica de origen se establece automáticamente en SEND cuando se emite el comando UPDATE NODE. La modalidad de réplica del nodo en el servidor de réplica de destino se establece automáticamente en RECEIVE.
- Si datos que pertenecen al nodo se han replicado previamente, la modalidad de réplica del nodo en el servidor de réplica de origen es SEND. La modalidad de réplica del nodo en el servidor de réplica de destino es RECEIVE.

#### REPLMode

Especifica si se deben sincronizar los datos que pertenecen a este nodo de cliente. Especifique este parámetro sólo si los datos que pertenecen al nodo de cliente se han exportado desde el servidor de réplica de origen y se han importado al servidor de réplica de destino. La sincronización se produce durante la réplica.

Para sincronizar los datos, debe emitir el mandato UPDATE NODE en los servidores de réplica de origen y destino, y especificar los parámetros REPLMODE y REPLSTATE. El valor que especifica para el parámetro REPLMODE depende de si el servidor es un

origen o un destino de los datos replicados.

Puede especificar uno de los siguientes valores:

#### SYNCSEnd

Especifica que los datos que pertenecen a este nodo de cliente se sincronizan con los datos en un servidor de destino durante la réplica. Especifique este valor sólo en el servidor que ha exportado los datos. Cuando la sincronización finaliza, la modalidad de réplica del nodo de cliente en el servidor de origen se establece automáticamente en SEND. La modalidad de réplica permanece en SEND a no ser que elimine el nodo emitiendo el comando REMOVE REPLNODE.

#### SYNCRECeive

Especifica que los datos que pertenecen a este nodo de cliente se sincronizan con los datos en un servidor de origen durante la réplica. Especifique este valor sólo en el servidor que ha importado los datos. Cuando la sincronización finaliza, la modalidad de réplica del nodo de cliente en el servidor de destino se establece automáticamente en RECEIVE. La modalidad de réplica permanece en RECEIVE a no ser que elimine el nodo emitiendo el comando REMOVE REPLNODE.

Restricciones:

- Puede establecer el parámetro REPLMODE solo si el estado de réplica inicial es NONE. Para sincronizar los datos, cambie el estado de réplica a ENABLED o DISABLED y especifique un valor para el parámetro REPLMODE.
- Los datos sólo pueden sincronizarse si especifica DATES=ABSOLUTE en el comando IMPORT NODE. Si ha especificado DATES=RELATIVE para importar datos, debe renombrar el nodo o suprimir sus datos antes de realizar la réplica. Si no sigue una de estas indicaciones, puede perder datos.
- Si el parámetro REPLMODE se ha establecido incorrectamente, debe emitir el mandato REMOVE REPLNODE antes de actualizar la definición del nodo de cliente. Por ejemplo, supongamos que ha actualizado la definición de un nodo de cliente cuyos datos deseaba replicar. Los datos que pertenecen al nodo se han exportado previamente al servidor de réplica de destino. Ha especificado ENABLED como el valor del parámetro REPLSTATE. Sin embargo, no ha especificado SYNCSEND en el servidor de réplica de origen. Como resultado, el parámetro REPLMODE se ha establecido automáticamente en SEND, y los datos pertenecientes al nodo no se han podido sincronizar o replicar.

La emisión de REMOVE REPLNODE establece el estado de réplica y la modalidad de réplica en NONE. Cuando finalice el comando REMOVE REPLNODE, vuelva a emitir el comando UPDATE NODE con los valores y los parámetros correctos.

#### RECOVERDamaged

Especifica si los archivos dañados pueden recuperarse para este nodo desde un servidor de réplica de destino. El parámetro es opcional. El valor predeterminado es YES. Puede especificar uno de los siguientes valores:

Yes

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino está habilitada para este nodo.

No

Especifica que la recuperación de archivos dañados a partir de un servidor de réplica de destino no está habilitada para este nodo.

Consejo: El valor del parámetro RECOVERDAMAGED es sólo uno de varios valores que determinan si se recuperan los archivos dañados. Para obtener información sobre cómo especificar los valores, consulte Valores que afectan a la recuperación de archivos dañados.

#### ROLEOVERRIDE

Especifica si se debe alterar temporalmente el rol notificado del cliente para la creación de informes de estimación de unidades de valor de procesador (PVU). El valor predeterminado es USEREPORTED.

El rol notificado por el cliente es un dispositivo de cliente (por ejemplo, una estación de trabajo) o un dispositivo de servidor (por ejemplo, un servidor de archivos/impresión, un servidor de aplicaciones o una base de datos). De forma predeterminada, el cliente notifica su rol basándose en el tipo de cliente y el sistema operativo. Todos los clientes notifican inicialmente su rol como dispositivo de servidor, excepto los clientes de archivado y copia de seguridad de IBM Spectrum Protect que ejecutan distribuciones de estaciones de trabajo de Microsoft Windows (Windows Vista) y Macintosh OS X.

Especifique uno de los siguientes valores:

Client

Especifica un dispositivo de cliente.

Server

Especifica un dispositivo de servidor.

Otro

Especifica que este nodo no se va a utilizar para la creación de informes de estimaciones de PVU. El valor Otro es útil cuando se despliegan varios nodos para un sistema físico (por ejemplo, entornos virtuales, nodos de prueba, nodos retirados y nodos que no estén en producción ni en clúster).

#### Usereported

Utilice el rol notificado que proporciona el cliente.

#### AUTHentication

Este parámetro determina el método de autenticación de la contraseña que utiliza; LDAP o local.

#### LOcal

Especifica que el nodo utiliza la base de datos del servidor de IBM Spectrum Protect local para almacenar las contraseñas.

#### LDap

Especifica que el nodo utiliza un servidor de directorios LDAP para autenticar las contraseñas. Las contraseñas no se almacenan en la base de datos de IBM Spectrum Protect.

#### SYNCldapdelete

Este parámetro solo se aplica si desea que un nodo que se autentica en un servidor de directorios LDAP (Lightweight Directory Access Protocol) pase a autenticarse con IBM Spectrum Protect. El parámetro especifica si se ha de eliminar el nodo del servidor LDAP.

#### Sí

Especifica que el nodo se elimina.

Restricción: No especifique el valor YES. (El valor de YES resulta adecuado solamente para usuarios del método de autenticación LDAP anterior, que se describe en Gestión de contraseñas y procedimientos de inicio de sesión).

#### No

Especifica que el nodo no se elimina. Este es el valor predeterminado.

#### SSLrequired (en desuso)

Especifica si el nodo debe utilizar el protocolo de capa de sockets seguros (SSL) para comunicarse con el servidor de IBM Spectrum Protect. El parámetro es opcional. Al autenticar contraseñas con un servidor de directorios LDAP, debe proteger las sesiones utilizando SSL u otro método de seguridad de red.

Importante: A partir de V8.1.2, este parámetro está en desuso. La validación que estaba habilitada por este parámetro de sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro SSLREQUIRED se ignora. Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

#### SESSIONSECurity

Especifica si el nodo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

#### STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor y el nodo. Para especificar si el servidor utilizará TLS 1.2 durante toda la sesión o solo para la autenticación, consulte la opción de cliente SSL.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el nodo pueda autenticarse en el servidor:

- Tanto el nodo como el servidor deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el nodo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre el servidor y el nodo.

Los nodos que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en el servidor.

#### TRANSitional

Especifica que se aplicarán los valores de seguridad más estrictos para el nodo. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el nodo no cumple nunca los requisitos para el valor STRICT, el nodo continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un nodo cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el nodo ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, el nodo ya no se puede autenticar con un protocolo menos seguro. Por ejemplo, si se actualiza un nodo que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, cuando el nodo se autentica en el servidor IBM Spectrum Protect como nodo de otro servidor.

#### SPLITLARGEObjects

Especifica si los objetos grandes que están almacenados por este nodo los divide en partes más pequeñas el servidor para optimizar su proceso. Si se especifica Sí, el servidor divide los objetos grandes (más de 10 GB) en partes más pequeñas cuando se almacenan en un nodo de cliente. Si se especifica No, se ignora este proceso. Especifique No solo si lo que pretende es maximizar el rendimiento de las copias de seguridad directamente en la cinta. El valor predeterminado es Yes (sí).

## Ejemplo: Actualice el nodo SIMON para que se autentique con un servidor de directorios LDAP y se conecte utilizando SSL

---

```
update node simon authentication=ldap sslrequired=yes
```

Cuando especifica el parámetro SSLREQUIRED, el servidor no se configura automáticamente para SSL. Debe seguir las instrucciones para conectarse a SSL para que el ejemplo funcione.

## Ejemplo: Actualizar todos los nodos para comunicarse con un servidor utilizando la seguridad de sesión estricta.

---

Actualice todos los nodos para utilizar la configuración de seguridad más estricta para autenticarse en el servidor.

```
update node * sessionsecurity=strict
```

## Ejemplo: actualizar un nodo con información de release de software para un futuro despliegue

---

La característica de despliegue de cliente permite actualizar un cliente de archivado y copia de seguridad a un nuevo release. La información que se genera a partir del mandato UPDATE NODE le ayudará cuando planifique un despliegue. La información se almacena para un futuro despliegue y puede verse emitiendo el comando QUERY NODE. Después del despliegue, puede emitir el comando QUERY NODE para ver el nivel actual y el nivel de destino. En este ejemplo, para actualizar el nodo LARRY al cliente de archivado y copia de seguridad versión 6.3.0.0.

```
update node LARRY targetlevel=6.3.0.0
```

## Ejemplo: actualizar la copia de seguridad de un nodo para comprimir los datos e impedir que el cliente pueda suprimir copias archivadas

---

Actualice el nodo LARRY para que los datos del nodo LARRY se compriman cuando IBM Spectrum Protect realice la copia de seguridad o el archivado de éstos, de modo que el cliente no pueda suprimir las copias archivadas.

```
update node larry compression=yes archdelete=no
```

## Ejemplo: actualizar el número de archivos de un nodo que pueden transferirse como grupo

---

Actualizar el nodo LARRY e incrementar el valor TXNGroupmax a 1.000.

```
update node larry txngroupmax=1000
```

## Ejemplo: actualización de un nodo y optimización de almacenamiento en el cliente

---

Actualice un nodo BOB para que puedan eliminarse los duplicados en el cliente.

```
update node bob deduplication=clientorserver
```

## Ejemplo: actualizar el rol del nodo BOB a un dispositivo de servidor para la creación de informes de estimación de PVU

---

Si desea acumular valores PVU, sólo se registran roles del dispositivo de servidor. Puede actualizar un nodo desde un dispositivo de cliente a un dispositivo de servidor emitiendo el mandato UPDATE NODE. En este ejemplo, el nodo BOB se actualiza a un dispositivo de servidor.

```
update node bob role=server
```

## Ejemplo: actualizar una definición de nodo en un servidor de réplica de origen

---

NODE1 está definido en un servidor de réplica de origen. Los datos que pertenecen a NODE1 se han exportado previamente a un servidor de réplica de destino. Actualice la regla de réplica para los datos de copia de seguridad que pertenecen a NODE1, para que los datos de copia de seguridad activos se repliquen con una prioridad alta. Active la réplica para el nodo. Configure la sincronización de datos con el servidor de réplica de destino.

```
update node node1 bkreplruledefault=active_data_high_priority
replstate=enabled replmode=syncsend
```

## Ejemplo: actualizar una definición de nodo para habilitar la recuperación de archivos dañados

Actualizar el nodo PAYROLL para habilitar la recuperación de archivos dañados a partir de un servidor de réplica de destino.

```
update node payroll recoverdamaged=yes
```

## Comandos relacionados

Tabla 2. Comandos relacionados con UPDATE NODE

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PVUESTIMATE	Muestra una estimación de los dispositivos de cliente y los dispositivos de servidor que se están gestionando.
QUERY REPLNODE	Muestra información sobre el estado de réplica de un nodo de cliente.
REGISTER ADMIN	Define un nuevo administrador sin otorgar autorización de administración.
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
REMOVE REPLNODE	Elimina un nodo de la réplica.
RENAME NODE	Cambia el nombre de un nodo cliente.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
RESET PASSEXP	Restablece la caducidad de contraseña para nodos o administradores.
SET DEDUPVERIFICATIONLEVEL	Especifica el porcentaje de extensiones verificadas por el servidor durante la optimización de almacenamiento del lado del cliente.
SET PASSEXP	Especifica el número de días para que una contraseña caduque y deba cambiarse.
SET REPLRECOVERDAMAGED	Especifica si la réplica de nodo está habilitada para recuperar los archivos dañados a partir de un servidor de réplica de destino.
UPDATE ADMIN	Cambia la información de contraseña o de contacto asociada con cualquier administrador.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.

**Información relacionada:**

Opción de cliente SSL

## UPDATE NODEGROUP (Actualizar un grupo de nodos)

Utilice este comando para modificar la descripción de un grupo de nodos.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de políticas sin restricciones.

### Sintaxis



```
>>-UPDate NODEGroup--nombre_grupo----->
>--DESCRiption--==--descripci3n-----><
```

## Parámetros

nombre\_grupo

Especifica el nombre del grupo de nodos cuya descripción desea actualizar.

DESCRiption (Obligatorio)

Especifica una descripción del grupo de nodos. Este parámetro es necesario. La longitud máxima de la descripción es de 255 caracteres. Si la descripción contiene blancos, encierre toda la descripción entre comillas.

## Ejemplo: actualizar la descripción de un grupo de nodos

Actualizar el grupo de nodos, `group1`, con una nueva descripción.

```
update nodegroup group1 description="Recursos Humanos"
```

## Comandos relacionados



Tabla 1. Comandos relacionados con UPDATE NODEGROUP

Comando	Descripción
DEFINE BACKUPSET	Define un juego de copias de seguridad previamente generadas en un servidor.
DEFINE NODEGROUP	Define un grupo de nodos.
DEFINE NODEGROUPMEMBER	Añade un nodo de cliente a un grupo de nodos.
DELETE BACKUPSET	Suprime un juego de copias de seguridad.
DELETE NODEGROUP	Suprime un grupo de nodos.
DELETE NODEGROUPMEMBER	Suprime un nodo cliente de un grupo de colocación.
GENERATE BACKUPSET	Genera un juego de copias de seguridad de datos de un cliente.
QUERY BACKUPSET	Visualiza juegos de copias de seguridad.
QUERY NODEGROUP	Visualiza información sobre grupos de nodos.
UPDATE BACKUPSET	Actualiza un valor de retención asociado a un conjunto de copias de seguridad.




## UPDATE PATH (cambiar una ruta)

Utilice este mandato para actualizar una definición de ruta.

Se proporcionan descripciones de sintaxis y parámetros para los siguientes tipos de ruta.

- UPDATE PATH (Cambiar una ruta cuando el destino es una unidad)
- UPDATE PATH (Cambiar una ruta cuando el destino es una biblioteca)
-  Sistemas operativos AIX  Sistemas operativos Linux UPDATE PATH (Actualizar una ruta cuando el destino es una biblioteca ZOSMEDIA)

Si quiere obtener información detallada y actual sobre soporte de dispositivos, consulte el sitio web Dispositivos soportados correspondiente a su sistema operativo:

-  Sistemas operativos AIX  Sistemas operativos Windows Dispositivos compatibles con AIX y Windows
-  Sistemas operativos Linux Dispositivos compatibles con Linux

## Comandos relacionados

Tabla 1. Mandatos relacionados con UPDATE PATH

Comando	Descripción
---------	-------------

Comando	Descripción
DEFINE DATAMOVER	Define un transportador de datos en el servidor de IBM Spectrum Protect.
DEFINE DRIVE	Asigna una unidad a una biblioteca.
DEFINE LIBRARY	Define una biblioteca automatizada o manual.
DEFINE PATH	Define una ruta de un origen a un destino.
DELETE PATH	Suprime una ruta de un origen a un destino.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
UPDATE DATAMOVER	Cambia la definición para un transportador de datos.

## UPDATE PATH (Cambiar una ruta cuando el destino es una unidad)

Utilice esta sintaxis cuando actualice una definición de ruta a una unidad.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>-UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType-----+--DATAMover-+--+-----+----->
      '-SERVer----'   '-AUTODetect-----+--No--+-'
                          '-Yes-'
>--DESTType-----DRive--LIBRARY--nombre_biblioteca----->
>--+-----+-----+-----+----->
      '-DEVICE-----nombre_dispositivo-'   '-ONLine-----+--Yes+--'
                                          '-No--'
>--+-----+-----+-----+-----<
      |           .,----- . |
      |           v           | |
      '-DIRectory--nombre_directorio-+-'
```

### Parámetros

nombre\_origen (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

nombre\_destino (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

SRCType (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

DATAMover

Especifica que el origen es un transportador de datos.

SERVer

Especifica que el origen es un servidor o un agente de almacenamiento.

AUTODetect

Especifica si se detectará, reportará y actualizará automáticamente el número de serie de una unidad o biblioteca en IBM Spectrum Protect. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una unidad o a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente.

Yes

Especifica que el número de serie se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica a IBM Spectrum Protect.

**Importante:**

1. Si anteriormente no ha especificado un número de serie, AUTODETECT toma YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. AUTODETECT=YES en este comando modifica el número de serie que se ha establecido en el comando DEFINE DRIVE.
3. Si establece DESTTYPE=DRIVE y AUTODETECT=YES, el número de elemento de la unidad que se encuentra en la base de datos de IBM Spectrum Protect cambiará automáticamente para reflejar el mismo número de elemento que corresponde al número de serie de esa unidad. Esto se aplica a las unidades de una biblioteca SCSI. Para obtener más información acerca del número de elemento, consulte el comando DEFINE DRIVE.
4. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

**DESTType=DRive (Obligatorio)**


Especifica que el destino es una unidad. Cuando el destino es una unidad, debe especificar un nombre de biblioteca. Este parámetro es necesario.

**LIBRARY**


Especifica el nombre de la biblioteca a la que se asigna la unidad. La biblioteca debe estar ya definida en el servidor. Si la ruta es de un transportador de datos NAS a una biblioteca, la biblioteca debe tener el LIBTYPE establecido en SCSI, 349x o ACSLS.


**DEVICE**

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.

 Sistemas operativos AIXEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 1 para obtener ejemplos.


**Tabla 1. Ejemplos de nombres de dispositivos**

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos AIX/dev/rmt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM® System Storage Serie N: rst01


 Sistemas operativos LinuxEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 2 para obtener ejemplos.

**Tabla 2. Ejemplos de nombres de dispositivos**

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	/dev/tmscsi/mt3
De un agente de almacenamiento a una unidad (no una unidad FILE)	/dev/tmscsi/mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: rst01 Servidor de archivos NAS EMC Celerra: c436t011 IBM System Storage Serie N: rst01

 Sistemas operativos WindowsEl origen utiliza el nombre de dispositivo para acceder a la unidad. Consulte la Tabla 3 para obtener ejemplos.

**Tabla 3. Ejemplos de nombres de dispositivos**

De origen a destino	Ejemplo
De servidor a unidad (no una unidad FILE)	 Sistemas operativos Windowsmt3
De servidor a unidad (unidad REMOVABLEFILE)	e:
De un agente de almacenamiento a una unidad (no una unidad FILE)	mt3
Del agente de almacenamiento a una unidad cuando la unidad es una unidad lógica en una biblioteca FILE	FILE

De origen a destino	Ejemplo
De un transportador de datos NAS a una unidad	Servidor de archivos NAS NetApp: <code>rst01</code> Servidor de archivos NAS EMC Celerra: <code>c436t011</code> IBM System Storage Serie N: <code>rst01</code>

Importante:

- En las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo `/etc/ibmatl.conf`. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el comando `SYSCONFIG`. Utilice este comando para determinar nombres de dispositivos para las unidades:

```
sysconfig -t
```

#### ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Por ejemplo, si la ruta desde un transportador de datos a una unidad está en línea, pero el transportador de datos o la unidad está fuera de línea, no puede utilizar la ruta.

#### DIRectory


Especifica la ubicación o ubicaciones de directorio de un agente de almacenamiento para el acceso a los archivos de una biblioteca FILE. El parámetro DIRECTORY también se utiliza para los dispositivos de tipo REMOVABLEFILE. Para los dispositivos REMOVABLEFILE, el parámetro DIRECTORY proporciona información para el servidor (no un agente de almacenamiento) junto con el parámetro DRIVE para describir acceso al dispositivo. Este parámetro es opcional.

En los agentes de almacenamiento, este parámetro sólo es válido cuando se cumplen *todas* las condiciones siguientes:

- El tipo de origen es SERVER (lo que significa que se ha definido como servidor un agente de almacenamiento en este servidor).
- El nombre de origen es el nombre del agente de almacenamiento y *no* del servidor.
- El destino es una unidad lógica que forma parte de una biblioteca FILE.
- Si se han especificado varios directorios para la clase de dispositivo que se asocia a la biblioteca FILE, debe especificarse, para cada unidad de la biblioteca FILE, el mismo número de directorios con el parámetro DIRectory del comando DEFINE PATH. Los directorios de agente de almacenamiento no se validan en el servidor. Si se especifican directorios incorrectos, se puede producir una anomalía de tiempo de ejecución.

El nombre o nombres de directorio identifican las ubicaciones en las que el agente de almacenamiento lee y graba los archivos que representan volúmenes de almacenamiento para la clase de dispositivo FILE asociada a la biblioteca FILE. El valor predeterminado de DIRECTORY es el directorio del servidor en el momento en que se emite el comando.

Utilice un convenio de denominación que le permita asociar el directorio a una unidad física determinada. Esto ayuda a garantizar que la configuración es válida para compartir la biblioteca FILE entre el servidor y el agente de almacenamiento. Si el agente de almacenamiento se encuentra en un sistema Windows, utilice un nombre del convenio de denominación universal (UNC). Cuando el agente de almacenamiento no disponga de permiso para acceder al almacenamiento remoto, el agente de almacenamiento sufrirá anomalías de montaje.

 Sistemas operativos Windows La cuenta asociada con el servicio del agente de almacenamiento debe ser una cuenta del grupo de administradores local o una cuenta del grupo de administradores del dominio. Si la cuenta está en el grupo de administradores local, el identificador de usuario y la contraseña deben corresponderse con los de la cuenta con autorización para acceder al almacenamiento, tal como fueron proporcionados por la máquina que administra los elementos compartidos remotos. Por ejemplo, si un servidor SAMBA proporciona acceso al almacenamiento remoto, el identificador de usuario y la contraseña de la configuración SAMBA deben coincidir con los del identificador de usuario y la contraseña del administrador local asociado al servicio del agente de almacenamiento.

```
define devclass file devtype=file shared=yes mountlimit=1
directory=d:\filedir\dir1
```


```
define path sta1 file1 srctype=server desttype=drive
library=file1 device=file directory=\\192.168.1.10\filedir\dir1
```

En el ejemplo anterior, el comando DEFINE DEVCLASS establece el sistema de archivos compartidos en el directorio al que el servidor accede como D:\FILEDIR\DIR1. No obstante, el agente de almacenamiento, está utilizando un nombre UNC \\192.168.1.10\FILEDIR\DIR1. Esto implica que la máquina con la dirección TCP/IP 192.168.1.10 está compartiendo el mismo directorio, que utiliza FILEDIR como nombre compartido. Asimismo, el servicio del agente de almacenamiento tiene una cuenta que puede acceder a este almacenamiento. Puede acceder a éste porque está asociado a una cuenta local con el mismo identificador de usuario y contraseña que 192.168.1.10 o a una cuenta de dominio disponible tanto en el agente de almacenamiento como en 192.168.1.10. Si es adecuado para la instalación, puede sustituir 192.168.1.10 por un nombre simbólico como:

example.yourcompany.com

Importante:


- IBM Spectrum Protect no crea recursos compartidos, permisos ni monta el sistema de archivos destino. Debe realizar estas acciones antes de iniciar el agente de almacenamiento.
- Sólo puede modificar una lista de directorios sustituyendo la lista completa.
- Debe asegurarse de que los agentes de almacenamiento puedan acceder a los volúmenes FILE recién creados. Para acceder a los volúmenes FILE, los agentes de almacenamiento sustituyen los nombres de la lista de directorios en la definición de clase de dispositivo por los nombres de la lista de directorios de la definición de ruta asociada. A continuación, se muestra la importancia de hacer corresponder clases de dispositivo y rutas para asegurarse de que los agentes de almacenamiento pueden acceder a volúmenes FILE recién creados.

Suponga que desea utilizar estos tres directorios en una biblioteca FILE:  Sistemas operativos Windows

- o c:\server
- o d:\server
- o e:\server

 Sistemas operativos AIX  Sistemas operativos Linux


- o /opt/tivoli1
- o /opt/tivoli2
- o /opt/tivoli3

1. Utilice el siguiente comando para configurar una biblioteca FILE denominada CLASSA con una unidad denominada CLASSA1 en SERVER1: 


```
define devclass classa devtype=file
directory="c:\server,d:\server,e:\server"
shared=yes mountlimit=1
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
define devclass classa devtype=file
directory="/opt/tivoli1,/opt/tivoli2,/opt/tivoli3"
shared=yes mountlimit=1
```



2. Desea que el agente de almacenamiento STA1 pueda utilizar la biblioteca FILE, por lo tanto, define la siguiente ruta para el agente de almacenamiento STA1: 


```
define path server1 sta1 srctype=server desttype=drive device=file
directory="\\192.168.1.10\c\server,\\192.168.1.10\d\server,
\\192.168.1.10\e\server" library=classa
```

 Sistemas operativos Windows En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio c:\server por el nombre de directorio \\192.168.1.10\c\server para poder acceder a los volúmenes FILE que se encuentran en el directorio c:\server del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux



```
define path server1 sta1 srctype=server desttype=drive device=file
directory="/opt/ibm1,/opt/ibm2,/opt/ibm3" library=classa
```

 Sistemas operativos AIX  Sistemas operativos Linux En este caso, el agente de almacenamiento, STA1, sustituirá el nombre de directorio /opt/tivoli1 por el nombre de directorio /opt/ibm1/ para poder acceder a los volúmenes FILE que se encuentran en el directorio /opt/tivoli1 del servidor.

3.  Sistemas operativos Windows SERVER1 crea el volumen de archivo c:\server\file1.dsm. Si cambia más adelante el primer directorio de la clase de dispositivo con el comando siguiente:

```
update devclass classa directory="c:\otherdir,d:\server,e:\server"
```

*SERVER1* todavía dispondrá de acceso al volumen de archivo `c:\server\file1.dsm`, pero el agente de almacenamiento *STA1* no podrá acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios `PATH`. Si no hay un nombre de directorio disponible en la lista de directorios asociados a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen `FILE` del directorio. Aunque todavía podrá accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen `FILE` puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

4.   Si se crea el volumen de archivo `/opt/tivoli1/file1.dsm` en *SERVER1*, y se emite el siguiente comando,

```
update devclass classa directory="/opt/otherdir,/opt/tivoli2,
/opt/tivoli3"
```

*SERVER1* todavía dispondrá de acceso al volumen de archivo `/opt/tivoli1/file1.dsm`, pero el agente de almacenamiento *STA1* no podrá acceder a éste porque ya no existe un nombre de directorio coincidente en la lista de directorios `PATH`. Si no hay un nombre de directorio disponible en la lista de directorios asociados a la clase de dispositivo, el agente de almacenamiento puede perder el acceso al volumen `FILE` del directorio. Aunque todavía podrá accederse al volumen desde el servidor para su lectura, si el agente de almacenamiento no puede acceder al volumen `FILE` puede hacer que las operaciones se reintenten en una ruta de sólo LAN o fallen.

## Ejemplo: definir una ruta desde un servidor de archivos NAS de transportador de datos hasta una unidad de cintas

Actualizar una ruta desde un transportador de datos, que es un servidor de archivos NAS, hasta la unidad *TAPEDRV2* que el transportador de datos utiliza para las operaciones de copia de seguridad y restauración. En este ejemplo, el transportador de datos NAS es *NAS1*, la biblioteca es *NASLIB* y el nombre de dispositivo de la unidad es *rst01*.

```
update path nas1 tapedrv2 srctype=datamover desttype=drive library=naslib
device=rst01
```

## UPDATE PATH (Cambiar una ruta cuando el destino es una biblioteca)

Utilice esta sintaxis cuando actualice una definición de ruta a una biblioteca.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

```
>>UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType-----+DATAMover+-----+----->
      '-SERVer----'  '-AUTODetect-----+No--+-'
                          '-Yes-'
>--DESTType-----LIBRARY--+-----+----->
      +-DEVIce-----nombre_dispositivo---+
      '-EXTERNALManager-----nombre_ruta-'
>+-----+-----><
      '-ONLine-----+Yes--+-'
                          '-No--'
```

### Parámetros

**nombre\_origen** (Obligatorio)

Especifica el nombre del origen de la ruta. Este parámetro es necesario.

**nombre\_destino** (Obligatorio)

Especifica el nombre del destino. Este parámetro es necesario.

Importante: Para definir una ruta de un transportador de datos NAS a una biblioteca, la biblioteca debe tener `LIBTYPE` establecido en `SCSI`, `349X` o `ACSL` (Automated Cartridge System Library Software).

**SRCType** (Obligatorio)

Especifica el tipo de origen. Este parámetro es necesario. Los valores posibles son:

`DATAMover`

SERVER  
Especifica que el origen es un transportador de datos.  
Especifica que el origen es un servidor o un agente de almacenamiento.

**AUTODetect**

Especifica si se detecta, notifica y actualiza automáticamente el número de serie de una unidad o biblioteca en IBM Spectrum Protect. Este parámetro es opcional. Este parámetro sólo es válido para las rutas que se han definido desde el servidor local a una biblioteca. Los valores posibles son:

No

Especifica que el número de serie no se actualizará automáticamente.

Yes

Especifica que el número de serie se actualiza automáticamente para reflejar el mismo número de serie que la unidad notifica a IBM Spectrum Protect.

Importante:

1. Si anteriormente no ha especificado un número de serie, AUTODETECT toma YES de forma predeterminada. Si anteriormente ha especificado un número de serie, AUTODETECT toma NO de forma predeterminada.
2. AUTODETECT=YES en este comando modifica el número de serie que se ha establecido en el comando DEFINE DRIVE.
3. En función de las posibilidades del dispositivo, puede que el parámetro AUTODETECT no esté admitido.

**DESTType=LIBRARY (Obligatorio)**

Especifica que el destino es una biblioteca. Este parámetro es necesario.

**DEVICE**

Especifica el nombre del dispositivo que identifica tal como lo identifica el origen, o FILE si el dispositivo es una unidad lógica en una biblioteca FILE.




 Sistemas operativos AIXEl origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 1 para obtener ejemplos.

Tabla 1. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos AIX/dev/lb4  Sistemas operativos Linux /dev/tsmcsci/lb4
De un transportador de datos NAS a una biblioteca	mc0


 Sistemas operativos LinuxEl origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 2 para obtener ejemplos.

Tabla 2. Ejemplos de nombres de dispositivos

De origen a destino	Ejemplo
De servidor a biblioteca	/dev/tsmcsci/lb4
De un transportador de datos NAS a una biblioteca	mc0



 Sistemas operativos WindowsEl origen utiliza el nombre de dispositivo para acceder a la unidad o biblioteca. Consulte la Tabla 3 para obtener ejemplos.

Tabla 3. Ejemplos de nombres de dispositivos


De origen a destino	Ejemplo
De servidor a biblioteca	 Sistemas operativos Windows lb4.1
De un transportador de datos NAS a una biblioteca	mc0

Importante:


- En las bibliotecas 349X, el nombre de alias es un nombre simbólico que se especifica en el archivo /etc/ibmatl.conf. Para obtener más información, consulte la publicación *IBM Tape Device Drivers Installation and User's Guide*, que puede descargarse del sitio de soporte de IBM® Systems en <http://www.ibm.com/support/docview.wss?uid=ssg1S7002972>.
- Para obtener información sobre cómo obtener nombres para dispositivos conectados a un servidor de archivos NAS, consulte la información del producto para el servidor de archivos. Por ejemplo, para un servidor de archivos NetApp, conéctese con el servidor de archivos mediante Telnet y emita el comando SYSCONFIG. Utilice este comando para determinar el nombre de dispositivo para una biblioteca:

```
sysconfig -m
```


**EXTERNALManager**

Especifica la ubicación del gestor de bibliotecas externo donde IBM Spectrum Protect puede enviar peticiones de acceso a medio. Especifique el valor de este parámetro entre comillas simples. Por ejemplo, especifique: Sistemas operativos AIX

/usr/lpp/GESedt-acsls/bin/elmdt

Sistemas operativos Linux

/opt/GESedt-acsls/bin/elmdt

Sistemas operativos Windows

C:\Archivos de programa\GES\EDT-ACSLs\bin\elmdt.exe

Este parámetro es necesario cuando el nombre de la biblioteca es una biblioteca externa.

#### ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.

No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Importante: Si la ruta a una biblioteca está desactivada, el servidor no podrá acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, no se inicializará la biblioteca.

Sistemas operativos AIX Sistemas operativos Linux

## UPDATE PATH (Actualizar una ruta cuando el destino es una biblioteca ZOSMEDIA)

---

Utilice esta sintaxis cuando actualice una ruta a una biblioteca ZOSMEDIA.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

### Sintaxis

---

```
>>-UPDate PATH--nombre_origen--nombre_destino----->
>--SRCType----SERVer--DESTType----LIBRary----->
>--ZOSMEDIASERVER----server_name--+-----+-----<
                                     '-ONLine-----+Yes+-'
                                     '-No--'
```

### Parámetros

---

nombre\_origen (Obligatorio)

Especifica el nombre del origen de la ruta.

nombre\_destino (Obligatorio)

Especifica el nombre del destino.

SRCType=SERVer (Obligatorio)

Especifica que el origen es el servidor de IBM Spectrum Protect o un agente de almacenamiento.

DESTType=LIBRary (Obligatorio)

Especifica que el destino es una biblioteca.

ZOSMEDIAServer (Obligatorio)

Especifica el nombre de servidor que representa un servidor de Tivoli Storage Manager for z/OS Media.

ONLine

Especifica si la ruta está disponible para utilizarla. Este parámetro es opcional. Los valores posibles son:

Yes

Especifica que la ruta está disponible para utilizarla.



No

Especifica que la ruta no está disponible para utilizarla.

El origen y el destino deben estar disponibles para utilizar la ruta.

Importante: Si la ruta a una biblioteca está desactivada, el servidor no puede acceder a la biblioteca. Si el servidor se detiene y se reinicia mientras la ruta a la biblioteca está desactivada, la biblioteca no se inicializa durante la inicialización del servidor. Se debe actualizar la ruta a ONLINE=YES para acceder a la biblioteca.

## UPDATE POLICYSET (Actualizar la descripción de un juego de políticas)

Utilice este comando para cambiar la descripción de un juego de políticas. No puede cambiar la descripción del juego de políticas ACTIVE.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

### Sintaxis

```
>>-UPDate Policyset--nombre_dominio--nombre_conjunto_políticas-->  
>--DESCRiption--===descripción-----><
```

### Parámetros

nombre\_dominio (Necesario)

Especifica el dominio de políticas al que pertenece el juego de políticas.

nombre\_juego\_políticas (Necesario)

Especifica el juego de políticas que se actualiza. No puede cambiar el juego de políticas ACTIVE.

DESCRiption (Obligatorio)

Especifica el texto que describe el juego de políticas. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("").

### Ejemplo: actualizar un juego de políticas

Actualizar un juego de políticas denominado VACATION para el dominio de políticas EMPLOYEE\_RECORDS con la descripción "Schedule Planning Information".

```
update policyset employee_records vacation  
description="schedule planning information"
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY MGMTCLASS	Crea una copia de una clase de gestión.
DEFINE DOMAIN	Define un dominio de políticas que puede asignarse a los clientes.
DEFINE MGMTCLASS	Define una clase de gestión.
DEFINE POLICYSET	Define un conjunto de políticas dentro del dominio de política especificado.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.

Comando	Descripción
VALIDATE POLICYSET	Verifica e informa acerca de las condiciones que ha de tener en cuenta el administrador antes de activar el juego de políticas.

## UPDATE PROFILE (Actualizar una descripción de perfil)

Utilice este comando en un gestor de configuración para actualizar una descripción de perfil.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UPDate PROFIle--nombre_perfil--DESCription---description--<<
```

### Parámetros

nombre\_perfil (Obligatorio)

Especifica el perfil que se actualiza.

DESCription (Obligatorio)

Especifica una descripción del perfil. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para eliminar una descripción, especifique una serie nula ("").

### Ejemplo: actualizar la descripción de un perfil

Actualizar la descripción del perfil DELTA.

```
update profile delta description="PAYROLL domain"
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE PROFILE

Comando	Descripción
COPY PROFILE	Crea una copia de un perfil.
DEFINE PROFASSOCIATION	Asocia objetos con un perfil.
DEFINE PROFILE	Define un perfil para distribuir información a los servidores gestionados.
DELETE PROFASSOCIATION	Suprime la asociación de un objeto con un perfil.
DELETE PROFILE	Suprime un perfil de un gestor de configuración.
LOCK PROFILE	Impide la distribución de un perfil de configuración.
QUERY PROFILE	Muestra información sobre perfiles de configuración.
SET CONFIGMANAGER	Especifica si un servidor es un gestor de configuración.
UNLOCK PROFILE	Activa la distribución de un perfil bloqueado a los servidores gestionados.

## UPDATE RECOVERYMEDIA (Actualizar medio de recuperación)

Utilice este comando para actualizar la información sobre los medios de recuperación.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```

>>-UPDate RECOVERYMedia--nombre_medio----->
>-----+-----+-----+-----+-----+-----+----->
|          .-.------. |
|          V             | |
|'-VOLumenames-----nombre_volumen+--'
>-----+-----+-----+-----+-----+-----+----->
|'-DESCription-----descripción-'
>-----+-----+-----+-----+-----+-----+----->
|'-LOcation-----ubicación-'  '-Type-----+--BOot--+-'
|                                 '-Other-'
>-----+-----+-----+-----+-----+-----+----->
|'-PRoDuct-----nombre_producto-'
>-----+-----+-----+-----+-----+-----+-----><
|'-PRoDUCTInfo-----información_producto-'

```

## Parámetros

### nombre\_soporte (Obligatorio)

Especifica el nombre del medio de recuperación que se ha de actualizar.

### VOLumenames

Especifica los de nombres de volúmenes que contienen datos recuperables (por ejemplo, copias de imágenes del sistema operativo). Si especifica TYPE=BOOT, debe especificar los nombres de los medios de arranque en el orden en que deben cargarse al efectuar la operación de recuperación. La lista de nombres de volúmenes puede tener hasta 255 caracteres. La lista debe estar delimitada por comillas si contiene algún carácter en blanco. Para eliminar todos los nombres de volúmenes, especifique una serie nula ("").

### DESCription

Especifica la descripción del medio de recuperación. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

### LOcation

Describe la ubicación del medio de recuperación. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para eliminar una descripción de ubicación, especifique una serie nula ("") como valor.

### Type

Especifica el tipo de medio de recuperación. Este parámetro es opcional. Los valores posibles son:

#### BOot

Especifica que este es un medio de arranque. Debe especificar los nombres de los volúmenes si el tipo es BOOT.

#### OTHer

Especifica que éste no es un medio de arranque. Por ejemplo, un CD que contiene los manuales del sistema operativo.

### PRoDuct

Especifica el nombre del producto que se ha grabado en este medio. Este parámetro es opcional. Puede utilizar hasta 16 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para suprimir un nombre de producto, especifique una serie nula ("") como valor.

### PRoDUCTInfo

Especifica la información acerca del producto que ha grabado en el medio que puede necesitar para restaurar la máquina. Este parámetro es opcional. Puede utilizar hasta 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco. Para eliminar la información del producto definida anteriormente, especifique una serie nula ("") para el valor.

## Ejemplo: actualizar la descripción de ubicación de los medios de recuperación

Actualizar la descripción de ubicación de los medios de recuperación DIST5RM por "Corporate Headquarters Data Vault."

```

update recoverymedia dist5rm
location="Corporate Headquarters Data Vault"

```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE RECOVERYMEDIA

Comando	Descripción
---------	-------------

Comando	Descripción
DEFINE RECOVERYMEDIA	Define el medio necesario para recuperar una máquina.
DELETE RECOVERYMEDIA	Suprime un medio de recuperación.
QUERY RECOVERYMEDIA	Muestra los medios disponibles para la recuperación de la máquina.

## UPDATE REPLRULE (Actualizar reglas de réplica)

Utilice este mandato para activar o desactivar una regla de réplica.

Emita este comando en el servidor que actúe como origen para los datos replicados.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UPDate REPLRule--nombre_regla----SState--====+-ENabled--++-----><
                                     '-DISabled-'
```

### Parámetros

nombre\_regla (Obligatorio)

Especifica el nombre de la regla de réplica que se va a actualizar. Puede utilizar caracteres comodín para especificar una o varias reglas. Puede especificar una de las reglas siguientes:

- ALL\_DATA
- ACTIVE\_DATA
- ALL\_DATA\_HIGH\_PRIORITY
- ACTIVE\_DATA\_HIGH\_PRIORITY

SState (Obligatorio)

Especifica si la réplica está permitida para la regla. Puede especificar uno de los siguientes valores:

ENabled

Especifica que los datos a los que se aplica la regla están preparados para replicarse.

DISabled

Especifica que la réplica no se realiza hasta que la activa.

### Ejemplo: desactivar la réplica de datos de copia de seguridad

Desactive la réplica de los datos de copia de seguridad activos, de prioridad normal, para todos los espacios de archivos de todos los nodos de cliente que están configurados para la réplica:

```
update replrule active_data state=disabled
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE REPLRULE

Comando	Descripción
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLICATION	Muestra información sobre los procesos de réplica de nodos.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.

Comando	Descripción
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.

## UPDATE SCHEDULE (Actualizar una planificación)

Utilice este comando para actualizar una planificación de cliente o de comando de administración.

El comando UPDATE SCHEDULE tiene dos formatos, dependiendo de si la planificación se aplica a las operaciones cliente o a comandos de administración. En estos dos formatos, puede seleccionar las planificaciones de estilo clásico o mejorado. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con UPDATE SCHEDULE

Comando	Descripción
COPY SCHEDULE	Crea una copia de una planificación.
DEFINE SCHEDULE	Define una planificación para una operación de cliente o para un comando de administración.
DELETE SCHEDULE	Suprime una planificación de la base de datos.
QUERY EVENT	Muestra información acerca de los eventos planificados y completados para clientes seleccionados.
QUERY SCHEDULE	Muestra información sobre planificaciones.
SET MAXCMDRETRIES	Especifica el número máximo de reintentos después de un intento no válido de ejecutar un comando planificado.
SET MAXSCHEDESESSIONS	Especifica el número máximo de sesiones cliente/servidor disponibles para procesar el trabajo planificado.
SET RETRYPERIOD	Especifica el período de tiempo entre reintentos del planificador del cliente.

- UPDATE SCHEDULE (Actualizar una planificación de cliente)  
Utilice el comando UPDATE SCHEDULE para actualizar parámetros seleccionados de una planificación de cliente.
- UPDATE SCHEDULE (Actualizar una planificación de administración)  
Utilice este comando para actualizar los parámetros seleccionados de una planificación de comandos de administración.

## UPDATE SCHEDULE (Actualizar una planificación de cliente)

Utilice el comando UPDATE SCHEDULE para actualizar parámetros seleccionados de una planificación de cliente.

Este comando no cambia las asociaciones de cliente que se han realizado en esta planificación. Todos los clientes asociados a la planificación original procesan la planificación modificada.

No todos los clientes pueden ejecutar todas las operaciones planificadas, aunque pueda definir la planificación en el servidor y asociar ésta al cliente. Por ejemplo, un cliente Macintosh no puede ejecutar una planificación cuando la acción sea restaurar o recuperar archivos o ejecutar un script ejecutable. En los diferentes sistemas operativos cliente, un script ejecutable, también se conoce como un archivo de comandos, un archivo por lotes o un script.

## Clase de privilegio

Para definir una planificación de cliente, debe tener privilegio de sistema, privilegio de políticas ilimitado o privilegio de políticas limitado al dominio de políticas al que pertenece la planificación.

## Sintaxis correspondiente a una planificación de cliente clásica

```

(1)
>>-UPDate SCHEDULE----->
>--nombre_dominio--nombre_planificación--+-----+----->
      '-Type-----Client-'
>+-----+----->
  '-DESCRIPTION-----descripción-'
>+-----+-----+----->
  '-ACTION-----+Incremental-----+-'
      +-Selectiva-----+
      +-Archive-----+
      |           |           |           |           |
      |           | '-SUBACTION-----+-----+-' |
      |           |           | '-FASTBack-' |
      +-Backup-----+-----+-----+
      |           |           |           |           |
      |           | '-SUBACTION-----+-----+-' |
      |           |           | '+FASTBack----+' |
      |           |           | '+SYSTEMState+' |
      |           |           | '-VM-----+' |
      +-REStore-----+-----+-----+
      +-REtrieve-----+-----+-----+
      +-IMAGEBACKup-----+-----+-----+
      +-IMAGERESTore-----+-----+-----+
      +-Command-----+-----+-----+
      +-Macro-----+-----+-----+
      '-Deploy-----+'
>+-----+-----+----->
  '-OPTIONS-----serie_opción-' '-OBJECTS-----serie_objeto-'
>+-----+-----+----->
  '-PRIORITY-----número-' '-STARTDate-----fecha-'
>+-----+-----+----->
  '-STARTTime-----hora-' '-DURATION -----número-'
>+-----+-----+-----+----->
  '-DURUnits-----+Minutes-----+' '-MAXRUNTime-----número-'
      +-Hours-----+
      +-Days-----+
      '-INDefinite-'
>+-----+-----+-----+----->
  '-SCHEDStyle-----Classic-' '-PERIOD-----número-'
>+-----+-----+-----+----->
  '-PERUnits-----+Hours-----+'
      +-Days-----+
      +-Weeks-----+
      +-Months-----+
      +-Years-----+
      '-Onetime-'
>+-----+-----+-----+----->
  '-DAYofweek-----+ANY-----+-'
      +-WEEKDay---+
      +-WEEKEnd---+
      +-SUNDay---+
      +-Monday---+
      +-TUESday---+
      +-WEDnesday--+
      +-THURsday--+
      +-FRIDay---+
      '-SATurday--'
>+-----+-----+-----+-----><
  '-EXPIration-----+Never--+-'

```

'-date--'

Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.

## Sintaxis correspondiente a una planificación de cliente mejorada

---

```
(1)
>>-UPDate SCHEDULE----->
>--nombre_dominio--nombre_planificación--+-----+----->
      '-Type-----Client-'
>--+-----+----->
      '-DESCRIPTION-----descripción-'
>--+-----+----->
      '-ACTION-----+Incremental-----+-'
          +-Selectiva-----+
          +-Archive--+-----+
          |           '-SUBACTION-----+' |
          |           '-FASTBack-' |
          +-Backup--+-----+
          |           '-SUBACTION-----+' |
          |           +-FASTBack----+ |
          |           +-SYSTEMState+ |
          |           +-VApp-----+ |
          |           '-VM-----' |
          +-REStore-----+
          +-REtrieve-----+
          +-IMAGEBACKup-----+
          +-IMAGERESTore-----+
          +-Command-----+
          '-Macro-----'
>--+-----+----->
      '-OPTIONS-----serie_opción-' '-OBJECTS-----serie_objeto-'
>--+-----+----->
      '-PRIORITY-----número-' '-STARTDate-----fecha-'
>--+-----+----->
      '-STARTTime-----hora-' '-DURATION -----número-'
>--+-----+----->
      '-DURUnits-----+Minutes+-' '-MAXRUNtime-----número-'
          +-Hours----+
          '-Days----'
>--+-----+----->
      '-SCHEDStyle-----Enhanced-' '-MONTH-----+ANY-----+'
          +-JANuary---+
          +-FebruAry---+
          +-MARCH-----+
          +-APRil-----+
          +-May-----+
          +-JUNe-----+
          +-JULy-----+
          +-AUGust----+
          +-September-+
          +-October---+
          +-November--+
          '-December--'
>--+-----+----->
      '-DAYOFMonth-----+ANY+-' '-WEEKofmonth-----+ANY-----+'
          '-Day-'
          +-First--+
          +-Second-+
          +-Third--+
          +-FOurth-+
          '-Last---'
>--+-----+----->
```

```

'-DAYofweek-----ANY-----+'
        +-WEEKDay---+
        +-WEEKEnd---+
        +-Sunday----+
        +-Monday----+
        +-TUesday---+
        +-Wednesday--+
        +-THursday--+
        +-Friday----+
        '-Saturday--'

>--+-----+-----<
    '-EXpiration-----Never-+-'
        '-date--'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.

## Parámetros

---

nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas al que pertenece la planificación.

nombre\_planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de actualizar.

Type=Client

Especifica que se actualiza una planificación de cliente. Este parámetro es opcional. El valor predeterminado es CLIENT.

DESCRIption

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("") para este valor.

ACTion

Especifica la acción que se produce cuando se procesa esta planificación. Los valores posibles son:

Incremental

Especifica que la planificación hace copia de seguridad de todos los archivos que son nuevos o que se han modificado desde la última copia de seguridad incremental. La copia de seguridad incremental también hace copia de seguridad de todos los archivos para el que se hayan podido caducar todas las copias de seguridad existentes.

Selective

Especifica que la planificación sólo hace copia de seguridad de los archivos especificados con el parámetro OBJECTS.

Archive

Especifica que la planificación hace copia archivada de los archivos especificados con el parámetro OBJECTS.

Backup

Especifica que la planificación realiza una copia de seguridad de los archivos especificados con el parámetro OBJECTS.

RESTore

Especifica que la planificación restaura los archivos especificados con el parámetro OBJECTS.

Cuando especifique ACTION=RESTORE para una operación planificada y se define la opción REPLACE como PROMPT, no se efectúa ninguna petición. Si establece la opción en PROMPT, se ignoran los archivos.

Si se especifica una segunda especificación de archivo, ésta actúa como destino de la restauración. Si necesita restaurar varios grupos de archivos, planifique una restauración para cada especificación de archivo que necesita restaurar.

RETRieve

Indica que la planificación recupera los archivos especificados con el parámetro OBJECTS.

Recuerde: Un segundo archivo especificado actúa como el destino de recuperación. Si necesita recuperar varios grupos de archivos, cree una planificación distinta para cada grupo de archivos.

IMAGEBACKup

Especifica que la planificación hace copia de seguridad de los volúmenes lógicos especificados con el parámetro OBJECTS.

IMAGERESTore

Especifica que la planificación restaura los volúmenes lógicos especificados con el parámetro OBJECTS.

Comando

Indica que la planificación procesa un comando de un sistema operativo de cliente o un script, especificado con el parámetro OBJECTS.

Macro

Especifica que un cliente procesa una macro cuyo nombre de archivo se especifica con el parámetro OBJECTS.



## SUBACTion

Puede especificar uno de los siguientes valores:

""

Cuando una serie vacía (dos dobles comillas) se especifica con ACTION=BACKUP, la copia de seguridad es incremental.

### FASTBacK

Especifica que una operación de cliente FastBack identificada por el parámetro ACTION se va a planificar para procesar. El parámetro ACTION debe ser ARCHIVE o BACKUP.

### SYSTEMState

Especifica que se ha programado una copia de seguridad del estado del sistema.

### VApp

Especifica que se planifique una copia de seguridad vApp del cliente. Una vApp es una recopilación de máquinas virtuales desplegadas previamente.

### VM

Especifica que se ha programado una copia de seguridad VMware del cliente.

## Deploy

Especifica si se actualizarán las estaciones de trabajo del cliente con paquetes de despliegue especificados con el parámetro OBJECTS. El parámetro OBJECTS debe contener dos especificaciones: los archivos del paquete que se deben recuperar y de dónde recuperarlos. Asegúrese de que los objetos están en orden *ubicación\_archivos*. Por ejemplo:

```
define schedule standard deploy_1 action=DEPLOY objects=  
"\\IBM_ANR_WIN\c$\tsm\maintenance\client\v6r2\Windows\X32\v620\v6200\  
..\IBM_ANR_WIN"
```

Los valores de las siguientes opciones estarán restringidos si se especifica ACTION=DEPLOY:

### PERUNITS

Especifique PERUNITS=ONETIME. Si especifica PERUNITS=PERIOD, el parámetro se omitirá.

### DURUNITS

Especifique MINUTES, HOURS o DAYS para el parámetro DURUNITS. No especifique INDEFINITE.

### SCHEDSTYLE

Especifique el estilo predeterminado, CLASSIC.


El comando SCHEDULE falla si los parámetros no coinciden con los valores de parámetro necesarios, como V.R.M.F.

## OPTions

Especifica las opciones que se especifican en el comando planificado en el momento en que se procesa la planificación. Este parámetro es opcional.

Con este parámetro únicamente se pueden especificar aquellas opciones que sean válidas en el comando planificado. Consulte el manual de cliente adecuado para obtener información sobre opciones válidas en la línea de comandos. Todas las opciones que se describen como válidas solamente en la línea de comandos inicial dan como resultado un error o se ignoran cuando se ejecuta la planificación desde el servidor. Por ejemplo, no incluya las opciones siguientes, ya que no tienen ningún efecto cuando el cliente procesa el comando planificado:

- MAXCMDRETRIES
- OPTFILE
- QUERYSCHEDPERIOD
- RETRYPERIOD
- SCHEDLOGNAME
- SCHEDMODE
- SERVERNAME
- TCPCLIENTADDRESS
- TCPCLIENTPORT

 Sistemas operativos Windows Cuando define un servicio de planificación mediante el comando DSMCUTIL o el asistente de la GUI del cliente de copia de seguridad/archivado, especifica un archivo de opciones. No es posible modificar temporalmente las opciones de dicho archivo de opciones emitiendo el comando planificado. Debe modificar las opciones en el servicio de planificación.

Si la serie de opciones contiene varias opciones y opciones con espacios intercalados, encierre toda la serie de opciones con un par de apóstrofes. Escriba las opciones individuales que contienen espacios entre comillas. Es necesario un signo menos delante de la opción. Se pueden producir errores si la serie de opciones contiene espacios que no se han incluido entre comillas.

Los ejemplos siguientes muestran cómo especificar algunas opciones de cliente:

- Para especificar `subdir=yes` y `domain all-local -systemobject`, escriba:

- options='-subdir=yes -domain="all-local -c: -systemobject"'
- Para especificar domain all-local -c: -d:, escriba:
  - options='-domain="all-local -c: -d:"'

#### Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

#### OBJECTS

Especifica los objetos para los que se realiza la acción especificada. Utilice un único espacio entre cada objeto. Este parámetro es necesario excepto cuando ACTION=INCREMENTAL. Si la acción es una operación de copia de seguridad, archivado, restauración o recuperación, los objetos serán espacios de archivos, directorios o volúmenes lógicos. Si la acción consiste en ejecutar un comando o una macro, el objeto será el nombre del comando o macro que debe ejecutarse.

Si especifica ACTION=INCREMENTAL sin especificar ningún valor para este parámetro, el comando planificado se invoca sin los objetos especificados e intenta procesar los objetos según están definidos en el archivo de opciones del cliente. Para seleccionar todos los espacios de archivos o directorios para una acción, enumérellos explícitamente en la serie de objetos. Si se especifica solamente un asterisco en la serie de objetos, la operación de copia de seguridad se producirá solamente en el directorio en el que se ha iniciado el planificador.

#### Importante:

- Si se especifica una segunda especificación de archivo, y ésta no es un destino válido, se recibirá el siguiente error:


```
ANS1082E Se ha escrito una especificación de archivo de
destino <espec_archivo> no válida.
```

- Si se especifican más de dos especificaciones de archivo, se recibirá el error siguiente:



```
ANS1102E Se han pasado al programa un número
excesivo de argumentos de línea de
comandos
```

Si especifica ACTION=ARCHIVE, INCREMENTAL o SELECTIVE para este parámetro, puede ver una lista de hasta veinte (20) especificaciones de archivo.

Incluya la serie de objetos archivos entre comillas si contiene caracteres (espacios) en blanco y luego incluya las comillas entre apóstrofes. Si la serie de objetos contiene varios nombres de archivo, incluya cada nombre de archivo entre comillas e incluya toda la serie en un par de apóstrofes. Se pueden producir errores si los nombres de archivo contienen un espacio que no se ha incluido entre comillas correctamente.

 Sistemas operativos Windows Si utiliza caracteres que pueden tener un significado especial para los usuarios de Windows como, por ejemplo, las comas, incluya el argumento completo entre comillas dobles e incluya toda la serie entre comillas simples. Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar C:\ARCHIVO 2, D:\ARCHIVOS GIF y E:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="'C:\ARCHIVO 2' 'D:\ARCHIVOS GIF' 'E:\ARCHIVO DE PRUEBA'"'
- Para especificar D:\ARCHIVO DE PRUEBA, escriba:
  - OBJECTS="'D:\ARCHIVO DE PRUEBA'"'
- Para especificar D:\PRUEBA,ARCHIVO:
  - OBJECTS="'D:\PRUEBA,ARCHIVO'"'

 Sistemas operativos AIX  Sistemas operativos Linux Los ejemplos siguientes muestran cómo especificar algunos nombres de archivo:

- Para especificar /home/archivo 2, /home/archivos gif y /home/archivo de prueba, escriba:
  - OBJECTS='"/home/archivo 2" "/home/archivos gif" "/home/archivo de prueba"'
- Para especificar /home/archivo de prueba, escriba:
  - OBJECTS='"/home/archivo de prueba"'

#### Sistemas operativos Windows Consejo:

Para los clientes de Windows que se ejecutan en la modalidad por lotes, si es necesario utilizar comillas dobles, utilice la modalidad interactiva o los caracteres de escape del sistema operativo. Para obtener más información, consulte los temas siguientes:

- Proceso de una serie de comandos del cliente de administración
- Proceso de mandatos individuales desde el cliente de administración

#### PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

#### STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este comando a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

#### DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha

de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

Consejo: Defina las planificaciones con duraciones de más de 10 minutos. Con ello, el planificador de IBM Spectrum Protect dispondrá de tiempo suficiente para procesar la planificación y avisar al cliente.

#### DURUNits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

#### Minutes

Especifica que la duración del margen se define en minutos.

#### Hours

Especifica que la duración del margen se define en horas.

#### Days

Especifica que la duración del margen se define en días.

#### INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

#### MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales todas las sesiones de cliente que inicia la operación planificada deben completarse. Si las sesiones se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejo: El tiempo máximo de ejecución se calcula desde el principio de la ventana de inicio y no desde la hora en que se inician las sesiones en la ventana de inicio.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

El parámetro es opcional. Puede especificar un número en el rango de 0-1440. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y no se emite ningún mensaje de aviso. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de una operación planificada son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todas las sesiones de cliente para esta operación deben finalizar a la 1:00 del mediodía. Si se siguen ejecutando una o varias sesiones después de la 1:00 del mediodía, el servidor emite un mensaje de aviso.

Consejo: También puede especificar un valor para *Alerta de tiempo de ejecución* de 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

#### SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se puede ejecutar una planificación, o los días en los que se puede ejecutar. El estilo puede ser clásica o mejorada. Este parámetro debe especificarse al cambiar una planificación de clásica a mejorada o de mejorada a clásica. En caso contrario, se utiliza el valor para la planificación existente.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH. Si el estilo de planificación anterior fuese el mejorado, se restablecen los parámetros MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. DAYOFWEEK, PERIOD y PERUNITS se establecen como valores predeterminados a menos que estén especificados con el comando de actualización.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS. Si el estilo de planificación anterior fuese el clásico, se

restablecen los parámetros DAYOFWEEK, PERIOD y PERUNITS. MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK se establecen como valores predeterminados a menos que estén especificados con el comando de actualización.

#### PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

#### PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

##### Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

##### Days

Especifica que el período entre márgenes de puesta en marcha es en días.

##### Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

##### Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

##### Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

##### Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

#### DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

##### Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

##### Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará

cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUNday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUesday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

Saturday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada mes del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es el -1, el penúltimo es el -2. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecuta una vez ese día.

El valor predeterminado es ANY, lo que significa que la planificación se ejecuta cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

Si una planificación existente especifica un valor distinto a ANY para DAYOFWEEK y WEEKOFMONTH y se actualiza DAYOFMONTH, DAYOFWEEK y WEEKOFMONTH se restablecen a ANY.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecuta cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecuta una vez durante esa semana.

El valor predeterminado es ANY. ANY significa que la planificación se ejecuta cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

EXPIration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha\_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

## Ejemplo: actualización de la prioridad de una planificación

---

Actualizar la planificación MONTHLY\_BACKUP que pertenece al dominio de políticas STANDARD estableciendo su valor de prioridad en 1.

```
update schedule standard monthly_backup priority=1
```

## Ejemplo: actualización de la fecha de caducidad de una planificación

---

Actualizar la planificación WEEKLY\_BACKUP que pertenece al dominio de políticas EMPLOYEE\_RECORDS de modo que caduque el 29 de Marzo de 1999 (03/29/1999).

```
update schedule employee_records weekly_backup expiration=03/29/1999
```

## Ejemplo: actualizar una planificación para que el archivado se realice el último viernes del mes

---

Actualizar una planificación de las copias archivadas trimestralmente el último viernes del mes para archivarlas el último día de los meses especificados.

```
update schedule employee_records quarterly_archive dayofmonth=-1
```

WEEKOFMONTH y DAYOFWEEK se restablecen a ANY.

## UPDATE SCHEDULE (Actualizar una planificación de administración)

---

Utilice este comando para actualizar los parámetros seleccionados de una planificación de comandos de administración.

No puede planificar comandos MACRO ni QUERY ACTLOG.

Una planificación de administración gestionada que se actualiza por medio de un gestor de configuración se establece en un estado inactivo en los servidores gestionados durante el proceso de renovación de configuración. Permanece en un estado inactivo hasta que se actualiza a un estado activo en esos servidores.

## Clase de privilegio

---

Para actualizar una planificación de administración, debe tener privilegio de sistema.

## Sintaxis

---

```
Planificación de administración clásica

(1)
>>-UPDate SCHEDULE-----nombre_planificación----->
>--+-----+-----+-----+-----+-----+-----+----->
>'-Type----Administrative-' '-CMD----comando-'
>--+-----+-----+-----+-----+-----+-----+----->
>'-ACTIVE-----+Yes-+-' '-DESCRiption----descripción-'
>'-No--'
>--+-----+-----+-----+-----+-----+-----+----->
>'-PRIority----número-' '-STARTDate----fecha-'
>--+-----+-----+-----+-----+-----+-----+----->
>'-STARTTime----hora-' '-DURATION ---número-'
>--+-----+-----+-----+-----+-----+-----+----->
>'-DURUnits----+Minutes----+' '-MAXRUNtime----número-'
>'-Hours-----+
>'-Days-----+
>'-INDefinite-'
>--+-----+-----+-----+-----+-----+-----+----->
>'-SCHEDStyle----Classic-' '-PERiod----número-'
```

```

>-----+----->
'-PERUnits-----+Hours---+'
      +-Days----+
      +-Weeks---+
      +-Months---+
      +-Years---+
      '-Onetime-'

>-----+----->
'-DAYofweek-----+ANY-----+-'
      +-WEEKDay---+
      +-WEEKEnd---+
      +-Sunday----+
      +-Monday----+
      +-Tuesday---+
      +-Wednesday--+
      +-Thursday--+
      +-Friday----+
      '-Saturday--'

>-----+-----<----->
'-EXPIration-----+Never--+-'
      '-date--'

```

Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.

## Sintaxis

---

Planificación de administración mejorada

```

(1)
>>-UPdate SCHEDULE-----nombre_planificación----->

>-----+----->
'-Type-----Administrative-' '-CMD-----comando-'

>-----+----->
'-ACTIVE-----+Yes-+-' '-DESCRIPTION-----descripción-'
      '-No--'

>-----+----->
'-PRIority-----número-' '-STARTDate-----fecha-'

>-----+----->
'-STARTTime-----hora-' '-DURATION -----número-'

>-----+----->
'-DURUnits-----+Minutes-+-' '-MAXRUNtime-----número-'
      +-Hours----+
      '-Days----'

>-----+----->
'-SCHEDStyle-----Enhanced-' '-MONTH-----+ANY-----+-'
      +-JANuary---+
      +-February--+
      +-MARch-----+
      +-APRil-----+
      +-May-----+
      +-JUNE-----+
      +-JULy-----+
      +-AUGust----+
      +-September--+
      +-October---+
      +-November--+
      '-December--'

>-----+----->
'-DAYOFMonth-----+ANY-+-' '-WEEKofmonth-----+ANY-----+-'
      '-Day-'
      +-First---+
      +-Second--+
      +-Third--+

```



+-FOurth-+  
'-Last---'

```
>---+-----+-----+-----+-----+-----+-----+-----+-----+-----+----->
'-DAYofweek-----+-ANY-----+-'
      +-WEEKDay---+
      +-WEEKEnd---+
      +-SUnDay----+
      +-Monday----+
      +-TUESday---+
      +-WednesDay-+
      +-THursday--+
      +-Friday----+
      '-SATurday--'

>---+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----<<
'-EXPIration=---+-Never-+-'
      '-date--'
```

#### Notas:

1. Debe especificar como mínimo un parámetro opcional en este comando.

## Parámetros

### nombre\_planificación (Obligatorio)

Especifica el nombre de la planificación que se ha de actualizar.

### Type=Administrative (Necesario)

Especifica que se actualiza una planificación de comandos de administración.

### CMD

Especifica el mandato de administración que se planificará para procesarlo. Este parámetro es opcional. El mandato que especifique puede contener hasta 512 caracteres. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco.

No puede especificar caracteres de redirección con este parámetro.

### ACTIVE

Especifica si el comando de administración puede seleccionarse para procesarlo. Este parámetro es opcional. Las planificaciones de mandatos de administración no se procesan si no se establecen en el estado activo. Los valores posibles son:

#### YES

Especifica que el comando de administración puede seleccionarse para procesarlo.

#### NO

Especifica que el mandato de administración no puede seleccionarse para procesarlo.

### DESCRiption

Especifica una descripción de la planificación. Este parámetro es opcional. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción definida anteriormente, especifique una serie nula ("") para este valor.

### PRIority

Especifica el valor de prioridad de una planificación. Este parámetro es opcional. Puede especificar un entero entre 1 y 10, siendo 1 el nivel de prioridad más alto y 10 el más bajo. El valor predeterminado es 5.

Si hay dos o más planificaciones que tienen la misma hora de inicio de margen de puesta en marcha, el valor especificado determina cuándo procesa IBM Spectrum Protect la planificación. La planificación que tenga el nivel de prioridad más alto se arrancará primero. Por ejemplo, una planificación con PRIORITY=3 se arrancará antes que una planificación con PRIORITY=5.

### STARTDate

Especifica la fecha del inicio del margen en el que se procesará por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la fecha actual. Utilice este parámetro junto con el parámetro STARTTIME para especificar cuándo empieza la ventana de inicio de sesión de la planificación.

Para especificar la fecha, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
MM/DD/AAAA	Una fecha concreta	09/15/1998
TODAY	La fecha actual	TODAY

Valor	Descripción	Ejemplo
TODAY+días o +días	La fecha actual más los días especificados. El número máximo de días que puede especificar es de 9999.	TODAY +3 o +3.
EOLM (fin del mes pasado)	El último día del mes anterior.	EOLM
EOLM-días	El último día del mes anterior menos los días especificados.	EOLM-1 Incluir los archivos que estaban activos un día antes del último día del mes anterior.
BOTM (Principios de este mes)	El primer día del mes actual.	BOTM
BOTM+días	El primer día del mes en curso, más los días especificados.	BOTM+9 Incluir los archivos que estaban activos el día 10 del mes actual.

#### STARTTime

Especifica la hora del inicio del margen en el que se procesa por primera vez la planificación. Este parámetro es opcional. El valor predeterminado es la hora actual. Este parámetro se utiliza junto con el parámetro STARTDATE para especificar cuándo comienza la ventana inicial de inicio de sesión.

Para especificar la hora, utilice uno de los siguientes valores:

Valor	Descripción	Ejemplo
HH:MM:SS	Una hora concreta	10:30:08
NOW	La hora actual	NOW
NOW+HH:MM o +HH:MM	La hora actual más las horas y minutos especificados	NOW+02:00 o +02:00. Si emite este comando a las 5:00 con STARTTIME=NOW+02:00 o STARTTIME=+02:00, el comienzo del margen de puesta en marcha es a las 7:00.
NOW-HH:MM o -HH:MM	La hora actual menos las horas y minutos especificados	NOW-02:00 o -02:00. Si emite este mandato a las 5:00 con el formato STARTTIME=NOW-02:00 o STARTTIME=-02:00, el comienzo del margen de puesta en marcha es a las 3:00.

#### DURation

Especifica el número de unidades que definen la duración del margen de puesta en marcha de la operación planificada. Este parámetro es opcional. Este valor debe estar entre 1 y 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro DURUNITS para especificar la duración de la ventana de inicio de sesión. Por ejemplo, si especifica DURATION=20 y DURUNITS=MINUTES, la planificación debe arrancarse al cabo de 20 minutos de la fecha de inicio y hora de inicio. La duración predeterminada del margen de puesta en marcha es de 1 hora. La duración del margen debe ser más breve que el período entre márgenes.

Este valor se ignora si se especifica DURUNITS=INDEFINITE.

#### DURUnits

Especifica las unidades horarias que se utilizan para determinar la duración del margen el que puede iniciarse la planificación. Este parámetro es opcional. El valor predeterminado es HOURS.

Utilice este parámetro junto con el parámetro DURATION para especificar durante cuánto tiempo permanece abierta la ventana de inicio de sesión para procesar la planificación. Por ejemplo, si DURATION=20 y DURUNITS=MINUTES, la planificación se debe arrancar en el plazo de 20 minutos de la fecha y hora de inicio. La planificación puede no completar necesariamente el proceso dentro de este margen. Si la planificación se ha de volver a intentar por algún motivo, los nuevos intentos han de comenzar antes de que transcurra el período de tiempo del margen de puesta en marcha, o la operación no se volverá a arrancar.

El valor predeterminado para la duración del margen de puesta en marcha es de 1 hora. Puede especificar uno de los siguientes valores:

Minutes

Especifica que la duración del margen se define en minutos.

Hours

Especifica que la duración del margen se define en horas.

Days

Especifica que la duración del margen se define en días.

INDefinite

Especifica que el margen de puesta en marcha de la operación planificada tiene una duración indefinida. La planificación se puede ejecutar en cualquier momento después de la hora de inicio, hasta que caduque la planificación. No puede especificar DURUNITS=INDEFINITE, a menos que especifique PERUNITS=ONETIME. El valor INDEFINITE no se admite en las planificaciones mejoradas.

MAXRUNtime

Especifica el tiempo máximo de ejecución, que es el número de minutos durante los cuales se deben completar los procesos del servidor que se han iniciado mediante los mandatos planificados. Si los procesos se siguen ejecutando después del tiempo máximo de ejecución, el servidor emite un mensaje de aviso, pero las sesiones continúan ejecutándose.

Consejos:

- Es posible que los procesos no finalicen inmediatamente después de que los haya cancelado el planificador central. Finalizan cuando registran la notificación de cancelación del planificador central.
- El tiempo de ejecución máximo se calcula comenzando desde el momento en que se inicia el servidor. Si el mandato de planificación inicia más de un proceso, se calcula tiempo máximo de ejecución de cada proceso a partir del inicio del proceso.
- Este parámetro no se aplica a algunos procesos, tales como procesos de identificación de duplicados, que puede continuar ejecutándose después de que el tiempo máximo de ejecución.
- Este parámetro no se aplica si el mandato planificado no inicia un proceso de servidor.
- Otra hora de cancelación puede estar asociada con algunos mandatos. Por ejemplo, el mandato MIGRATE STGPPOOL puede incluir un parámetro que especifica el periodo de tiempo que la migración de la agrupación de almacenamiento se ejecuta antes de que se cancele la migración automáticamente. Si planifica un mandato para el que se ha definido un tiempo de cancelación y también define un tiempo máximo de ejecución para la planificación, los procesos se cancelan en cualquier momento de cancelación que se alcance primero.

Restricciones:

- El valor del parámetro no se distribuye a los servidores que están gestionados por un gestor de configuración empresarial.
- El valor del parámetro no se exporta mediante el mandato EXPORT.

Este parámetro es opcional. Puede especificar un número en el rango de 0-1440. Un valor de 0 significa que el tiempo máximo de ejecución es indefinido y el planificador central no cancela los procesos. El tiempo máximo de ejecución debe ser mayor que la duración de la ventana de inicio, que se define por los parámetros DURATION y DURUNITS.

Por ejemplo, si la hora inicial de un mandato planificado son las 21:00 y la duración de la ventana de inicio es de 2 horas, la ventana de inicio es 21:00 - 23:00. Si el tiempo máximo de ejecución es de 240 minutos, es decir, 4 horas, todos los procesos de servidor aplicables iniciados por el mandato se deben finalizar a la 1:00 del mediodía. Si uno o varios procesos aplicaciones continúan ejecutándose pasadas la 1:00 del mediodía, el planificador central cancela los procesos.

Consejo: También puede especificar como *hora de finalización* la 1:00 AM en el centro de operaciones de IBM Spectrum Protect.

SCHEDStyle

Este parámetro es opcional. SCHEDSTYLE define el intervalo entre las horas en las que se debe ejecutar una planificación, o los días en los que se debe ejecutar. El estilo puede ser clásica o mejorada. Este parámetro debe especificarse al cambiar una planificación de clásica a mejorada o de mejorada a clásica. En caso contrario, se utiliza el valor para la planificación existente.

Para las planificaciones clásicas, se permiten estos parámetros: PERIOD, PERUNITS y DAYOFWEEK. No se permiten los parámetros MONTH, DAYOFMONTH y WEEKOFMONTH. Si el estilo de planificación anterior fuese el mejorado, se restablecerían los parámetros MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. DAYOFWEEK, PERIOD y PERUNITS se establecerán como valores predeterminados a menos que estén especificados con el mandato de actualización.

Para las planificaciones mejoradas, se permiten los siguientes parámetros: MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK. No se permiten los parámetros PERIOD y PERUNITS. Si el estilo de planificación anterior fuese el clásico, se restablecerían los parámetros DAYOFWEEK, PERIOD y PERUNITS. MONTH, DAYOFMONTH, WEEKOFMONTH y DAYOFWEEK se establecerán como valores predeterminados a menos que estén especificados con el mandato de actualización.

PERiod

Especifica el período de tiempo entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. Puede especificar un entero de 1 a 999. El valor predeterminado es 1.

Utilice este parámetro junto con el parámetro PERUNITS para especificar el período entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación está planificada para

ejecutarse cada cinco días a continuación de la fecha de inicio y hora de inicio iniciales. El período entre márgenes de puesta en marcha debe sobrepasar la duración de cada margen. El valor predeterminado es 1.

Este valor se ignora si se especifica PERUNITS=ONETIME.

#### PERUnits

Especifica las unidades horarias que se utilizan para determinar el período entre márgenes de puesta en marcha para esta planificación. Este parámetro es opcional. Este parámetro se utiliza sólo con las planificaciones clásicas. El valor predeterminado es DAYS.

Utilice este parámetro junto con el parámetro PERIOD para especificar el periodo entre ventanas de inicio de sesión. Por ejemplo, si especifica PERIOD=5 y PERUNITS=DAYS (suponiendo que DAYOFWEEK=ANY), la operación se planifica para ejecutarse cada 5 días después de la fecha de inicio y hora de inicio iniciales. El valor predeterminado es 1. Puede especificar uno de los siguientes valores:

##### Hours

Especifica que el período entre márgenes de puesta en marcha es en horas.

##### Days

Especifica que el período entre márgenes de puesta en marcha es en días.

##### Weeks

Especifica que el período entre márgenes de puesta en marcha es en semanas.

##### Months

Especifica que el período entre márgenes de puesta en marcha es en meses.

Si especifica PERUNITS=MONTHS, la operación planificada se procesará el mismo día de cada mes. Por ejemplo, si la fecha de inicio de la operación planificada es 02/04/1998, la planificación se procesará el día cuatro de cada mes a partir de entonces. Sin embargo, si la fecha no es válida para el mes siguiente, entonces la operación planificada se procesará la última fecha válida del mes. A partir de entonces, las operaciones siguientes se basarán en esa nueva fecha. Por ejemplo, si la fecha de inicio es 03/31/1998, la operación del mes siguiente estará planificada para el 04/30/1998. A partir de entonces, todas las operaciones siguientes serán para el día 30 del mes hasta Febrero. Dado que Febrero tiene sólo 28 días, la operación se planificará para el 02/28/1999. Las operaciones siguientes se procesarán el 28 del mes.

##### Years

Especifica que el período entre márgenes de puesta en marcha para la planificación ha de ser en años.

Si especifica PERUNITS=YEARS, la operación planificada se procesará el mismo mes y la misma fecha de cada año. Por ejemplo, si la fecha de inicio de la operación planificada es el 02/29/2004, la operación planificada del año siguiente será el 02/28/2005 porque Febrero sólo tiene 28 días. A partir de entonces, las operaciones siguientes se planificarán para el 28 de Febrero.

##### Onetime

Especifica que la planificación se procesa una vez. Este valor sustituye al valor especificado para el parámetro PERIOD.

#### DAYofweek

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar opciones distintas para el parámetro DAYofweek, en función de si el estilo de planificación se ha definido como Classic o como Enhanced:

##### Planificación clásica

Especifica el día de la semana en que se inicia el margen de puesta en marcha para la planificación. Este parámetro es opcional. Puede especificar un día de la semana o bien WEEKDAY, WEEKEND o ANY. Si la fecha de inicio y la hora de inicio caen en un día que no se corresponda con el día especificado, la fecha de inicio y la hora de inicio se adelantarán en incrementos de 24 horas hasta que se ajuste al valor del parámetro DAYOFWEEK.

Si selecciona un valor de DAYOFWEEK distinto de ANY, y dependiendo de los valores de PERIOD y PERUNITS, es posible que las planificaciones no se procesen cuando estaba previsto. El valor predeterminado es ANY.

##### Planificación mejorada

Especifica los días de la semana en que se ejecutará la planificación. Puede especificar varios valores separados con comas sin espacios en blanco, o bien WEEKDAY, WEEKEND o ANY. Si especifica varios días, la planificación se ejecutará cada uno de los días especificados. Si especifica WEEKDAY o WEEKEND, también debe especificar WEEKOFMONTH=FIRST o WEEKOFMONTH=LAST, y la planificación se ejecutará sólo una vez al mes.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada día de la semana o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFWEEK debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con el parámetro DAYOFMONTH.

Los valores posibles del parámetro DAYofweek son:

ANY

Especifica que el margen de puesta en marcha puede comenzar en cualquier día de la semana.

WEEKDay

Especifica que el margen de puesta en marcha puede comenzar en Lunes, Martes, Miércoles, Jueves o Viernes.

WEEKEnd

Especifica que el margen de puesta en marcha puede comenzar en Sábados o Domingos.

SUnday

Especifica que el margen de puesta en marcha comienza en Domingo.

Monday

Especifica que el margen de puesta en marcha comienza en Lunes.

TUesday

Especifica que el margen de puesta en marcha comienza en Martes.

Wednesday

Especifica que el margen de puesta en marcha comienza en Miércoles.

THursday

Especifica que el margen de puesta en marcha comienza en Jueves.

Friday

Especifica que el margen de puesta en marcha comienza en Viernes.

SATurday

Especifica que el margen de puesta en marcha comienza en Sábado.

MONth

Especifica los meses del año en que se ejecutará la planificación. Este parámetro se utiliza sólo con las planificaciones mejoradas. Puede especificar varios valores separados con comas sin espacios en blanco. El valor predeterminado es ANY. Esto significa que la planificación se ejecutará todos los meses del año.

DAYOFMonth

Especifica el día del mes en que se ejecutará la programación. Sólo se puede especificar este parámetro con planificaciones mejoradas. Puede especificar ANY o un número entre -31 y 31, excepto el cero. Los valores negativos son un día a partir del fin de mes, contando hacia atrás. Por ejemplo, el último día del mes es -1, el penúltimo es -2, etc. Puede especificar varios valores separados mediante comas, sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada uno de los días especificados del mes. Si se resuelven varios valores en el mismo día, la planificación sólo se ejecutará una vez ese día.

El valor predeterminado es ANY. Esto significa que la planificación se ejecutará cada día del mes o los días determinados por otros parámetros de planificación mejorados. El valor de DAYOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el comando) cuando se utiliza con los parámetros DAYOFWEEK o WEEKOFMONTH.

WEEKofmonth

Especifica la semana del mes en que se ejecutará la planificación. Sólo se puede especificar este parámetro con planificaciones mejoradas. Se considera como semana cualquier período de siete días que no empiece en un día determinado de la semana. Puede especificar FIRST, SECOND, THIRD, FOURTH, LAST o ANY. Puede especificar varios valores separados con comas sin espacios en blanco. Si especifica varios valores, la planificación se ejecutará cada una de las semanas especificadas del mes. Si se resuelven varios valores en la misma semana, la planificación sólo se ejecutará una vez durante esa semana.

El valor predeterminado es ANY, lo que significa que la planificación se ejecutará cada semana del mes o los días determinados por otros parámetros de planificación mejorados. El valor de WEEKOFMONTH debe ser ANY (ya sea de forma predeterminada o especificándolo con el mandato) cuando se utiliza con el parámetro DAYOFMONTH.

EXPIration

Especifica la fecha en la que deja de utilizarse esta planificación. Este parámetro es opcional. El valor predeterminado es NEVER. Puede especificar uno de los siguientes valores:

Never

Especifica que la planificación no caduca nunca.

fecha\_caducidad

Especifica la fecha en la que caduca esta planificación, con el formato MM/DD/AAAA. Si especifica una fecha de caducidad, la planificación caduca a las 23:59:59 de la fecha especificada.

## **Ejemplo: actualizar una planificación de copia de seguridad para que ésta se realice cada tres días**

Actualizar una planificación de administración existente denominada BACKUP\_BACKUPPOOL, de modo que, a partir de hoy, se realice una copia de seguridad de la agrupación de almacenamiento primaria BACKUPPOOL en la agrupación de almacenamiento de copia COPYSTG cada tres días a las 22:00 horas.

```
update schedule backup_backuppool type=administrative cmd="backup
stgpool backuppool copystg" active=yes starttime=22:00 period=3
```

## Ejemplo: actualizar una planificación de copia de seguridad para que se realice el primer y el tercer viernes de cada mes

Actualizar una planificación denominada BACKUP\_ARCHIVEPOOL que efectúe copias de seguridad de la agrupación de almacenamiento primario ARCHIVEPOOL en la agrupación de almacenamiento de copia RECOVERYPOOL. La planificación existente se ejecuta el primer y el décimo día de cada mes. Actualícelo para ejecutarse el primer y el tercer viernes de cada mes.

```
update schedule backup_archivepool
dayofweek=friday
weekofmonth=first,third
```

DAYOFMONTH se restablecerá a ANY.

## UPDATE SCRATCHPADENTRY (Actualizar una entrada de registro)

Utilice este mandato para actualizar datos en una línea en el registro.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UPDate SCRATCHPadentry--major_category--minor_category----->
>--subject--Line -===número--Data-----datos-----><
```

### Parámetros

major\_category (obligatorio)

Especifica la categoría principal en la que los datos se van a actualizar. Este parámetro distingue entre mayúsculas y minúsculas.

minor\_category (obligatorio)

Especifica la categoría secundaria en la que se actualizarán los datos. Este parámetro distingue entre mayúsculas y minúsculas.

subject (obligatorio)

Especifica el asunto bajo el que se actualizarán los datos. Este parámetro distingue entre mayúsculas y minúsculas.

Line (obligatorio)

Especifica el número de la línea en la que se actualizarán los datos.

Data (obligatorio)

Especifica los datos nuevos que se almacenarán en la línea. Se suprimen los datos anteriores. Puede entrar un máximo de 1000 caracteres. Ponga los datos entre comillas si los datos contienen uno o más espacios en blanco. Los datos distinguen entre mayúsculas y minúsculas.

### Ejemplo: Actualizar una entrada de registro

Actualice los detalles de contacto de vacaciones de un administrador, Jane, en una base de datos que almacena información sobre la ubicación de todos los administradores:

```
update scratchpadentry admin_info location jane line=2 data=
"Fuera de la oficina hasta el 18 de Nov."
```

### Comandos relacionados

Tabla 1. Mandatos relacionados con UPDATE SCRATCHPADENTRY

Comando	Descripción
DEFINE SCRATCHPADENTRY	Crea una línea de datos en la anotación.
DELETE SCRATCHPADENTRY	Suprime una línea de datos de la anotación.
QUERY SCRATCHPADENTRY	Muestra información que está contenida en la anotación.
SET SCRATCHPADRETENTION	Especifica la cantidad de tiempo durante el cual se retienen las entradas de anotación.

# UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)

---

Utilice este comando para cambiar una línea de comandos existente o para agregar una nueva línea de comandos a un script de IBM Spectrum Protect.

Restricción: No puede redirigir la salida de un mandato desde un script de IBM Spectrum Protect. En su lugar, ejecute el script, y luego especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

## Clase de privilegio

---

Para emitir este mandato, el administrador debe haber definido el script con anterioridad o debe tener privilegio de sistema.

## Sintaxis

---

```
>>-UPDate SCRIpt--nombre_script----->
>--+-----+----->
  '-línea_comandos--+-----+'
                        '-Line ---número-'
>--+-----+-----<
  '-DESCRiption----descripción-'
```

## Parámetros

---

nombre\_script (Obligatorio)

Especifica el nombre del script que se va a actualizar.

línea\_comandos

Especifica el mandato nuevo o actualizado que se procesará en un script. Al emitir este mandato, debe actualizar un mandato, una descripción o ambos.

El mandato puede contener variables de sustitución y se puede continuar en varias líneas si especifica un carácter de continuación (-) como último carácter del mandato. Puede especificar hasta 1200 caracteres para el mandato. El mandato debe estar delimitado por comillas si contiene algún carácter en blanco. Si especifica este parámetro, opcionalmente puede especificar el parámetro siguiente.

Tiene las opciones de ejecutar los mandatos en serie, en paralelo o en serie y en paralelo, especificando los mandatos de script SERIAL o PARALLEL para este parámetro. Puede ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente. Los mandatos se ejecutarán en serie hasta que se encuentre un mandato en paralelo.

Pueden utilizarse sentencias de flujo lógico condicional. Estas sentencias incluyen IF, EXIT y GOTO.

Line

Especifica el número de línea del comando. Si no especifica un número de línea, la línea de mandatos se agregará al final de la serie de líneas de mandatos existente. Se asignará a la línea de mandatos agregada un número de línea cinco unidades mayor que el último número de línea de mandatos de la secuencia. Por ejemplo, si la última línea del script es 015, a la línea de mandatos agregada se asigna el número 020.

Si especifica un número de línea, el mandato sustituirá una línea existente (si el número es el mismo que el de una línea existente). O insertará la línea especificada (si el número de línea no se corresponde con un número de línea existente de la secuencia de línea de mandatos).

DESCRiption

Especifica la descripción del script. Puede especificar hasta 255 caracteres para la descripción. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

## Ejemplo: agregar un comando al final de un script

---

Imaginemos que ha definido el siguiente script de tres líneas, denominado QSAMPLE, y que desea agregar el mandato QUERY SESSION al final del script.

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
```

```
010 QUERY PROCESS
```

```
update script qsample "query session"
```

Después de haberse procesado el comando, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION
```

## Ejemplo: actualizar una línea específica de un script

Mediante la utilización del script del ejemplo anterior, cambiar la línea 010 para que procese el mandato QUERY STGPPOOL en lugar del mandato QUERY PROCESS:

```
update script qsample "query stgpool" line=010
```

Después de haberse procesado el comando, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
010 QUERY STGPPOOL
015 QUERY SESSION
```

## Ejemplo: insertar un comando en la parte central de un script

Mediante la utilización del script del ejemplo anterior, inserte una nueva línea de mandatos (QUERY NODE OPEN) después de la línea de mandatos QUERY STATUS del script QSAMPLE:

```
update script qsample "query node"
line=007
```

Después de haberse procesado el mandato, ahora el script consta de las líneas siguientes:

```
001 /* Éste es un script de ejemplo */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPPOOL
015 QUERY SESSION
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE SCRIPT

Comando	Descripción
COPY SCRIPT	Crea una copia de un script.
DEFINE SCRIPT	Define un script para el servidor de IBM Spectrum Protect.
DELETE SCRIPT	Suprime el script o líneas individuales del script.
QUERY SCRIPT	Muestra información sobre scripts.
RENAME SCRIPT	Redenomina un script con un nuevo nombre.
RUN	Ejecuta un script.

### Tareas relacionadas:

- Ejecución de mandatos en paralelo o en serie
- Inclusión de sentencias de flujo lógico en un script
- Realización de tareas simultáneamente en varios servidores
- Definición de un script del servidor

### Referencia relacionada:

Códigos de retorno de los scripts para IBM Spectrum Protect

## UPDATE SERVER (Actualizar un servidor definido para las comunicaciones de servidor a servidor)



Utilice este comando para actualizar la definición de un servidor.

Restricción: Si el servidor es un servidor de origen para una operación de volumen virtual, cambiar cualquiera de estos valores puede afectar a la capacidad del servidor de origen de acceder y gestionar los datos que están almacenados en el servidor de destino correspondiente. Cambiar el nombre del servidor utilizando el mandato SET SERVERNAME podría tener implicaciones adicionales, que varían en función del sistema operativo. Los siguientes son los valores posibles:

- Puede que las contraseñas dejen de ser válidas.
- Puede que la información de dispositivos se vea afectada.
- La información de registro sobre sistemas operativos Windows puede cambiar



## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema.


### Sintaxis de:

---

- **Configuración de Enterprise**
- **Anotación de eventos Enterprise**
- **Direccionamiento de comandos**
- **Agente de almacenamiento**
- **Servidores de origen y destino de réplica de nodos**
-  Sistemas operativos AIX  Sistemas operativos Linux **servidor de medios de z/OS**

```
>>-UPDate--SERver--nombre_servidor----->
>--+-----+
  '-SERVERPAssword---contraseña-'
>--+-----+-----+-----+-----+----->
  '-HLAddress---ip_address-' '-LLAddress---puerto_tcp-'
>--+-----+-----+-----+----->
  '-COMMmethod---TCPiP-' '-URL---url-'
>--+-----+-----+-----+----->
  '-ALLOWReplace---+Yes-+-'
                          '-No--'
>--+-----+-----+-----+----->
  '-DEScRiption---descripción-' '-FORCESync---+Yes-+-'
                                          '-No--'
>--+-----+-----+-----+----->
  | (1) |
  '------VALIDateprotocol---+No--+-'
                          '-All-'
>--+-----+-----+-----+----->
  '-SSL---+No-+-'
                          '-Yes-'
.-SESSIONSECurity---TRANSitional-.
>--+-----+-----+-----+----->
  '-SESSIONSECurity---+STRict-----+-'
                          '-TRANSitional-'
.-TRANSFERMethod---TcpiP-----.
>--+-----+-----+-----+-----><
  '-TRANSFERMethod---+TcpiP---+-'
                          | (2) |
                          '-Fasp-----'
```

Notas:

1. El parámetro VALIDATEPROTOCOL está en desuso y sólo se aplica a las definiciones del agente de almacenamiento.
2.  Sistemas operativos Linux El parámetro TRANSFERMETHOD solo está disponible en sistemas operativos Linux x86\_64 .

## Sintaxis correspondiente a volúmenes virtuales

---

```

>>-UPDate--SERver--nombre_servidor----->
>--+-----+--+-----+----->
  '-PAssword----contraseña-'  '-HLAddress----ip_address-'
>--+-----+--+-----+----->
  '-LLAddress----puerto_tcp-'  '-COMMmethod----TCPIP-'
>--+-----+--+-----+----->
  '-URL----url-'  '-DELgraceperiod----días-'
>--+-----+--+-----+----->
  '-NODEName----nombre_nodo-'  '-SSL----Yes-'
  .-SESSIONSECurity----TRANSitional----.
>--+-----+--+-----+----->
  '-SESSIONSECurity----+STRict-----+-'
                                '-TRANSitional-'
>--+-----+--+-----+-----><
  '-FORCESync----+Yes+-'  '-DESCRiption----descripción-'
                                '-No--'

```

## Parámetros

### nombre\_servidor (Obligatorio)

Especifica el nombre del servidor que se va a actualizar. Este parámetro es necesario.

### PAssword

Especifica la contraseña que se utiliza para iniciar la sesión en el servidor de destino para los volúmenes virtuales. Este parámetro es opcional.

### SERVERPAssword

Especifica la contraseña del servidor, que se utiliza para las funciones de configuración de enterprise, direccionamiento de comandos y anotación de eventos de servidor a servidor. Esta contraseña debe coincidir con la contraseña del servidor que se ha establecido con el comando SET SERVERPASSWORD. Este parámetro es opcional.

### HLAddress

Especifica la dirección IP (con formato de coma decimal) del servidor. Este parámetro es opcional.

### LLAddress

Especifica la dirección de bajo nivel del servidor. Esta dirección suele coincidir con la dirección de la opción de servidor TCPPOINT del servidor destino. Cuando SSL=YES, el puerto ya debe estar designado para comunicaciones SSL en el servidor de destino.

### COMMmethod

Especifica el método de comunicación que se utiliza para conectar con el servidor. Este parámetro es opcional.

### URL

Especifica la dirección de URL que se utiliza para acceder a este servidor desde Centro de administración. El parámetro es opcional.

### DELgraceperiod

Especifica un número de días en que el objeto permanece en el servidor de destino después de haber sido marcado para suprimirlo. Puede especificar un valor de 0 a 9999. El valor predeterminado es 5. Este parámetro es opcional.

### NODEName

Especifica un nombre de nodo que ha de utilizar el servidor para conectarse con el servidor destino. Este parámetro es opcional.

### DESCRiption

Especifica la descripción del servidor. Este parámetro es opcional. La descripción puede tener hasta 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

### FORCESync

Especifica si se restablece la clave de verificación del servidor en la siguiente conexión del servidor origen con el servidor destino. Una clave de verificación válida permite que un servidor origen pueda colocar nuevos objetos en el servidor destino, gestionar el valor del período de gracia para la supresión y actualizar la contraseña, si se conoce la contraseña actual y coincide la clave de verificación. El parámetro es opcional. Puede especificar uno de los siguientes valores:

#### Yes

Especifica que se enviará una nueva clave de verificación al servidor destino y que éste la aceptará si se recibe una contraseña válida.

#### No

Especifica que no se enviará una nueva clave de verificación al servidor destino.

### VALIdateprotocol (en desuso)

Especifica si una comprobación de redundancia cíclica valida los datos enviados entre el agente de almacenamiento y el servidor de IBM Spectrum Protect. El parámetro es opcional. El valor predeterminado es NO.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2, la validación que está habilitada por este parámetro se sustituye por el protocolo TLS 1.2, que se impone por el parámetro SESSIONSECURITY. El parámetro VALIDATEPROTOCOL se ignora.

Actualice la configuración para utilizar el parámetro SESSIONSECURITY.

#### ALLOWReplace

Especifica si una definición de servidor que ha definido un servidor gestionado puede sustituirse por una definición del gestor de configuración. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

Yes

Especifica que una definición de servidor puede sustituirse por una definición del gestor de configuración.

No

Especifica que una definición de servidor no puede sustituirse por la definición del gestor de configuración.

#### SSL

Especifica la modalidad de comunicación del servidor.

Importante: A partir de V8.1.2, se utiliza SSL para cifrar ciertas comunicaciones con el servidor especificado, incluso si se especifica NO.

Las siguientes condiciones y consideraciones se aplican cuando especifica el parámetro SSL:

- Antes de iniciar los servidores, los certificados autofirmados de los servidores asociados deben estar en el archivo de base de datos de claves (cert.kdb) de cada uno de los servidores.
- Puede definir varios nombres de servidor con distintos parámetros en el mismo servidor de destino.

Puede especificar uno de los siguientes valores:

No

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, excepto si el servidor envía o recibe datos de objeto. Los datos de objeto se envían y se reciben mediante TCP/IP. Si elige no cifrar los objetos de datos, el rendimiento del servidor será similar a la comunicación mediante una sesión TCP/IP y la sesión es segura.

Yes

Especifica una sesión SSL para todas las comunicaciones con el servidor especificado, incluso si el servidor envía o recibe datos de objeto.

#### SESSIONSECurity

Especifica si el servidor que está definiendo debe utilizar los ajustes más seguros para comunicarse con el servidor de IBM Spectrum Protect. Este parámetro es opcional.

Puede especificar uno de los siguientes valores:

STRict

Especifica que se aplicarán los valores de seguridad más estrictos para el servidor que se define. El valor STRICT utiliza el protocolo de comunicaciones más seguro disponible, que en la actualidad es TLS 1.2. El protocolo TLS 1.2 se utiliza con las sesiones SSL entre el servidor especificado y un servidor IBM Spectrum Protect.

Para utilizar el valor STRICT, deben cumplirse los siguientes requisitos para asegurarse de que el servidor especificado pueda autenticarse en el servidor IBM Spectrum Protect:

- Tanto el servidor que se define como el servidor IBM Spectrum Protect deben utilizar software de IBM Spectrum Protect que admita el parámetro SESSIONSECURITY.
- Es necesario configurar el servidor que está definiendo para utilizar el protocolo TLS 1.2 para las sesiones SSL entre él mismo y el servidor IBM Spectrum Protect.

Los servidores que tienen definido el valor STRICT que no cumplan con estos requisitos no podrán autenticarse en IBM Spectrum Protect.


TRANSitional

Especifica que se aplican los valores de seguridad existentes para el servidor. Este es el valor predeterminado. Este valor está pensado para utilizarlo de forma temporal mientras se actualiza la configuración de seguridad para cumplir con los requisitos del valor STRICT.

Si SESSIONSECURITY=TRANSITIONAL y el servidor no cumplen nunca los requisitos para el valor STRICT, el servidor continuará la autenticación utilizando el valor TRANSITIONAL. Sin embargo, cuando un servidor cumpla los requisitos del valor STRICT, el valor de parámetro SESSIONSECURITY se actualizará automáticamente de TRANSITIONAL a STRICT. Después, el servidor ya no se podrá autenticar utilizando una versión del cliente o un protocolo SSL/TLS que no cumpla con los requisitos para STRICT. Además, cuando el servidor se autentica correctamente mediante un protocolo de comunicación más seguro, ya no se puede autenticar con protocolos menos seguros. Por ejemplo, si se actualiza un servidor que no utiliza SSL y se autentica correctamente mediante TLS 1.2, ya no se podrá autenticar sin protocolo SSL o con TLS 1.1. Esta restricción se aplica también al utilizar funciones, como volúmenes virtuales, el direccionamiento de

mandatos o la exportación entre servidores, cuando un nodo o un administrador se autentica en el servidor IBM Spectrum Protect como nodo o administrador de otro servidor.

#### Sistemas operativos Linux TRANSFERMethod

 Sistemas operativos Linux Especifica el método que se utiliza para la transferencia de datos de servidor a servidor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### Tcpip

Especifica que se utiliza TCP/IP para transferir datos. Este es el valor predeterminado.

##### Fasp

Especifica que se utiliza la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para transferir datos. La tecnología Aspera FASP permite optimizar la transferencia de datos en una red de área amplia (WAN).

Restricciones:

- Antes de habilitar la tecnología Aspera FASP, determine si la tecnología es adecuada para su entorno de sistema e instale las licencias adecuadas. Para ver instrucciones, consulte Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema. Si faltan licencias o estas han caducado, las operaciones de transferencia de datos fallan.
- Si el rendimiento de WAN cumple sus necesidades de negocio, no habilite la tecnología Aspera FASP.
- Si especifica TRANSFERMETHOD=FASP en el mandato PROTECT STGPOOL o REPLICATE NODE, ese valor altera temporalmente el parámetro TRANSFERMETHOD en los mandatos DEFINE SERVER y UPDATE SERVER.

## Ejemplo: actualizar un periodo de gracia de supresión para un servidor

Actualice la definición de SERVER2 para especifica que los objetos permanecen en el servidor de destino durante 10 días, después de que se hayan marcado para la supresión.

```
update server server2 delgraceperiod=10
```

## Ejemplo: actualizar el URL de un servidor

Actualizar la definición NEWSERVER para especificar que su dirección URL sea http://newserver:1580/.

```
update server newserver url=http://newserver:1580/
```

## Ejemplo: Actualizar todos los servidores para comunicarse con el servidor IBM Spectrum Protect utilizando la seguridad de sesión estricta.

Actualice la definición de todos los servidores para utilizar la configuración de seguridad más estricta para autenticarse en IBM Spectrum Protect.

```
update server * sessionsecurity=strict
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE SERVER

Comando	Descripción
DEFINE DEVCLASS	Define una clase de dispositivo.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
DELETE DEVCLASS	Elimina una clase de dispositivo.
DELETE FILESPACE	Suprime los datos asociados a los espacios de archivos de los clientes. Si un espacio de archivos es parte de un grupo de proximidad y elimina el espacio de archivos de un nodo, el espacio de archivos se eliminará del grupo de proximidad.
DELETE SERVER	Suprime la definición de un servidor.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY SERVER	Muestra información sobre servidores.
RECONCILE VOLUMES	Reconcilia las definiciones de volúmenes virtuales del servidor origen con los objetos de copia archivada del servidor destino.

Comando	Descripción
REGISTER NODE	Define un nodo cliente en el servidor y establece las opciones para dicho usuario.
REMOVE NODE	Suprime un cliente de la lista de nodos registrados de dominio de políticas especificado.
UPDATE DEVCLASS	Cambia los atributos de una clase de dispositivo.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.

## UPDATE SERVERGROUP (Actualizar una descripción de grupo de servidores)

Utilice este comando para actualizar la descripción de un grupo de servidores.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-UPDate SERVERGroup--nombre_grupo----->
>--DESCRiption--==--descripción-----<<
```

### Parámetros

nombre\_grupo (Obligatorio)

Especifica el grupo de servidores que se actualiza.

DESCRiption (Obligatorio)

Especifica una descripción del grupo de servidores. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco.

### Ejemplo: Actualizar la descripción de un grupo de servidores

Actualizar la descripción del grupo de servidores denominado WEST\_COMPLEX por "Western Region Complex".

```
update servergroup west_complex
description="western region complex"
```

### Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE SERVERGROUP

Comando	Descripción
COPY SERVERGROUP	Crea una copia de un grupo de servidores.
DEFINE SERVERGROUP	Define un nuevo grupo de servidores.
DELETE SERVERGROUP	Suprime un grupo de servidores.
QUERY SERVERGROUP	Muestra información sobre grupos de servidores.
RENAME SERVERGROUP	Redenomina un grupo de servidores.

## UPDATE SPACETRIGGER (Actualizar los desencadenantes de espacio)

Utilice este comando para actualizar los valores de los desencadenantes que determinan cuándo y cómo ha de resolver el servidor las insuficiencias de las agrupaciones de almacenamiento que utilizan clases de dispositivo FILE de acceso secuencial y DISK de acceso aleatorio.

En el caso de las agrupaciones de almacenamiento con un parámetro RECLAMATIONTYPE=SNAPLOCK, no están activados los desencadenantes de espacio.

Importante: Las funciones de desencadenante de espacio y los cálculos de espacio de la agrupación de almacenamiento tienen en cuenta el espacio que queda en cada directorio. Se recomienda asociar cada directorio a un sistema de archivos distinto. Si especifica varios directorios para una clase de dispositivo y los directorios residen en el mismo sistema de archivos, el servidor calcula el espacio añadiendo valores que representan el espacio que resta en cada directorio. Estos cálculos de espacio serán incorrectos. En lugar de seleccionar una agrupación de almacenamiento con espacio suficiente para una operación, puede que el servidor seleccione la agrupación de almacenamiento incorrecta y que se produzca una condición de insuficiencia de espacio de forma prematura. Para los desencadenantes de espacio, un cálculo no preciso podría dar lugar a la imposibilidad de expandir el espacio disponible en una agrupación de almacenamiento. La imposibilidad de expandir espacio en una agrupación de almacenamiento es una de las condiciones que pueden causar que un desencadenante pase a estar inhabilitado. Si un desencadenante se inhabilita porque el espacio de una agrupación de almacenamiento no ha podido expandirse, puede volver a habilitar el desencadenante con el siguiente comando: `update spacetrigger stg`. No es necesario realizar más cambios en el desencadenante de espacio.

Consulte el comando `DEFINE SPACETRIGGER` para obtener más información.

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento sin restricciones.

## Sintaxis

```
>>-UPDate SPACETrigger--STG--+-+-----+----->
                               '-Fullpct----porcentaje-'
>-+-----+----->
  '-SPACEexpansion----porcentaje-'
>-+-----+----->
  '-EXPansionprefix----prefijo-'
>-+-----+-----<
  '-STGPOOL----nombre_agrupación_almacenamiento-'
```

## Parámetros

### STG (Necesario)

Especifica un desencadenante de espacio de la agrupación de almacenamiento.

### Fullpct

Este parámetro especifica el porcentaje de utilización de la agrupación de almacenamiento.

Cuando se sobrepasa este valor, el desencadenante de espacio crea nuevos volúmenes.


Puede determinar la utilización de la agrupación de almacenamiento ejecutando el comando `QUERY STGPOOL` con `FORMAT=DETAILED`. El porcentaje de utilización de la agrupación de almacenamiento se muestra en el campo "Util. desencadenante espacio". El cálculo de este porcentaje no incluye volúmenes reutilizables potenciales. El cálculo de la utilización del porcentaje utilizado para la migración y la reclamación, no obstante, sí incluye los volúmenes reutilizables potenciales.


### SPACEexpansion

Para los desencadenantes de espacio de las agrupaciones de almacenamiento de tipo `FILE` de acceso secuencial, este parámetro se utiliza para determinar el número de volúmenes adicionales que se crean en la agrupación de almacenamiento. Los volúmenes se crean utilizando el valor de `MAXCAPACITY` de la clase de dispositivo de la agrupación de almacenamiento. En desencadenantes de espacio para las agrupaciones de almacenamiento `DISK` de acceso aleatorio, el desencadenante de espacio crea un único volumen por medio del valor `EXPANSIONPREFIX`.

### EXPansionprefix

Este parámetro especifica el prefijo que el servidor utiliza para crear nuevos archivos de agrupación de almacenamiento. Este parámetro es opcional y sólo se aplica a la clase de dispositivo `DISK` de acceso aleatorio. El prefijo predeterminado es la ruta de instalación del servidor.



El prefijo puede incluir uno o varios caracteres de separación de directorios; por ejemplo:  Sistemas operativos AIX


 Sistemas operativos Linux

`/opt/tivoli/tsm/server/bin/`

 Sistemas operativos Windows

`c:\Archivos de programa\tivoli\tsm\`

 Sistemas operativos AIX  Sistemas operativos Linux Puede especificar hasta 250 caracteres. Si especifica un prefijo que no es válido, la expansión automática podría no ejecutarse correctamente.

 Sistemas operativos Windows Puede especificar hasta 200 caracteres. Si el servidor se ejecuta como servicio de Windows, el prefijo predeterminado es el directorio c:\wnnt\system32. Si especifica un prefijo que no es válido, la expansión automática podría no ejecutarse correctamente.

Este parámetro no es válido para desencadenantes de espacio de agrupaciones de almacenamiento de acceso secuencial FILE. Los prefijos se obtienen de los directorios especificados con la clase de dispositivo asociada.

#### STGPOOL

Especifica la agrupación de almacenamiento asociada a este desencadenante de espacio. Si no se especifica el parámetro STGPOOL, se actualizará el desencadenante de espacio de agrupación de almacenamiento predeterminado.

Este parámetro no se aplica a las agrupaciones de almacenamiento con el parámetro RECLAMATIONTYPE=SNAPLOCK.

## Ejemplo: incrementar la cantidad de espacio para una agrupación de almacenamiento

Incrementar la cantidad de espacio de una agrupación de almacenamiento un 50 por ciento cuando se alcance el 80 por ciento de utilización de los volúmenes existentes. Se creará el espacio en los directorios asociados con la clase de dispositivo.

```
update spacetrigger stg spaceexpansion=50 stgpool=file
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE SPACETRIGGER

Comando	Descripción
DEFINE SPACETRIGGER	Define un desencadenante de espacio para ampliar el espacio de una agrupación de almacenamiento.
DELETE SPACETRIGGER	Elimina el desencadenante de espacio de agrupación de almacenamiento.
QUERY SPACETRIGGER	Visualiza información acerca de un desencadenante de espacio de agrupación de almacenamiento.

## UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)

Utilice este mandato para actualizar un umbral de supervisión de estado existente.

Los umbrales de supervisión de estado comparan las condiciones definidas con las consultas de servidor de supervisión de estado e insertan los resultados en la tabla de supervisión de estado.

Se pueden definir varios umbrales para una actividad. Por ejemplo, puede crear un umbral que proporcione un estado de aviso si la utilización de capacidad de agrupación de almacenamiento es superior al 80%. A continuación, puede crear otro umbral que proporcione el estado de error si la utilización de capacidad de agrupación de almacenamiento es superior al 90%.

Nota: Si ya se ha definido un umbral para una condición EXISTS, no puede definir otro umbral con uno de los otros tipos de condición.

## Sintaxis

```
>>--UPDate STAtusthreshold--nombre_umbral--+-----+-->
                                   '-Activity---nombre_actividad-'
>--+-----+-----+-----+----->
   '-Condition--++EXists--+'  '-Value---valor-'
      +-GT-----+
      +-GE-----+
      +-LT-----+
      +-LE-----+
      '-Equal--'
>--+-----+-----+-----><
   '-Status---++Normal--+'
      +-Warning--+
```

## Parámetros

---

nombre\_umbral (Necesario)

Especifica el nombre de umbral que desea actualizar. El nombre de no puede tener más de 48 caracteres de longitud.

actividad

Especifique este valor para cambiar la actividad para un umbral existente. Este parámetro es opcional. Especifique uno de los siguientes valores:

PROCESSSUMMARY

Especifica el número de procesos que están activos actualmente.

SESSIONSUMMARY

Especifica el número de sesiones que están activas actualmente.

CLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente que están activas actualmente.

SCHEDCLIENTSESSIONSUMMARY

Especifica el número de sesiones de cliente planificadas.

DBUTIL

Especifica el porcentaje de utilización de base de datos. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DBFREESPACE

Especifica el espacio libre disponible en la base de datos en gigabytes.

DBUSEDSPACE

Especifica la cantidad de espacio de base de datos que se utiliza, en gigabytes.

ARCHIVELOGFREESPACE

Especifica el espacio libre que está disponible en el registro de archivo, en gigabytes.

STGPOOLUTIL

Especifica el porcentaje de utilización de agrupación de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

STGPOOLCAPACITY

Especifica la capacidad de agrupación de almacenamiento en gigabytes.

AVGSTGPOOLUTIL

Especifica el porcentaje medio de utilización de agrupación de almacenamiento en todas las agrupaciones de almacenamiento. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

TOTSTGPOOLCAPACITY

Especifica la capacidad total de agrupación de almacenamiento en gigabytes para todas las agrupaciones de almacenamiento disponibles.

TOTSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas.

TOTRWSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas que se puede leer o en las que se puede escribir.

TOTNOTRWSTGPOOLS

Especifica el número de agrupaciones de almacenamiento definidas que no se pueden leer o en las que no se puede escribir.

STGPOOLINUSEANDDEFINED

Especifica el número total de volúmenes definidos que se están utilizando.

ACTIVELOGUTIL

Especifica el porcentaje de utilización actual del registro activo. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

ARCHLOGUTIL

Especifica la utilización actual del registro de archivado. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

CPYSTGPOOLUTIL

Especifica el porcentaje de utilización para una agrupación de almacenamiento de copia. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

PMRYSTGPOOLUTIL

Especifica el porcentaje de utilización para una agrupación de almacenamiento primario. El valor de umbral de aviso predeterminado es el 80% y el valor de umbral de error predeterminado es el 90%.

DEVCLASSPCTDRVOFFLINE

Especifica el porcentaje de utilización de las unidades que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

DEVCLASSPCTDRVPOLLING



Especifica el sondeo de unidades, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTLIBPATHSOFFLINE**

Especifica las rutas de biblioteca que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTPATHSOFFLINE**

Especifica el porcentaje de rutas de clase de dispositivo que están fuera de línea, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTDISKSNOTRW**

Especifica el porcentaje de discos que no se pueden grabar para la clase de dispositivo de disco. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**DEVCLASSPCTDISKSUNAVAILABLE**

Especifica el porcentaje de volúmenes de disco que no están disponibles, por clase de dispositivo. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**FILEDEVCLASSPCTSCRUNALLOCATABLE**

Especifica el porcentaje de volúmenes reutilizables que el servidor no puede asignar para una determinada clase de dispositivo de archivo no compartido. El valor de umbral de aviso predeterminado es el 25% y el valor de umbral de error predeterminado es el 50%.

**Condition**

Especifique este valor para cambiar la condición de un umbral existente. Este parámetro es opcional. Especifique uno de los siguientes valores:

**EXists**

Crea un indicador de supervisión de estado si existe la actividad.

**GT**

Crea un indicador de supervisión de estado si la salida de actividad es mayor que el valor especificado.

**GE**

Crea un indicador de supervisión de estado si la salida de actividad es mayor que o igual al valor especificado.

**LT**

Crea un indicador de supervisión de estado si la salida de actividad es menor que el valor especificado.

**LE**

Crea un indicador de supervisión de estado si la salida de actividad es menor que o igual al valor especificado.

**EQual**

Crea un indicador de supervisión de estado si la salida de actividad es igual al valor especificado.

**Value**

Especifique este parámetro para cambiar el valor que se compara con la salida de actividad para la condición especificada. Puede especificar un entero en el rango 0 – 999999999999999.

**Status**

Especifique este valor para cambiar el estado del indicador que se crea en la supervisión de estado si pasa la condición que se está evaluando. Este parámetro es opcional. Especifique uno de los siguientes valores:

**Normal**

Especifica que el indicador de estado tiene un valor de estado normal.

**Aviso**

Especifica que el indicador de estado tiene un valor de estado de aviso.

**Error**

Especifica que el indicador de estado tiene un valor de estado de error.

## Actualizar un umbral de estado existente

Actualice un umbral de estado para el porcentaje medio de programa de utilidad de agrupación de almacenamiento emitiendo el mandato siguiente:

```
update statusthreshold avgstgpl "AVGSTGPOOLUTIL" value=90 condition=gt status=error
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con UPDATE STATUSTHRESHOLD

Comando	Descripción
DELETE STATUSTHRESHOLD (Suprimir un umbral de supervisión de estado)	Suprime un umbral de supervisión de estado.

Comando	Descripción
QUERY MONITORSTATUS (Consultar el estado de supervisión)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY MONITORSETTINGS (consultar la configuración de los valores de alertas de supervisión y de estado del servidor)	Muestra información sobre los valores de las alertas de supervisión y el estado del servidor.
QUERY STATUSTHRESHOLD (Consultar umbrales de supervisión de estado)	Visualiza información sobre un umbral de supervisión de estado.
SET STATUSMONITOR (Especifica si se debe habilitar la supervisión de estado)	Especifica si se debe habilitar la supervisión de estado.
SET STATUSATRISKINTERVAL (Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente)	Especifica si se debe habilitar la evaluación de intervalo de actividad en peligro de cliente.
SET STATUSREFRESHINTERVAL (Defina el intervalo de renovación para la supervisión de estado)	Especifica el intervalo de renovación para la supervisión de estado.
SET STATUSSKIPASFAILURE (Especifica si se deben utilizar archivos omitidos en peligro de cliente como evaluación de error)	Especifica si se deben utilizar los archivos ignorados en peligro de cliente como evaluación de error.
UPDATE STATUSTHRESHOLD (Actualizar un umbral de supervisión de estado)	Cambia los atributos de un umbral de supervisión de estado existente.

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento)

Utilice este comando para cambiar una agrupación de almacenamiento.

Restricción: Si un cliente utiliza la función de escritura simultánea y la deduplicación de datos, la función de deduplicación de datos se desactiva durante el proceso de copia de seguridad en una agrupación de almacenamiento.




El mandato UPDATE STGPOOL tiene seis formatos. La sintaxis y los parámetros de cada formato se definen por separado.

Tabla 1. Comandos relacionados con UPDATE STGPOOL

Comando	Descripción
BACKUP STGPOOL	Realiza una copia de seguridad de una agrupación de almacenamiento primaria en una agrupación de almacenamiento de copia.
COPY ACTIVATEDATA	Copia los datos de copia de seguridad activos.
DEFINE COLLOGROUP	Define un grupo de proximidad.
DEFINE COLLOCMEMBER	Agrega un nodo de cliente o espacio de archivos a un grupo de proximidad.
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DELETE COLLOGROUP	Suprime un grupo de proximidad.
DELETE COLLOCMEMBER	Suprime un nodo de cliente o espacio de archivos de un grupo de proximidad.
DELETE STGPOOL	Suprime una agrupación de almacenamiento de un almacenamiento del servidor.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
MOVE MEDIA	Mueve los volúmenes de agrupaciones de almacenamiento gestionados por una biblioteca automatizada.
QUERY COLLOGROUP	Muestra información acerca de los grupos de proximidad.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY NODEDATA	Visualiza información sobre la ubicación y el tamaño de los datos para un nodo cliente.
QUERY SHREDSTATUS	Muestra información sobre datos en espera de ser destruidos.

Comando	Descripción
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
RESTORE STGPOOL	Restaura los archivos en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento de copia.
RESTORE VOLUME	Restaura los archivos almacenados en volúmenes especificados en una agrupación de almacenamiento primaria desde las agrupaciones de almacenamiento primarias.
SET DRMDBBACKUPEXPIREDDAYS	Especifica el criterio para la caducidad de la serie de copia de seguridad de base de datos.
SHRED DATA	Inicia manualmente el proceso de destruir datos suprimidos.
UPDATE COLLOCGROUP	Actualiza la descripción de un grupo de proximidad.

- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores en la nube)  
Utilice este mandato para actualizar una agrupación de almacenamiento de contenedor en un entorno de nube. Las agrupaciones de almacenamiento en la nube no están soportadas en Linux on System z.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de directorio)  
Utilice este mandato para actualizar una agrupación de almacenamiento de contenedores de directorio.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)  
Utilice este mandato para actualizar una agrupación de almacenamiento de copia de contenedor.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso aleatorio)  
Utilice este comando para actualizar una agrupación de almacenamiento de acceso aleatorio.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso secuencial)  
Utilice este comando para actualizar una agrupación de almacenamiento de acceso secuencial.
- UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de acceso secuencial)  
Utilice este comando para actualizar una agrupación de almacenamiento de copia de acceso secuencial.
- UPDATE STGPOOL (Actualizar un acceso secuencial de datos activos)  
Utilice este comando para actualizar una agrupación de datos activos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores en la nube)

Utilice este mandato para actualizar una agrupación de almacenamiento de contenedor en un entorno de nube. Las agrupaciones de almacenamiento en la nube no están soportadas en Linux on System z.

El método preferido para definir y configurar una agrupación de almacenamiento del contenedor en la nube es utilizar Centro de operaciones. Para obtener instrucciones y sugerencias para el Centro de operaciones y la interfaz de línea de mandatos, consulte la sección Configuración de una agrupación de almacenamiento de contenedor en la nube para el almacenamiento de datos.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

### Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DESCRiption----descripción-'
>--+-----+--+-----+----->
  '-CLOUDType---+---Swift-----+'  '-CLOUDUrl----url_nube-'
      +-Softlayer-+
      '-VlSwift---'
>--+-----+----->
  |                                     (1) |
  '-IDentity----identidad_nube-----'
```

```

>-----+-----+-----+-----+----->
  '-Password-----contraseña-'

>-----+-----+-----+-----+----->
  '-CLOUDLocation-----+OFFpremise+-'
                          '-ONpremise--'

>-----+-----+-----+-----+----->
  |                               (2) |
  '-BUCKETName-----nombre_grupo-----'

>-----+-----+-----+-----+----->
  '-ACCEss-----+READWrite-----+'
                      +-READOnly-----+
                      +-UNAvailable-+
                      '-DESTroyed---'

>-----+-----+-----+-----+----->
  '-MAXWriters-----+NOLimit-----+-'
                          '-máximo_grabadores-'

>-----+-----+-----+-----+----->
  '-REUsedelay-----días-'

>-----+-----+-----+-----+-----<
  |                               .-COMPRession-----Yes-----.|
  '-ENCRypt-----+Yes-+-+-----+-----+-----+-----+-----+'
                      '-No--'   '-COMPRession-----+Yes-+-'
                                   '-No--'

```

**Notas:**

1. Si ha especificado CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY.
2. Este parámetro solo es válido si especifica CLOUDTYPE=S3.

## Parámetros

**nombre\_agrupación (Obligatorio)**

Especifica la agrupación de almacenamiento que se actualiza. Este parámetro es necesario.

**DESCRiption**

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

**CLOUDType**

Especifica el tipo de entorno de nube donde está configurando una agrupación de almacenamiento. Este parámetro es opcional. Especifique uno de los siguientes valores:

**SOftlayer**

Especifica que la agrupación de almacenamiento utiliza un sistema de computación en la nube SoftLayer de IBM.

**SWift**

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 2 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

**V1Swift**

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

**Restricción:** Si ha utilizado el mandato DEFINE STGPOOL para definir una agrupación de almacenamiento con CLOUDTYPE=S3 (Simple Storage Service), no puede cambiar a otro tipo de nube utilizando el mandato UPDATE STGPOOL. Asimismo, no puede cambiar el tipo de nube de una agrupación de almacenamiento no S3 a S3 utilizando el mandato UPDATE STGPOOL.

**CLOUDUrL**

Especifica el URL del entorno de nube donde está configurando la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un URL de punto final de región, una dirección IP de aplicación de acceso, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo <https://> o <http://> al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL no se valida hasta que empieza la primera copia de seguridad.

Para obtener más información sobre cómo encontrar estos valores, seleccione su proveedor de servicios en la nube de la lista que aparece en la página Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos.

Consejo: Para utilizar más de una aplicación de accesos de IBM® Cloud Object Storage, liste las direcciones IP de las aplicaciones de accesos separadas por una barra vertical (|), sin espacios, como `CLOUDURL=<accesser_URL1>|<accesser_URL2>|<accesser_URL3>`. Utilice varios accesoros para mejorar el rendimiento. Si está utilizando la solución IBM SoftLayer Cloud Object Store S3, sólo se necesita un accesor.

#### Identity

Especifica el ID de usuario para la nube que se ha especificado en el parámetro `STGTYPE=CLOUD`. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si ha especificado `CLOUDTYPE=AZURE`, no especifique el parámetro `IDENTITY`. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

#### PASSword (Obligatorio)

Especifica la contraseña para la nube especificada en el parámetro `STGTYPE=CLOUD`. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres. Los parámetros `IDENTITY` y `PASSWORD` no se validan hasta que empieza la primera copia de seguridad.

#### CLOUDLocation

Especifica la ubicación física de la nube que se especifica en el parámetro `CLOUD`. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

- OFFpremise
- ONpremise

#### BUCKETName

Especifica el nombre para un grupo AWS (Amazon Web Services) o una caja fuerte IBM Cloud Object Storage que se va a utilizar con esta agrupación de almacenamiento. Los grupos AWS y las cajas fuertes de IBM Cloud Object Storage se utilizan del mismo modo que los contenedores en una agrupación de almacenamiento de contenedores en la nube. Este parámetro es opcional y sólo es válido si el tipo de nube de esta agrupación de almacenamiento es S3. Si no existe el nombre que especifica, el servidor crea un grupo o caja fuerte con el nombre especificado antes de utilizar el grupo o caja fuerte. Siga las restricciones de asignación de nombres de su proveedor de nube cuando especifique este parámetro. Revise los permisos del grupo o caja fuerte y asegúrese de que las credenciales de esta agrupación de almacenamiento tienen permiso de lectura, grabación, lista y supresión de objetos en este grupo o caja fuerte.

Restricción: No puede cambiar el grupo o caja fuerte si existen contenedores en la nube en esta agrupación de almacenamiento.

#### ACCess

Especifica cómo acceden los nodos cliente y los procesos de servidor a la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### READWrite

Especifica que los nodos de cliente y los procesos de servidor pueden realizar operaciones de lectura y grabación en la agrupación de almacenamiento.

##### READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en la agrupación de almacenamiento.

##### UNAVailable

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento. Como resultado, las copias de seguridad y las restauraciones fallan para esta agrupación de almacenamiento. Puede utilizar este valor para especificar que el proveedor de servicios de nube no está disponible temporalmente.

##### DESTroyed

Especifica que los nodos cliente y los procesos del servidor no pueden acceder a la agrupación de almacenamiento porque el proveedor de servicios de nube está permanentemente no disponible. Las copias de seguridad y las restauraciones fallan para esta agrupación de almacenamiento, pero los intentos de suprimir objetos y contenedores de esta agrupación de almacenamiento se completan satisfactoriamente.

#### MAXWriters

Especifica el número máximo de sesiones de grabación que se pueden ejecutar simultáneamente en la agrupación de almacenamiento. Especifique un número máximo de sesiones de grabación para controlar que el rendimiento de la agrupación de almacenamiento en la nube no afecte negativamente a otros recursos del sistema. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### NOLimit

Especifica que no existe un límite de tamaño máximo para el número de grabadores que puede utilizar. Este es el valor predeterminado.

##### máximo\_grabadores

Limita el número máximo de grabadores que puede utilizar. Especifique un número entero del 1 al 99999.

#### REUsedelay

Especifica el número de días que deben transcurrir después de que se hayan eliminado todas las extensiones deduplicadas de una agrupación de almacenamiento en la nube. Este parámetro controla la duración con que las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento en la nube. Cuando caduca el valor especificado para este parámetro las extensiones deduplicadas se suprimen de la agrupación de almacenamiento en la nube. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento en la nube pasado un día.

días

Puede especificar un entero en el rango 0 – 9999.

Consejo: Defina este parámetro en un valor que sea mayor que el número especificado para el mandato SET DRMDBBACKUPEXPIREDDAYS. Al establecer este parámetro en un valor superior, puede garantizar que cuando restaure la base de datos a un nivel anterior, las referencias a los archivos de la agrupación de almacenamiento seguirán siendo válidas.

#### ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente.

Este parámetro es opcional. El valor predeterminado depende de la ubicación física de la nube, que se especifica mediante el parámetro CLOUDLOCATION. Si la nube está fuera de las instalaciones, el servidor cifra los datos de forma predeterminada. Si la nube está en las instalaciones, el servidor no cifra los datos de forma predeterminada.

#### COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

## Ejemplo 1: actualizar una agrupación de almacenamiento en la nube para especificar un número máximo de sesiones de datos

---

Actualice una agrupación de almacenamiento en la nube denominada STGPOOL1 y especifique un máximo de 10 sesiones de datos.

```
update stgpool stgpool1 maxwriters=10
```

## Ejemplo 2: Actualizar la descripción de una agrupación de almacenamiento en la nube




---

Actualice una agrupación de almacenamiento en la nube denominada STGPOOL2. Elimine la descripción existente de la agrupación de almacenamiento.

```
update stgpool stgpool2 cloudurl=http://123.234.123.234:5000/v2.0  
identity=admin:admin password=password description=""
```

#### Tareas relacionadas:

Configuración de una agrupación de almacenamiento de contenedor de nube para el almacenamiento de datos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de contenedores de directorio)

---

Utilice este mandato para actualizar una agrupación de almacenamiento de contenedores de directorio.

### Clase de privilegio

---



Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. El valor predeterminado es NOLIMIT. Especifique uno de los siguientes valores:

**NOLimit**

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

**tamaño\_máximo\_archivo**

Limita el tamaño máximo de archivo físico. Puede especificar un entero del 1 al 999999, seguido de un factor de ajuste proporcional. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo para esta agrupación de almacenamiento son 5 GB. Utilice uno de las siguientes unidades de medida:

Tabla 1. Factor de escala para el tamaño de archivo máximo

Factor de escala	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

Consejo: Si no especifica una unidad de medida para el tamaño máximo de archivo, el valor se especifica en bytes.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 2. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

Agrupación especificada	Resultado
No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor no almacena el archivo.
Se ha especificado una agrupación como la siguiente agrupación de almacenamiento de la jerarquía.	El servidor almacena el archivo en la agrupación de almacenamiento que ha especificado.

Consejo: Si también especifica el parámetro NEXTstgpool, actualice una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos durante el proceso de deduplicación de datos, el servidor considera que el tamaño del proceso de deduplicación de datos es el tamaño de archivo. Si el tamaño total de todos los archivos del proceso es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

**MAXWriters**

Especifica el número máximo de hebras de E/S que se pueden ejecutar simultáneamente en la agrupación de almacenamiento. Especifique un número máximo de hebras de E/S para controlar el número de hebras de E/S que se graban al mismo tiempo en la agrupación de almacenamiento de contenedores de directorio. Este parámetro es opcional. Como práctica recomendada, utilice el valor predeterminado NOLIMIT. Puede especificar uno de los siguientes valores:

**NOLimit**

Especifica que no se graba ningún número máximo de hebras de E/S en la agrupación de almacenamiento.

**máximo\_grabadores**

Limita el número máximo de hebras de E/S que puede utilizar. Especifique un número entero del 1 al 99999.

**NEXTstgpool**

Especifica el nombre de una agrupación de almacenamiento secuencial primaria o de acceso aleatorio en la que se almacenan los archivos cuando la agrupación de almacenamiento de contenedores de directorio está llena. Este parámetro es opcional.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

**PROTECTstgpool**

Especifica el nombre de la agrupación de almacenamiento de contenedores de directorio en el servidor de destino donde se realiza la copia de seguridad de los datos cuando utiliza el mandato PROTECT STGPOOL para esta agrupación de



almacenamiento. Este parámetro es opcional.

#### PROTECTLOCALstgpools

Especifica el nombre de la agrupación de almacenamiento de copia de contenedor en un dispositivo local en el que se realiza la copia de seguridad de los datos. Esta agrupación de almacenamiento de copia de contenedor será una agrupación de almacenamiento de destino local cuando utilice el mandato PROTECT STGPOOL. Puede especificar un máximo de dos nombres de agrupación de almacenamiento de copia de contenedor para actualizarlos. Puede separar varios nombres con comas y sin espacios intercalados. La longitud máxima de cada nombre es de 30 caracteres. Este parámetro es opcional.

Para añadir o eliminar agrupaciones de almacenamiento de copia de contenedor, especifique los nombres de agrupación de almacenamiento de copia de contenedor a incluir. Por ejemplo, si la agrupación de almacenamiento de copia de contenedor incluye COPY1 y desea añadir COPY2, especifique PROTECTLOCALSTGPOOLS=COPY1,COPY2. Para eliminar todas las agrupaciones de almacenamiento de copia de contenedor existentes asociadas a la agrupación de almacenamiento primaria, especifique una serie nula (""). Por ejemplo, COPYSTGPOOLS="".

#### REUsedelay

Especifica el número de días que deben transcurrir antes de que se eliminen todas las extensiones con duplicados eliminados de una agrupación de almacenamiento de contenedores de directorio. Este parámetro controla el tiempo durante el cual las extensiones con duplicados eliminados están asociadas a una agrupación de almacenamiento de contenedores de directorio. Cuando expira el período de tiempo especificado para el parámetro, las extensiones con duplicados eliminados se suprimen de la agrupación de almacenamiento de contenedores de directorio. El valor predeterminado es 1. Especifique uno de los siguientes valores:

días

Especifique un número entero del 0 al 9999.

1

Especifica que las extensiones con duplicados eliminados se suprimen de una agrupación de almacenamiento de contenedores de directorio al cabo de un día.

Consejo: Establezca este parámetro en un valor mayor que el número especificado como periodo de copia de seguridad de base de datos, para asegurarse de que las extensiones de datos continúan siendo válidas cuando restaura la base de datos a otro nivel.

#### ENCRypt

Especifica si el servidor cifra los datos de cliente antes de que se graben en la agrupación de almacenamiento. Puede especificar los siguientes valores:

Yes

Especifica que el servidor cifra los datos de cliente.

No

Especifica que el servidor no cifra los datos de cliente.

#### COMPRession

Especifica si los datos están comprimidos en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

No

Especifica que los datos no están comprimidos en la agrupación de almacenamiento.

Yes

Especifica que los datos están comprimidos en la agrupación de almacenamiento. Este es el valor predeterminado.

## Ejemplo: Actualización de una agrupación de almacenamiento para especificar un número máximo de sesiones de datos

---

Actualice una agrupación de almacenamiento denominada STGPOOL1 y especifique un máximo de 10 sesiones de datos.

```
update stgpool stgpool1 maxwriters=10
```

## Ejemplo: Actualización de una agrupación de almacenamiento para especificar el tamaño máximo

---

Actualice una agrupación de almacenamiento denominada STGPOOL2. La agrupación de almacenamiento especifica el tamaño máximo de archivo que el servidor puede almacenar en la agrupación de almacenamiento en 100 megabytes.

```
update stgpool stgpool2 maxsize=100M
```







## Ejemplo: Actualización de la descripción de una agrupación de almacenamiento

---

Actualice una agrupación de almacenamiento denominada STGPOOL3. Elimine la descripción existente de la agrupación de almacenamiento.

```
update stgpool stgpool3 description=""
```

Tabla 3. Comandos relacionados con UPDATE STGPOOL

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY CONTAINER	Visualiza información sobre un contenedor.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows           UPDATE STGPOOLDIRECTORY	Cambia los atributos de un directorio de agrupaciones de almacenamiento.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows	

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)

Utilice este mandato para actualizar una agrupación de almacenamiento de copia de contenedor.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

### Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+-----+-----+-----+----->
  '-MAXSCRatch---número-' '-DEscription---descripción-'
>--+-----+-----+-----+-----+----->
  '-ACCess---+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>--+-----+-----+-----+-----+----->
  '-PROTECTProcess---número-' '-REclaim---porcentaje-'
>--+-----+-----+-----+-----+----->
  '-RECLAIMLIMit---+NOLimit---+'
      '-límite_vol-'
>--+-----+-----+-----+-----+-----><
  '-REUsedelay---días-'
```

### Parámetros

nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de actualizar.

MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Puede especificar un entero en el rango 0 - 100000000. Si el servidor puede solicitar volúmenes reutilizables según sean necesarios, no tiene que definir cada volumen que se va a utilizar.

El valor de este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

#### DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

#### ACCess

Especifica cómo pueden acceder a los datos de la agrupación de almacenamiento los procesos como por ejemplo la protección y la reparación de agrupación de almacenamiento. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

##### READWrite

Especifica que el servidor puede leer y grabar en volúmenes de la agrupación de almacenamiento.

##### READOnly

Especifica que el servidor sólo puede leer volúmenes de la agrupación de almacenamiento. El servidor puede utilizar datos de la agrupación de almacenamiento para restaurar extensiones en agrupaciones de almacenamiento de contenedor de directorios. No se permiten operaciones que graban en la agrupación de almacenamiento de contenedor de directorios.

##### UNAVailable

Especifica que el servidor no puede acceder a los datos almacenados en volúmenes de la agrupación de almacenamiento.

#### PROTECTPRocess

Especifica el número máximo de procesos paralelos que se utilizan cuando se emite el mandato PROTECT STGPOOL para copiar datos en esta agrupación desde una agrupación de almacenamiento de contenedor de directorios. Este parámetro es opcional. Especifique un valor del 1 al 20.

El tiempo que es necesario para realizar la operación de copia se puede reducir utilizando varios procesos paralelos. Sin embargo, en algunos casos, cuando se ejecutan varios procesos, uno o varios procesos deben esperar a utilizar un volumen que ya está en uso por un proceso distinto.

Al seleccionar este valor, tenga en cuenta el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de cinta, el servidor utiliza un punto de montaje y una unidad. El número de puntos de montaje y unidades disponibles depende del límite de montaje de la clase de dispositivo de la agrupación de almacenamiento y de otra actividad del servidor y del sistema.

Si utiliza la opción de vista previa en el mandato PROTECT STGPOOL, sólo se utiliza un proceso y no se necesitan puntos de montaje ni unidades.

#### REClaim

Especifica cuando un volumen pasa a ser seleccionable para la reclamación y la reutilización. Especifica la elegibilidad como el porcentaje de espacio de un volumen que está ocupado por las extensiones que ya no se almacenan en la agrupación de almacenamiento de contenedor de directorios. La reclamación mueve cualesquiera extensiones que sigan almacenadas en la agrupación de almacenamiento de contenedor de directorios de volúmenes elegibles a otros volúmenes. La reclamación se produce sólo cuando un mandato PROTECT STGPOOL almacena datos en esta agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero en el rango 1 - 100. El valor 100 especifica que los volúmenes de esta agrupación de almacenamiento no se reclaman.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Al establecer un valor de reclamación de 50 o superior, los datos que se mueven de dos volúmenes reclamados no utilizan más del equivalente de un nuevo volumen.

Tenga cuidado al utilizar la reclamación con las agrupaciones de almacenamiento de copia de contenedor que tienen volúmenes fuera del local. Cuando un volumen fuera del local pasa a ser seleccionable para reclamación, el servidor devuelve las extensiones del volumen a la ubicación del local. Si se produce un siniestro en el local, el servidor puede obtener extensiones del volumen fuera del local si la base de datos restaurada hace referencia a las extensiones del volumen de fuera del local. Por lo tanto, para fines de recuperación ante siniestro, asegúrese de que planifica las copias de seguridad de bases de datos para que se ejecuten después de que se hayan ejecutado las planificaciones de protección de agrupaciones de almacenamiento y las planificaciones de desplazamiento de DRM, y asegúrese de que todos los volúmenes de copia de seguridad de bases de datos se trasladen fuera del local junto con los volúmenes de DRM.

Consejo: Establezca diferentes valores de reclamación para las agrupaciones de almacenamiento de copia de contenedor fuera del local y dentro del local. Debido a que las agrupaciones de almacenamiento de copia de contenedor almacenan datos de eliminaciones de duplicados, las extensiones de datos abarcan varios volúmenes de cinta. Cuando seleccione un umbral de reclamación para una copia fuera del local, tenga en cuenta el número de puntos de montaje disponibles y el número de volúmenes de cinta que debe recuperar en caso de siniestro. Establecer un umbral más alto, significa que se deberán recuperar

más volúmenes que si se establece la reclamación en un valor inferior. Si se utiliza un umbral más bajo se reduce el número de puntos de montaje necesarios en caso de siniestro. El método preferido consiste en definir el valor de reclamación para copias externas en 60 y, para copias internas, en el intervalo 90 - 100.

**RECLAIMLIMIT**

Especifica el número máximo de volúmenes que reclama el servidor cuando se emite el mandato PROTECT STGPOOL y se especifican las opciones RECLAIM=YESLIMITED o RECLAIM=ONLYLIMITED. Este parámetro solo es válido para las agrupaciones de almacenamiento de copia de contenedor. Este parámetro es opcional. Puede especificar uno de los siguientes valores:

**NOLimit**

Especifica que todos los volúmenes de la agrupación de almacenamiento de copia de contenedor se procesen para la reclamación.

**límite\_vol**

Especifica el número máximo de volúmenes de la agrupación de almacenamiento de copia de contenedor que se reclaman. El valor que se especifique determinará cuántas nuevas cintas reutilizables están disponibles una vez completado el proceso de reclamación. Puede especificar un número comprendido entre 1 y 100000.

**REUsedelay**

Especifica el número de días que deben transcurrir desde que se suprimen todas las extensiones de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva al estado reutilizable. Este parámetro es opcional. Puede especificar un entero en el rango 0 – 9999. Un valor de 0 significa que un volumen se puede volver a grabar o devolver al estado reutilizable tan pronto como se han suprimido todas las extensiones del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a extensiones de la agrupación de almacenamiento seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. Si utiliza gestor recuperación ante siniestro, el número de días que se especifica para este parámetro debe ser igual al número que se especifica para el mandato SET DRMDBBACKUPEXPIREDDAYS.

## Ejemplo: Actualizar una agrupación de almacenamiento de copia de contenedor para retardar 30 días la reutilización de volumen

Actualizar la agrupación de almacenamiento llamada CONTAINER1\_COPY2 para cambiar el retardo de la reutilización de volumen a 30 días.

```
update stgpool container1_copy2 reusedelay=30
```

## Ejemplo: actualizar una agrupación de almacenamiento de copia de contenedor para limitar el número de volúmenes de cintas reclamados a 10

Actualice la agrupación de almacenamiento denominada CONTAINER1\_COPY2 para cambiar el límite de reclamación a 10 volúmenes.

```
update stgpool container1_copy2 reclaimlimit=10
```

Tabla 1. Mandatos relacionados con UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de contenedor)

Comando	Descripción
DEFINE STGPOOL (copia de contenedor)	Definir una agrupación de almacenamiento de copia de contenedor que almacena copias de datos de una agrupación de almacenamiento de contenedores de directorio.
PROTECT STGPOOL	Protege una agrupación de almacenamiento de contenedores de directorio.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.
REPAIR STGPOOL	Repara una agrupación de almacenamiento de contenedores de directorio.
UPDATE STGPOOL (contenedor de directorios)	Actualizar una agrupación de almacenamiento de contenedores de directorios.

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso aleatorio)

Utilice este comando para actualizar una agrupación de almacenamiento de acceso aleatorio.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

## Sintaxis

---

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+-----+----->
  '-DESCRiption----descripción-'
>--+-----+-----+----->
  '-ACCess----+READWrite----+'
    +-READOnly----+
    '-UNAVailable-'
>--+-----+-----+----->
  '-MAXSize----+tamaño_máximo_archivo+-'
    '-NOLimit-----'
>--+-----+-----+----->
  '-CRCData----+Yes+-'
    '-No--'
>--+-----+-----+----->
  '-NEXTstgpool----nombre_agrupación-'
>--+-----+-----+----->
  '-HIGhmig----percent-' '-LOWmig----percent-'
>--+-----+-----+----->
  '-CACHe----+Yes+-' '-MIGPRocess----number-'
    '-No--'
>--+-----+-----+----->
  '-MIGDelay----días-' '-MIGContinue----+Yes+-'
    '-No--'
>--+-----+-----+----->
  '-AUTOCopy----+None-----+'
    +-CLient----+
    +-MIGRation+-
    '-All-----'
>--+-----+-----+----->
  |           .-,------. |
  |           v             | |
  '-COPYSTGpools-----nombre_agrupación_copia+-'
>--+-----+-----+----->
  '-COPYContinue----+Yes+-'
    '-No--'
>--+-----+-----+----->
  |           .-,------. |
  |           v             | |
  '-ACTIVEDATApools-----nombre_agrupación_datos_activos+-'
  .-SHRED----0-----
>--+-----+-----+-----<
  '-SHRED----recuento_sobregrabación-'
```

## Parámetros

---

nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que se actualiza. Este parámetro es necesario.

DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

#### ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los siguientes valores:

##### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

##### READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

##### UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

#### MAXSize

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

##### NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

##### tamaño\_máximo\_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Consulte la tabla siguiente para obtener información sobre dónde se almacena un archivo cuando su tamaño excede el parámetro MAXSIZE.

Tabla 1. Dónde se almacena un archivo según el tamaño del archivo y la agrupación especificada

<b>El tamaño de archivo</b>	<b>Agrupación especificada</b>	<b>Resultado</b>
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Si especifica el siguiente parámetro de agrupación de almacenamiento, defina una agrupación de almacenamiento de la jerarquía para que no tenga límite acerca del tamaño máximo de archivo. Al no tener ningún límite sobre el tamaño como mínimo en una agrupación, se garantiza que el servidor puede almacenar el archivo al margen de su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

#### CRCDATA

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

##### Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se produce una carga general adicional para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

##### No

Especifica que los datos se almacenan sin información de CRC.

#### NEXTSTGPOOL

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. Este parámetro es opcional.

Para suprimir de la jerarquía de almacenamiento una agrupación de almacenamiento definida anteriormente, especifique una serie nula ("") para este valor.

Si no especifica ninguna agrupación de almacenamiento siguiente, se producen las acciones siguientes:

- El servidor no puede migrar los archivos de esta agrupación de almacenamiento
- El servidor no puede almacenar archivos que superen el tamaño máximo de esta agrupación de almacenamiento en otra agrupación de almacenamiento

#### Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor en la nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.

#### HIGHMIG

Especifica que el servidor inicia la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Este parámetro es opcional. Puede especificar un entero de 0 a 100.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por nodo, a la siguiente agrupación de almacenamiento, según se ha definido con el parámetro NEXTSTGPOOL. Puede especificar HIGHMIG=100 para impedir que se produzca la migración en esta agrupación de almacenamiento.

#### LOWMIG

Especifica que el servidor detiene la migración en esta agrupación de almacenamiento cuando la cantidad de datos que hay en la agrupación alcanza este porcentaje de la capacidad estimada de la agrupación. Puede especificar un entero del 0 al 99 para este parámetro opcional.

Cuando la migración se realiza por nodo o espacio de archivos, en función de la proximidad, el nivel de ocupación de la agrupación de almacenamiento puede caer por debajo del valor que ha especificado para este parámetro. Para vaciar la agrupación de almacenamiento, establezca LOWMIG=0.

#### CACHe

Especifica si el proceso de migración deja una copia en caché de un archivo en esta agrupación de almacenamiento una vez migrado el archivo a la siguiente agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

Yes

Especifica que está activada la función de caché.

No

Especifica que está desactivada la función de caché.

Si se utiliza la función de caché se puede mejorar la posibilidad de recuperar archivos, pero puede afectar al rendimiento de otros procesos.

#### MIGPRocess

Especifica el número de procesos que se utilizan para migrar los archivos de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero del 1 al 999.

Durante la migración, estos procesos se ejecutan en paralelo para proporcionar el potencial de mejorar los índices de migración.

Consejos:

- El número de procesos de migración depende de los siguientes valores:
  - El valor del parámetro MIGPROCESS
  - El valor de proximidad de la agrupación siguiente
  - El número de nodos o el número de grupos de proximidad con datos en la agrupación de almacenamiento que se está migrando

Para este ejemplo, `MIGPROCESS =6`, el parámetro `COLLOCATE` de la siguiente agrupación es `NODE`, pero hay solo dos nodos con datos en la agrupación de almacenamiento. El proceso de migración consta solo de dos procesos, no de seis. Si el parámetro `COLLOCATE` es el grupo `GROUP` y ambos nodos están en el mismo grupo, el proceso de migración consta solamente de un proceso. Si el parámetro `COLLOCATE` es `NO` o el grupo `FILESPACE`, y cada nodo tiene dos espacios de archivos con datos de copia de seguridad, el proceso de migración consta solamente de cuatro procesos.

- Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

#### MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Para calcular un valor para comparar con el valor `MIGDELAY` especificado, el servidor cuenta los elementos siguientes:

- El número de días que el archivo ha estado en la agrupación de almacenamiento
- El número de días, si hay alguno, desde que un cliente recuperó el archivo

El menor de ambos valores se compara con el valor de `MIGDELAY` especificado. Por ejemplo, si se cumplen todas las condiciones siguientes, no se migrará un archivo:

- Un archivo ha permanecido en una agrupación de almacenamiento durante cinco días.
- Un cliente ha accedido al archivo en los tres últimos días.
- El valor especificado para el parámetro `MIGDELAY` es cuatro días.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor predeterminado es 0, que significa que no se retardará la migración.

Si desea que el servidor cuente el número de días basándose tan solo en el momento en que se almacenó un archivo y no en el momento en el que se recuperó, utilice la opción del servidor `NORETRIEVEDATE`.

#### MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.



Puede especificar uno de los siguientes valores:

Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no satisfacen el tiempo de retardo de migración.

Si permite varios procesos de migración para la agrupación de almacenamiento, es posible que se migren algunos archivos que no satisfacen el tiempo de retardo de migración de forma innecesaria. Mientras un proceso migra los archivos que satisfacen el tiempo de retardo de migración, un segundo proceso puede empezar a migrar archivos que no satisfacen el tiempo de retardo de migración para alcanzar el umbral inferior de migración. El primer proceso que sigue migrando los archivos que satisfacen el tiempo de retardo de migración puede haber ocasionado que se alcance el umbral inferior de migración.

No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra archivos si éstos no cumplen el tiempo de retardo de migración.

#### AUTOCopy

Especifica cuándo IBM Spectrum Protect ejecuta operaciones de grabación simultáneamente en las agrupaciones de almacenamiento de copia y activas. Este parámetro afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPOLS. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDATAPOLS.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea esta inhabilitada.

CLient

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

#### COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Para agregar o eliminar una o varias agrupaciones de almacenamiento de copia, especifique el nombre de las agrupaciones que desee incluir en la lista actualizada. Por ejemplo, si la lista de agrupaciones de almacenamiento de copia incluye COPY1 y COPY2 y desea añadir COPY3, especifique COPYSTGPOLS=COPY1,COPY2,COPY3. Para eliminar todas las agrupaciones de almacenamiento de copia existentes asociadas con la agrupación de almacenamiento de copia principal, especifique una serie nula ("" ) para el valor (por ejemplo, COPYSTGPOLS="").

Al especificar un valor para el parámetro COPYSTGPOLS, también puede especificar un valor para el parámetro COPYCONTINUE. Si desea obtener más información, consulte el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPOOLS y ACTIVEATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia en las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect
- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricciones: No se admite la función de grabación simultánea en las siguientes operaciones de almacenamiento:

- Cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
- Operaciones de copias de seguridad de NAS. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia:
  - Las agrupaciones de almacenamiento de copia se ignoran
  - Los datos solo se almacenan en la agrupación de almacenamiento primaria

Atención: La función que proporciona el parámetro COPYSTGPOOLS no tiene como finalidad sustituir el mandato BACKUP STGPOOL. Si utiliza el parámetro COPYSTGPOOLS, continúe utilizando el mandato BACKUP STGPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

#### COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOOLS. Este parámetro es opcional. Cuando se especifica el parámetro COPYCONTINUE, debe existir una lista COPYSTGPOOLS o especificarse también el parámetro COPYSTGPOOLS.

Puede especificar los valores siguientes:

#### Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

#### No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

#### ACTIVEATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSGTPOOLS y ACTIVEATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro solamente está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos "NATIVE" o "NONBLOCK". Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - o NETAPPDUMP
  - o CELERRADUMP
  - o NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando se utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se aplica la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria especificada en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos:
  - o Las agrupaciones de datos activos se ignoran
  - o Los datos solo se almacenan en la agrupación de almacenamiento primaria
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el comando COPY ACTIVEATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVEATAPOOLS no tiene como finalidad sustituir al mandato COPY ACTIVEATA. Si utiliza el parámetro ACTIVEATAPOOLS, utilice el mandato COPY ACTIVEATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

#### SHRED

Especifica si los datos se van a sobregabar físicamente cuando se supriman. Este parámetro es opcional. Puede especificar un entero del 0 al 10.

Si especifica un valor de cero, el servidor suprime los datos de la base de datos. Sin embargo, el almacenamiento que se utiliza para contener los datos no se sobregaba, y los datos existirán en el almacenamiento hasta que se reutilice el almacenamiento para otros datos. Los datos se podrían descubrir y reconstruir tras haberlos suprimido. Si se cambia el valor (por ejemplo, se restablece en 0) no afecta a los datos que ya se han suprimido y están a la espera de sobregabarse.

Si especifica un valor superior a 0, el servidor suprime los datos lógicamente y físicamente. El servidor sobregaba el almacenamiento utilizado para contener los datos el número especificado de veces. Esta sobregabación aumenta la dificultad de descubrir y reconstruir los datos tras su supresión.

Para asegurarse de que todas las copias de los datos se destruyen, especifique un valor SHRED superior a cero para la agrupación de almacenamiento especificada en el parámetro NEXTSTGPOOL. No especifique ni COPYSTGPOOLS ni ACTIVEATAPOOLS. Normalmente la especificación de valores relativamente altos para el recuento de sobregabación mejora el nivel de seguridad, pero podría afectar negativamente al rendimiento.

La sobregabación de datos suprimidos se realiza de forma asíncrona tras completarse la operación de supresión. Por lo tanto, el espacio ocupado por los datos suprimidos permanecerá ocupado durante algún tiempo. El espacio no está disponible como espacio libre para nuevos datos.

No se puede utilizar un valor SHRED superior a cero si el valor del parámetro CACHE es YES. Si desea habilitar la destrucción de datos para una agrupación de almacenamiento existente para la que ya está habilitada la función de caché, debe cambiar el valor del parámetro CACHE a NO. Los archivos en caché existentes permanecerán en el almacenamiento, de forma que las posteriores solicitudes de recuperación se puedan cumplir rápidamente. Si se necesita espacio para almacenar datos nuevos, se borrarán los archivos en caché existentes de modo que el espacio que han ocupado pueda utilizarse para datos nuevos. Los archivos en caché existentes no se destruyen cuando se borran.

Importante: Después de que haya finalizado una operación de exportación y se hayan identificado los archivos para la exportación, los cambios que se realicen en el valor SHRED se ignorarán. Una operación de exportación que se ha suspendido retiene el valor de SHRED original durante toda la operación. Puede optar por cancelar la operación de exportación si considera

que el valor SHRED de la agrupación de almacenamiento compromete la operación. Puede volver a emitir el mandato de exportación después de realizar la operación de limpieza necesaria.

## Ejemplo: actualizar una agrupación de almacenamiento de acceso aleatorio para permitir la función de caché

Actualizar la agrupación de almacenamiento denominada BACKUPPOOL que es aleatoria para permitir la función de caché cuando el servidor migra los archivos a la siguiente agrupación de almacenamiento.

```
update stgpool backuppool cache=yes
```

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento primaria de acceso secuencial)

Utilice este comando para actualizar una agrupación de almacenamiento de acceso secuencial.

Restricciones:

1. No es posible utilizar este comando para cambiar el formato de datos de una agrupación de almacenamiento.
2. Si el valor de DATAFORMAT es NETAPPDUMP, CELERRADUMP o NDMPDUMP, sólo puede modificar los atributos siguientes:
  - o DESCRIPTION
  - o ACCESS
  - o COLLOCATE
  - o MAXSCRATCH
  - o REUSEDELAY

## Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

## Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DESCRiption----descripción-'
>--+-----+----->
  '-ACCess----+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>--+-----+----->
  |                                     (1) (2) |
  '-MAXSize----+tamaño_máximo_archivo+-----'
      '-NOLimit-----'
>--+-----+----->
  |                                     (1) |
  '-CRCData----+Yes+-----'
      '-No--'
>--+-----+----->
  |                                     (1) (2) |
  '-NEXTstgpool----pool_name-----'
>--+-----+----->
  |                                     (1) (2) |
  '-HIghmig----percent-----'
>--+-----+----->
  |                                     (1) (2) |
  '-LOWmig----percent-----'
>--+-----+----->
  |                                     (1) (2) |
  '-REClaim----porcentaje-----'
```

```

>----->
|                                     (1) (2) |
|'-RECLAIMProcess-----number-----'|
>----->
|                                     (1) (2) |
|'-RECLAIMSTGpool-----pool_name-----'|
>----->
|                                     (2) |
|'-COLlocate-----+No-----+-----'|
|                                     +-Group-----+
|                                     +-NODE-----+
|                                     '-Filespace- '|
>----->
|                                     (2) | |                                     (2) |
|'-MAXSCRatch-----número-----' |'-REUsedelay-----days-----'|
>----->
|                                     (1) (2) |
|'-OVFLocation-----ubicación-----'|
>----->
|                                     (1) (2) |
|'-MIGDelay-----days-----'|
>----->
|                                     (1) (2) |
|'-MIGContinue-----+Yes-+-----'|
|                                     '-No-- '|
>----->
|                                     (1) (2) |
|'-MIGProcess-----number-----'|
>----->
|'-AUTOCopy-----+None-----+ '|
|                                     +-Client-----+
|                                     +-MIGration-+
|                                     '-All-----'|
>----->
|                                     .-,----- . |
|                                     v                                     (1) (2) | |
|'-COPYSTGpools-----nombre_agrupación_copia-----+ '|
>----->
|                                     (1) (2) |
|'-COPYContinue-----+Yes-+-----'|
|                                     '-No-- '|
>----->
|                                     .-,----- . |
|                                     v                                     | |
|'-ACTIVEDATApools-----nombre_agrupación_datos_activos-----+ '|
>----->
|'-DEDuplicate-----+No-----+ '|
|                                     | (3) |
|                                     '-Yes-----'|
>-----<
|                                     (4) |
|'-IDENTIFYProcess-----número-----'|

```

Notas:

1. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos NETAPPDUMP, CELERRADUMP o NDMPDUMP.
2. Este parámetro no está disponible para las agrupaciones de almacenamiento CENTERA.
3. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
4. Este parámetro sólo está disponible si el valor del parámetro DEDUPLICATE es YES.

## Parámetros

### nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento que se ha de actualizar.

### DESCRiption

Especifica una descripción de la agrupación de almacenamiento. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

### ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, migración y reclamación) pueden acceder a los archivos de la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

#### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

#### READOnly

Especifica que los nodos cliente sólo pueden leer los archivos de los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *sólo lectura*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

#### UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento.

Los procesos del servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento y también pueden traspasar o copiar archivos de esta agrupación de almacenamiento a otra agrupación de almacenamiento. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de otros volúmenes externos a ella.

Si esta agrupación de almacenamiento se ha especificado como una agrupación de almacenamiento subordinada, (con el parámetro NEXTSTGPOOL) y se ha definido como de *no disponible*, la agrupación de almacenamiento se salta cuando los procesos del servidor intentan grabar archivos en ella.

### MAXSIze

Especifica el tamaño máximo de un archivo físico que el servidor puede almacenar en la agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

#### NOLimit

Especifica que no hay ningún límite de tamaño máximo para los archivos físicos almacenados en la agrupación de almacenamiento.

#### tamaño\_máximo\_archivo

Limita el tamaño máximo de archivo físico. Especifique un entero de 1 a 999999 terabytes, seguido de un factor de escala. Por ejemplo, MAXSIZE=5G especifica que el tamaño máximo de archivo de esta agrupación de almacenamiento es de 5 gigabytes. Las unidades de medida son:

Unidades de medida	Significado
K	kilobytes
M	megabyte
G	gigabytes
T	terabytes

El cliente calcula el tamaño de los archivos que se envían al servidor. La estimación del cliente se utiliza en lugar de la cantidad real de datos que se envían al servidor. Las opciones de cliente, como eliminación de duplicados, compresión y cifrado, pueden provocar que la cantidad de datos que se envía al servidor sea mayor o menor que la estimación de tamaño. Por ejemplo, la compresión de un archivo podría ser menor en tamaño que la estimación y, por consiguiente, enviar menos datos que la estimación. Además, un archivo binario podría ser superior en tamaño después del proceso de compresión y, por consiguiente, enviar más datos que la estimación.

Cuando el tamaño físico de la agrupación de almacenamiento sobrepasa el parámetro MAXSIZE, la tabla siguiente muestra dónde están almacenados normalmente los archivos.

Tabla 1. La ubicación de un archivo según el tamaño del archivo y la agrupación que se ha especificado

El tamaño de archivo	Agrupación especificada	Resultado
Supera el tamaño máximo	No hay ninguna agrupación especificada como la siguiente agrupación de almacenamiento de la jerarquía	El servidor no almacena el archivo
	Se especifica una agrupación como la siguiente agrupación de almacenamiento de la jerarquía	El servidor almacena el archivo en la siguiente agrupación de almacenamiento que puede aceptar el tamaño de archivo

Consejo: Si también especifica el parámetro NEXTstgpool, defina una agrupación de almacenamiento de la jerarquía para no tener ningún límite sobre el tamaño máximo de archivo especificando el parámetro MAXSIZE=NOLimit. Si tiene al menos una agrupación sin límite de tamaño, se asegura de que el servidor podrá guardar el archivo sin importar cuál sea su tamaño.

Si se envían varios archivos en una sola transacción, el servidor considera que el tamaño de la transacción es el tamaño de archivo. Si el tamaño total de todos los archivos de la transacción es mayor que el límite de tamaño máximo, el servidor no guarda los archivos en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### CRCData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCData en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

#### Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

#### No

Especifica que los datos se almacenan sin información de CRC.

#### Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

#### NEXTstgpool

Especifica una agrupación de almacenamiento primaria a la que se migran los archivos. No puede migrar datos de una agrupación de almacenamiento de acceso secuencial a una agrupación de almacenamiento de acceso aleatorio. Este parámetro es opcional. La siguiente agrupación de almacenamiento debe ser una agrupación de almacenamiento primaria.

Para suprimir un valor existente, especifique una serie nula ("").

Si esta agrupación de almacenamiento no tiene una agrupación de almacenamiento que le siga, el servidor no puede migrar los archivos de esta agrupación de almacenamiento y no puede almacenar en otra agrupación de almacenamiento los archivos que sobrepasan el tamaño máximo de esta agrupación de almacenamiento.

Cuando no hay suficiente espacio disponible en la agrupación de almacenamiento actual, el parámetro NEXTSTGPOOL para las agrupaciones de almacenamiento de acceso secuencial no permite que los datos se almacenen en la agrupación siguiente. En este caso, el servidor emite un mensaje y la transacción no se efectúa correctamente.

Para las siguientes agrupaciones de almacenamiento con un tipo de dispositivo FILE, el servidor realiza una comprobación preliminar para determinar si hay disponible espacio suficiente. Si no hay espacio disponible, el servidor salta a la siguiente agrupación de almacenamiento de la jerarquía. Si hay espacio disponible, el servidor intenta almacenar datos en esa agrupación. No obstante, es posible que falle la operación de almacenamiento porque cuando se intenta realmente realizar la operación de almacenamiento el espacio ya no está disponible.

Restricciones:

- Para asegurarse de que no crea una cadena de agrupaciones de almacenamiento que conduzca a un bucle infinito, especifique como mínimo una agrupación de almacenamiento de la jerarquía sin ningún valor.
- Si especifica una agrupación de acceso secuencial como la siguiente agrupación de almacenamiento, la agrupación debe tener el formato de datos NATIVE o NONBLOCK.
- No especifique una agrupación de almacenamiento de contenedor de directorios o de contenedor de nube.
- No utilice este parámetro para especificar una agrupación de almacenamiento para la migración de datos.
- Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP

#### HIghmig

Especifica que el servidor inicia la migración cuando la utilización de la agrupación de almacenamiento alcanza este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 100.

Cuando la agrupación de almacenamiento sobrepasa el umbral superior de migración, el servidor puede iniciar la migración de los archivos por volumen, a la siguiente agrupación de almacenamiento definida para la agrupación de almacenamiento. Puede establecer el umbral superior de migración en 100 para impedir la migración en la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### LOwmig

Especifica que el servidor detiene la migración cuando la utilización de la agrupación de almacenamiento es igual o inferior a este porcentaje. En el caso de las agrupaciones de almacenamiento de disco de acceso secuencial (FILE), la utilización es el porcentaje de datos en una agrupación de almacenamiento respecto a la capacidad de datos estimada total de la agrupación, incluida la capacidad de todos los volúmenes reutilizables especificados para la agrupación. En el caso de las agrupaciones de almacenamiento que utilizan medios de cinta, la utilización es el porcentaje de volúmenes que contienen datos respecto al número total de volúmenes de la agrupación de almacenamiento. El número total de volúmenes incluye el número máximo de volúmenes reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 99.

Cuando la agrupación de almacenamiento alcanza el umbral inferior de migración, el servidor no inicia la migración de los archivos de otro volumen. Puede establecer el umbral inferior de migración en 0 para permitir que la migración vacíe la agrupación de almacenamiento.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos





de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes que no están caducados de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Especifique el 50 % o más como valor de este parámetro para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

 Sistemas operativos AIX  Sistemas operativos Windows Para las agrupaciones de almacenamiento que utilizan dispositivos WORM, se puede bajar el valor predeterminado 100. Al bajar el valor, el servidor puede consolidar los datos en menos volúmenes cuando sea necesario. Los volúmenes que se vacían por la operación de reclamación se pueden dar de baja de la biblioteca, con lo que quedan ranuras libres para nuevos volúmenes. Los volúmenes no se pueden reutilizar porque son de una sola operación de grabación.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999. Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento primaria de acceso secuencial.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que no se ha especificado el parámetro RECLAIMSTGPOOL o que la agrupación de almacenamiento de reclamación tiene la misma clase de dispositivo que la agrupación de almacenamiento que se reclama, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 16 como mínimo.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### RECLAIMSTGpool

Especifica otra agrupación de almacenamiento primaria como destino de los datos reclamados de esta agrupación de almacenamiento. Este parámetro es opcional. Cuando el servidor reclama volúmenes para la agrupación de almacenamiento, los datos sin caducar de los volúmenes que se están reclamando se traspasan a la agrupación de almacenamiento indicada en este parámetro.

Para suprimir un valor existente, especifique una serie nula ("").

Una agrupación de almacenamiento de reclamación tiene la mayor utilidad para una agrupación de almacenamiento que sólo tenga una unidad en su biblioteca. Al especificar este parámetro, el servidor traspasa todos los datos de los volúmenes reclamados a la agrupación de almacenamiento de reclamación independientemente del número de unidades de la biblioteca.

Para volver a traspasar los datos de la agrupación de almacenamiento de reclamación a la agrupación de almacenamiento original, utilice la jerarquía de agrupaciones de almacenamiento. Especifique la agrupación de almacenamiento original como la siguiente agrupación de almacenamiento de la agrupación de almacenamiento de reclamación.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario. La función de proximidad también pueden afectar al número de procesos que migran discos a agrupación secuencial.

Puede especificar una de las opciones siguientes:

#### No

Especifica que la función de proximidad está desactivada. Durante la migración de disco, los procesos se crean a un nivel de espacio de archivos.

#### GROup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Se recomienda utilizar cintas cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para nodos agrupados, y en el nivel de nodo para nodos no agrupados.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos que se denominan A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.
- Durante la migración de disco, el servidor crea procesos de migración en el nivel de grupo de proximidad para espacios de archivos agrupados.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

#### NODE

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

Para COLLOCATE=NODE, el servidor crea procesos en el nivel de nodo cuando se migran datos del disco.

#### Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

Para COLLOCATE=FILESPACE, el servidor crea procesos en el nivel de espacio de archivos al migrar datos del disco.

#### MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables, se evita tener que definir cada volumen que se va a utilizar.

El valor especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento y la capacidad correspondiente estimada para la agrupación de almacenamiento.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Cuando se suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Al especificar este parámetro, puede asegurarse de que la base de datos se pueda restaurar a un nivel anterior y que las referencias de base de datos a los archivos de la agrupación de almacenamiento todavía sean válidas.

#### OVFLocation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el comando MOVE MEDIA. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGDelay

Especifica el número mínimo de días que debe permanecer un archivo en una agrupación de almacenamiento antes de que el archivo pueda seleccionarse para migración. Todos los archivos de un volumen deben poder seleccionarse para una operación de migración antes de que el servidor seleccione el volumen para migración. Para calcular un valor para comparar con el valor MIGDELAY especificado, el servidor cuenta el número de días que el archivo ha permanecido en la agrupación de almacenamiento.

Este parámetro es opcional. Puede especificar un entero de 0 a 9999.

Si desea que el servidor cuente el número de días sólo basándose en el momento en que se almacenó un archivo y no en el momento en que se recuperó, utilice la opción del servidor NORETRIEVEDATE.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGContinue

Especifica si el servidor puede migrar los archivos que no cumplen el tiempo de retardo de migración. Este parámetro es opcional.

Puesto que puede ser necesario que los archivos permanezcan en la agrupación de almacenamiento durante un número mínimo de días, el servidor puede migrar todos los archivos seleccionables a la siguiente agrupación de almacenamiento aunque no se haya alcanzado el umbral inferior de migración. Este parámetro permite especificar si el servidor puede continuar el proceso de migración migrando los archivos que no cumplen el tiempo de retardo de migración.

Puede especificar uno de los siguientes valores:

#### Yes

Especifica que, cuando es necesario alcanzar el umbral inferior de migración, el servidor continúa migrando los archivos que no han estado almacenados en la agrupación de almacenamiento el número de días que especifica el período de retardo de migración.

#### No

Especifica que el servidor detiene la migración cuando no quedan archivos seleccionables para migrar, incluso antes de alcanzar el umbral inferior de migración. El servidor no migra los archivos si no han estado almacenados en la agrupación de almacenamiento el número de días que especifica el período de retardo de migración.

Restricción: Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:

- NETAPPDUMP
- CELERRADUMP
- NDMPDUMP

#### MIGProcess

Especifica el número de procesos paralelos que se utilizará para migrar los archivos de los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta el número de agrupaciones de almacenamiento secuenciales que participarán en la migración y el número de unidades lógicas y físicas que pueden estar dedicadas a esta operación. Para acceder a un volumen de acceso secuencial, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física. El número de puntos de montaje y unidades disponibles depende de otras actividades de IBM Spectrum Protect y del sistema, y de los límites de montaje de las clases de dispositivo para las agrupaciones de almacenamiento de acceso secuencial que participan en la migración.

Por ejemplo, supongamos que desea migrar los volúmenes de dos agrupaciones de almacenamiento secuencial primarias simultáneamente y que desea especificar tres procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Si damos por supuesto que la agrupación de almacenamiento a la que se están migrando los archivos tienen la misma clase de dispositivo que la agrupación de almacenamiento de la que se migran, cada proceso de reclamación requiere dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una unidad corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar simultáneamente seis procesos de migración, necesita como mínimo un total de 12 puntos de montaje y 12 unidades. La clase de dispositivo para las dos agrupaciones de almacenamiento debe tener un límite de montaje de 12 como mínimo.

Si el número de procesos de migración especificados es mayor que el número de puntos de montaje o unidades disponibles, los procesos que no obtengan puntos de montaje o unidades esperarán a que haya puntos de montaje o unidades disponibles. Si las unidades o los puntos de montaje no pasan a estar disponibles dentro del tiempo MOUNTWAIT, los procesos de migración finalizarán. Para obtener información acerca de la especificación del tiempo MOUNTWAIT, consulte el apartado DEFINE DEVCLASS (Definir una clase de dispositivo).

El servidor de IBM Spectrum Protect iniciará el número especificado de procesos de migración independientemente del número de volúmenes elegibles para la migración. Por ejemplo, si especifica diez procesos de migración y sólo seis volúmenes son elegibles para migración, el servidor iniciará diez procesos y cuatro de ellos terminarán sin que se procesen volúmenes.

Nota: Cuando especifique este parámetro, tenga en cuenta si está activada la función de grabación simultánea para la migración de datos del servidor. Cada proceso de migración necesita un punto de montaje y una unidad para cada agrupación de almacenamiento de copia y agrupación de datos activos definida en la agrupación de almacenamiento de destino.

#### AUTOCopy

Especifica si IBM Spectrum Protect ejecuta operaciones de grabación simultánea. Este parámetro afecta a las siguientes operaciones:

- Sesiones de almacenamiento del cliente
- Procesos de importación del servidor
- Procesos de importación de datos del servidor

Si la opción AUTOCOPY se establece en ALL o CLIENT y existe como mínimo una agrupación de almacenamiento que aparece listada en las opciones COPYSTGPools o ACTIVEDataPools, la eliminación de duplicados del lado del cliente está inhabilitada.

Si se produce un error mientras los datos se están grabando simultáneamente en una agrupación de datos activos o de almacenamiento de copia durante un proceso de migración, el servidor deja de grabar en las agrupaciones de almacenamiento fallidas durante el resto de proceso. Sin embargo, el servidor seguirá almacenando archivos en la agrupación de almacenamiento primaria y las demás agrupaciones de datos activos o de almacenamiento de copia. Estas agrupaciones permanecen activas durante el proceso de migración. Las agrupaciones de almacenamiento de copia se especifican mediante el parámetro COPYSTGPools. Las agrupaciones de datos activos se especifican mediante el parámetro ACTIVEDataPools.

Puede especificar uno de los siguientes valores:

None

Especifica que la función de grabación simultánea está inhabilitada.

Client

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente o los procesos de importación del servidor. Durante los procesos de importación del servidor, los datos sólo se graban simultáneamente en las agrupaciones de almacenamiento de copia. Los datos no se graban en agrupaciones de datos activos durante procesos de importación del servidor.

MIGRation

Especifica que los datos se graban simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos sólo durante la migración a esta agrupación de almacenamiento. Durante los procesos de migración de datos del servidor, los datos se graban simultáneamente en las agrupaciones de almacenamiento de copia y las agrupaciones de datos activos si los datos no existen en dichas agrupaciones. Los nodos cuyos datos se están migrando deben estar en un dominio asociado con una agrupación de datos activos. Si los nodos no están en un dominio asociado con una agrupación activa, los datos no se pueden grabar en la agrupación.

All

Especifica que los datos se graben simultáneamente en agrupaciones de almacenamiento de copia o agrupaciones de datos activos durante las sesiones de almacenamiento del cliente, los procesos de importación del servidor o los procesos de migración de datos del servidor. Al especificar este valor, se asegurará de que la grabación simultánea se produzca cuando esta agrupación sea el destino de cualquiera de las operaciones elegibles.

#### COPYSTGpools

Especifica los nombres de las agrupaciones de almacenamiento de copia en las que el servidor graba datos de modo simultáneo. Puede especificar un máximo de tres nombres de agrupaciones de copia separados por comas. No se permiten espacios entre los nombres de agrupaciones de copia. Para agregar o eliminar una o varias agrupaciones de almacenamiento de copia, especifique el nombre de las agrupaciones que desee incluir en la lista actualizada. Por ejemplo, si la lista de agrupaciones de almacenamiento de copia incluye COPY1 y COPY2 y desea añadir COPY3, especifique COPYSTGPools=COPY1,COPY2,COPY3. Para eliminar todas las agrupaciones de almacenamiento de copia existentes asociadas con la agrupación de almacenamiento de copia principal, especifique una serie nula ("") para el valor (por ejemplo, COPYSTGPools="").

Al especificar un valor para el parámetro COPYSTGPools, también puede especificar un valor para el parámetro COPYCONTINUE. Si desea obtener más información, consulte el parámetro COPYCONTINUE.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSTGPools y ACTIVEDataPools no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento primaria a la siguiente, ésta hereda la lista de agrupaciones de almacenamiento de copia y el valor COPYCONTINUE de la primaria. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos simultáneamente en las agrupaciones de almacenamiento de copia durante las siguientes operaciones:

- Operaciones de copia de seguridad y archivado de clientes de copia de seguridad/archivado de IBM Spectrum Protect o clientes de aplicación que utilizan la API de IBM Spectrum Protect

- Operaciones de migración realizadas por clientes de IBM Spectrum Protect for Space Management
- Operaciones de importación que implican la copia de datos de archivos exportados desde medios externos en una agrupación de almacenamiento primaria asociada con una lista de agrupaciones de almacenamiento de copia

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - NETAPPDUMP
  - CELERRADUMP
  - NDMPDUMP
2. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se da soporte a la grabación simultánea en las siguientes operaciones de almacenamiento. Si la agrupación de almacenamiento primaria especificada por DESTINATION o TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de almacenamiento de copia, éstas se pasarán por alto y los datos se almacenarán únicamente en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.

Atención: La función que proporciona el parámetro COPYSTGPOLLS no tiene como finalidad sustituir el mandato BACKUP STGPPOOL. Si utiliza el parámetro COPYSTGPOLLS, continúe utilizando el mandato BACKUP STGPPOOL para garantizar que las agrupaciones de almacenamiento de copia son copias completas de la agrupación de almacenamiento primaria. Existen casos en los que no se puede crear una copia. Si desea obtener más información, consulte la descripción del parámetro COPYCONTINUE.

COPYContinue

Especifica cómo reacciona el servidor ante una anomalía de grabación de una agrupación de almacenamiento de copia en cualquiera de las agrupaciones de almacenamiento de copia especificadas en el parámetro COPYSTGPOLLS. Este parámetro es opcional. El valor predeterminado es YES. Cuando se especifica el parámetro COPYCONTINUE, debe existir una lista COPYSTGPOLLS o especificarse también el parámetro COPYSTGPOLLS.

El parámetro COPYCONTINUE no afecta a la función de grabación simultánea durante la migración.

Puede especificar los siguientes valores:

Yes

Si el parámetro COPYCONTINUE se establece en YES, el servidor detendrá la grabación en las agrupaciones de copia con errores durante el resto de la sesión, pero seguirá guardando archivos en la agrupación primaria y en el resto de las agrupaciones de copia. La lista de agrupaciones de almacenamiento de copia sólo está activa durante la duración de la sesión de cliente y se aplica a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.

No

Si el parámetro COPYCONTINUE está definido como NO, el servidor generará un error de la transacción actual y detendrá la operación de almacenamiento.

Restricciones:

- El valor del parámetro COPYCONTINUE no afecta a las agrupaciones de datos activos. Si se produce un error de grabación en una de las agrupaciones de datos activos, el servidor detendrá la grabación en las agrupaciones de datos activos anómalas durante el resto de la sesión, pero seguirá almacenando archivos en la agrupación primaria y en el resto de las agrupaciones de datos activos y de almacenamiento de copia. La lista de agrupaciones de datos activos sólo estará activa durante la sesión y se aplicará a todas las agrupaciones de almacenamiento primarias de una jerarquía de agrupaciones de almacenamiento determinada.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la importación del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento primaria o en la de copia, el proceso de importación del servidor fallará.
- El valor del parámetro COPYCONTINUE no afecta a la función de escritura simultánea durante la migración de datos del servidor. Si los datos se graban de forma simultánea y se produce un error de grabación en la agrupación de almacenamiento de copia o en la de datos activos, la agrupación de almacenamiento anómala se eliminará y continuará el proceso de migración de datos. Los errores de grabación en la agrupación de almacenamiento primaria hacen que el proceso de migración falle.

ACTIVEDATApools

Especifica los nombres de las agrupaciones de datos activos en las que el servidor graba datos de forma simultánea durante una operación de copia de seguridad de un cliente. El parámetro ACTIVEDATAPOOLS es opcional. No se permiten espacios entre los nombres de agrupaciones de datos activos.

El número total combinado de agrupaciones de almacenamiento especificado en los parámetros COPYSGTPOOLS y ACTIVEATAPOOLS no puede exceder de tres.

Cuando una operación de almacenamiento de datos pasa de una agrupación de almacenamiento principal a la siguiente, ésta hereda la lista de agrupaciones de datos activos de la agrupación de almacenamiento de destino especificada en el grupo de copia. La principal se especifica mediante el grupo de copia de la clase de gestión vinculada con los datos.

El servidor puede grabar datos de forma simultánea en agrupaciones de datos activos únicamente durante las operaciones de copia de seguridad de clientes de copia de seguridad/archivado de IBM Spectrum Protect o de clientes de aplicación que utilizan la API de IBM Spectrum Protect.

Restricciones:

1. Este parámetro sólo está disponible para las agrupaciones de almacenamiento primarias que utilizan el formato de datos NATIVE o NONBLOCK. Este parámetro no está disponible para las agrupaciones de almacenamiento que utilizan los formatos de datos siguientes:
  - o NETAPPDUMP
  - o CELERRADUMP
  - o NDMPDUMP
2. No se admite la grabación simultánea de datos en agrupaciones de datos activos cuando la operación utiliza el traspaso de datos fuera de la LAN. Las operaciones de grabación simultánea tienen preferencia sobre el traspaso de datos fuera de la LAN, lo que hace que las operaciones se realicen a través de la LAN. Sin embargo, se acepta la configuración de la grabación simultánea.
3. No se admite la función de grabación simultánea cuando una operación de copia de seguridad de NAS está grabando un archivo TOC. Si la agrupación de almacenamiento primaria que se ha especificado en TOCDESTINATION en el grupo de copia de la clase de gestión tiene definidas agrupaciones de datos activos, éstas se pasarán por alto y los datos sólo se almacenarán en la agrupación de almacenamiento primaria.
4. La función de grabación simultánea no puede utilizarse con dispositivos de almacenamiento CENTERA.
5. Los datos que se importan no se almacenan en las agrupaciones de datos activos. Después de haber realizado una operación de importación, utilice el comando COPY ACTIVEATA para almacenar los datos importados en una agrupación de datos activos.

Atención: La función que proporciona el parámetro ACTIVEATAPOOLS no tiene como finalidad sustituir al mandato COPY ACTIVEATA. Si utiliza el parámetro ACTIVEATAPOOLS, utilice el mandato COPY ACTIVEATA para garantizar que las agrupaciones de datos activos contienen todos los datos activos de la agrupación de almacenamiento primaria.

#### DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE.

#### IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo asociada al tipo de dispositivo FILE. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

## Ejemplo: actualizar los volúmenes reutilizables que pueden montarse de la agrupación de almacenamiento primaria secuencial

---

Actualice la agrupación de almacenamiento secuencial primaria que se denomina TAPEPOOL1 para permitir que se monten 10 volúmenes reutilizables como máximo.

```
update stgpool tapepool1 maxscratch=10
```

## UPDATE STGPOOL (Actualizar una agrupación de almacenamiento de copia de acceso secuencial)

---

Utilice este comando para actualizar una agrupación de almacenamiento de copia de acceso secuencial.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

## Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>--+-----+----->
  '-DEScRiption---descripción-'
>--+-----+----->
  '-ACCess---+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>--+-----+----->
  '-COLlocate---+No-----+'
      +-GRoup-----+
      +-NODE-----+
      '-Filespace-'
>--+-----+----->
  '-REClaim---porcentaje-' '-RECLAIMPRocess---number-'
>--+-----+----->
  '-OFFSITERECLAIMLimit---+NOLimit--+'
      '-número--'
>--+-----+----->
  '-MAXScRatch---número-' '-REUsedelay---dias-'
>--+-----+----->
  '-OVFLOcation---ubicación-' '-CRCDATA---+Yes-+-'
      '-No--'
>--+-----+----->
  '-DEDUPLICATE---+No-----+'
      | (1) |
      '-Yes-----'
>--+-----+-----><
  | (2) |
  '-IDENTIFYPRocess---número-----'
```

### Notas:

1. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
2. Este parámetro sólo está disponible si el valor del parámetro DEDUPLICATE es YES.

## Parámetros

### nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de almacenamiento de copia que se ha de actualizar.

### DEScRiption

Especifica la descripción de la agrupación de almacenamiento de copia. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

### ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor acceder a los archivos de la agrupación de almacenamiento de copia. Este parámetro es opcional. Puede especificar los valores siguientes:

#### READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de almacenamiento de copia.

#### READOnly

Especifica que los nodos cliente sólo puedan leer archivos que están almacenados en los volúmenes en la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de



almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

#### UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de almacenamiento de copia.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de almacenamiento de copia para restaurar archivos en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de almacenamiento de copia de otros volúmenes externos a la agrupación de almacenamiento. No se puede hacer copia de seguridad de una agrupación de almacenamiento en la agrupación de almacenamiento de copia.

#### COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

#### No

Especifica que la función de proximidad está desactivada.

#### GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

#### NODe

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios

de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

#### FIlespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

#### REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación hace que el espacio fragmentado de los volúmenes pueda volverse a utilizar ya que traspasa los archivos restantes activos de un volumen a otro volumen, y de este modo hace que el volumen original esté disponible para volver a ser utilizado. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor 100 significa que no se realizará la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado 100, especifique el 50 % o más como valor para que los archivos almacenados en dos volúmenes se puedan combinar en un solo volumen de salida.

Cuando un volumen de agrupación de copia que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación de almacenamiento de copia o primaria que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de almacenamiento de copia original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de almacenamiento de copia.

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para cada agrupación de almacenamiento debe tener un límite de montaje de ocho como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de almacenamiento de copia. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de copia de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

#### OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

#### NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.  
número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, suponga que una agrupación de almacenamiento de copias contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclamarán los tres volúmenes cuando se ejecute la reclamación. Si se especifica un valor de 2, sólo se reclamarán VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclamará VOL1.

#### MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se ha especificado para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de almacenamiento de copia y la capacidad correspondiente estimada para la agrupación de almacenamiento de copia.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de almacenamiento de copia mientras no se cambie la modalidad de acceso. Un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor de IBM Spectrum Protect no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de almacenamiento de copia seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el comando SET DRMDBBACKUPEXPIREDAYS.

#### OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el comando MOVE MEDIA. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

#### CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes

Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.

## Ejemplo: actualizar una agrupación de almacenamiento de copia para una reutilización de volumen 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente

---

Actualizar la agrupación de almacenamiento de copia que se denomina TAPEPOOL2 de modo que el retardo de reutilización de volúmenes se cambie por 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente.

```
update stgpool tapepool2 reusedelay=30 collocate=node
```

**Referencia relacionada:**

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

## UPDATE STGPOOL (Actualizar un acceso secuencial de datos activos)

---

Utilice este comando para actualizar una agrupación de datos activos.

### Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones, o privilegio de almacenamiento con restricciones a la agrupación de almacenamiento que se ha de actualizar.

## Sintaxis

```
>>-UPDate STGpool--nombre_agrupación----->
>+-----+----->
  '-DESCRiption----descripción-'
>+-----+----->
  '-ACCess----+READWrite---+'
      +-READOnly----+
      '-UNAVailable-'
>+-----+----->
  '-COLlocate---+No-----+'
      +-GRoup-----+
      +-NODE-----+
      '-Filespace-'
>+-----+----->
  '-RECLaim----porcentaje-' '-RECLAIMPRocess----number-'
>+-----+----->
  '-OFFSITERECLAIMLimit---+NOLimit--+'
      '-número--'
>+-----+----->
  '-MAXSCRatch----número-' '-REUsedelay----días-'
>+-----+----->
  '-OVFLocation----ubicación-' '-CRCDData----+Yes-+-'
      '-No--'
>+-----+----->
  '-DEDUPLICATE---+No-----+'
      |         (1) |
      '-Yes-----'
>+-----+-----><
  |         (2) |
  '-IDENTIFYPRocess----número-----'
```

### Notas:

1. Este parámetro sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.
2. Este parámetro sólo está disponible si el valor del parámetro DEDUPLICATE es YES.

## Parámetros

### nombre\_agrupación (Obligatorio)

Especifica el nombre de la agrupación de datos activos que se ha de actualizar.

### DESCRiption

Especifica una descripción de la agrupación de datos activos. Este parámetro es opcional. La longitud máxima de la descripción es de 255 caracteres. La descripción debe estar delimitada por comillas si contiene algún carácter en blanco. Para suprimir una descripción existente, especifique una serie nula ("").

### ACCess

Especifica cómo los nodos cliente y los procesos del servidor (como, por ejemplo, reclamación) pueden acceder a los archivos de la agrupación de datos activos. Este parámetro es opcional. Puede especificar los siguientes valores:

#### READWrite

Especifica que los archivos se pueden leer y grabar en los volúmenes de la agrupación de datos activos.

#### READOnly

Especifica que los nodos cliente pueden leer sólo los archivos que están almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar las versiones activas de los archivos de copia de seguridad en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

#### UNAVailable

Especifica que los nodos cliente no pueden acceder a los archivos almacenados en los volúmenes de la agrupación de datos activos.

Los procesos de servidor pueden traspasar archivos entre los volúmenes de la agrupación de almacenamiento. El servidor puede utilizar los archivos de la agrupación de datos activos para restaurar las versiones activas de los archivos de copia de seguridad en las agrupaciones de almacenamiento primarias. Sin embargo, no se permiten nuevas grabaciones en los volúmenes de la agrupación de datos activos de otros volúmenes externos a ella. Una agrupación de almacenamiento no puede copiarse en la agrupación de datos activos.

#### COLlocate

Especifica si el servidor intenta mantener los datos, que están almacenados en el menor número de volúmenes posible, que pertenecen a una de las opciones siguientes:

- Un nodo de cliente individual
- Un grupo de espacios de archivos
- Un grupo de nodos de cliente
- Un espacio de archivos de cliente

Este parámetro es opcional.

La proximidad disminuye el número de montajes de medio de acceso secuencial para las operaciones de recuperación y llamada. Sin embargo, la proximidad aumenta tanto la cantidad de tiempo que necesita el servidor para que los archivos estén en proximidad en el almacenamiento como el número de volúmenes necesario.

Puede especificar una de las opciones siguientes:

#### No

Especifica que la función de proximidad está desactivada.

#### GRoup

Especifica que la proximidad está activada en el nivel de grupo de los nodos de cliente o espacios de archivos. Para los grupos de proximidad, el servidor intenta colocar los datos de nodos o espacios de archivos pertenecientes al mismo grupo de proximidad en el menor número de volúmenes posible.

Si especifica COLLOCATE=GROUP pero no define ningún grupo de proximidad o si no agrega nodos o espacios de archivos a un grupo de proximidad, los datos se ubican por proximidad en función del nodo. Considere el uso de cinta cuando organice nodos de cliente o espacios de archivos en grupos de proximidad.

Por ejemplo, si una agrupación de almacenamiento basado en cinta está formada por datos de nodos y especifica COLLOCATE=GROUP, el servidor realiza las siguientes acciones:

- Aproxima los datos por grupo para nodos agrupados. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de nodos en una sola cinta o en la menor cantidad de cintas posible. Los datos de un solo nodo también pueden distribuirse en varias cintas asociadas con un grupo.
- Aproxima los datos por nodo para nodos no agrupados. Siempre que sea posible, el servidor almacena los datos de un solo nodo en una sola cinta. Se utilizan todas las cintas disponibles que ya tienen datos del nodo antes de utilizar el espacio disponible en cualquier otra cinta.

Si una agrupación de almacenamiento basado en cinta consta de datos de espacios de archivos agrupados y se especifica COLLOCATE=GROUP, el servidor completa las acciones siguientes:

- Aproxima por grupo, los datos para espacios de archivos agrupados solamente. Siempre que sea posible, el servidor aproxima los datos que pertenecen a un grupo de espacios de archivos en una única cinta o en la menor cantidad de cintas posible. Los datos de un solo espacio de archivos también pueden distribuirse en varias cintas asociadas con un grupo.
- Asigna los datos por nodo (por espacios de archivos que no se definen de forma explícita con un grupo de asignación de espacio de archivo). Por ejemplo, node1 tiene espacios de archivos denominados A, B, C, D y E. Los espacios de archivos A y B pertenecen a un grupo de proximidad del espacio, pero C, D y E no. Los espacios de archivos A y B se asignan por grupo de asignación del espacio, mientras C, D y E se asignan por nodo.

Los datos se colocan en la menor cantidad de volúmenes de acceso secuencial.

#### NODe

Especifica que la función de proximidad está activada en el nivel de nodo cliente. Para los grupos de proximidad, el servidor intenta colocar los datos de un nodo en el menor número posible de volúmenes. Si el nodo tiene varios espacios de archivos, el servidor no realiza ningún intento de aproximar dichos espacios de archivos. Para mantener la compatibilidad con una versión anterior, el servidor todavía acepta COLLOCATE=YES para especificar la proximidad en el nivel de nodo de cliente.

Si una agrupación de almacenamiento contiene datos de un nodo que es miembro de un grupo de proximidad y especifica COLLOCATE=NODE, los datos se aproximarán por nodo.

#### Filespace

Especifica que la proximidad está activada en el nivel de espacio de archivos de los nodos cliente. El servidor intenta poner los datos de un nodo y espacio de archivos en el menor número de volúmenes posible. Si un nodo tiene varios espacios de archivos, el servidor intenta colocar los datos de espacios de archivos distintos en volúmenes distintos.

#### REClaim

Especifica cuándo reclama el servidor un volumen, en función del porcentual de espacio reclamable que hay en un volumen. El espacio reclamable es la cantidad de espacio ocupado por los archivos que han caducado o se han suprimido de la base de datos de IBM Spectrum Protect.

La reclamación produce que el espacio fragmentado y el espacio que ocupan los archivos de copia de seguridad inactivos en los volúmenes pueda volver a utilizarse traspasando los restantes archivos no caducados y los archivos de copia de seguridad activos desde un volumen hasta otro volumen. Esta acción hace que el volumen original esté disponible para su reutilización. Este parámetro es opcional. Puede especificar un entero de 1 a 100. El valor 100 significa que no se realizará la reclamación.

El servidor determina que el volumen es un candidato a reclamación si el porcentaje de espacio reclamable de un volumen es mayor que el umbral de reclamación de la agrupación de almacenamiento.

Si cambia el valor predeterminado, que es 60, especifique un valor que represente, como mínimo, el 50 % para que los archivos almacenados en dos volúmenes puedan combinarse en un único volumen de salida.

Cuando un volumen de agrupación de datos activos que está fuera del local pasa a ser seleccionable para reclamación, el proceso de reclamación intenta obtener los archivos activos del volumen reclamable desde una agrupación primaria o de datos activos que está en el local. El proceso después graba esos archivos en un volumen disponible de la agrupación de datos activos original. Realmente, esos archivos se vuelven a traspasar a la ubicación del local. Sin embargo, los archivos pueden obtenerse del volumen de fuera del local después de un siniestro, si se utiliza una copia de seguridad de base de datos que haga referencia a los archivos del volumen que está fuera del local. Debido al modo en que funciona el proceso de reclamación con los volúmenes, preste mucha atención cuando lo utilice con las agrupaciones de datos activos.

#### RECLAIMProcess

Especifica el número de procesos paralelos que se utilizará para reclamar los volúmenes de esta agrupación de almacenamiento. Este parámetro es opcional. Entre un valor de 1 – 999.

Al calcular el valor para este parámetro, tenga en cuenta los siguientes recursos que son necesarios para el proceso de reclamación :

- El número de agrupaciones de almacenamiento secuenciales.
- El número de unidades lógicas y físicas dedicadas a la operación.

Para acceder a los volúmenes secuenciales, IBM Spectrum Protect utiliza un punto de montaje y, si el tipo de dispositivo no es FILE, una unidad física.

Por ejemplo, supongamos que desea reclamar los volúmenes de dos agrupaciones de almacenamiento secuencial simultáneamente y que desea especificar cuatro procesos para cada una de las agrupaciones de almacenamiento. Las agrupaciones de almacenamiento tienen la misma clase de dispositivo. Cada proceso necesita dos puntos de montaje y, si el tipo de dispositivo no es FILE, dos unidades. (Una de las unidades corresponde al volumen de entrada y la otra unidad corresponde al volumen de salida.) Para ejecutar ocho procesos de reclamación simultáneamente, necesita como mínimo un total de 16 puntos de montaje y 16 unidades. La clase de dispositivo para cada agrupación de almacenamiento debe tener un límite de montaje de ocho como mínimo.

Puede especificar uno o más procesos de reclamación para cada agrupación de datos activos. Puede especificar varios procesos de reclamación simultáneos para una sola agrupación de datos activos de una sola, lo que permite mejorar el uso de las unidades de cintas o volúmenes FILE disponibles. If multiple concurrent processing is not necessary, specify a value of 1 for the RECLAIMPROCESS parameter.

#### OFFSITERECLAIMLimit

Especifica el número de volúmenes desde los que se reclama espacio durante la reclamación de esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar los valores siguientes:

#### NOLimit

Especifica que desea reclamar el espacio en todos los volúmenes fuera del local.

#### número

Especifica el número de volúmenes fuera del local cuyo espacio se desea reclamar. Puede especificar un entero del 0 al 99999. Si el valor es cero significa que no se reclamará ninguno de los volúmenes fuera del local.

Consejo:

Para determinar el valor de OFFSITERECLAIMLIMIT, utilice la información estadística del mensaje que se ha emitido al final de la operación de reclamación de los volúmenes fuera del local. La información estadística incluye los elementos siguientes:

- El número de volúmenes fuera del local que se han procesado
- El número de procesos paralelos que se han utilizado
- La cantidad de tiempo total necesaria para el proceso

El orden en el cual se reclaman los volúmenes fuera del local está basado en la cantidad de espacio sin utilizar en un volumen. (El espacio no utilizado incluye tanto el espacio que nunca se ha utilizado en el volumen como el espacio que se ha vaciado debido a la supresión de archivos.) Los volúmenes con la cantidad mayor de espacio sin utilizar se reclaman antes.

Por ejemplo, imaginemos que una agrupación de datos activos contiene tres volúmenes: VOL1, VOL2 y VOL3. VOL1 tiene la mayor cantidad de espacio sin utilizar y VOL3 tiene la cantidad más pequeña de espacio sin utilizar. Suponga también que el porcentaje de espacio sin utilizar en cada uno de los tres volúmenes es mayor que el valor del parámetro RECLAIM. Si no especifica ningún valor para el parámetro OFFSITERECLAIMLIMIT, se reclaman los tres volúmenes cuando se ejecuta la reclamación. Si especifica un valor de 2, sólo se reclaman VOL1 y VOL2 cuando se ejecute la reclamación. Si especifica un valor de 1, sólo se reclama VOL1.

#### MAXSCRatch

Especifica el número máximo de volúmenes reutilizables que puede solicitar el servidor para esta agrupación de almacenamiento. Este parámetro es opcional. Puede especificar un entero de 0 a 100000000. Al permitir que el servidor solicite volúmenes reutilizables según sean necesarios, se evita tener que definir cada volumen que se va a utilizar.

El valor que se especifica para este parámetro se utiliza para calcular el número total de volúmenes disponibles en la agrupación de datos activos y la capacidad correspondiente estimada para la agrupación de datos activos.

Los volúmenes reutilizables se suprimen automáticamente de la agrupación de almacenamiento cuando se vacían. Sin embargo, si la modalidad de acceso de un volumen reutilizable es OFFSITE, el volumen no se suprimirá de la agrupación de datos activos mientras no se cambie la modalidad de acceso. Un administrador puede consultar al servidor los volúmenes reutilizables vacíos, fuera del local y devolverlos a la ubicación del local.

Cuando se vacían y suprimen volúmenes reutilizables con el tipo de dispositivo FILE, el servidor libera el espacio que ocupan los volúmenes y lo devuelve al sistema de archivos.

Consejo: Para las operaciones de servidor a servidor que utilizan volúmenes virtuales y que almacenan pequeñas cantidades de datos, considere la posibilidad de especificar un valor para el parámetro MAXSCRATCH que sea mayor que el valor que normalmente especifica para las operaciones de grabación en otros tipos de volúmenes. Después de haberse realizado una operación de grabación en un volumen virtual, IBM Spectrum Protect marca el volumen como lleno, FULL, aunque no se haya alcanzado el valor del parámetro MAXCAPACITY de la definición de clase de dispositivo. El servidor de IBM Spectrum Protect no conserva los volúmenes virtuales en estado FILLING y no realiza adiciones a éstos. Si el valor del parámetro MAXSCRATCH es demasiado bajo, las operaciones de servidor a servidor podrían no ejecutarse correctamente.

#### REUsedelay

Especifica el número de días que deben transcurrir desde que se suprimen todos los archivos de un volumen hasta que pueda volver a grabarse en el volumen o que se devuelva a la agrupación de reutilizables. Este parámetro es opcional. Puede especificar un entero de 0 a 9999. El valor 0 significa que se puede grabar encima de un volumen o devolverlo a la agrupación de reutilizables, en cuanto se hayan suprimido todos los archivos del volumen.

Consejo: Utilice este parámetro para asegurarse de que al restaurar la base de datos a un nivel anterior, las referencias de la base de datos a archivos de la agrupación de datos activos seguirán siendo válidas. Debe establecer este parámetro en un valor mayor que el número de días que piensa retener la copia de seguridad de base de datos más antigua. El número de días que se especifica para este parámetro debe ser igual al número que se especifica para el comando SET DRMDBBACKUPEXPIREDAYS.

#### OVFLOcation

Especifica la ubicación de desbordamiento de la agrupación de almacenamiento. El servidor asigna este nombre de ubicación a un volumen que se expulsa de la biblioteca mediante el comando MOVE MEDIA. Este parámetro es opcional. El nombre de ubicación puede tener una longitud máxima de 255 caracteres. El nombre de ubicación debe estar delimitado por comillas si contiene caracteres en blanco.

Para suprimir un valor existente, especifique una serie nula ("").

#### CRCDData

Especifica si una comprobación de redundancia cíclica (CRC) debe validar los datos de la agrupación de almacenamiento cuando se produce el proceso de auditoría de volumen en el servidor. Este parámetro sólo es válido para agrupaciones de almacenamiento con el formato NATIVE. Este parámetro es opcional. El valor predeterminado es NO. Si establece CRCDATA en YES y planifica un mandato AUDIT VOLUME, puede garantizar de forma continua la integridad de los datos que se almacenan en la jerarquía de almacenamiento. Puede especificar los valores siguientes:

Yes



Especifica que los datos se almacenan con información de CRC, lo que permite que el proceso de auditoría de volumen valide los datos de la agrupación de almacenamiento. Esta modalidad afecta al rendimiento, puesto que se requiere más proceso para calcular y comparar los valores de CRC entre la agrupación de almacenamiento y el servidor.

No

Especifica que los datos se almacenan sin información de CRC.

Consejo:

Para agrupaciones de almacenamiento asociadas con el tipo de dispositivo 3592, LTO o ECARTRIDGE, la protección de bloques lógicos proporciona una mejor protección contra daños en los datos que la validación de CRC para una agrupación de almacenamiento. Si especifica validación de CRC para una agrupación de almacenamiento, los datos sólo se validan durante las operaciones de auditoría de volúmenes. Los errores se identifican después de grabar los datos en cinta.

Para habilitar la protección de bloques lógicos, especifique un valor READWRITE para el parámetro LBPROTECT en los comandos DEFINE DEVCLASS y UPDATE DEVCLASS para los tipos de dispositivo 3592, LTO o ECARTRIDGE. La protección de bloques lógicos sólo está soportada en los siguientes tipos de unidades y soportes:

- IBM® LTO5 y posterior.
- Unidades IBM 3592 de tercera generación y posterior con soporte de 3592 de segunda generación y posterior.
- Unidades Oracle StorageTek T10000C y T10000D.

DEDuplicate

Especifica si los datos que se almacenan en esta agrupación de almacenamiento son duplicados. Este parámetro es opcional y sólo es válido para las agrupaciones de almacenamiento definidas con una clase de dispositivo de tipo FILE.

IDENTIFYProcess

Especifica el número de procesos paralelos que han de utilizarse para la eliminación de duplicados de datos del lado del servidor. Este parámetro es opcional y sólo es válido para agrupaciones de almacenamiento definidas con una clase de dispositivo FILE. Especifique un valor del 1 al 50.

Recuerde: Los procesos de eliminación de duplicados pueden estar activos o inactivos. Los procesos que trabajan en archivos están activos. Los procesos que esperan para trabajar en archivos están inactivos. Los procesos permanecen inactivos hasta que pasan a estas disponibles volúmenes con datos para los que deben eliminarse duplicados. La salida del comando QUERY PROCESS para la eliminación de duplicados incluye el número total de bytes y archivos que se han procesado desde que se ha iniciado por primera vez el proceso. Por ejemplo, si un proceso de eliminación de duplicados procesa cuatro archivos, pasa a estar desocupado y, a continuación, procesa cinco archivos más, el número total de archivos procesados es de nueve. Los procesos sólo finalizan cuando se cancelan o cuando el número de procesos de eliminación de duplicados para la agrupación de almacenamiento ha cambiado a un valor inferior al número actualmente especificado.




## Ejemplo: actualizar una agrupación de datos activos

Actualizar la agrupación de datos activos que se denomina TAPEPOOL2 de modo que el retardo de reutilización de volúmenes se cambie por 30 días y que la función de proximidad tenga el criterio de almacenar los archivos por nodo cliente.

```
update stgpool tapepool3 reusedelay=30 collocate=node
```

**Referencia relacionada:**

SET DRMDBBACKUPEXPIREDAYS (Especificar la caducidad de la serie de copia de seguridad de la base de datos)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## UPDATE STGPOOLDIRECTORY (Actualización de un directorio de agrupaciones de almacenamiento)

Utilice este mandato para actualizar un directorio de agrupaciones de almacenamiento.

### Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de almacenamiento sin restricciones o privilegio de almacenamiento restringido.

### Sintaxis

```
>>-UPDate STGPOOLDIRectory--nombre_agrupación--directorio----->
                                     .-MAXPProcess-----4-----.
>----ACCess-----+READWrite-----+-----+-----+-----+----->
```

```

+-READOnly-----+      '-MAXProcess-----número-'
+-DEStroyed----+
'-UNAVailable-'

.-Wait---No-----,
>-----+-----><
'-Wait---No---+'
      '-Yes-'

```

## Parámetros

nombre\_agrupación (Obligatorio)

Especifica la agrupación de almacenamiento que contiene el directorio que se debe actualizar. Este parámetro es necesario.

directorio (Obligatorio)

Especifica un directorio del sistema de archivos de la agrupación de almacenamiento. Este parámetro es necesario.

ACCess (Obligatorio)

Especifica la forma en que los nodos cliente y los procesos del servidor pueden acceder a los archivos en el directorio de agrupaciones de almacenamiento. Este parámetro es necesario. Son posibles los siguientes valores:

READWrite

Especifica que los archivos se pueden leer desde un directorio de agrupaciones de almacenamiento y grabarse en él.

READOnly

Especifica que los archivos se pueden leer desde el directorio de agrupaciones de almacenamiento.

DEStroyed

Especifica que los archivos están dañados de forma permanente y se deben destruir en el directorio de agrupaciones de almacenamiento. Utilice esta modalidad de acceso para indicar que se debe recuperar un directorio completo de agrupaciones de almacenamiento.

Consejos:

- Marque los directorios de agrupaciones de almacenamiento como `DESTROYED` antes de realizar la recuperación de datos. Cuando el directorio de agrupaciones de almacenamiento se marca como destruido, puede recuperar extensiones de datos en el servidor de réplica de destino.
- Utilice el parámetro `MAXPROCESS` para especificar el número de procesos paralelos que se pueden utilizar para actualizar un directorio de agrupaciones de almacenamiento.

UNAVailable

Especifica que no se puede acceder a los archivos en el directorio de agrupaciones de almacenamiento.

MAXPRocess

Especifica el número máximo de procesos paralelos que utilizar para actualizar un directorio de agrupaciones de almacenamiento. Este parámetro es opcional. Puede especificar un valor comprendido entre 1 y 99. El valor predeterminado es 4.

Restricción: Sólo puede utilizar este parámetro cuando se especifica el parámetro `ACCESS=DESTROYED`.

Si especifica el parámetro `ACCESS=DESTROYED`, cada contenedor del directorio de agrupaciones de almacenamiento se actualiza por medio de un proceso. Si el número máximo de procesos paralelos es mayor o igual que el número de contenedores que hay que actualizar, solo se crea un proceso para cada contenedor. Si el número de contenedores supera el valor del parámetro `MAXPROCESS`, el mandato espera a que los mandatos hijo finalicen para poder iniciar nuevos procesos.

Wait

Este parámetro opcional especifica si se ha de esperar a que el servidor de IBM Spectrum Protect complete el proceso de este mandato de forma subordinada. El valor predeterminado es `NO`. Puede especificar los valores siguientes:

No

El servidor procesa este mandato de forma subordinada y puede continuar con otras tareas mientras se procesa el mandato. Los mensajes relacionados con el proceso subordinado se muestran en el archivo de registro de actividades o en la consola de servidor dependiendo de dónde estén registrados los mensajes.

Yes

El servidor procesa este mandato de forma subordinada. La operación debe haber terminado su proceso para poder continuar con otras tareas. Los mensajes se visualizan en el registro de anotaciones de actividades, en la consola del servidor o en ambas, en función de dónde se anoten los mensajes.

Restricción: No se puede especificar `WAIT=YES` desde la consola del servidor.

## Ejemplo: Actualización de un directorio de agrupaciones de almacenamiento para destruirlo

Actualice un directorio de agrupaciones de almacenamiento que se denomina DIR1 en la agrupación de almacenamiento POOL1 para marcarlo como destruido.

```
update stgpooldirectory pool1 dir1 access=destroyed
```

## Ejemplo: actualización de un directorio de agrupaciones de almacenamiento para destruirlo en una agrupación de almacenamiento de contenedores en la nube

Actualizar un directorio de agrupación de almacenamiento llamado DIR3 en la agrupación de almacenamiento de contenedor en la nube CLOUDLOCALDISK1 para marcarlo como destruido.

```
update stgpooldirectory cloudlocaldisk1 dir3 access=destroyed
```

## Ejemplo: Actualice un directorio de agrupaciones de almacenamiento para que ya no esté disponible

Cuando el directorio de agrupaciones de almacenamiento no está disponible, el servidor no lee datos del directorio ni graba datos en el directorio. Para cambiar la modalidad de acceso a no disponible para un directorio de agrupaciones de almacenamiento, `dir1`, en una agrupación de almacenamiento denominada `pool1`, emita el siguiente mandato:

```
update stgpooldirectory pool1 dir1 access=unavailable
```

Tabla 1. Mandatos relacionados con UPDATE STGPOOLDIRECTORY

Comando	Descripción
DEFINE STGPOOL	Define una agrupación de almacenamiento como una agrupación de medios del servidor.
DEFINE STGPOOLDIRECTORY	Define un directorio de agrupación de almacenamiento en una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
DELETE STGPOOLDIRECTORY	Suprime un directorio de agrupación de almacenamiento de una agrupación de almacenamiento de contenedores de directorio o contenedores de nube.
QUERY STGPOOLDIRECTORY	Muestra información sobre directorios de agrupaciones de almacenamiento.

## UPDATE VIRTUALFSMAPPING (Actualizar una correlación de espacios de archivos virtuales)

Utilice este mandato para actualizar una definición de correlación de espacio de archivos virtuales.

Restricción: No puede utilizar el mandato UPDATE VIRTUALFSMAPPING para actualizar una correlación de espacio de archivos virtuales para un dispositivo NAS EMC Celerra o EMC VNX. Debe utilizar el mandato DEFINE VIRTUALFSMAPPING.

El dispositivo NAS necesita una definición de desplazador de datos asociados porque cuando el servidor actualiza una correlación de espacio de archivos virtuales, el servidor contacta con el dispositivo NAS para validar el sistema de archivos virtual y el nombre del sistema de archivos.

### Clase de privilegio

Para emitir este mandato, debe tener una de las clases de privilegio siguientes:

- Privilegio de sistema
- Privilegio de políticas sin restricciones
- Privilegio de políticas restringido para el dominio al que está asignado el nodo NAS.

### Sintaxis

```
>>-UPDate VIRTUALFSMapping--nombre_nodo--nombre_espacio_archivos_virtual-->
>>+-----+----->
  '-FILESystem---nuevo_nombre_sistema_archivos-'
```

```

>-----+><
| .-NAMEType-----SERVER----- . |
|'-PATH-----nuevo_nombre_ruta-----+'
|'-NAMEType-----+SERVER-----+'
|'-HEXadecimal-'

```

## Parámetros

nombre\_nodo (Necesario)

Especifica el nodo NAS en el que residen la ruta y el sistema de archivos. No es posible utilizar caracteres comodín ni una lista de nombres.

nombre\_espacio\_archivos\_virtual (Obligatorio)

Especifica la correlación de espacios de archivos virtuales que se actualizará. No es posible utilizar caracteres comodín ni una lista de nombres.

FILESystem

Especifica el nuevo nombre del sistema de archivos en el que se encuentra la ruta. El nombre del sistema de archivos debe existir en el nodo NAS especificado. El nombre del sistema de archivos no puede contener caracteres comodín. El nombre del sistema de archivos sólo debería modificarse cuando el nombre del sistema de archivos se ha modificado en el dispositivo NAS o, por ejemplo, cuando se ha trasladado el directorio a un sistema de archivos distinto. Este parámetro es opcional.

PATH

Especifica la nueva ruta desde la raíz del sistema de archivos hasta el directorio. La ruta sólo puede hacer referencia a un directorio. Sólo debería modificarse cuando se ha modificado la ruta del dispositivo NAS o, por ejemplo, cuando se ha trasladado el directorio a una ruta distinta. La longitud máxima de la ruta es de 1024 caracteres. El nombre de ruta es sensible a las mayúsculas y minúsculas. Este parámetro es opcional.

NAMEType

Especifica la forma en la que el servidor debe interpretar el nombre de ruta especificado. Especifique este parámetro sólo si especifica una ruta. Este parámetro es útil cuando una ruta contiene caracteres que no forman parte de la página de códigos en que se ejecuta el servidor. El valor predeterminado es SERVER.

Los valores posibles son:

SERVER

La página de código en la que se está ejecutando el servidor se utiliza para interpretar la ruta.

HEXadecimal

El servidor interpreta el nombre de ruta que ha entrado como la representación hexadecimal de la ruta. Esta opción debe utilizarse cuando una ruta contenga caracteres que no se pueden entrar. Por ejemplo, esto podría ocurrir si el sistema de archivos NAS se establece en un idioma diferente de aquél en que se ejecuta el servidor.

## Ejemplo: modificar la ruta de una correlación de espacios de archivos virtuales

Actualizar la correlación de espacios de archivos virtuales /mikeshomedir para el nodo NAS NAS1 modificando la ruta.

```
update virtualfsmapping nas1 /mikeshomedir path=/new/home/mike
```

## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE VIRTUALFSMAPPING

Comando	Descripción
DEFINE VIRTUALFSMAPPING	Define una correlación de espacios de archivos virtuales.
DELETE VIRTUALFSMAPPING	Suprime una correlación de espacios de archivos virtuales.
QUERY VIRTUALFSMAPPING	Consulta una correlación de espacios de archivos virtuales.

## UPDATE VOLHISTORY (Actualizar información histórica de volúmenes secuenciales)

Utilice este comando para actualizar la información histórica de volúmenes de un volumen generado por una copia de seguridad de base de datos o una operación de exportación. Este comando no se utiliza con los volúmenes de agrupaciones de almacenamiento.

Utilice el comando UPDATE BACKUPSET para actualizar la información de volúmenes del juego de copias de seguridad en el archivo histórico de volúmenes. No utilice el mandato UPDATE VOLHISTORY para actualizar en el archivo histórico de volúmenes la información de volúmenes correspondiente al juego de copias de seguridad.

## Clase de privilegio

---

Para emitir este comando, debe tener privilegio de sistema o privilegio de almacenamiento ilimitado.

## Sintaxis

---

```
>>-UPDate VOLHistory--nombre_volumen----->
>--DEVclass-----nombre_clase_dispositivo----->
>--+-----+----->
  '-LLocation-----ubicación-'
>--+-----+-----<
  '-ORMState-----+MOUNTable-----+'
    +-NOTMOUNTable-----+
    +-COUrier-----+
    +-VAult-----+
    '-COURIERRetrieve-'
```

## Parámetros

---

nombre\_volumen (Necesario)

Especifica el nombre del volumen. El volumen debe haberse utilizado para una copia de seguridad de base de datos o una operación de exportación.

DEVclass (Necesario)

Especifica el nombre de la clase de dispositivo del volumen.

LOcation

Especifica la ubicación del volumen. Este parámetro es obligatorio si el parámetro ORMSTATE no se ha especificado. La longitud máxima del texto son 255 caracteres. El texto debe estar delimitado por comillas si contiene algún carácter en blanco.

Consejo: El comando UPDATE VOLHISTORY admite actualizaciones en la información de ubicación y ORMSTATE para los volúmenes de copia de seguridad de instantánea de base de datos.

ORMState

Especifica un cambio en el estado de un volumen de copia de seguridad de base de datos. Este parámetro es necesario si el parámetro LOCATION no se ha especificado. Este parámetro solo se admite en sistemas con licencia de Disaster Recovery Manager. Los estados posibles son:

MOUNTable

El volumen contiene datos válidos y se puede acceder a él para el proceso en el local.

NOTMOUNTable

El volumen está en el local, contiene datos válidos y no se puede acceder a él para proceso en el local.

COUrier

El volumen se está trasladando fuera del local.

VAult

El volumen está fuera del local, contiene datos válidos y no se puede acceder a él para proceso en el local.

COURIERRetrieve

El volumen se está trasladando al local.

## Ejemplo: actualizar la ubicación de un volumen que se utiliza para la copia de seguridad de la base de datos

---

Actualizar la ubicación de un volumen que se utiliza para la copia de seguridad de base de datos, BACKUP1, para mostrar que se ha trasladado a una ubicación fuera del local.

```
update volhistory backup1 devclass=tapebkup
location="700 w. magee rd."
```

## Comandos relacionados

---

Tabla 1. Comandos relacionados con UPDATE VOLHISTORY

Comando	Descripción
BACKUP VOLHISTORY	Graba la información histórica de volúmenes en archivos externos.
DELETE VOLHISTORY	Elimina la información histórica de volúmenes del archivo histórico de volúmenes.
MOVE DRMEDIA	Mueve el medio DRM fuera y dentro del local.
PREPARE	Crea un archivo de plan de recuperación.
QUERY DRMEDIA	Visualiza información acerca de los volúmenes de recuperación ante siniestro.
QUERY VOLHISTORY	Visualiza información histórica de volúmenes secuenciales recogida por el servidor.

## UPDATE VOLUME (Actualizar un volumen de agrupación de almacenamiento)

Utilice este comando para cambiar la modalidad de acceso para uno o varios volúmenes de agrupaciones de almacenamiento.

Una condición de error asociada a un volumen se puede corregir actualizando el volumen a la modalidad de acceso READWRITE. También se puede utilizar este comando para cambiar la información de ubicación para uno o más volúmenes de agrupaciones de almacenamiento de acceso secuencial.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

### Sintaxis

```

(1)
>>-UPDate Volume-----nombre_volumen----->
>-----+-----+-----+-----+----->
  '-ACCess-----+READWrite-----+-'
    +-READOnly-----+
    +-UNAVailable---+
    |           (2) |
    +-DEStroyed-----+
    |           (3) |
    '-Offsite-----'
>-----+-----+-----+-----+----->
  |           (4) |
  '-LLocation-----ubicación-'
  .-WHERESTGpool----*-----
>-----+-----+-----+-----+----->
  '-WHERESTGpool----nombre_agrupación-'
  .-WHEREDEVclass----*-----
>-----+-----+-----+-----+----->
  '-WHEREDEVclass----nombre_clase_dispositivo-'
>-----+-----+-----+-----+----->
  |           .-,-----|
  |           V         |
  '-WHEREACCess-----+READWrite-----+-'
    +-READOnly-----+
    +-UNAVailable-+
    +-Offsite-----+
    '-DEStroyed---'
>-----+-----+-----+-----+----->
  |           .-,-----|
  |           V         |
  '-WHERESTatus-----+ONline-----+-'
    +-Offline-+
  
```

```

+-EMPTy---+
+-PENding-+
+-FILLing-+
'-FULL----'

.-Preview ----No-----
>-----+-----><
'-Preview----+No--+-'
'-Yes-'

```

#### Notas:

1. Debe actualizar como mínimo un atributo (ACCESS o LOCATION).
2. Este valor sólo es válido para los volúmenes de agrupaciones de almacenamiento primarias.
3. Este valor sólo es válido para los volúmenes de agrupaciones de almacenamiento de copia.
4. Este parámetro sólo es válido para los volúmenes de agrupaciones de almacenamiento de acceso secuencial.

## Parámetros

---

### nombre\_volumen (Necesario)

Especifica el volumen de agrupación de almacenamiento que se actualiza. Puede utilizar caracteres comodín para especificar nombres.

### ACCess

Especifica cómo pueden los nodos cliente y los procesos de servidor (como, por ejemplo, migración) acceder a los archivos del volumen de agrupación de almacenamiento. Este parámetro es opcional. Los valores posibles son:

#### READWrite

Especifica que los nodos cliente y los procesos del servidor pueden realizar operaciones de lectura y grabación en los archivos almacenados en el volumen.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

#### READOnly

Especifica que los nodos cliente y los procesos del servidor sólo pueden realizar operaciones de lectura en los archivos almacenados en el volumen.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

#### UNAVailable

Especifica que ni los nodos cliente ni los procesos del servidor pueden acceder a los archivos almacenados en el volumen.

Para que un volumen de acceso aleatorio se convierta en UNAVAILABLE, debe desactivar el volumen. Una vez convertido un volumen de acceso aleatorio en UNAVAILABLE, el volumen no se puede activar.

Si hace que un volumen de acceso secuencial deje de estar disponible, el servidor no intentará montarlo.

Si el volumen que está actualizándose es un volumen reutilizable vacío que tiene la modalidad de acceso OFFSITE, el servidor suprimirá el volumen de la base de datos.

#### DESTroyed

Especifica que un volumen de agrupación de almacenamiento primaria se ha dañado de modo permanente. Ni los nodos cliente ni los procesos del servidor pueden acceder a los archivos almacenados en el volumen. Utilice esta modalidad de acceso para indicar un volumen completo que debe restaurarse con el comando RESTORE STGPOOL. Una vez que todos los archivos de un volumen DESTROYED se han restaurado en otros volúmenes, el servidor suprime automáticamente de la base de datos el volumen DESTROYED.

Sólo se pueden actualizar a DESTROYED los volúmenes de agrupaciones de almacenamiento primarias.

Para poder actualizar un volumen de acceso aleatorio al acceso DESTROYED, debe desactivar el volumen. Una vez actualizado el volumen de acceso aleatorio a DESTROYED, no se puede activar el volumen.

Si actualiza un volumen de acceso secuencial a DESTROYED, el servidor no intentará montar el volumen.

Si un volumen no contiene ningún archivo y la modalidad de acceso se cambia a DESTROYED, el servidor suprime el volumen de la base de datos.

#### Offsite

Especifica que hay un volumen de agrupación de almacenamiento de copia o de datos activos en una ubicación fuera del local desde la que no se puede montar. Sólo pueden tener la modalidad de acceso OFFSITE los volúmenes de las agrupaciones de almacenamiento de copia o de datos activos.

Si especifica valores para ambos parámetros ACCESS y LOCATION, pero la modalidad de acceso no se puede actualizar para un volumen determinado, el atributo de ubicación no se actualiza tampoco para dicho volumen. Por ejemplo, si especifica ACCESS=OFFSITE y el valor LOCATION para un volumen de agrupación de almacenamiento primaria, no se actualizan los valores de acceso ni los de ubicación porque un volumen de agrupación de almacenamiento primaria no puede tener la modalidad de acceso OFFSITE.

#### Location

Especifica la ubicación del volumen. Este parámetro es opcional. Este parámetro únicamente puede especificarse para los volúmenes de agrupaciones de almacenamiento de acceso secuencial. La longitud máxima de la lista de la ubicación es de 255 caracteres. La ubicación debe estar encerrada entre comillas si contiene espacios en blanco. Para suprimir una ubicación definida anteriormente, especifique una serie nula ("").

#### WHERESTGpool

Especifica el nombre de la agrupación de almacenamiento para los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización por agrupación de almacenamiento. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de agrupación de almacenamiento, se actualizarán los volúmenes que pertenezcan a cualquier agrupación de almacenamiento.

#### WHEREDEVclass

Especifica el nombre de la clase de dispositivo de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización por clase de dispositivo. Este parámetro es opcional. Puede utilizar caracteres comodín para especificar nombres. Si no especifica un nombre de clase de dispositivo, se actualizarán los volúmenes que pertenezcan a cualquier clase de dispositivo.

#### WHEREACcess

Especifica la modalidad de acceso actual de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización a los volúmenes que tienen la modalidad de acceso especificada. Este parámetro es opcional. Puede especificar varias modalidades de acceso separando las modalidades con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la actualización no se restringirá por la modalidad de acceso actual de un volumen. Los valores posibles son:

##### READWrite

Se actualizan los volúmenes con la modalidad de acceso READWRITE.

##### READOnly

Se actualizan los volúmenes con la modalidad de acceso READONLY.

##### UNAVailable

Se actualizan los volúmenes con la modalidad de acceso UNAVAILABLE.

##### Offsite

Se actualizan los volúmenes con la modalidad de acceso OFFSITE.

##### DESTroyed

Se actualizan los volúmenes con la modalidad de acceso DESTROYED.

#### WHEREStatus

Especifica el estado de los volúmenes que se han de actualizar. Utilice este parámetro para restringir la actualización a los volúmenes que tienen un estado especificado. Este parámetro es opcional. Puede especificar varios valores de estado separando los valores con comas y sin espacios intercalados. Si no especifica un valor para este parámetro, la actualización no se restringirá por estado de volumen. Los valores posibles son:

##### ONline

Se actualizan los volúmenes con el estado ONLINE.

##### OFFline

Se actualizan los volúmenes con el estado OFFLINE.

##### EMPTy

Se actualizan los volúmenes con el estado EMPTY.

##### PENding

Se actualizan los volúmenes con el estado PENDING. Estos son los volúmenes a los que se les han suprimido todos los archivos, pero para los que no ha transcurrido el tiempo especificado mediante el parámetro REUSEDELAY.

##### FILLing

Se actualizan los volúmenes con el estado FILLING.

##### FULL

Se actualizan los volúmenes con el estado FULL.

#### Preview

Especifica si desea previsualizar la operación de actualización sin actualizar realmente los volúmenes. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:



No

Especifica que los volúmenes se actualizarán.

Yes

Especifica que sólo desea previsualizar la operación de actualización. Esta opción visualiza los volúmenes que se actualizarán, si realiza la operación de actualización.

## Ejemplo: establecer que un volumen de cinta no esté disponible

Actualizar un volumen de cinta denominado DSMT20 para que esté no disponible para los nodos cliente y los procesos del servidor.

```
update volume dsmt20 access=unavailable
```

## Ejemplo: actualizar la modalidad de acceso de todos los volúmenes fuera del local de una agrupación de almacenamiento específica

Actualizar todos los volúmenes de fuera del local vacíos de la agrupación de almacenamiento TAPEPOOL2. Establecer la modalidad de acceso en READWRITE y suprimir la información de ubicación para los volúmenes actualizados.

```
update volume * access=readwrite location="" wherestgpool=tapepool2  
whereaccess=offsite wherestatus=empty
```





## Comandos relacionados

Tabla 1. Comandos relacionados con UPDATE VOLUME

Comando	Descripción
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.
VARY	Especifica si está disponible un volumen de disco para el servidor.

## Comandos VALIDATE

Utilice el comando VALIDATE para verificar que un objeto esté completo o sea válido para IBM Spectrum Protect.

-  Sistemas operativos Linux VALIDATE ASPERA (Validación de una configuración Aspera FASP)
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows VALIDATE CLOUD (Validar credenciales de nube)
- VALIDATE LANFREE (Validar rutas fuera de la LAN)
- VALIDATE POLICYSET (Verificar un juego de políticas)
- VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)
- VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

 Sistemas operativos Linux

## VALIDATE ASPERA (Validación de una configuración Aspera FASP)

Utilice este mandato para determinar si se puede utilizar la tecnología Aspera Fast Adaptive Secure Protocol (FASP) para optimizar la transferencia de datos en el entorno del sistema. Específicamente, puede determinar si la tecnología Aspera FASP podría resultar en un mejor rendimiento de la red que la tecnología TCP/IP.

Esta mandato verifica los siguientes elementos adicionales:

- Si el entorno del sistema se ha configurado correctamente para utilizar tecnología Aspera FASP
- Si se han instalado las licencias necesarias para habilitar la tecnología Aspera FASP

La tecnología Aspera FASP se utiliza para optimizar la transferencia de datos para la réplica de nodos o para la protección de agrupaciones de almacenamiento en una red de área amplia (WAN). Sin embargo, no es necesario configurar el sistema para que la réplica de nodos o la protección de agrupaciones de almacenamiento ejecuten el mandato VALIDATE ASPERA. Si el sistema se ha configurado para la réplica de nodos o la protección de agrupaciones de almacenamiento en un entorno local, puede emitir el mandato para evaluar si los datos se pueden replicar correctamente en un servidor remoto.

Este mandato solo está disponible en sistemas operativos Linux x86\_64.

Antes de emitir el mandato, complete las tareas siguientes:

1. Asegúrese de haber definido al menos un servidor en su entorno del sistema. Emita el mandato PING SERVER para asegurarse de que se puede conectar al servidor definido. Por ejemplo, si el servidor se denomina VMRH6T, emita el mandato siguiente:  

```
ping server vmrh6t
```
2. Para utilizar el mandato VALIDATE ASPERA para determinar la velocidad del rendimiento de red, instale licencias de evaluación de 30 días o licencias completas e ilimitadas en los servidores de origen y destino. Por ejemplo, instale licencias en los servidores de origen y destino, VMRH6 y VMRH6T. Para obtener instrucciones sobre cómo obtener e instalar licencias, consulte el apartado Determinación de si la tecnología Aspera FASP puede optimizar la transferencia de datos en el entorno del sistema.

Para simular un entorno que utiliza varias sesiones, puede ejecutar varias instancias del mandato VALIDATE ASPERA de forma simultánea. Si quiere ejecutar varias sesiones, es posible que quiera limitar el ancho de banda de cada conexión de red para asegurarse de que hay el suficiente ancho de banda disponible para todas las conexiones de red. Para limitar el ancho de banda, especifique la opción de servidor FASPTARGETRATE, tal y como se describe en el apartado FASPTARGETRATE.

Para consultar la cantidad que se está transfiriendo actualmente, emita el mandato QUERY PROCESS:

```
proceso de consulta
```

Puede obtener el número de proceso de la salida del mandato QUERY PROCESS. Puede cancelar el proceso emitiendo el mandato CANCEL PROCESS y especificando el número de proceso, por ejemplo:

```
cancel process 3
```

## Clase de privilegio

---

Cualquier administrador puede emitir este mandato.

## Sintaxis

---

```
>>-VALidate ASPera--+-+-----+-----+----->
                        '---nombre_servidor_destino---'
                        .-Wait-----No-----.
>--+-----+-----+-----<<
  '-DURation---segundos-'  '-Wait---+No---+'
                          '-Yes-'
```

## Parámetros

---

nombre\_servidor\_destino

Especifica un servidor definido previamente. Este parámetro es opcional. Para especificar este parámetro, siga las directrices:

- Para determinar si Aspera FASP puede optimizar un proceso de réplica de nodo, especifique un servidor de destino que se haya configurado para la réplica de nodos.
- Para determinar si Aspera FASP puede optimizar un proceso de protección de agrupaciones de almacenamiento, especifique un servidor de destino que se haya configurado para la protección de agrupaciones de almacenamiento.
- Para determinar si Aspera FASP puede optimizar la transferencia de datos a un servidor remoto definido, pero no configurado, para la réplica de nodos o la protección de agrupaciones de almacenamiento, especifique ese servidor de destino.
- Si no especifica un servidor de destino, la salida del mandato indica si el servidor de origen se han configurado correctamente para la transmisión de datos de Aspera FASP. La salida indica también si se ha instalado una licencia válida para Aspera FASP en el servidor de origen.

DURation

Especifica el tiempo asignado, en segundos, para transferir datos a través de la red y evaluar el rendimiento. Este parámetro es opcional. El valor predeterminado es de 120 segundos. Puede especificar un valor comprendido entre 120 y 3600000 segundos. El tiempo asignado se divide entre las transferencias de datos Aspera FASP y TCPIP.

Wait

Especifica si se debe esperar a que el servidor termine el proceso de mandato. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los valores siguientes:

No

Especifica que el servidor procesa el mandato en segundo plano. Puede continuar trabajando con otras tareas mientras se procesa el mandato. Si especifica NO, los mensajes de salida se visualizarán en el registro de actividad.

Yes

Especifica que el servidor procesa el mandato en primer plano. La operación debe haber terminado su proceso para poder continuar con otras tareas. Si especifica YES, los mensajes de salida se visualizan en el cliente de línea de mandatos administrativos.

Restricción: No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: visualización de información sobre el estado de una configuración de Aspera FASP

---

En el servidor de origen, ejecute el mandato `VALIDATE ASPERA`. Para asegurarse de que los mensajes se visualicen en el cliente de línea de mandatos administrativos, especifique `WAIT=YES`. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
validate aspera wait=yes
```

```
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.  
Amount transferred using FASP: 0 MB per second. Amount transferred using  
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: OK. Days until  
license expires: Never.
```

## Ejemplo: verificar si se han instalado las licencias necesarias

---

En el servidor de origen, ejecute el mandato `VALIDATE ASPERA` y especifique el servidor de réplica de destino. Para asegurarse de que los mensajes se visualicen en el cliente de línea de mandatos administrativos, especifique `WAIT=YES`. Consulte el apartado Descripciones de los campos para obtener las descripciones de los campos.

```
validate aspera vmrh6t wait=yes
```

```
ANR0984I Process 8 for VALIDATE ASPERA started in the FOREGROUND at 09:35:21 AM.  
ANR3672E The license file that is required to enable Aspera Fast Adaptive  
Secure Protocol (FASP) technology was not found on the VMRH6 server.  
ANR3836I Validation of the Aspera FASP connection from VMRH6 to localhost.  
Amount transferred using FASP: 0 MB per second. Amount transferred using  
TCP/IP: 0 MB per second. Latency: 0 microseconds. Status: Invalid  
configuration. Days until license expires: Expired.  
ANR0985I Process 8 for VALIDATE ASPERA running in the FOREGROUND completed with  
completion state FAILURE at 09:35:21 AM.  
ANR1893E Process 8 for VALIDATE ASPERA completed with a completion state of  
FAILURE.
```

## Descripciones de los campos

---

### Estado

Estado de la configuración. Son posibles los siguientes valores:

- `OK` indica que no se han detectado problemas.
- `Invalid configuration` indica que falta un archivo de configuración, archivo de licencia o archivo de biblioteca de Aspera FASP.
- `License issue` indica que hay una licencia que falta, que está caducada o que no es válida.
- `Server failure` indica que se están utilizando todos los puertos, que se ha producido un error de lectura/escritura de red o que no se puede grabar en el archivo de registro de Aspera FASP.
- `Invalid target configuration` indica que falta un archivo de configuración, un archivo de configuración o un archivo de licencia de Aspera FASP en el servidor de destino.
- `Failure on target server` indica que se están utilizando todos los puertos, que se ha producido un error de lectura/escritura de red o que no se puede grabar en el archivo de registro de Aspera FASP.
- `License issue on target server` indica que hay una licencia no válida o caducada en el servidor de destino.
- `Unsupported operating system` indica que se ha instalado un sistema operativo distinto a Linux x86\_64 en uno de los servidores o en ambos.
- `Unknown` indica que se ha producido un error inesperado. Para identificar el error, revise los mensajes de registro.

Días que faltan hasta que caduque la licencia

Son posibles los siguientes valores:

- `Never` indica que se ha instalado una licencia completa e ilimitada.
- `Today` indica que se ha instalado una licencia de evaluación de 30 días que caduca hoy.

- `Expired` indica que se ha instalado una licencia de evaluación de 30 días, pero ya ha caducado.
- `Number` indica que se ha instalado una licencia de evaluación de 30 días que caducará dentro del número de días especificado.
- `License not found` indica que no se ha encontrado ninguna licencia.

Cantidad transferida utilizando TCP/IP

La velocidad de la transferencia de datos, en megabytes por segundo, utilizando tecnología TCP/IP.

Cantidad transferida utilizando FASP

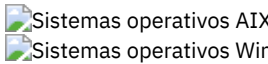
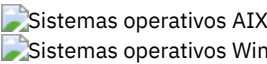
Velocidad de la transferencia de datos, en megabytes por segundo, utilizando tecnología Aspera FASP.

Latencia

Latencia de la transferencia de datos en microsegundos.

## Comandos relacionados

Tabla 1. Mandatos relacionados con VALIDATE ASPERA

Comando	Descripción
CANCEL SESSION	Cancela las sesiones activas con el servidor.
DEFINE SERVER	Define un servidor para las comunicaciones de servidor a servidor.
PING SERVER	Prueba las conexiones entre servidores.
 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Windows PROTECT STGPOOL	 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Windows Protege una agrupación de almacenamiento de contenedores de directorio.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.

## VALIDATE CLOUD (Validar credenciales de nube)

Utilice este mandato antes de definir una agrupación de almacenamiento para asegurarse de que las credenciales de una agrupación de almacenamiento de contenedores de nube sean válidas y de que el usuario tenga asignados los permisos necesarios.

### Clase de privilegio

Cualquier administrador puede emitir este mandato.

### Sintaxis

```

      .-CLOUDType---Swift-----
>>-VALidate CLOud----->
      '-CLOUDType---+Azure---+'
                +-S3-----+
                +-Softlayer-+
                +-Swift-----+
                '-V1Swift---'
                                     (1)
>--CLOUDUrl-----url_nube--IDentity---identidad_nube----->
>--PAssword-----contraseña----->
>--+-----+<
|                                     (2) |
| '-BUCKETName---bucket_name-----'

```

Notas:

1. Si especifica CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY.
2. El parámetro BUCKETNAME es válido sólo si especifica CLOUDTYPE=S3.

### Parámetros

CLOUDType

Especifica el tipo de entorno de nube donde está configurando la agrupación de almacenamiento.

Puede especificar uno de los siguientes valores:

**Azure**

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing Microsoft Azure.

**S3**

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing con el protocolo de servicio de almacenamiento simple (S3), como IBM® Cloud Object Storage o Amazon Web Services (AWS) S3.

**Softlayer**

Especifica que la agrupación de almacenamiento utiliza un sistema cloud computing IBM SoftLayer (IBM Bluemix) con un sistema cloud computing OpenStack Swift.

**Swift**

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 2 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

**V1Swift**

Especifica que la agrupación de almacenamiento utiliza un sistema de nube de OpenStack Swift. Este valor también especifica que la agrupación de almacenamiento utiliza la versión 1 del protocolo para la autenticación en la nube. El URL de la nube suele contener el número de versión del protocolo que se utiliza.

Este parámetro es opcional. Si no especifica el parámetro, se utiliza el valor predeterminado SWIFT.

**CLOUDUrl (Obligatorio)**

Especifica la URL del entorno de nube donde se configura la agrupación de almacenamiento. En función del proveedor de nube, puede utilizar un punto final de servicio blob, una URL de punto final de región, una dirección IP de accesor, un punto final de autenticación pública o un valor similar para este parámetro. Asegúrese de incluir el protocolo, como por ejemplo `https://` o `http://` al principio del URL. La longitud máxima de la dirección web es de 870 caracteres. El parámetro CLOUDURL se valida cuando empieza la primera copia de seguridad.

**Identity (Obligatorio)**

Especifica el ID de usuario para la nube. Este parámetro es necesario para todos los sistemas de computación en la nube excepto Azure. Si especifica CLOUDTYPE=AZURE, no especifique el parámetro IDENTITY. En función del proveedor de nubes, puede utilizar un ID de clave de acceso, un nombre de usuario o un valor similar para este parámetro. La longitud máxima del ID de usuario es de 255 caracteres.

**PAssword (Obligatorio)**

Especifica la contraseña para la nube. En función del proveedor de nube, puede utilizar una firma de acceso compartido (SAS), una clave de acceso secreta, una clave de API, una contraseña o un valor similar para este parámetro. Este parámetro es obligatorio. La longitud máxima de la contraseña es de 255 caracteres.

**BUCKETName**

Especifica el nombre de un grupo de AWS S3 o una caja fuerte de IBM Cloud Object Storage que se van a utilizar con esta agrupación de almacenamiento, en lugar de utilizar el nombre de grupo o el nombre de caja fuerte predeterminados. Este parámetro es opcional y sólo es válido si especifica CLOUDTYPE=S3. Si existe un grupo o una caja fuerte con el nombre que ha especificado, dicho grupo o dicha caja fuerte se prueba para garantizar que se han establecido los permisos adecuados. Si el grupo o la caja fuerte no existen, el parámetro verifica sólo que el grupo o la caja fuerte con dicho nombre no existan. Siga las restricciones de nombre para el proveedor de nube cuando especifica este parámetro. Revise los permisos del grupo o de la caja fuerte y asegúrese de que las credenciales tengan permiso para leer, escribir, listar y suprimir objetos de este grupo o caja fuerte. Consejo: Si no especifica el parámetro BUCKETNAME, el ID exclusivo de duplicación global se utilizará como nombre de grupo predeterminado. El valor predeterminado es

`ibmsp guid`

donde `guid` es el valor REPLICATION GLOBALLY UNIQUE ID, menos los puntos, en la salida del mandato QUERY REPLSERVER. Por ejemplo, si el ID exclusivo de duplicación global es 52.82.39.20.64.d0.11.e6.9d.77.0a.00.27.00.00.00, el nombre de grupo predeterminado será `ibmsp.5282392064d011e69d770a0027000000`.

## Ejemplo: Verificar las credenciales de una agrupación de almacenamiento en el contenedor de nubes S3

Valide las credenciales de la agrupación de almacenamiento en el contenedor de nubes.

```
validate cloud
cloudtype=s3 clouurl=http://123.234.123.234:5000/v2.0
password=protect8991 bucketname=ibmsp.5282392064d011e69d770a0027000000
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con VALIDATE CLOUD

Comando	Descripción
---------	-------------

Comando	Descripción
DEFINE STGPOOL (contenedor en la nube)	Defina una agrupación de almacenamiento de contenedor en la nube.
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
UPDATE STGPOOL (contenedor de nubes)	Actualizar una agrupación de almacenamiento de contenedores de nube.

## VALIDATE LANFREE (Validar rutas fuera de la LAN)

Utilice este mandato para determinar qué destinos de un nodo determinado pueden realizar movimientos de datos sin LAN utilizando un agente de almacenamiento específico.

### Clase de privilegio

Para emitir este comando, debe tener privilegio de sistema.

### Sintaxis

```
>>-VALidate LAnfree--nombre_nodo--nombre_agente_alm-----><
```

### Parámetros

nombre\_nodo (Obligatorio)

El nombre del nodo que se evaluará.

nombre\_stgagent (Obligatorio)

El nombre del agente de almacenamiento que se evaluará.

### Ejemplo: validar una configuración fuera de la LAN actual

Validar la configuración y las definiciones de servidor actuales para el nodo TIGER para utilizar el agente de almacenamiento AIX\_STA1 para operaciones de datos fuera de la LAN.

```
validate lanfree tiger aix_stal
```

Nomb. nodo	Agente almacen.	Operación	Nom. clase gestión	Nombre destino	Pos. fuera de LAN?	Explicación	
TIGER	AIX_STA1	COPIA	SEG	STANDARD	OUTPOOL	NO	No hay rutas activas disp.
TIGER	AIX_STA1	COPIA	SEG	STANDARD	PRIMARY	NO	Agrupación almac. destino está configurada para grabación simultánea.
TIGER	AIX_STA1	COPIA	SEG	STANDARD	SHRPOOL	SÍ	
TIGER	AIX_STA1	BACKUP	NOARCH	LFFILE	NO	Agrupación almac. contiene datos desduplicados por clientes y no es accesible para almacenamiento agentes V6.1 o anterior.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	OUTPOOL	NO	No hay rutas activas disp.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	PRIMARY	NO	Agrupación almac. destino está configurada para grabación simultánea.	
TIGER	AIX_STA1	ARCHIVADO	STANDARD	SHRPOOL	SÍ		

### Comandos relacionados

Tabla 1. Comandos relacionados con VALIDATE LANFREE

Comando	Descripción
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY DEVCLASS	Muestra información acerca de las clases de dispositivo.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY DRIVE	Muestra información sobre las unidades.
QUERY LIBRARY	Visualiza información sobre una o más bibliotecas.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY PATH	Muestra información sobre la ruta de un origen a un destino.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
QUERY STGPOOL	Visualiza información acerca de agrupaciones de almacenamiento.

## VALIDATE POLICYSET (Verificar un juego de políticas)

Utilice este comando para verificar que un juego de políticas está completo y es válido antes de activarlo. El comando examina las definiciones de clase de gestión y de grupo de copia del juego de políticas especificado y notifica las condiciones que debe tener en cuenta antes de activar el juego de políticas.

El comando VALIDATE POLICYSET no se ejecutará correctamente si se da alguna de las condiciones que se indican a continuación:

- El juego de políticas no tiene ninguna clase de gestión predeterminada.
- Un grupo de copia dentro del juego de políticas especifica una agrupación de almacenamiento de copia como su destino.
- Una clase de gestión especifica una agrupación de almacenamiento de copias como destino de los archivos que se han migrado mediante el cliente de IBM Spectrum Protect for Space Management.
- Se ha especificado un parámetro TOCDESTINATION y la agrupación de almacenamiento es una agrupación de copia o bien tiene un formato de datos distinto de NATIVE o NONBLOCK.

El servidor emite mensajes de aviso para las condiciones siguientes:

- Un grupo de copia especifica una agrupación de almacenamiento que no existe como destino.

Si activa un juego de políticas con grupos de copia que especifican agrupaciones de almacenamiento inexistentes, las operaciones de copia de seguridad o de archivado del cliente no se podrán realizar.

- Una clase de gestión especifica una agrupación de almacenamiento que no existe como destino de los archivos migrados mediante los clientes IBM Spectrum Protect for Space Management.
- El juego de políticas no tiene una o varias de las clases de gestión que existen en el juego de políticas ACTIVE actual.

Si activa el juego de políticas, los archivos de copia de seguridad vinculados con las clases de gestión suprimidas, se volverán a vincular con la clase de gestión predeterminada del nuevo juego de políticas activo.

- El juego de políticas no tiene uno o varios de los grupos de copia que existen en el juego de políticas ACTIVE actual.

Si activa el juego de políticas, dejan de ejecutarse operaciones de copia de seguridad y archivado de los archivos vinculados a las clases de gestión con grupos de copia suprimidos.

- La clase de gestión predeterminada del juego de políticas no contiene un grupo de copia de seguridad o copia archivada.

Si activa el juego de políticas con esta clase de gestión predeterminada, los clientes que utilicen el valor predeterminado no podrán hacer copias de seguridad ni copia archivadas de los archivos.

- Una clase de gestión especifica que debe existir una versión de copia de seguridad para que pueda migrarse un archivo desde un nodo cliente (MIGREQUIRESBKUP=YES), pero la clase de gestión no contiene ningún grupo de copia de seguridad.

Si el servidor tiene la protección de retención de datos activada, deben darse las condiciones siguientes:

- Todas las clases de gestión del juego de políticas que se va a validar deben contener un grupo de copia archivada.
- Si existe una clase de gestión en el juego de políticas activo, debe existir una clase de gestión con el mismo nombre en el juego de políticas que se va a validar.
- Si existe un grupo de copia archivada en el juego de políticas activo, el grupo de copia correspondiente en el juego de políticas que se va a validar debe tener un valor de RETVER que sea por lo menos tan alto como los valores correspondientes en el grupo de copia activo.

## Clase de privilegio

Para emitir este mandato, debe tener privilegio de sistema, privilegio de políticas no limitado o privilegio de políticas limitado para el dominio de políticas al que pertenece el juego de políticas.

## Sintaxis

```
>>-VALidate Policyset--nombre_dominio--nombre_juego_politicas--><
```

## Parámetros

nombre\_dominio (Necesario)

Especifica el nombre del dominio de políticas al que se ha asignado el juego de políticas.

nombre\_juego\_políticas (Necesario)

Especifica el nombre del juego de políticas que se valida.

## Ejemplo: validar un juego de políticas específico

Validar el juego de políticas `VACATION` que se encuentra en el dominio de políticas `EMPLOYEE_RECORDS`.

```
validate policyset employee_records vacation
```

## Comandos relacionados

Tabla 1. Comandos relacionados con VALIDATE POLICYSET

Comando	Descripción
ACTIVATE POLICYSET	Valida y activa un juego de políticas.
COPY POLICYSET	Crear una copia de un juego de políticas.
DEFINE COPYGROUP	Define un grupo de copia para el proceso de copias de seguridad o copias archivadas en una clase de gestión especificada.
DEFINE MGMTCLASS	Define una clase de gestión.
DELETE POLICYSET	Elimina un juego de políticas y sus clases de gestión y grupos de copias, de un dominio de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
UPDATE COPYGROUP	Cambia uno o más atributos de un grupo de copia.
UPDATE POLICYSET	Cambia la descripción de un juego de políticas.

## VALIDATE REPLICATION (Validar la réplica de un nodo de cliente)

Utilice esta mandato para identificar las reglas de réplica que se aplican a los espacios de archivos en los nodos de cliente que están configurados para la réplica. También puede utilizar este mandato para verificar que el servidor de réplica de origen puede comunicarse con el servidor de réplica de destino.

Antes de iniciar el proceso de réplica, utilice el mandato `VALIDATE REPLICATION` para determinar si la configuración de réplica es correcta.

Emita este comando en el servidor que actúe como origen para los datos replicados.

## Clase de privilegio



Para emitir este comando, debe tener privilegio de sistema.

## Sintaxis

```
      .-+-----+-.
      V             |
>>-VALidate REPLication-----nombre_nodo---+----->
      .-VERIFYconnection----No-----
>--+-----+-----+-----><
      '-VERIFYconnection----+-No--+-'
      '-Yes--'
```

## Parámetros

nombre\_nodo (Obligatorio)

Especifica el nombre del nodo de cliente cuyos espacios de archivos desea mostrar. Para especificar varios nombres de nodos de cliente, debe separarlos con comas y sin espacios intercalados. Puede utilizar caracteres comodín para especificar nombres.

Sólo se muestra información para los nodos de cliente que se han activado o desactivado para la réplica. La modalidad de réplica debe ser SEND. Para determinar si un nodo de cliente está activado o desactivado para la réplica y su modalidad, emita el mandato QUERY NODE. Busque los valores en los campos Estado de réplica y Modalidad de réplica.

VERIFYconnection

Especifica si se debe comprobar la conexión con un servidor de réplica de destino. La versión del servidor de réplica de destino también se comprueba para verificar que sea la versión 6.3 o posterior. Este parámetro es opcional. El valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No

No se comprueban la conexión y la versión del servidor de réplica de destino.

Sí

Se comprueban la conexión y la versión del servidor de réplica de destino.

## Ejemplo: validar la réplica de un nodo de cliente

El nombre del nodo de cliente es NODE1. Verifique el estado de conexión entre los servidores de réplica de origen y destino.

```
validate replication node1 verifyconnection=yes

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: C.S.
Regla de réplica de control: ACTIVE_DATA
Nivel de regla de réplica: Nivel de sistema
Nombre de servidor: DRSRV
Estado de conexión: Conexión válida

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: Arch
Regla de réplica de control: ALL_DATA_HIGH_PRIORITY
Nivel de regla de réplica: Nivel de nodo
Nombre de servidor: DRSRV
Estado de conexión: Conexión válida

      Nombre nodo: NODE1
      Nombre de espacio de archivos: \\node1\c$
      FSID: 1
      Tipo: SpMg
Regla de réplica de control: ALL_DATA
Nivel de regla de réplica: Nivel de sistema
Nombre de servidor: DRSRV
Estado de conexión: Conexión válida
```

Se muestra la salida para todos los tipos de datos, independientemente de si el espacio de archivos contiene los tipos de datos. Por ejemplo, si un espacio de archivos sólo contiene datos de copia de seguridad y archivado, la salida del mandato VALIDATE REPLICATION también contiene información relevante para los datos gestionados por espacio.

## Descripciones de los campos

---

### Nombre de nodo

El nodo propietario de los datos replicados.

### Nombre de espacio de archivos

El nombre del espacio de archivos que pertenece al nodo.

Los nombres de espacio de archivos pueden estar en una página de códigos o un entorno local distintos de los del servidor. Si este es el caso, los nombres en el Centro de operaciones y la interfaz de línea de s de administración puede que no visualicen correctamente. Se efectúa una copia de seguridad de los datos, que se pueden restaurar de la forma normal, pero el nombre del espacio de archivos o el nombre del archivo pueden visualizarse con una combinación de caracteres no válidos o espacios en blanco.

Si el nombre del espacio de archivos está habilitado para Unicode, el nombre se convierte en la página de códigos del servidor para su visualización. El éxito de la conversión depende del sistema operativo, de los caracteres del nombre y de la página de códigos del servidor. La conversión puede estar incompleta si la serie incluye caracteres que no están disponibles en la página de códigos del servidor o si el servidor no puede acceder a las rutinas de conversión del sistema. Si la conversión está incompleta, es posible que el nombre contenga signos de interrogación, espacios en blanco, caracteres no imprimibles o puntos suspensivos (...).

### FSID

El identificador de espacio de archivos del espacio de archivos. El servidor asigna un FSID único cuando un espacio de archivo se almacena por primera vez en el servidor.

### Tipo

El tipo de datos. Son posibles los siguientes valores:

#### Arch

Datos de archivado

#### C.S.

Datos de copia de seguridad

#### G.E.

Datos que se han migrado mediante un cliente de IBM Spectrum Protect for Space Management.

### Control de norma de réplica

El nombre de la regla de réplica que controla la réplica de un tipo de datos en un espacio de archivos. Para determinar si la regla de control es una regla de espacio de archivos o una regla de servidor, consulte el campo Nivel de regla de réplica.

### Nivel de norma de réplica

El nivel de la regla de control en la jerarquía de reglas de réplica. Son posibles los siguientes valores:

#### Espacio de archivos

La regla de control se asigna a un tipo de datos en el espacio de archivos.

#### Nodo

La regla de control se asigna a un tipo de datos para un nodo de cliente.

#### Servidor

La regla de control se asigna a un tipo de datos para todos los espacios de archivos de todos los nodos de cliente que están configurados para la réplica.

### Nombre del servidor

El nombre del servidor de réplica de destino que se va a consultar.

### Estado de conexión

El estado de conexión entre los servidores de réplica de origen y destino. Son posibles los siguientes valores:

#### Conexión válida

La comunicación con el servidor de réplica de destino ha sido satisfactoria y el servidor de réplica de destino es un servidor V6.3.

#### Servidor destino no establecido

El servidor de réplica de destino no se ha establecido. Para establecer el servidor de réplica de destino, emita el comando SET REPLSERVER.

#### Anomalía en la comunicación

El servidor de réplica de origen no ha podido ponerse en contacto con el servidor de réplica de destino. Examine el registro de anotaciones de actividad para ver los mensajes de error sobre las comunicaciones anómalas. Las causas posibles son las siguientes:

- La configuración de réplica en el servidor de réplica de origen no es válida. Pueden darse uno o varios de los problemas siguientes:
  - La definición de servidor del servidor de réplica de destino no es correcta.

- Si la definición del servidor de réplica de destino se ha suprimido y redefinido, emita el comando PING SERVER para probar la conexión entre el servidor de réplica de origen y destino. Si el comando PING SERVER es satisfactorio, emita el comando UPDATE SERVER y especifique FORCESYNC=YES para restablecer las claves de verificación del servidor.
  - El nombre del servidor, la dirección de bajo nivel del servidor, la dirección de alto nivel del servidor y la contraseña del servidor no coinciden con los valores que se han especificado en la definición de servidor en el servidor de réplica de destino.
- La configuración de réplica en el servidor de réplica de destino no es válida. Pueden darse uno o varios de los problemas siguientes:
  - La versión del servidor de réplica de destino es anterior a V6.3.
  - La definición de servidor del servidor de réplica de origen no es correcta.
  - El nombre del servidor, la dirección de bajo nivel del servidor, la dirección de alto nivel del servidor y la contraseña del servidor no coinciden con los valores que se han especificado en la definición de servidor en el servidor de réplica de origen.
- Las comunicaciones de red no están disponibles. Para probar la conexión entre el servidor de origen y destino, emita el mandato PING SERVER.
- El servidor de réplica de destino no está disponible.
- Las sesiones entre los servidores de réplica de origen y destino están desactivadas. Para verificar el estado de las sesiones, emita el comando QUERY STATUS.

#### Réplica suspendida

El proceso de réplica se suspende cuando restaura la base de datos en el servidor de réplica de origen o inhabilita el proceso de réplica en este servidor emitiendo el mandato DISABLE REPLICATION.

## Comandos relacionados

Tabla 1. Comandos relacionados con VALIDATE REPLICATION

Comando	Descripción
DISABLE REPLICATION	Impide el proceso de réplica de salida en un servidor.
ENABLE REPLICATION	Permite el proceso de réplica de salida en un servidor.
ENABLE SESSIONS	Reanuda la actividad del servidor después del comando DISABLE o del comando ACCEPT DATE.
QUERY FILESPACE	Visualiza información acerca de los datos de los espacios de archivos que pertenecen a un cliente.
QUERY NODE	Visualiza información parcial o completa sobre uno o más clientes.
QUERY REPLRULE	Muestra información sobre las reglas de réplica de nodos.
QUERY SERVER	Muestra información sobre servidores.
QUERY STATUS	Visualiza los valores de los parámetros del servidor, como por ejemplo los seleccionados mediante los comandos SET.
REPLICATE NODE	Replica los datos de los espacios de archivos que pertenecen a un nodo de cliente.
SET ARREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de archivado.
SET BKREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos de copia de seguridad.
SET REPLSERVER	Especifica un servidor de réplica de destino.
SET SPREPLRULEDEFAULT	Especifica la regla de réplica de nodos de servidor para los datos gestionados por espacio.
UPDATE FILESPACE	Cambia las reglas de réplica de nodos del espacio de archivos.
UPDATE NODE	Cambia los atributos que están asociados con un nodo de cliente.
UPDATE REPLRULE	Activa o desactiva las reglas de réplica.
UPDATE SERVER	Actualiza la información sobre un servidor.

# VALIDATE REPLPOLICY (Verificar las políticas en el servidor de réplica de destino)

Utilice este mandato para comparar las políticas para nodos cliente en el servidor de réplica de origen con las mismas políticas en el servidor de réplica de destino donde se replican los datos del nodo cliente.

El mandato muestra las diferencias entre estas políticas para que pueda verificar que las diferencias entre las políticas en los servidores de réplica de origen y destino están pensadas o pueden modificar las políticas en el servidor de réplica de destino.

Asegúrese de que esté instalado IBM Spectrum Protect versión 7.1.1 o posterior en los servidores de réplica de origen y destino antes de emitir este mandato. Emita este mandato en el servidor de réplica de origen.

## Clase de privilegio

Cualquier administrador puede emitir este comando.

## Sintaxis

```
>>-VALidate REPLPolicy--+-+-----+-----<<  
                    '-nombre_servidor-'
```

## Parámetros

nombre\_servidor

Especifica el nombre del servidor de réplica de destino que tiene políticas que desea verificar. Este parámetro es opcional. Si no especifica este parámetro, el mandato establece el servidor de réplica predeterminado como servidor de réplica de destino.

## Ejemplo: Visualizar las diferencias entre las políticas de réplica en un servidor de réplica de origen y destino

Para visualizar las diferencias entre las políticas en el servidor de réplica de origen y las políticas en el servidor de réplica de destino, CVTCVS\_LXS\_SRV2, donde se replican los datos del cliente, emita el mandato siguiente en el servidor de réplica de origen:

```
VALIDATE REPLPOLICY CVTCVS_LXS_SRV2
```

Policy domain name on this server	Policy domain name on target server	Target server name
STANDARD	STANDARD	CVTCVS_LXS_SRV2
Diferencias en conjunto de políticas:		
Change detected	Source server value	Target server value
Mgmt class only on target	Not applicable	STANDARD2
Mgmt Class only on source	STANDARD1	Not applicable
Differences in backup copy group	STANDARD in management class	STANDARD
Change detected	Source server value	Target server value
Versions data exists	2	20

```
Affected nodes
```

```
-----  
NODE1,NODE2,NODE3,NODE4,NODE5
```

## Descripciones de los campos

Nombre de dominio de políticas en este servidor

Especifica el nombre de dominio de políticas en el servidor de réplica de origen donde se emite el mandato.

Nombre de dominio de políticas en el servidor de destino

Especifica el nombre de dominio de políticas en el servidor de réplica de destino.

Nombre del servidor de destino

Especifica el nombre del servidor de réplica de destino.

Diferencias en conjunto de políticas:

Especifica las diferencias entre las políticas que están definidas en los servidores de réplica de origen y destino. Las diferencias entre las políticas se listan en los campos siguientes:

Cambio detectado

Especifica la lista de elementos de políticas que son diferentes entre los servidores de réplica de origen y destino.

Valor de servidor de origen

Especifica el valor para el elemento de la política en el servidor de réplica de origen.

Valor de servidor de destino

Especifica el valor para el elemento de política en el servidor de réplica de destino.

Las diferencias entre el grupo de copia de seguridad <nombre\_grupo\_copia\_seguridad> en la clase de gestión predeterminada O las diferencias en el grupo de copia archivada <nombre\_grupo\_copia\_archivada> en la clase de gestión predeterminada

Especifica las diferencias entre el grupo de copias de seguridad o el grupo de copias archivadas en la clase de gestión. Las diferencias se listan en los campos siguientes:

Cambio detectado

Especifica la lista de campos de grupos de copias que son diferentes.

Valor de servidor de origen

Especifica el valor en el campo de grupo de copia en el servidor de réplica de origen.

Valor de servidor de destino

Especifica el valor en el campo de grupo de copia en el servidor de réplica de destino.

Nodos afectados

Especifica los nombres de todos los nodos cliente que se ven afectados por los cambios que se muestran en esta salida.

## Comandos relacionados

Tabla 1. Mandatos relacionados con VALIDATE REPLPOLICY

Comando	Descripción
VALIDATE REPLICATION	Verifica la réplica para los espacios de archivos y los tipos de datos.
QUERY REPLSERVER	Muestra información sobre servidores de réplica.
SET DISSIMILARPOLICIES	Habilitar las políticas en el servidor de réplica de destino para gestionar los datos replicados.
QUERY DOMAIN	Muestra información sobre los dominios de políticas.
QUERY POLICYSET	Muestra información sobre conjuntos de políticas.
QUERY COPYGROUP	Muestra los atributos de un grupo de copia.
QUERY MGMTCLASS	Muestra información sobre las clases de gestión.

## VARY (Activar o desactivar un volumen de acceso aleatorio)

Utilice este comando para activar o desactivar un volumen de agrupación de almacenamiento de acceso aleatorio en el servidor.

### Clase de privilegio

Este comando sólo es válido para los volúmenes de dispositivos de acceso aleatorio. Este comando se utiliza, por ejemplo, durante el mantenimiento o durante una acción correctiva de un volumen de acceso aleatorio. No puede activarse un volumen de acceso aleatorio que se haya definido como UNAVAILABLE.

Para emitir este comando, debe tener privilegio de sistema o privilegio de operador.

### Sintaxis

```
>>-VARY---ONline---nombre_volumen-----<
      '-Offline-'          '-Wait-----No---'
                          '-Yes-'
```

## Parámetros

### ONline

Especifica que el servidor puede utilizar el volumen de acceso aleatorio.

### OFFline

Especifica que el servidor no puede utilizar el volumen.

### nombre\_volumen (Necesario)

Especifica el identificador del volumen. Los nombres de volumen no pueden contener espacios en blanco intercalados ni signos de igual.

### Wait




Especifica si es necesario esperar a que termine el servidor para completar el proceso en primer plano de este comando. Este parámetro es opcional. El valor predeterminado es NO. Los valores posibles son:

#### No





Especifica que el servidor procesa este comando como proceso subordinado mientras tiene lugar la ejecución de otras tareas. El servidor visualiza los mensajes que se han creado a partir del proceso subordinado en las anotaciones de actividades o en la consola del servidor, en función del lugar en el que se han anotado los mensajes.

#### Yes



Especifica que el servidor procesa este mandato en primer plano. Espere a que el comando finalice antes de continuar con otras tareas. El servidor muestra los mensajes de salida al cliente de administración cuando finaliza el comando.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows No se puede especificar WAIT=YES desde la consola del servidor.

## Ejemplo: activar el volumen

 Sistemas operativos AIX  Sistemas operativos Linux Establecer que el volumen /adsm/stgvol/1 esté disponible para que el servidor pueda utilizarlo como volumen de agrupación de almacenamiento.  Sistemas operativos AIX  Sistemas operativos Linux

```
vary online /adsm/stgvol/1
```

 Sistemas operativos Windows Establecer que el volumen j:\storage\pool001 esté disponible para que el servidor pueda utilizarlo como volumen de agrupación de almacenamiento.  Sistemas operativos Windows

```
vary online j:\storage\pool001
```

## Comandos relacionados

Tabla 1. Comandos relacionados con VARY

Comando	Descripción
CANCEL PROCESS	Cancela un proceso de servidor subordinado.
DEFINE VOLUME	Asigna un volumen que se ha de utilizar para el almacenamiento en una agrupación de almacenamiento especificada.
DELETE VOLUME	Suprime un volumen de una agrupación de almacenamiento.
QUERY PROCESS	Muestra información sobre procesos subordinados.
QUERY VOLUME	Muestra información sobre volúmenes de agrupación de almacenamiento.

## Opciones de servidor

Durante la instalación, IBM Spectrum Protect proporciona un archivo de opciones de servidor que contiene un conjunto de opciones predeterminadas para iniciar el servidor.

El archivo es:

- dmserv.opt en el directorio de instancia de servidor

Las opciones de servidor permiten personalizar lo siguiente:


- Comunicaciones
- Almacenamiento de servidor


- Cliente-servidor
- Fecha, número, hora e idioma
- Anotaciones de recuperación y base de datos
- Transferencia de datos
- Mensaje
- Anotaciones de eventos
- Seguridad y sistema de licencias

Varias opciones que pueden utilizarse para diversas finalidades. Estas opciones no documentadas están pensadas para que las utilice solo el soporte de IBM®.







Para visualizar los valores actuales de las opciones, escriba:





```
query option
```

- **Modificación de opciones del servidor**  
El servidor lee el archivo de opciones del servidor durante la inicialización del servidor. Cuando actualiza una opción del servidor editando el archivo, debe detener y arrancar el servidor para activar el archivo de opciones del servidor actualizado.
- **Tipos de opciones del servidor**  
Las opciones del servidor le permiten personalizar el modo en que funcionan algunas funciones y procesos.
- **3494SHARED**  
La opción 3494SHARED especifica si una biblioteca IBM 3494 puede compartir aplicaciones distintas de IBM Spectrum Protect.
- **ACSACCESSID**  
La opción ACSACCESSID especifica el identificador del control de acceso de ACS para una biblioteca ACSLS.
- **ACSLOCKDRIVE**  
La opción ACSLOCKDRIVE especifica si las unidades de las bibliotecas ACSLS están bloqueadas. Al bloquear las unidades, se garantiza el uso exclusivo de la unidad de la biblioteca ACSLS en un entorno compartido. Sin embargo, el rendimiento es mejor si las bibliotecas no se bloquean. Cuando otras aplicaciones no comparten las unidades de IBM Spectrum Protect, no es necesario bloquear las unidades.
- **ACSQUICKINIT**  
La opción ACSQUICKINIT especifica si, en el arranque del servidor, la inicialización de la biblioteca ACSLS es rápida o completa. El valor predeterminado es Yes. Una inicialización rápida evita la sobrecarga asociada con la sincronización del inventario del servidor de IBM Spectrum Protect con el inventario de biblioteca ACSLS (mediante una auditoría de la biblioteca).
- **ACSTIMEOUTX**  
La opción ACSTIMEOUTX especifica el múltiplo del valor de tiempo de espera incorporado de las API ACSLS. El valor de tiempo de espera incorporado de la API de introducción, expulsión y auditoría ACS son 1800 segundos; el valor de todas las demás API ACSLS son 600 segundos. Por ejemplo, si el múltiplo especificado es 5, el valor de tiempo de espera de la API de auditoría serán 9000 segundos y el valor de todas las demás API serán 3000 segundos.
- **ACTIVELOGDIRECTORY**  
La opción ACTIVELOGDIRECTORY especifica el nombre del directorio donde están almacenados todos los registros activos.
- **ACTIVELOGSIZE**  
La opción ACTIVELOGSIZE establece el tamaño total del registro.
- **ADMINCOMMTIMEOUT**  
La opción ADMINCOMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos.
- **ADMINIDLETIMEOUT**  
La opción ADMINIDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente administrativo puede estar desocupada antes de que la cancele el servidor.
- **ADMINONCLIENTPORT**  
La opción ADMINONCLIENTPORT especifica si las sesiones administrativas pueden utilizar TCPPOINT. El valor predeterminado es YES.
-  **Sistemas operativos WindowsADSMGROUPNAME**  
La opción ADSMGROUPNAME especifica el nombre de un grupo Windows. Un nodo cliente debe ser miembro de este grupo para poder utilizar el servidor de IBM Spectrum Protect a través de NT Unified Logon. El nodo de cliente también debe ser un nodo de cliente de IBM Spectrum Protect registrado.
- **ALIASHALT**  
La opción ALIASHALT permite a los administradores asignar un nombre diferente a un comando **HALT** de IBM Spectrum Protect.
- **ALLOWDESAUTH**  
La opción ALLOWDESAUTH especifica si se debe permitir la utilización del algoritmo DES (Data Encryption Standard) para la autenticación entre un servidor y un cliente de archivado y copia de seguridad.
- **ALLOWREORGINDEX**  
La opción ALLOWREORGINDEX especifica si la reorganización de índice iniciada por el servidor está activada o desactivada.
- **ALLOWREORGTABLE**  
La opción ALLOWREORGTABLE especifica si la reorganización de tabla iniciada por el servidor está activada o desactivada.
- **ARCHFAILOVERLOGDIRECTORY**  
La opción ARCHFAILOVERLOGDIRECTORY especifica el directorio que utiliza el servidor para almacenar los archivos de registro














- de archivado que no se pueden almacenar en el directorio de registros de archivado.
- **ARCHLOGCOMPRESS**  
Puede habilitar o inhabilitar la compresión de registros de archivado en el servidor de IBM Spectrum Protect. Al comprimir los registros de archivado, se reduce la cantidad de espacio necesaria para el almacenamiento.
  - **ARCHLOGDIRECTORY**  
La opción ARCHLOGDIRECTORY especifica un directorio en el que el gestor de base de datos puede archivar un archivo de registro una vez completadas todas las transacciones representadas en dicho archivo de registro.
  - **ARCHLOGUSEDTHRESHOLD**  
La opción ARCHLOGUSEDTHRESHOLD especifica cuándo iniciar una copia de seguridad de base de datos automática en relación con el porcentaje de espacio de archivo de anotaciones de archivado utilizado. El valor predeterminado es el 80 por ciento.
  - **ASSISTVCRRECOVERY**  
La opción ASSISTVCRRECOVERY especifica si IBM Spectrum Protect debe ayudar a una unidad IBM 3590 a recuperarse de una condición de VCR (Vital Cartridge Records) perdidos o dañados. Si especifica YES (el valor predeterminado) y si IBM Spectrum Protect detecta un error durante el proceso de montaje, se sitúa al final de los datos durante el proceso de desmontaje para permitir que las unidades restauren el VCR. Durante la operación de cinta, es posible que se produzca un pequeño efecto sobre el rendimiento ya que la unidad no puede realizar una búsqueda rápida con un VCR perdido o dañado. Sin embargo, no se produce ninguna pérdida de datos.
  - **AUDITSTORAGE**  
Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento del servidor utilizado para operaciones de copia de seguridad y archivado, y para archivos bajo gestión de espacio. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de CPU y puede detener otras actividades del servidor. Puede utilizar la opción AUDITSTORAGE para especificar que el almacenamiento no se ha de calcular como parte de una auditoría de licencias.
  - **BACKUPINITIATIONROOT**  
La opción BACKUPINITIATIONROOT especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.
  - **CHECKTAPEPOS**  
La opción CHECKTAPEPOS especifica si el servidor de IBM Spectrum Protect valida la posición de los bloques de datos en la cinta.
  - **CLIENTDEDUPTXNLIMIT**  
La opción CLIENTDEDUPTXNLIMIT especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.
  - **COMMMETHOD**  
La opción COMMMETHOD especifica el método de comunicaciones que utilizará el servidor.
  - **COMMTIMEOUT**  
La opción COMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente durante una operación que produce una actualización de la base de datos. Si el tiempo supera este tiempo de espera, el servidor finaliza la sesión con el cliente. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera. Los clientes pueden exceder el tiempo de espera si existe una gran carga de red en el entorno o realizan copias de seguridad de archivos grandes.
  - **CONTAINERRESOURCESTIMEOUT**  
La opción CONTAINERRESOURCESTIMEOUT especifica durante cuánto tiempo espera el servidor a completar una operación de almacén de datos en una agrupación de almacenamiento de contenedor.
  -  **Sistemas operativos Windows DATEFORMAT**  
La opción DATEFORMAT especifica el formato que el servidor ha de utilizar para visualizar las fechas.
  - **DBDIAGLOGSIZE**  
Esta opción permite controlar el espacio que utilizan los archivos de registro de diagnóstico.
  - **DBDIAGPATHFSTHRESHOLD**  
La opción DBDIAGPATHFSTHRESHOLD especifica un umbral para el espacio libre en el sistema de archivos o disco que contiene el archivo db2diag.log.
  - **DBMEMPERCENT**  
Utilice esta opción para especificar el porcentaje de memoria del espacio de direcciones virtuales dedicado a procesos del gestor de bases de datos.
  - **DBMTCPPORT**  
La opción DBMTCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del gestor de base de datos espera las peticiones de sesiones de cliente.
  - **DEDUPREQUIRESBACKUP**  
La opción DEDUPREQUIRESBACKUP especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la deduplicación de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.
  - **DEDUPTIER2FILESIZE**  
La opción DEDUPTIER2FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 2.
  - **DEDUPTIER3FILESIZE**  
La opción DEDUPTIER3FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación






- de datos duplicados de nivel 3.
- DEVCONFIG  
La opción DEVCONFIG especifica el nombre de un archivo en el que el usuario quiere que IBM Spectrum Protect almacene una copia de seguridad de la información de configuración del dispositivo.
- DISABLEREORGTABLE  
La opción DISABLEREORGTABLE especifica si está inhabilitada la reorganización de tabla para los nombres de tabla especificado en la lista de tablas.
- DISABLESCHEDULES  
La opción DISABLESCHEDULES especifica si se desactivan las planificaciones de cliente y de administración durante una recuperación del servidor de IBM Spectrum Protect.
- DISPLAYLFINFO  
La opción DISPLAYLFINFO especifica el modo en que los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del nodo.
- DNSLOOKUP  
La opción DNSLOOKUP especifica si el servidor utiliza llamadas de API del sistema para determinar los nombres de servidor de nombres de dominio (DNS) de los sistemas que establecen contacto con el servidor.
- DRIVEACQUIRERETRY  
La opción DRIVEACQUIRERETRY le permite especificar el número de veces que el servidor reintentará la adquisición de una unidad en una biblioteca IBM 349x. Si se comparte la biblioteca entre varias aplicaciones, puede parecer que sus unidades están disponibles en el servidor (mediante un proceso subordinado de sondeo), cuando en realidad no lo están.
- ENABLENASDEDUP  
La opción de servidor ENABLENASDEDUP especifica si el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos de almacenamiento conectado a red (NAS). Esta opción solo se aplica a los servidores de archivos NetApp.
- EVENTSERVER  
La opción EVENTSERVER especifica si, en el momento del arranque, el servidor debe intentar establecer contacto con el servidor de eventos.
- EXPINTERVAL  
La opción EXPINTERVAL especifica el intervalo, en horas, que ha de transcurrir entre los procesos automáticos de caducidad de inventario que realiza IBM Spectrum Protect. El proceso de caducidad de inventario elimina las copias de seguridad y las copias archivadas del servidor, según se haya especificado mediante las clases de gestión a las que están vinculados los archivos del cliente. Si no se ejecuta periódicamente el proceso de caducidad, no se reclamará el espacio de agrupación de almacenamiento de los archivos del cliente caducados, y el servidor necesitará más espacio de almacenamiento del que necesita según la política.
- EXPQUIET  
La opción EXPQUIET especifica si IBM Spectrum Protect ha de enviar mensajes detallados durante el proceso de caducidad.
-  Sistemas operativos Linux  Sistemas operativos Windows FASPBEGPORT  
La opción FASPBEGPORT especifica el número inicial en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).
-  Sistemas operativos Linux  Sistemas operativos Windows FASPENDPORT  
La opción FASPENDPORT especifica el número final en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).
-  Sistemas operativos Linux  Sistemas operativos Windows FASPTARGETRATE  
La opción FASPTARGETRATE especifica la tasa de destino para la transferencia de datos con la tecnología Aspera Fast Adaptive Secure Protocol (FASP). Si especifica la tasa de destino, limita el ancho de banda de cada conexión de red que utiliza la tecnología Aspera FASP. De este modo, puede asegurarse de que hay suficiente ancho de banda disponible para todas las conexiones de red.
- FFDCLOGLEVEL  
La opción FFDCLOGLEVEL especifica el tipo de mensajes del servidor generales que se muestran en el registro FFDC (First Failure Data Capture).
- FFDCLOGNAME  
La opción FFDCLOGNAME especifica un nombre del registro FFDC (First Failure Data Capture).
- FFDCMAXLOGSIZE  
La opción FFDCMAXLOGSIZE especifica el tamaño del archivo de registro FFDC (First Failure Data Capture).
- FFDCNUMLOGS  
La opción FFDCNUMLOGS especifica el número de archivos de registro que se pueden utilizar para el registro circular. El valor predeterminado es 10.
- FILEEXIT  
La opción FILEEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es un registro del archivo.
- FILETEXTEXIT  
La opción FILETEXTEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.
- FSUSEDTHRESHOLD  
La opción FSUSEDTHRESHOLD especifica qué porcentaje del sistema de archivos puede llenar la base de datos antes emitir un

- mensaje de alerta.
- IDLETIMEOUT  
La opción IDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente puede estar desocupada antes de que la cancele el servidor. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera si existe una gran carga en la red del entorno. Observe, sin embargo, que una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.
  - KEEPALIVE  
La opción KEEPALIVE especifica si la función keepalive del protocolo de control de transmisiones (TCP) está habilitada para los sockets TCP de salida. La función keepalive TCP envía una transmisión de un dispositivo a otro para comprobar que el enlace entre los dos dispositivos está operativo.
  - KEEPALIVETIME  
La opción KEEPALIVETIME especifica la frecuencia con la que TCP envía una transmisión de estado activo cuando recibe una respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.
  - KEEPALIVEINTERVAL  
La opción KEEPALIVEINTERVAL especifica la frecuencia con la que se envía una transmisión de estado activo, si no se recibe ninguna respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.
  - LANGUAGE  
La opción LANGUAGE controla la inicialización de los entornos nacionales. Un entorno nacional incluye el idioma y los formatos de fecha, hora y número que se han de utilizar para la consola y el servidor.
  - LDAPCACHEDURATION  
La opción LDAPCACHEDURATION determina la cantidad de tiempo que el servidor IBM Spectrum Protect almacena en memoria caché la información de autenticación de contraseña LDAP.
  - LDAPURL  
La opción LDAPURL especifica la ubicación de un servidor LDAP (Lightweight Directory Access Protocol). Establezca la opción de LDAPURL después de configurar el servidor LDAP.
  - MAXSESSIONS  
La opción MAXSESSIONS especifica el número máximo de sesiones cliente simultáneas que se pueden conectar con el servidor.
  - MESSAGEFORMAT  
La opción MESSAGEFORMAT especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.
  - MIRRORLOGDIRECTORY  
La opción MIRRORLOGDIRECTORY especifica el directorio para duplicar la vía de acceso de registro activo.
  - MOVEBATCHSIZE  
La opción MOVEBATCHSIZE especifica el número de archivos cliente que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Este movimiento de datos es el resultado de las operaciones de restauración y copia de seguridad de agrupaciones de almacenamiento, de migración, reclamación y MOVE DATA. Esta opción funciona con la opción MOVESIZETHRESH.
  - MOVESIZETHRESH  
La opción MOVESIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Cuando se alcance este umbral, no se agregarán más archivos al lote actual, y se arrancará una nueva transacción después de que se haya trasladado el lote actual.
  - MSGINTERVAL  
La opción MSGINTERVAL especifica el tiempo, en minutos, entre los mensajes que solicitan a un operador que monte una cinta para el servidor.
  -  Sistemas operativos Windows NAMEDPIPENAME  
La opción NAMEDPIPENAME especifica un método de comunicaciones que permite que los procesos se comuniquen entre sí sin tener que saber dónde los procesos del emisor y remitente están ubicados. El nombre actúa como un alias, y conecta los dos procesos independientemente de si están en el mismo sistema o en otros dominios conectados.
  - NDMPCONNECTIONTIMEOUT  
La opción de servidor NDMPCONNECTIONTIMEOUT especifica el tiempo, en horas, que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante las operaciones de restauración NDMP a través de la LAN. Las operaciones de restauración NDMP de sistemas de archivos NAS de gran tamaño puede tener periodos prolongados de inactividad. El valor predeterminado es 6.
  - NDMPCONTROLPORT  
La opción NDMPCONTROLPORT especifica el número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP (Network Data Management Protocol). El servidor de IBM Spectrum Protect no funciona como un servidor de cintas NDMP de uso general.
  - NDMPENABLEKEEPALIVE  
La opción del servidor NDMPENABLEKEEPALIVE especifica si el servidor de IBM Spectrum Protect habilita el mantenido en actividad de TCP (Transmission Control Protocol) en las conexiones control NDMP (network data-management protocol) en dispositivos NAS (network-attached storage). El valor predeterminado es NO.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NDMPKEEPIDLEMINUTES  
La opción de servidor NDMPKEEPIDLEMINUTES especifica la cantidad de tiempo, en minutos, antes de que el sistema operativo transmita el primer paquete de estado activo TCP (Transmission Control Protocol) en una conexión de control NDMP (Network Data-Management Protocol). El valor predeterminado son 120 minutos.

- **NDMPPORTRANGE**  
La opción NDMPPORTRANGE especifica el rango de números de puerto por los que IBM Spectrum Protect pasa en secuencia para obtener un número de puerto para aceptar una sesión de un dispositivo NAS (almacenamiento conectado a red) para la transferencia de datos. El valor predeterminado es 0,0, que significa que IBM Spectrum Protect deja que el sistema operativo proporcione un puerto (puerto efímero).
- **NDMPPREFDATAINTERFACE**  
Esta opción especifica la dirección IP que se asocia a la interfaz en la que desea que el servidor reciba todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
- **NOPREEMPT**  
El servidor permite que determinadas operaciones tengan prioridad sobre otras operaciones para acceder a volúmenes y dispositivos. Puede especificar la opción NOPREEMPT para desactivar la prioridad. Cuando se desactiva la prioridad, ninguna operación puede tener prioridad sobre otra para acceder a un volumen, y únicamente una operación de copia de seguridad de base de datos puede tener prioridad sobre otra operación para acceder a un dispositivo.
- **NORETRIEVEDATE**  
La opción NORETRIEVEDATE especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo. Esta opción y el parámetro MIGDELAY de agrupación de almacenamiento controlan cuándo el servidor migra los archivos.
-  **Sistemas operativos WindowsNPAUDITFAILURE**  
La opción NPAUDITFAILURE especifica si ha de enviarse un evento a las anotaciones de eventos cuando un nodo se conecte con el servidor utilizando un nombre que se encuentra en el grupo de Windows pero que no coincide con el nombre de inicio de sesión de cuenta de Windows. Para garantizar que un nodo pueda acceder sólo a sus propios datos, el nombre del nodo y el nombre de cuenta Windows deben coincidir.
-  **Sistemas operativos WindowsNPAUDITSUCCESS**  
La opción NPAUDITSUCCESS especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.
-  **Sistemas operativos WindowsNPBUFFERSIZE**  
La opción NPBUFFERSIZE especifica el tamaño del búfer de comunicaciones de Named Pipes.
-  **Sistemas operativos WindowsNUMBERFORMAT**  
La opción NUMBERFORMAT especifica el formato de numeración que el servidor utiliza para visualizar los números.
- **NUMOPENVOLSALLOWED**  
La opción NUMOPENVOLSALLOWED especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.
- **PUSHSTATUS**  
La opción PUSHSTATUS se utiliza en servidores de radio para asegurarse de que la información de estado se envía al servidor concentrador. No actualice esta opción a menos que deba restaurar la configuración del Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o de radio.
- **QUERYAUTH**  
La opción QUERYAUTH especifica el nivel de autorización de administración necesario para emitir los comandos QUERY o SQL SELECT. De forma predeterminada, cualquier administrador puede emitir los comandos QUERY y SELECT. Puede utilizar esta opción para restringir el uso de estos comandos.
- **RECLAIMDELAY**  
Esta opción retrasa la reclamación de un volumen SnapLock y permite que los datos restantes caduquen para que no haya necesidad de reclamar el volumen.
- **RECLAIMPERIOD**  
Esta opción permite definir el número de días para el periodo de reclamación de un volumen SnapLock.
- **REORGBEGINTIME**  
La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o índice.
- **REORGDURATION**  
La opción REORGDURATION especifica un intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.
- **REPORTRETRIEVE**  
La opción REPORTRETRIEVE genera informes sobre las operaciones de restauración o recuperación que realizan los nodos clientes o los administradores. El valor predeterminado es NO.
- **REPLBATCHSIZE**  
La opción REPLBATCHSIZE especifica el número de archivos de cliente que se van a replicar en proceso por lotes, dentro de la misma transacción de servidor. Esta opción afecta únicamente a los procesos de réplica de nodo y funciona con la opción REPLSIZETHRESH para mejorar el proceso de réplica de nodo.
- **REPLSIZETHRESH**  
La opción REPLSIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos replicados, dentro de la misma transacción del servidor.
- **REQSYSAUTHOUTFILE**  
La opción REQSYSAUTHOUTFILE especifica si es necesaria la autorización del sistema para los comandos de administración que hacen que IBM Spectrum Protect realice una grabación en un archivo externo.

- **RESOURCETIMEOUT**  
La opción RESOURCETIMEOUT especifica el intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso. Cuando se exceda el tiempo de espera, la petición del recurso se cancelará.
- **RESTOREINTERVAL**  
La opción RESTOREINTERVAL especifica durante cuánto tiempo se puede guardar una sesión de restauración rearrancable en la base de datos del servidor. Siempre y cuando la sesión de restauración se haya guardado en la base de datos, se puede volver a arrancar desde el punto en el que se ha detenido.
- **RETENTIONEXTENSION**  
La opción RETENTIONEXTENSION especifica el número de días que ha de ampliarse la fecha de retención de un volumen de SnapLock. Esta opción permite que el servidor amplíe la fecha de retención de un volumen de SnapLock para evitar las reclamaciones excesivas.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANDISCOVERY**  
La opción SANDISCOVERY especifica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANDISCOVERYTIMEOUT**  
La opción SANDISCOVERYTIMEOUT especifica la cantidad de tiempo permitido para que respondan los adaptadores de bus de host si se consultan mediante el proceso de descubrimiento de SAN. Cuando se alcance el tiempo especificado en SANDISCOVERYTIMEOUT, el proceso excede el tiempo de espera.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **SANREFRESHTIME**  
La opción SANREFRESHTIME especifica la cantidad de tiempo que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. La opción SANREFRESHTIME tiene un valor predeterminado de 0, que significa que no hay caché de descubrimiento de SAN. La información se obtiene directamente del adaptador de bus de host (HBA) cada vez que el servidor ejecuta una operación de descubrimiento de SAN.
- **SEARCHMPQUEUE**  
La opción SEARCHMPQUEUE especifica el orden en el que el servidor da respuesta a las peticiones de la cola de montaje. Si se especifica la opción, el servidor primero intenta satisfacer las peticiones de los volúmenes que ya están montados. Estas peticiones pueden ser satisfechas antes que otras peticiones, aunque estas otras hayan estado esperando más tiempo el punto de montaje. Si no se especifica esta opción, el servidor satisface las peticiones en el orden en que éstas se reciben.
-  Sistemas operativos Windows **SECUREPIPES**  
Cuando se utiliza el protocolo Named Pipes, si se activa SECUREPIPES, el servidor se ve forzado a comprobar el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.
- **SERVERDEDUPTXNLIMIT**  
La opción SERVERDEDUPTXNLIMIT especifica el tamaño máximo de los objetos que pueden tener optimización de almacenamiento en el servidor.
- **SHMPORT**  
 Sistemas operativos AIX  Sistemas operativos Linux La opción SHMPORT especifica la dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Todas las comunicaciones de memoria compartida comienzan por una conexión TCP/IP.  Sistemas operativos Windows La opción SHMPORT especifica el puerto en el que el servidor está a la escucha de conexiones de memoria compartida.
- **SHREDDING**  
La opción SHREDDING especifica si la destrucción de datos confidenciales suprimidos se lleva a cabo automática o manualmente. La destrucción sólo se aplica a los datos de las agrupaciones de almacenamiento que se han configurado explícitamente para dar soporte a la destrucción.
- **SNMPHEARTBEATINTERVAL**  
La opción SNMPHEARTBEATINTERVAL especifica el intervalo en minutos entre consultas del servidor de IBM Spectrum Protect.
- **SNMPMESSAGECATEGORY**  
La opción SNMPMESSAGECATEGORY especifica los tipos de detecciones que se utilizan cuando se envían los mensajes desde el servidor, a través del subagente SNMP (Simple Network Management Protocol), al gestor SNMP.
- **SNMPSUBAGENT**  
La opción SNMPSUBAGENT especifica los parámetros necesarios para que el subagente de IBM Spectrum Protect se comunique con el daemon SNMP (Simple Network Management Protocol). Esta opción únicamente sirve para configurar el subagente SNMP para las comunicaciones con el agente SNMP; el servidor la ignora.
- **SNMPSUBAGENTHOST**  
La opción SNMPSUBAGENTHOST especifica la ubicación del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect. El valor predeterminado para esta opción es 127.0.0.1.
- **SNMPSUBAGENTPORT**  
La opción SNMPSUBAGENTPORT especifica el número de puerto del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect.
- **SSLFIPSMODE**  
La opción SSLFIPSMODE especifica si se aplica la modalidad Estándar federal de procesamiento de información (FIPS) para la capa de sockets seguros (SSL). El valor predeterminado es NO.
- **SSLINITTIMEOUT**  
La opción SSLINITTIMEOUT especifica el tiempo, en minutos, que el servidor espera a que finalice la inicialización de una sesión SSL (capa de sockets seguros) antes de que cancelar la sesión.

- **SSLTCPADMINPORT**  
La opción SSLTCPADMINPORT especifica la dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera peticiones solo de sesiones con SSL habilitado. Las sesiones son para el cliente de administración de línea de comandos.
- **SSLTCPPOINT**  
La opción SSLTCPPOINT especifica el número de puerto de capa de sockets seguros (SSL) solo para las sesiones compatibles con SSL. La unidad de comunicación TCP/IP del servidor espera peticiones en este puerto para sesiones con SSL activada del cliente.
- **TCPADMINPORT**  
La opción TCPADMINPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las peticiones de sesiones compatibles con TCP/IP y SSL distintas de las sesiones de cliente. Esto incluye las sesiones de administración, las sesiones de servidor a servidor, las sesiones del agente de almacenamiento, las sesiones del cliente de biblioteca, las sesiones de servidor gestionado y las sesiones del servidor de eventos.
-   **TCPBUFSIZE**  
La opción TCPBUFSIZE especifica el tamaño del búfer utilizado para peticiones de envío TCP/IP. Durante una restauración, los datos de cliente se traspasan del componente de sesión IBM Spectrum Protect a un controlador de comunicaciones TCP. La opción TCPBUFSIZE determina si el servidor envía los datos directamente desde el búfer de la sesión o copia los datos en el búfer TCP. Un tamaño de búfer de 32 KB dará lugar a que servidor copie forzosamente los datos en su búfer de comunicaciones y al vaciado del búfer cuando éste esté lleno.
- **TCPNODELAY**  
La opción TCPNODELAY especifica si el servidor inhabilita el retraso al enviar pequeños paquetes sucesivos en la red.
- **TCPPORT**  
La opción TCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. El controlador de comunicación TCP/IP de servidor escucha este puerto tanto para las sesiones TCP/IP como para las sesiones compatibles con SSL desde el cliente.
- **TCPWINDOWSIZE**  
La opción TCPWINDOWSIZE especifica, en kilobytes, la cantidad de datos de recepción que se pueden almacenar en el búfer a la vez en una conexión TCP/IP. El host emisor no puede enviar más datos hasta que reciba una confirmación y una actualización de ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP anunciada en la conexión. Una ventana más grande permite que el emisor continúe enviando datos y puede mejorar el rendimiento de las comunicaciones, sobre todo en las redes rápidas con una latencia elevada.
- **TECBEGINEVENTLOGGING**  
La opción TECBEGINEVENTLOGGING especifica si las anotaciones de eventos del receptor de TIVOLI deben empezar cuando se inicie el servidor. Si se especifica la opción TECHOST, TECBEGINEVENTLOGGING toma de forma predeterminada el valor YES.
- **TECHOST**  
La opción TECHOST especifica el nombre de host o dirección IP del servidor de eventos de Tivoli.
- **TECPORT**  
La opción TECPORT especifica la dirección de puerto TCP/IP en la que el servidor de eventos Tivoli está a la escucha. Esta opción sólo es necesaria si el servidor de eventos Tivoli se encuentra en un sistema que no tiene un servicio PortMapper en funcionamiento.
- **TECUTF8EVENT**  
La opción TECUTF8EVENT permite al administrador de IBM Spectrum Protect enviar información al servidor de Tivoli Enterprise Console (TEC) en formato de datos UTF-8. El valor predeterminado es No. Puede visualizar si esta opción está activada o no mediante la emisión del comando QUERY OPTION.
- **THROUGHPUTDATATHRESHOLD**  
La opción THROUGHPUTDATATHRESHOLD especifica un umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele después de que se haya alcanzado el umbral de tiempo.
- **THROUGHPUTTIMETHRESHOLD**  
La opción THROUGHPUTTIMETHRESHOLD especifica el umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.
-  **TIMEFORMAT**  
La opción TIMEFORMAT especifica el formato mediante el cual el servidor visualiza la hora.
- **TXNGROUPMAX**  
La opción TXNGROUPMAX especifica el número de objetos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones. El valor mínimo es de 4 objetos y el valor máximo es de 65000 objetos. El valor predeterminado son 4096 objetos. Los objetos transferidos son directorios, archivos reales o ambos. El servidor cuenta cada archivo o directorio como un objeto.
- **UNIQUEDPTECEVENTS**  
La opción UNIQUEDPTECEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect, incluidos los mensajes del cliente, del servidor y del cliente de IBM Spectrum Protect. El valor predeterminado es No.
- **UNIQUETECEVENTS**  
La opción UNIQUETECEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect. El valor predeterminado es No.
- **USEREXIT**  
La opción USEREXIT especifica la salida definida por el usuario a la que se otorgará control para poder gestionar un evento.



- VERBCHECK  
La opción VERBCHECK especifica que el servidor realizará una comprobación de errores adicional en la estructura de comandos que el cliente ha enviado. Esta opción sólo debe habilitarse cuando el cliente envía al servidor solicitudes con un formato incorrecto, lo que provoca que el servidor se cuelgue. Cuando esta opción está habilitada, obtendrá un error de protocolo en lugar de que el servidor se cuelgue.
- VOLUMEHISTORY  
La opción VOLUMEHISTORY especifica los nombres de los archivos que se actualizarán automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor. No existe un valor predeterminado para esta opción.


## Modificación de opciones del servidor

El servidor lee el archivo de opciones del servidor durante la inicialización del servidor. Cuando actualiza una opción del servidor editando el archivo, debe detener y arrancar el servidor para activar el archivo de opciones del servidor actualizado.

### Acerca de esta tarea

Con el comando SETOPT puede cambiar algunas opciones dinámicamente, sin necesidad de detener e iniciar el servidor. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica) para obtener más detalles.

  El archivo dsmserv.opt.smp (que también se proporciona durante la instalación) contiene el formato del archivo de opciones y todos los valores predeterminados. Puede cambiar cualquiera de las opciones del archivo dsmserv.opt.smp. Para que el servidor utilice las opciones que se han cambiado, debe cambiar el nombre del archivo por dsmserv.opt. Para activar una opción del archivo de opciones del servidor, elimine el símbolo \*>>> que precede a la opción. El servidor pasa por alto cualquier opción que vaya precedida del símbolo \*>>>.

 Puede modificar las opciones del servidor utilizando el editor de archivos de opciones que se incluye en la consola de IBM Spectrum Protect. Este editor proporciona la detección de parámetros de comunicaciones, la validación de valores y ayuda para todas las opciones. El editor de archivos de opciones es el modo preferido de cambiar las opciones del servidor, pero también puede utilizar un editor de texto.

## Tipos de opciones del servidor

Las opciones del servidor le permiten personalizar el modo en que funcionan algunas funciones y procesos.

- Opciones de comunicación del servidor  
Puede utilizar las opciones del servidor para especificar los métodos de comunicaciones del servidor y sus características.
- Opciones de almacenamiento del servidor  
IBM Spectrum Protect proporciona diferentes opciones que puede especificar para configurar determinadas operaciones de almacenamiento del servidor y de los dispositivos.
- Opciones de cliente/servidor  
Puede utilizar las opciones de servidor para controlar el proceso de cliente/servidor.
- Opciones de fecha, número, hora e idioma  
Puede utilizar las opciones de servidor para especificar los formatos de las fechas, horas, números e idioma nacional.
- Opciones de la base de datos  
Puede utilizar las opciones del servidor para controlar algunos aspectos del proceso de bases de datos.
- Opciones de transferencia de datos  
Puede utilizar las opciones del servidor para controlar el modo en que IBM Spectrum Protect agrupa y transfiere los datos.
- Opciones de mensajes  
Puede utilizar las opciones para obtener más flexibilidad en el modo en que IBM Spectrum Protect emite los mensajes.
- Opciones de anotaciones de eventos  
Opciones que pueden ayudarle a gestionar los receptores de anotaciones de eventos.
- Opciones de seguridad y del sistema de licencias  
Puede utilizar las opciones del servidor para personalizar la seguridad del servidor y las auditorías de licencias.
- Opciones varias  
Puede usar una serie de opciones varias para personalizar IBM Spectrum Protect.





## Opciones de comunicación del servidor

Puede utilizar las opciones del servidor para especificar los métodos de comunicaciones del servidor y sus características.

Tabla 1. Opciones de comunicaciones

Opción	Descripción
--------	-------------

Opción	Descripción
ADMINCOMMTIMEOUT	La cantidad de tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos
ADMINIDLETIMEOUT	La cantidad de tiempo que puede estar desocupada una sesión del cliente administrativo
ADMINONCLIENTPORT	Puerto que determina si las sesiones de administración pueden utilizar el puerto especificado en la opción TCPPOINT
COMMMETHOD	El método de comunicaciones del servidor
DBMTCPPOINT	El número de puerto en el que el controlador de comunicación TCP/IP para el gestor de base de datos espera las solicitudes de la sesión de cliente
DNSLOOKUP	Control de uso de Servicios de nombres de dominios para consultar nombres de sistemas que se pongan en contacto con el servidor
LDAPCACHEDURATION	Determina la cantidad de tiempo que se omiten las sesiones de autenticación, en el mismo nodo o administrador. Es posible que vea un ligero aumento de rendimiento cuando se omiten las sesiones.
LDAPURL	Especifica el servidor de directorios LDAP. Cada valor debe tener el nombre del servidor de directorios LDAP, un número de puerto y el nombre distinguido base del espacio de nombres o el sufijo que mantiene el servidor.
 Sistemas operativos Windows NAMEDPIPENAME	 Sistemas operativos Windows El método de comunicaciones de conexiones de entrada/salida nombrado
NDMPCONTROLPOINT	El puerto de comunicaciones internas utilizado para determinadas operaciones NDMP (Network Data Management Protocol).
NDMPENABLEKEEPALIVE	El mecanismo de estado activo TCP
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows NDMPKEEPIDLEMINUTES	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows La cantidad de tiempo de inactividad antes de que se envíe el primer paquete de estado activo TCP
 Sistemas operativos Windows NPBUFFERSIZE	 Sistemas operativos Windows El tamaño del búfer de comunicaciones de Named Pipes.
SHMPOINT	 Sistemas operativos AIX  Sistemas operativos Linux La dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida  Sistemas operativos Windows El puerto en el que el servidor está a la escucha de conexiones de memoria compartida

Opción	Descripción
SNMPHEARTBEATINTERVAL	El intervalo en minutos entre consultas del servidor de IBM Spectrum Protect
SNMPMESSAGECATEGORY	Los tipos de condición de excepción utilizados cuando se reenvían los mensajes desde el servidor.
SNMPSUBAGENT	Los parámetros necesarios para que el subagente IBM Spectrum Protect se comunique con el daemon SNMP
SNMPSUBAGENTHOST	La ubicación del subagente IBM Spectrum Protect SNMP
SNMPSUBAGENTPORT	La dirección del puerto del subagente IBM Spectrum Protect SNMP
SSLFIPSMODE	Especifica si se aplica la modalidad FIPS (Federal Information Processing Standards) para la capa de sockets seguros (SSL)
SSLTCPADMINPORT	La dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL para el cliente de administración de línea de comandos
SSLTCPPOINT	El número de puerto sólo SSL en el que el controlador de comunicaciones TCP/IP del servidor espera solicitudes de sesiones habilitadas para SSL procedentes de los siguientes orígenes: <ul style="list-style-type: none"> <li>• Cliente de archivado y copia de seguridad de línea de mandatos</li> <li>• GUI de archivado y copia de seguridad</li> <li>• Cliente de administración</li> <li>• Interfaz de programación de aplicaciones (API)</li> </ul>
TCPADMINPORT	El número de puerto TCP/IP para las sesiones de administración
 Sistemas operativos AIX  Sistemas operativos LinuxTCPBUFSIZE	 Sistemas operativos AIX  Sistemas operativos LinuxEl tamaño del búfer que se utiliza para las peticiones de envío TCP/IP
TCPPOINT	El número de puerto TCP/IP para las sesiones de cliente
TCPWINDOWSIZE	La ventana deslizante TCP/IP del nodo cliente

















## Opciones de almacenamiento del servidor

IBM Spectrum Protect proporciona diferentes opciones que puede especificar para configurar determinadas operaciones de almacenamiento del servidor y de los dispositivos.

Tabla 1. Opciones de almacenamiento del servidor

Opción	Descripción
3494SHARED	Permite compartir una biblioteca 3494 con otras aplicaciones excepto IBM Spectrum Protect.
ACSACCESSID	El ID del control de acceso de ACS.



Opción	Descripción
ACSLCKDRIVE	Permite bloquear las unidades de las bibliotecas ACSLS.
ACSQUICKINIT	Permite una inicialización rápida o completa de la biblioteca ACSLS.
ACSTIMEOUTX	El múltiplo del valor de tiempo de espera incorporado de la API ACSLS.
ASSISTVCRRECOVERY	Especifica si el servidor debe asistir a una unidad IBM 3590 a recuperarse de una condición de VCR (registros vitales de cartucho) perdidos o dañados.
CHECKTAPEPOS	Especifica si el servidor valida la posición de datos en cinta.
CLIENTDEDUPTXNLIMIT	Especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.
DEDUPREQUIRESBACKUP	Especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para optimización de almacenamiento de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.
DEDUPTIER2FILESIZE	Tamaño de archivo con el que se utiliza el procesamiento de nivel 2 para la deduplicación de datos.
DEDUPTIER3FILESIZE	Tamaño de archivo con el que se utiliza el procesamiento de nivel 3 para la deduplicación de datos.
DEVCONFIG	El archivo que almacena copias de seguridad de la información de configuración de dispositivos.
DRIVEACQUIRERETRY	El número de veces que un servidor intenta adquirir una unidad en una biblioteca IBM 349x compartida entre varias aplicaciones.
ENABLENASDEDUP	Especifica si el servidor elimina los datos duplicados almacenados por un servidor de archivos de almacenamiento conectado a red (NAS) NetApp.
NUMOPENVOLSALLOWED	El número de entradas los volúmenes FILE en una agrupación de almacenamiento deduplicada que se pueden abrir a la vez.
RECLAIMDELAY	El número de días que se retrasa la reclamación de un volumen SnapLock.
RECLAIMPERIOD	El número de días del periodo de reclamación de un volumen SnapLock
RESOURCETIMEOUT	El intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso.
RETENTIONEXTENSION	El número de días para ampliar la fecha de retención de un volumen de SnapLock.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANDISCOVERY	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Indica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANDISCOVERYTIMEOUT	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Tiempo que transcurre antes de que el proceso de descubrimiento de SAN exceda el tiempo de espera.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows SANREFRESHTIME	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Tiempo que transcurre antes de renovar la información de descubrimiento de la SAN.
SEARCHMPQUEUE	El orden en que el servidor atiende las peticiones en la cola de montaje.
SERVERDEDUPTXNLIMIT	Especifica el tamaño máximo de los objeto de los que se puede optimizar el almacenamiento en el servidor.

## Opciones de cliente/servidor

Puede utilizar las opciones de servidor para controlar el proceso de cliente/servidor.

Tabla 1. Opciones de cliente/servidor







Opción	Descripción
--------	-------------

Opción	Descripción
COMMTIMEOUT	El número máximo de segundos que el servidor espera a obtener una respuesta de un cliente antes de desactivar la sesión cliente por tiempo excedido.
DISABLESCHEDS	Si las planificaciones de administración y de cliente se desactivan durante una situación de recuperación del servidor de IBM Spectrum Protect.
IDLETIMEOUT	El número de minutos que el servidor permite que una sesión cliente permanezca desocupada antes de desactivar la sesión cliente por tiempo excedido.
MAXSESSIONS	El número máximo de sesiones cliente simultáneas en el servidor.
THROUGHPUTDATATHRESHOLD	El umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele tras haberse alcanzado el umbral de tiempo.
THROUGHPUTTIMETHRESHOLD	El umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.
VERBCHECK	Si se realiza una comprobación de errores adicional de los comandos que envía el cliente

## Opciones de fecha, número, hora e idioma

Puede utilizar las opciones de servidor para especificar los formatos de las fechas, horas, números e idioma nacional.

Tabla 1. Opciones de fecha, número, hora e idioma

Opción	Descripción
 Sistemas operativos Windows DATEFORMAT	 Sistemas operativos Windows El formato en el que se visualizarán las fechas
LANGUAGE	El idioma nacional que se utilizará para presentar los mensajes del cliente
 Sistemas operativos Windows NUMBERFORMAT	 Sistemas operativos Windows El formato para visualizar los números
 Sistemas operativos Windows TIMEFORMAT	 Sistemas operativos Windows El formato para visualizar la hora

## Opciones de la base de datos

Puede utilizar las opciones del servidor para controlar algunos aspectos del proceso de bases de datos.

Tabla 1. Opciones de la base de datos

Opción	Descripción
ACTIVELOGDIRECTORY	Nuevo directorio de la ubicación en la que se almacenan las anotaciones activas. Utilice esta opción para cambiar la ubicación de las anotaciones activas.
ACTIVELOGSIZE	Tamaño máximo de las anotaciones activas.
ALLOWREORGINDEX	Reorganización de índice iniciada por el servidor.
ALLOWREORGTABLE	Reorganización de tabla iniciada por el servidor.
ARCHLOGDIRECTORY	El directorio en el que el gestor de bases de datos puede archivar un archivo de anotaciones una vez finalizadas todas las transacciones representadas en dicho archivo de anotaciones.
ARCHFAILOVERLOGDIRECTORY	El directorio en el que el servidor intenta almacenar los archivos de anotaciones de archivado que no pueden guardarse en el directorio de anotaciones de archivado.
DBDIAGLOGSIZE	El tamaño máximo de los archivos de registro de diagnóstico del gestor de base de datos.
DBDIAGPATHFSTHRESHOLD	El umbral de espacio libre en el sistema de archivos o en el disco que contiene los archivos de diagnóstico del gestor de base de datos.
DBMEMPERCENT	Porcentaje de memoria del sistema que se dedica a la base de datos.
DISABLEREORGTABLE	Inhabilita la reorganización de tablas para tablas específicas.

Opción	Descripción
FSUSEDTHRESHOLD	El porcentaje de sistema de archivos que puede utilizar la base de datos antes de emitir un mensaje de alerta.
MIRRORLOGDIRECTORY	El directorio para duplicar la ruta de anotaciones activas.
REORGBEGINTIME	La hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o de índice.
REORGDURATION	El intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.

## Opciones de transferencia de datos

Puede utilizar las opciones del servidor para controlar el modo en que IBM Spectrum Protect agrupa y transfiere los datos.

Tabla 1. Opciones de agrupación

Opción	Descripción
MOVEBATCHSIZE	El número de archivos que se trasladarán y agruparán en un lote dentro de una transacción.
MOVESIZETHRESH	El umbral de la cantidad de datos trasladados como un lote en la misma transacción del servidor.
NDMPPORTRANGE	Dirección IP que se asocia a la interfaz en la que el servidor recibe todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
NDMPREFDATAINTERFACE	Dirección IP que se asocia a la interfaz en la que el servidor recibe todos los datos de copia de seguridad NDMP (Network Data Management Protocol).
REPLBATCHSIZE	El número de archivos que se van a replicar en un lote, dentro de la misma transacción de servidor.
REPLSIZETHRESH	El umbral de la cantidad de datos duplicados como un lote en la misma transacción del servidor.
TXNGROUPMAX	El número máximo de archivos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones.

## Opciones de mensajes

Puede utilizar las opciones para obtener más flexibilidad en el modo en que IBM Spectrum Protect emite los mensajes.

Tabla 1. Opciones de mensajes

Opción	Descripción
EXPQUIET	Especifica si IBM Spectrum Protect envía mensajes informativos detallados durante el proceso de caducidad.
MESSAGEFORMAT	Especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.
MSGINTERVAL	El tiempo, en minutos, que debe transcurrir entre los mensajes que solicitan a un operador que monte una cinta para IBM Spectrum Protect.

## Opciones de anotaciones de eventos

Opciones que pueden ayudarle a gestionar los receptores de anotaciones de eventos.

Tabla 1. Opciones de anotaciones de eventos









Opción	Descripción
EVENTSERVER	Si el servidor debe intentar establecer contacto con el servidor de eventos al arrancar el servidor.
FILEEXIT	Un archivo al que se direccionan los eventos activados (formato binario)

Opción	Descripción
FILETEXTXIT	Un archivo al que se direccionan los eventos activados (formato legible)
REPORTRETRIEVE	Registra las operaciones de restauración y recuperación de clientes.
TECBEGINEVENTLOGGING	Especifica si la anotación de eventos del receptor TIVOLI debe empezar cuando arranca el servidor.
TECHOST	Especifica el nombre de host o la dirección IP del servidor de eventos de Tivoli Enterprise Console (TEC).
TECPORT	La dirección del puerto TCP/IP en la que está conectado el servidor de eventos de Tivoli Enterprise Console.
TECUTF8EVENT	Un evento Tivoli Enterprise Console enviado desde el servidor de IBM Spectrum Protect en formato UTF8
UNIQUEDPTECEVENTS	Los eventos procedentes de un cliente de IBM Spectrum Protect Data Protection que se envían a Tivoli Enterprise Console como eventos exclusivos
UNIQUETECEVENTS	Eventos enviados a Tivoli Enterprise Console como exclusivos
USEREXIT	Salida definida por el usuario a la que se otorgará control para poder gestionar un evento

## Opciones de seguridad y del sistema de licencias

Puede utilizar las opciones del servidor para personalizar la seguridad del servidor y las auditorías de licencias.

Tabla 1. Opciones de seguridad y del sistema de licencias

Opción	Descripción
 Sistemas operativos Windows ADSMGROUPNAME	 Sistemas operativos Windows El nombre de un grupo Windows
AUDITSTORAGE	Especifica que durante una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento de gestión de espacio, de copia de seguridad/archivado que está utilizándose.
BACKUPINITIATIONROOT	Especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.
LDAPURL	Especifica el servidor de directorios LDAP. Cada valor debe tener el nombre del servidor de directorios LDAP, un número de puerto y el nombre distinguido base del espacio de nombres o el sufijo que mantiene el servidor.
 Sistemas operativos Windows NPAUDITFAILURE	 Sistemas operativos Windows Especifica que un nodo sólo puede acceder a sus propios datos.
 Sistemas operativos Windows NPAUDITSUCCESS	 Sistemas operativos Windows Especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.
QUERYAUTH	El nivel de autorización de administración necesario para emitir los mandatos QUERY o SQL SELECT.
REQSYSAUTHOUTFILE	Especifica si es necesaria la autorización del sistema para los comandos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo.
 Sistemas operativos Windows SECUREPIPES	 Sistemas operativos Windows Con el protocolo Named Pipes, especifica que el servidor comprueba el grupo Windows a fin de autenticar un cliente.
SHREDDING	Especifica si la fragmentación de datos confidenciales suprimidos se hace de forma automática o manual

### Referencia relacionada:

Opciones de comunicación del servidor

## Opciones varias

Puede usar una serie de opciones varias para personalizar IBM Spectrum Protect.

Tabla 1. Opciones varias

Opción	Descripción
ALIASHALT	Permite a los administradores asignar un nombre diferente a un comando HALT de IBM Spectrum Protect.
DISPLAYLFINFO	Especifica si los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del agente de almacenamiento
EXPINTERVAL	El intervalo entre procesos de caducidad de inventario automáticas
FFDCLOGNAME	El nombre para el registro FFDC (first failure data capture)
FFDCMAXLOGSIZE	El tamaño máximo del registro FFDC (First Failure Data Capture)
NOPREEMPT	Especifica que ninguna operación puede adelantarse a otra para acceder a un volumen y que únicamente una operación de copia de seguridad de base de datos puede adelantarse a otra operación para acceder a un dispositivo.
NORETRIEVEDATE	Especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo.
RESTOREINTERVAL	Intervalo de tiempo durante el que se puede guardar una sesión de restauración reinicializable en la base de datos del servidor.
VOLUMEHISTORY	El archivo que se actualizará automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor.

## 3494SHARED

La opción 3494SHARED especifica si una biblioteca IBM® 3494 puede compartir aplicaciones distintas de IBM Spectrum Protect.

El valor predeterminado es NO, que significa que la biblioteca 3494 no se puede compartir con ninguna otra aplicación excepto IBM Spectrum Protect. Si establece esta opción en YES, IBM Spectrum Protect determina para cada petición de montaje si se están utilizando las unidades. Una vez realizada la consulta, IBM Spectrum Protect selecciona una unidad disponible que no utilice otra aplicación. Sólo debe activarse la posibilidad de compartir si en la biblioteca hay más de dos unidades. Si actualmente comparte una biblioteca IBM 3494 con otras aplicaciones, debe especificar esta opción.

### Sintaxis

```
>>-3494SHARED---+-Yes-+-----<<
      '-No--'
```

### Parámetros

- Yes  
Especifica que otras aplicaciones pueden compartir la biblioteca 3494.
- No  
Especifica que ninguna otra aplicación puede compartir la biblioteca 3494.

### Ejemplos

Activar el compartimiento de una biblioteca 3494:

3494shared yes

## ACSACCESSID

---

La opción ACSACCESSID especifica el identificador del control de acceso de ACS para una biblioteca ACSLS.

### Sintaxis

---

```
>>-ACSACCESSID--nombre-----<<
```

### Parámetros

---

nombre

Especifica un identificador de 1 a 64 caracteres. El identificador predeterminada es el nombre de host local.

### Ejemplos

---

```
acsaccessid region
```

## ACSLOCKDRIVE

---

La opción ACSLOCKDRIVE especifica si las unidades de las bibliotecas ACSLS están bloqueadas. Al bloquear las unidades, se garantiza el uso exclusivo de la unidad de la biblioteca ACSLS en un entorno compartido. Sin embargo, el rendimiento es mejor si las bibliotecas no se bloquean. Cuando otras aplicaciones no comparten las unidades de IBM Spectrum Protect, no es necesario bloquear las unidades.

### Sintaxis

---

```
>>-ACSLOCKDRIVE--+-Yes-+-----<<  
                '-No--'
```

### Parámetros

---

Yes

Especifica que las unidades están bloqueadas.

No

Especifica que las unidades no están bloqueadas.

### Ejemplos

---

```
acslockdrive yes
```

## ACSQUICKINIT

---

La opción ACSQUICKINIT especifica si, en el arranque del servidor, la inicialización de la biblioteca ACSLS es rápida o completa. El valor predeterminado es Yes. Una inicialización rápida evita la sobrecarga asociada con la sincronización del inventario del servidor de IBM Spectrum Protect con el inventario de biblioteca ACSLS (mediante una auditoría de la biblioteca).

### Sintaxis

---

```
>>-ACSQUICKINIT--+-Yes-+-----<<  
                '-No--'
```

### Parámetros

---

Yes

Especifica que se lleve a cabo una inicialización rápida de la biblioteca ACSLS. Cuando la opción se establece en Yes, IBM Spectrum Protect omite la verificación del inventario de biblioteca, e inicializa rápidamente la biblioteca haciendo que IBM Spectrum Protect pueda disponer de la misma antes que si se llevara a cabo una inicialización completa.

Esta opción debe establecerse en Yes cuando se sabe que el inventario de biblioteca física y el inventario de biblioteca de IBM Spectrum Protect no han cambiado y que no es necesario realizar una auditoría.

No

Especifica que se lleve a cabo una inicialización completa de la biblioteca ACSLS y del inventario de biblioteca. Cuando la opción se establece en No, IBM Spectrum Protect sincroniza su inventario de volúmenes de la biblioteca con lo que notifica el gestor de bibliotecas ACSLS.

## Ejemplos

---

```
acsquickinit yes
```

## ACSTIMEOUTX

---

La opción ACSTIMEOUTX especifica el múltiplo del valor de tiempo de espera incorporado de las API ACSLS. El valor de tiempo de espera incorporado de la API de introducción, expulsión y auditoría ACS son 1800 segundos; el valor de todas las demás API ACSLS son 600 segundos. Por ejemplo, si el múltiplo especificado es 5, el valor de tiempo de espera de la API de auditoría serán 9000 segundos y el valor de todas las demás API serán 3000 segundos.

## Sintaxis

---

```
>>-ACSTIMEOUTX--valor-----<<
```

## Parámetros

---

valor

Especifica el múltiplo del valor de tiempo de espera incorporado de la API ACSLS. El rango es de 1 a 100. El valor predeterminado es 1.

## Ejemplos

---

```
acstimeoutx 1
```

## ACTIVELOGDIRECTORY

---

La opción ACTIVELOGDIRECTORY especifica el nombre del directorio donde están almacenados todos los registros activos.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT. En condiciones generales de utilización, no es necesario cambiar la opción. Consulte el apartado DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones) para obtener ayuda para esta opción.

## Sintaxis

---

```
>>-ACTIVELOGDirectory--dir_name-----<<
```

## Parámetros

---

nombre\_dir


Especifica un nombre de directorio cualificado al completo. El directorio debe existir, debe estar vacío, y debe ser accesible mediante el ID de usuario del gestor de base de datos. Si cambia el directorio de anotaciones activas, IBM Spectrum Protect moverá las anotaciones activas existentes a la ubicación que este directorio especifica. El número máximo de caracteres es 175.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux

activelogdirectory /tsm/activelogdir

 Sistemas operativos Windows

activelogdirectory c:\tsmserv1\activelogdir

## ACTIVELOGSIZE

La opción ACTIVELOGSIZE establece el tamaño total del registro.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSEVERV FORMAT. En condiciones generales de utilización, no es necesario cambiar la opción. Consulte el apartado DSMSEVERV FORMAT (Dar formato a la base de datos y a las anotaciones) para obtener ayuda para esta opción.

### Sintaxis

```
.-16GB-----.  
>>-ACTIVELOGSize--+-megabytes+-----<<
```

### Parámetros

**megabytes**

Especifica el tamaño del archivo de anotaciones activas en megabytes. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16.384 MB (16 GB).

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

### Ejemplos

```
activelogsize 8192
```

## ADMINCOMMTIMEOUT

La opción ADMINCOMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente administrativo durante una operación que produce una actualización de la base de datos.

Si el tiempo supera este periodo de tiempo de espera, el servidor finaliza la sesión con el cliente administrativo. Puede aumentar el valor de tiempo de espera para evitar que las sesiones de los clientes administrativos excedan el tiempo de espera.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

### Sintaxis

```
.-60-----.  
>>-ADMINCOMMTIMEout--+-segundos+-----<<
```

### Parámetros

**seconds**

Especifica el número máximo de segundos que el servidor espera una respuesta del cliente administrativo. El valor predeterminado es 60. El valor mínimo es 1.



## Ejemplos

---

```
admincomtimeout 60
```

## ADMINIDLETIMEOUT

---

La opción ADMINIDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente administrativo puede estar desocupada antes de que la cancele el servidor.

Si hay una gran carga de red en el entorno, puede aumentar el valor de tiempo de espera para evitar que los clientes administrativos excedan el tiempo de espera. No obstante, una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
                .-15-----.  
>>-ADMINIDLETIMEOUT--+-minutos+-----<<
```

## Parámetros

---

minutos

Especifica el número máximo de minutos que el servidor espera a un cliente administrativo desocupado. El valor predeterminado es de 15 minutos. El valor mínimo es de 1 minuto.

## Ejemplos

---

```
adminidletimeout 20
```

## ADMINONCLIENTPORT

---

La opción ADMINONCLIENTPORT especifica si las sesiones administrativas pueden utilizar TCPPOINT. El valor predeterminado es YES.

## Sintaxis

---

```
>>-ADMINONCLIENTPORT--+-YES+-----<<  
                '-NO--'
```

## Parámetros

---

YES

Si la opción está establecida en YES, o si TCPPOINT y TCPADMINPORT tienen el mismo valor (es así de forma predeterminada), las sesiones administrativas pueden utilizar TCPPOINT.

NO

Si la opción está establecida en NO, y si el valor de TCPADMINPORT es distinto del valor TCPPOINT, las sesiones administrativas no pueden utilizar TCPPOINT.

## Ejemplos

---

Especificar que las sesiones de administración pueden utilizar TCPPOINT.

```
adminonclientport yes
```

 Sistemas operativos Windows

## ADSMGROUPNAME

---

La opción ADMSGROUPNAME especifica el nombre de un grupo Windows. Un nodo cliente debe ser miembro de este grupo para poder utilizar el servidor de IBM Spectrum Protect a través de NT Unified Logon. El nodo de cliente también debe ser un nodo de cliente de IBM Spectrum Protect registrado.

## Sintaxis

---

```
>>-ADSMGROUPName--nombre_grupo-----<<
```

## Parámetros

---

nombre\_grupo  
Especifica un nombre de grupo Windows.

## Ejemplos

---

Especificar IDD como un grupo Windows:

```
adsmgroup idd
```

## ALIASHALT

---

La opción ALIASHALT permite a los administradores asignar un nombre diferente a un comando **HALT** de IBM Spectrum Protect.

El cliente de administración reconoce un alias para el comando HALT cuando el cliente se inicia habiéndose especificado la opción CHECKALIASHALT. Consulte el apartado Opciones de cliente de administración para obtener más detalles.

## Sintaxis

---

```
>>-ALIASHALT--nombre_nuevo-----<<
```

## Parámetros

---

nombre\_nuevo  
Especifica el alias del comando HALT para concluir el servidor de IBM Spectrum Protect. La longitud mínima de *nombre\_nuevo* es 1 y la máxima de 16.

## Ejemplos

---

```
aliashalt tsmhalt
```

## ALLOWDESAUTH

---

La opción ALLOWDESAUTH especifica si se debe permitir la utilización del algoritmo DES (Data Encryption Standard) para la autenticación entre un servidor y un cliente de archivado y copia de seguridad.

Para impedir la utilización de DES, especifique el valor NO para la opción ALLOWDESAUTH.

Para configurar el servidor de IBM Spectrum Protect para que esté en conformidad con el estándar NIST SP800-131A, establezca esta opción en NO.

Restricciones:

- El cliente de archivado y copia de seguridad debe estar ejecutando la versión 6.3 o posterior si se autentica en un servidor con la opción ALLOWDESAUTH establecida en NO.
- El despliegue automático del cliente de archivado y copia de seguridad falla si esta opción está establecida en NO.

## Sintaxis

---

```
.-ALLOWDESAUTH--Yes-----.  
>>+-----+<<  
'-ALLOWDESAUTH--+-No--+-'
```

'-Yes-'

## Parámetros

---

Yes

Especifica que el servidor permite la autenticación con los clientes de archivado y copia de seguridad que utilizan cifrado basado en DES. El valor predeterminado es YES.

No

Especifica que el servidor rechaza los clientes de archivado/copia de seguridad que intentan autenticarse con cifrado basado en DES.

## Ejemplos

---

Especificar que el servidor rechace los clientes de archivado/copia de seguridad que intentan autenticarse con cifrado basado en DES:

```
allowdesauth no
```

Especificar que el servidor permita la autenticación con los clientes de archivado/copia de seguridad que utilizan cifrado basado en DES:

```
allowdesauth yes
```

## ALLOWREORGINDEX

---

La opción ALLOWREORGINDEX especifica si la reorganización de índice iniciada por el servidor está activada o desactivada.

El valor predeterminado es YES.

## Sintaxis

---

```
>>-ALLOWREORGINDEX--+-Yes-+-----<<  
'-No--'
```

## Parámetros

---

Yes

Especifica que la reorganización de índice iniciada por el servidor está activada.

No

Especifica que la reorganización de índice iniciada por el servidor no está activada.

## Ejemplo

---

Especificar que la reorganización de índice iniciada por el servidor está activada.

```
allowreorgindex yes
```

## ALLOWREORGTABLE

---

La opción ALLOWREORGTABLE especifica si la reorganización de tabla iniciada por el servidor está activada o desactivada.

El valor predeterminado es YES.

## Sintaxis

---

```
>>-ALLOWREORGTABLE--+-Yes-+-----<<  
'-No--'
```

## Parámetros

---

Yes

Especifica que la reorganización de tabla iniciada por el servidor está activada.

No

Especifica que la reorganización de tabla iniciada por el servidor no está activada.

## Ejemplos

---

Especifique que la reorganización de tabla iniciada por el servidor no está activada.

```
allowreorgtable no
```

## ARCHFAILOVERLOGDIRECTORY

---

La opción ARCHFAILOVERLOGDIRECTORY especifica el directorio que utiliza el servidor para almacenar los archivos de registro de archivado que no se pueden almacenar en el directorio de registros de archivado.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSEV FORMAT. Normalmente no es necesario cambiar el directorio.

## Sintaxis

---

```
>>-ARCHFailoverlogdirectory--dir_name-----<<
```

## Parámetros

---

nombre\_dir


Especifica un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux

```
archfailoverlogdirectory /tsm/archfailoverlog
```

 Sistemas operativos Windows

```
archfailoverlogdirectory c:\tsmserv1\archfailoverlog
```

## ARCHLOGCOMPRESS

---

Puede habilitar o inhabilitar la compresión de registros de archivado en el servidor de IBM Spectrum Protect. Al comprimir los registros de archivado, se reduce la cantidad de espacio necesaria para el almacenamiento.

La opción del servidor ARCHLOGCOMPRESS especifica si se comprimen archivos de registro en que se graban en el directorio de archivado para registros.

## Sintaxis

---

```
>>-ARCHLOGCOMPRESS--+-No-- .  
                        +-----+-----<<  
                        '-Yes-'
```

## Parámetros

---

No

Especifica que los archivos que se graban en el directorio del registro de archivado no se comprimen. El valor predeterminado es No.

Yes

Especifica que los archivos que se graban en el directorio del registro de archivado se comprimen.

Restricción: Preste atención cuando habilite la opción ARCHLOGCOMPRESS en sistemas con un alto volumen de utilización sostenido y mucha carga de trabajo. Si esta opción se habilita en este entorno del sistema pueden producirse retardos en el archivado de los archivos de registro de archivado desde el sistema de archivos de registro activos al sistema de archivos de registro de archivado. Este retardo puede provocar que el sistema de archivos de registro activos se quede sin espacio. Asegúrese de supervisar el espacio

disponible en el sistema de archivos de registro activos después de habilitar la comprensión de archivos de registro. Si el uso sistema de archivos del directorio de registro activo está alcanzando condiciones de falta de espacio, se debe inhabilitar la opción del servidor ARCHLOGCOMPRESS. Puede utilizar el mandato SETOPT para inhabilitar la comprensión del registro de archivado de forma inmediata sin detener el servidor.

## Ejemplo

---

Para permitir la compresión de archivos de registro que se graban en el directorio de registro de archivado, especifique la opción siguiente:

```
archlogcompress yes
```

## ARCHLOGDIRECTORY

---

La opción ARCHLOGDIRECTORY especifica un directorio en el que el gestor de base de datos puede archivar un archivo de registro una vez completadas todas las transacciones representadas en dicho archivo de registro.

Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT.

## Sintaxis

---

```
>>-ARCHLOGDirectory--dir_name-----<<
```

## Parámetros

---

nombre\_dir

Especifica un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux

```
archlogdirectory /tsm/archlog
```

 Sistemas operativos Windows

```
archlogdirectory d:\tmserv1\archlog
```

## ARCHLOGUSEDTHRESHOLD

---

La opción ARCHLOGUSEDTHRESHOLD especifica cuándo iniciar una copia de seguridad de base de datos automática en relación con el porcentaje de espacio de archivo de anotaciones de archivado utilizado. El valor predeterminado es el 80 por ciento.

La opción ARCHLOGUSEDTHRESHOLD impide copias de seguridad automáticas frecuentes. Por ejemplo, si el directorio de archivos de registro de archivado reside en un sistema de archivos o la unidad de 400 GB, se realizará una copia de seguridad de la base de datos si hay menos de 80 GB de espacio libre. Las copias de seguridad de la base de datos hacen que el servidor utilice una cantidad excesiva de cintas reutilizables.

## Sintaxis

---

```
>>-ARCHLOGUSEDTHRESHOLD--+-valor-+-----<<
```

## Parámetros

---

valor

El porcentaje de espacio de archivo de registro de archivado utilizado antes de que empiece la copia de seguridad.

Especifique para iniciar una copia de seguridad automática cuando se haya utilizado el 90 por ciento de espacio de archivos de registro de archivado.

```
archlogusedthreshold 90
```

## ASSISTVCRRECOVERY

---

La opción ASSISTVCRRECOVERY especifica si IBM Spectrum Protect debe ayudar a una unidad IBM® 3590 a recuperarse de una condición de VCR (Vital Cartridge Records) perdidos o dañados. Si especifica YES (el valor predeterminado) y si IBM Spectrum Protect detecta un error durante el proceso de montaje, se sitúa al final de los datos durante el proceso de desmontaje para permitir que las unidades restauren el VCR. Durante la operación de cinta, es posible que se produzca un pequeño efecto sobre el rendimiento ya que la unidad no puede realizar una búsqueda rápida con un VCR perdido o dañado. Sin embargo, no se produce ninguna pérdida de datos.

### Sintaxis

---

```
>>-ASSISTVCRREcovery--+-Yes-+-----<<
                        '-No--'
```

### Parámetros

---

- Yes  
Especifica que el servidor proporcionará ayuda para la recuperación.
- No  
Especifica que el servidor no proporcionará ayuda para la recuperación.

### Ejemplos

---

Desactivar la ayuda para la recuperación:

```
assistvcrrecovery no
```

## AUDITSTORAGE

---

Como parte de una operación de auditoría de licencias, el servidor calcula, por nodo, la cantidad de almacenamiento del servidor utilizado para operaciones de copia de seguridad y archivado, y para archivos bajo gestión de espacio. Para los servidores que gestionan grandes cantidades de datos, este cálculo puede ocupar una gran cantidad de tiempo de CPU y puede detener otras actividades del servidor. Puede utilizar la opción AUDITSTORAGE para especificar que el almacenamiento no se ha de calcular como parte de una auditoría de licencias.

Nota: Esta opción anteriormente se llamaba NOAUDITSTORAGE.

### Sintaxis

---

```
>>-AUDITStorage--+-Yes-+-----<<
                        '-No--'
```

### Parámetros

---

- Yes  
Especifica que el almacenamiento se calculará como parte de una auditoría de licencias. El valor predeterminado es Yes.
- No  
Especifica que el almacenamiento no se calculará como parte de una auditoría de licencias.

### Ejemplos

---

```
auditstorage yes
```

## BACKUPINITIATIONROOT

---

La opción BACKUPINITIATIONROOT especifica si el servidor sustituye los valores de los parámetros del nodo para los usuarios que no son usuarios autorizados por IBM Spectrum Protect.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
>>-BACKUPINITIATIONROOT--+-ON--+-+-----><
      '-Off-'
```

## Parámetros

---

ON

Especifica las sesiones de los clientes en los sistemas operativos AIX, Linux, Mac OS X y Solaris, en las que los usuarios que no son usuarios autorizados de IBM Spectrum Protect no puede iniciar operaciones de copia de seguridad. Este es el valor predeterminado. El servidor sustituye el valor del servidor para el parámetro BACKUPINITIATION que se especifica en los mandatos REGISTER NODE y UPDATE NODE.

Consejo: Para obtener una visión general de los usuarios autorizados de IBM Spectrum Protect, consulte la sección Cliente raíz de UNIX y Linux y tareas de usuario autorizadas.

OFF

Especifica que se utiliza el valor del nodo para el parámetro BACKUPINITIATION. El parámetro BACKUPINITIATION se especifica en los mandatos REGISTER NODE y UPDATE NODE.

## Ejemplo

---

Especifique que se ha de utilizar el valor del nodo para el parámetro BACKUPINITIATION.

```
backupinitiationroot off
```

## CHECKTAPEPOS

---

La opción CHECKTAPEPOS especifica si el servidor de IBM Spectrum Protect valida la posición de los bloques de datos en la cinta.

La opción CHECKTAPEPOS se aplica solo a operaciones que utilizan unidades de cintas. No se aplica a clases de dispositivos de acceso secuencial que no sean de cinta, como por ejemplo FILE. Si la información del servidor sobre la posición no coincide con la posición detectada por la unidad, se muestra un mensaje de error, la transacción se retrotrae y los datos no se confirman en la base de datos.

Utilizando la opción CHECKTAPEPOS puede habilitar la modalidad de sólo agregar para las unidades IBM LTO Generation 5 y posteriores y para cualquier unidad que dé soporte a esta característica. Cuando está activada, la unidad emite un error después de recibir instrucciones de sobrescribir los datos en el volumen montado actualmente. El servidor de IBM Spectrum Protect vuelve a colocar la cinta en el bloque correcto y continúa escribiendo datos. La modalidad de sólo agregar ofrece una protección agregada al impedir la mayoría de situaciones de sobrescritura de datos. Si utiliza una unidad que da soporte a esta característica, puede validar la posición de los datos en la cinta utilizando IBM Spectrum Protect y la unidad, o puede activar una opción o la otra.

Nota: Al utilizar las funciones de aceleración de cinta SAN en Fabric, establezca CHECKTAPEPOS en DRIVEonly o No para evitar errores de posicionamiento falso positivo. La opción de servidor IBM Spectrum Protect CHECKTAPEPOS no requiere que una unidad con posibilidad de sólo agregar.

Los cambios en la opción CHECKTAPEPOS sólo afectan a los montajes una vez completada la actualización a la unidad.

El valor predeterminado es YES.

## Sintaxis

---

```
>>-CHECKTAPEPOS--+-Yes-----+-----><
      +-No-----+
      +-TSMonly---+
      '-DRIVEonly-'
```

## Parámetros

---

Yes

Especifica que el servidor de IBM Spectrum Protect valida la posición de datos en la cinta. Para las unidades que dan soporte a la modalidad de sólo agregar, este parámetro especifica que IBM Spectrum Protect permite a la unidad validar también la posición de los datos durante cada operación WRITE para impedir la sobrescritura de estos. El valor predeterminado es Yes.

No

Especifica que la validación de la posición de todos los datos está desactivada.

TSMonly

Especifica que el servidor de IBM Spectrum Protect valida la posición de datos en la cinta. El servidor no utiliza la modalidad de sólo agregar aunque la unidad dé soporte a la característica.

DRIVEonly

Especifica que el servidor de IBM Spectrum Protect activa la modalidad de sólo agregar para las unidades que dan soporte a esta característica. El servidor no valida la posición de los datos en la cinta.

## Ejemplo

---

Valide la posición de los datos en la cinta y active la modalidad de sólo agregar para una unidad soportada:

```
checktapepos yes
```

## CLIENTDEDUPTXNLIMIT

---

La opción CLIENTDEDUPTXNLIMIT especifica el tamaño máximo de una transacción cuando se realizan copias de seguridad o se archivan datos con almacenamiento optimizado en el lado del cliente.

Cuando se usa optimización de almacenamiento en el lado del cliente para objetos de gran tamaño, puede producirse una actividad intensiva en la base de datos por las transacciones de ejecución larga necesarias para actualizar dicha base de datos. Unos niveles altos de actividad de la base de datos pueden producir los siguientes síntomas:

- Rendimiento reducido para las operaciones de copia de seguridad y de archivado del cliente
- Contienda de recursos debido a operaciones simultáneas del servidor
- Actividad excesiva del registro de recuperación

La medida en que se producen estos síntomas depende del número y del tamaño de los objetos que se almacenan utilizando optimización de almacenamiento por el cliente, la intensidad y el tipo de las operaciones que tienen lugar en el servidor de IBM Spectrum Protect y la configuración de servidor de IBM Spectrum Protect.

Con la opción de servidor CLIENTDEDUPTXNLIMIT es posible especificar un tamaño máximo, en gigabytes, para las transacciones cuando se realizan copias de seguridad o se archivan los datos del cliente con almacenamiento optimizado. Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por CLIENTDEDUPTXNLIMIT, dichos objetos no tienen optimización del almacenamiento por parte del cliente y la transacción puede fallar. Es posible especificar un valor de 32 a 102400 GB. El valor predeterminado es 5120 GB.

Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por CLIENTDEDUPTXNLIMIT, los objetos o el conjunto de objetos no tienen optimización del almacenamiento por parte del cliente. Sin embargo, los objetos se envían al servidor. Estos objetos pueden tener optimización de almacenamiento en el servidor, en función de si la agrupación de almacenamiento de destino está configurada para dicha optimización y del valor de la opción SERVERDEDUPTXNLIMIT. Los objetos en una agrupación de almacenamiento con optimización de almacenamiento habilitada inferiores al valor de SERVERDEDUPTXNLIMIT sí se optimizan mediante un proceso de identificación de duplicación del servidor.

El valor adecuado para esta opción depende de la configuración de servidor de IBM Spectrum Protect y de la actividad simultánea del servidor. Es posible especificar un valor alto para esta opción si se minimiza la contienda de recursos. Para minimizar la contienda de recursos, realice operaciones como copia de seguridad, archivado, identificación de duplicados (el mandato IDENTIFY DUPLICATES) y reclamación en distintos momentos.

Para actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor, utilice el mandato SETOPT.

## Sintaxis

---

```
.-5120-----.  
>>-CLIENTDEDUPTXNlimit---+gigabytes+-----<<
```

## Parámetros

---

**gigabytes**

Especifica el tamaño máximo, en gigabytes, de los objeto de los que se pueden archivar o hacer copia de seguridad usando optimización de almacenamiento de datos en el lado del cliente. Es posible especificar un valor de 32 a 102400. El valor predeterminado es 5120.

## Ejemplos

---



Inhabilitar la optimización de almacenamiento de datos en el lado del cliente para todos los objetos de más de 80 GB:

```
clientdeduptxnlimit 80
```

## COMMMETHOD

La opción COMMMETHOD especifica el método de comunicaciones que utilizará el servidor.

Puede configurar el servidor para que utilice varios métodos de comunicaciones. Los métodos de comunicaciones que se utilizan con más frecuencia son TCPIP, V6TCPIP y SHAREDMEM. Para especificar varios métodos de comunicaciones, habilite cada método agregando una stanza COMMMETHOD al archivo de opciones dsmserv.opt.


Importante: Cuando habilita un método de comunicaciones, también debe añadir al archivo de opciones las opciones específicas del método de comunicaciones.


## Sintaxis

```
.-TCPIP----- .
>>-COMMMethod--+-NAMEDPIPE-+-----><
+-NONE-----+
+-SHAREDMEM-+
+-SNMP-----+
+-TCPIP-----+
'-V6TCPIP---'
```

## Parámetros

Puede seleccionar uno de los siguientes métodos de comunicaciones:

 Sistemas operativos Windows NAMEDPIPES

 Sistemas operativos Windows Especifica la opción del método de comunicaciones de conexiones de entrada/salida nombrado.

NONE

Especifica que no se utilizará ningún método de comunicaciones. Esta opción no permite a los usuarios conectarse con el servidor y resulta útil para experimentar con comandos de política.

SHAREDMEM

Especifica la opción del método de comunicaciones de memoria compartida. Este método utiliza la misma área de memoria para enviar datos entre varias aplicaciones a la vez. Tanto el servidor como el cliente de archivado y copia de seguridad deben estar configurados para dar soporte al método de comunicación de memoria compartida y deben estar instalados en el mismo sistema.

SNMP

Especifica la opción del método de comunicaciones SNMP.

TCPIP

Especifica la opción del método de comunicaciones TCP/IP. Esta opción es la opción predeterminada. Si se especifica TCPIP, solamente se utiliza TCP/IP Versión 4.

V6TCPIP

Especifica la opción del método de comunicaciones TCP/IP. Si TCP/IP Versión 4 y Versión 6 están configuradas, IBM Spectrum Protect utiliza simultáneamente ambos protocolos. Si se especifican COMMMETHOD TCPIP y COMMMETHOD V6TCPIP, V6TCPIP prevalece sobre la especificación de TCPIP. Debe haber un entorno de servidor de nombres de dominio (DNS) para utilizar TCP/IP V4 o TCP/IP V6 si se especifica esta opción.

## Ejemplos

Ejemplo de especificación de métodos de comunicación que va a utilizar el servidor (TCP/IP y TCP/IP versión 6):

```
commmethod tcpip
commmethod v6tcpip
```

## COMMTIMEOUT

La opción COMMTIMEOUT especifica el tiempo que el servidor espera un mensaje del cliente durante una operación que produce una actualización de la base de datos. Si el tiempo supera este tiempo de espera, el servidor finaliza la sesión con el cliente. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera. Los clientes pueden exceder el tiempo de espera si existe una gran carga de red en el entorno o realizan copias de seguridad de archivos grandes.

La opción de servidor COMMTIMEOUT se utiliza en las sesiones no administrativas. Consulte la opción ADMINCOMMTIMEOUT para las sesiones de cliente administrativas.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el comando SETOPT.

## Sintaxis

---

```
.-60-----.  
>>-COMMTIMEout--+-segundos-+-----><
```

## Parámetros

---




seconds

Especifica el número máximo de segundos que el servidor espera una respuesta del cliente. El valor predeterminado es 60. El valor mínimo es 1.

## Ejemplos

---

```
commtimeout 60
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## CONTAINERRESOURCETIMEOUT

---

La opción CONTAINERRESOURCETIMEOUT especifica durante cuánto tiempo espera el servidor a completar una operación de almacén de datos en una agrupación de almacenamiento de contenedor.

## Sintaxis

---

Cuando se excede el tiempo de espera, los datos almacenados en la agrupación de almacenamiento de contenedor se conservan. La operación de almacenamiento de datos finaliza y se cancela la solicitud para el recurso de contenedor.

```
.-180-----.  
>>-CONTAINERRESOURCETIMEout--+-minutos-+-----><
```

## Parámetros

---

minutos


Especifica el número máximo de minutos que espera el servidor antes de que se cancele una operación. El valor predeterminado es de 180 minutos. El valor mínimo es de 1 minuto.

## Ejemplo

---

Especifique que el servidor ha de esperar 4 horas antes de que se cancele una operación de almacenamiento de datos en una agrupación de almacenamiento de contenedor.

```
containerresourcetimeout 240
```

 Sistemas operativos Windows

## DATEFORMAT

---

La opción DATEFORMAT especifica el formato que el servidor ha de utilizar para visualizar las fechas.

El formato del entorno local altera temporalmente el valor DATEFORMAT si el entorno local se inicializa durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

## Sintaxis

---

```
>>-DATEformat--n-----><
```

## Parámetros

---

n

Seleccione un número de 1 a 5 para identificar el formato de fecha que utiliza el servidor. El valor predeterminado es 1.

1	MM/DD/AAAA
2	DD-MM-AAAA
3	AAAA-MM-DD
4	DD.MM.AAAA
5	AAAA.MM.DD

## Ejemplos

---

```
dateformat 4
```

## DBDIAGLOGSIZE

---

Esta opción permite controlar el espacio que utilizan los archivos de registro de diagnóstico.

El gestor de base de datos utiliza archivos de registro de diagnóstico para registrar mensajes. Debe controlar el tamaño de los archivos de registro para que no se llene el sistema de archivos. Utilice la opción DBDIAGLOGSIZE para establecer la cantidad de espacio que utilizan los archivos de registro.

Si establece un valor del 2 al 9999, se retiene un máximo de 10 archivos de registro de diagnóstico rotatorios. Cada nombre de archivo indica el orden en que se ha creado. Cuando un archivo se llena, se crea el siguiente archivo. Cuando se llena el décimo archivo, se suprime el archivo más antiguo y se crea un nuevo archivo. A continuación, se muestra un ejemplo de cómo serían los archivos de registro rotatorios:

```
db2diag.14.log, db2diag.15.log, ... , db2diag.22.log, db2diag.23.log
```

Cuando db2diag.23.log está lleno, se suprime db2diag.14.log y se crea db2diag.24.log.

El servidor comprueba el espacio de archivo que contiene los archivos de registro de diagnóstico cada hora. Aparecen mensajes cada 12 horas si se produce alguna de las siguientes condiciones:

- El espacio disponible en el sistema de archivos donde se encuentran los archivos de registro de diagnóstico es menor del 20% del espacio del sistema de archivos total.
- El espacio disponible en el sistema de archivos donde se encuentra el directorio de la instancia de servidor es menor que 1 GB.

Si especifica el valor 0, sólo se utiliza un archivo de registro, db2diag.log, para todos los mensajes de diagnóstico. No se imponen límites sobre el tamaño del archivo de registro.

Restricción: Debe supervisar el tamaño de los archivos de registro para asegurarse de que no utilizan todo el espacio disponible en el sistema de archivos. Si no hay suficiente espacio disponible, es posible que el servidor deje de responder.

## Sintaxis

---

```
.-1024-----.  
>>-DBDIAGLOGSize--+-megabytes+-----<<
```

## Parámetros

---

**megabytes**

Especifica el espacio que utilizan los archivos de registro de diagnóstico en megabytes. Especifique un valor del 2 al 9999, o bien el valor 0. El valor predeterminado es 1024.

Si especifica un valor del 2 al 9999, se utilizan archivos de registro rotatorios y el valor especifica el tamaño en megabytes de los 10 archivos en total. El valor se restablece a 1024 siempre que se reinicia el servidor.

Si especifica el valor 0, se utiliza un archivo de registro y no se impone ningún límite sobre su tamaño.

Si desea archivar mensajes, especifique el valor 0 para asegurarse de que el archivo db2diag.log puede utilizar todo el espacio disponible sin utilizar los archivos de registro rotativos.

Después de establecer el valor del parámetro megabytes en 0 utilizando la opción DBDIAGLOGSIZE, los mensajes se graban inicialmente en los archivos de registro rotativos. Tras reiniciar el servidor, los mensajes se graban en el archivo db2diag.log .

Consejo: Si especifica un valor del 2 al 9999 utilizando el archivo de opciones de servidor, dsmserv.opt, el valor no se reinicia automáticamente al iniciar el servidor. El valor sigue siendo el mismo hasta que se cambia o se elimina del archivo dsmserv.opt con el mandato SETOPT.

## Ejemplo: especificar un tamaño máximo de 5120 megabytes

---

Especificar el tamaño de los archivos de registro de diagnóstico en 5120 megabytes (5 GB):

```
dbdiaglogsize 5120
```

## Ejemplo: archivar los mensajes en un único archivo de registro

---

Archivar los mensajes especificando que éstos se graban en el archivo db2diag.log:

```
dbdiaglogsize 0
```

### Información relacionada:

[Información del producto DB2 V10.5](#)

## DBDIAGPATHFSTHRESHOLD

---

La opción DBDIAGPATHFSTHRESHOLD especifica un umbral para el espacio libre en el sistema de archivos o disco que contiene el archivo db2diag.log .

Cuando la cantidad de espacio libre es igual o menor que el umbral especificado, se muestra el mensaje de error ANR1545W . De forma predeterminada, el mensaje se muestra cuando el sistema de archivos o el disco tiene un 20% o menos de espacio de disco libre.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
>>-DBDIAGPATHFSTHreshold--percent-----<<
```

## Parámetro

---

porcentaje

Especifica el porcentaje de espacio disponible en el sistema de archivos. Los valores válidos están en el rango de 0 - 100. El valor predeterminado es 20.

Consejo: Para obtener mejores resultados, no configure un valor superior o inferior percent para el parámetro. Un valor bajo puede hacer que el sistema de archivos se llene antes de que pueda corregir el problema. Un sistema de archivos lleno puede dañar la base de datos del servidor. Un valor alto podría dar como resultado muchos mensajes ANR1545W en el registro de actividad del servidor.

## Ejemplo

---

Establezca el valor del umbral a 10%.

```
setopt DBDIAGPATHFSTH 10
```

## DBMEMPERCENT

---

Utilice esta opción para especificar el porcentaje de memoria del espacio de direcciones virtuales dedicado a procesos del gestor de bases de datos.

Si en el sistema se ejecutan aplicaciones distintas del servidor de IBM Spectrum Protect, asegúrese de que el valor permite la memoria adecuada para que puedan ejecutarse las otras aplicaciones.

## Sintaxis

---

```
>>-DBMEMPERCENT--+-porcentaje-+-----><
      '-AUTO-----'
```

## Parámetros

---

### porcentaje

Establezca un valor de 10 a 99.

### AUTO

El gestor de bases de datos establece el porcentaje automáticamente en un valor entre el 75 por ciento o el 90 por ciento de la RAM del sistema. El valor predeterminado es AUTO.

## Ejemplos

---

```
dbmempercent 50
```

## DBMTCPPORT

---

La opción DBMTCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del gestor de base de datos espera las peticiones de sesiones de cliente.

El número de puerto especificado debe estar reservado para el uso del gestor de bases de datos.

De forma predeterminada, el servidor IBM Spectrum Protect utiliza IPC (Interprocess Communications) para establecer conexiones para las primeras dos agrupaciones de conexiones, con un máximo de 480 conexiones para cada agrupación. Una vez establecidas las primeras 960 conexiones, el servidor IBM Spectrum Protect utiliza TCP/IP para cualquier conexión adicional.

## Sintaxis

---

```
>>-DBMTCPPort--número_puerto-----><
```

## Parámetros

---

### número\_puerto

Especifica el número del puerto TCP/IP en el que el servidor de bases de datos espera las comunicaciones del servidor. Los valores válidos son los enteros del 1024 al 65535.

El número de puerto predeterminado es el valor de la opción TCPPOINT del servidor más 50.000. Por ejemplo, si la opción TCPPOINT del servidor es 1500, el número de puerto de DBMTCPPORT predeterminado sería 51500.

Si la opción de servidor TCPPOINT es mayor que 9999, sume los últimos cuatro dígitos de su valor a 50000. Por ejemplo, si la opción TCPPOINT es 11500, se suma 1550 a 50000, que da como resultado un número de puerto de DBMTCPPORT de 51500.

## Ejemplo

---

```
dbmtcport 51500
```

## DEDUPREQUIRESBACKUP

---

La opción DEDUPREQUIRESBACKUP especifica si los volúmenes de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la deduplicación de datos pueden reclamarse y si los datos duplicados pueden descartarse antes de la realización de la copia de seguridad de las agrupaciones de almacenamiento.

Si el valor de esta opción es YES (el valor predeterminado), debe realizar la copia de seguridad de los datos en agrupaciones de almacenamiento de copia que no se hayan establecido para la eliminación de datos duplicados. Utilice el mandato BACKUP STGPOOL para efectuar una copia de seguridad de los datos en agrupaciones de almacenamiento de copias.

Tenga en cuenta que es posible que la reclamación de un volumen de una agrupación de almacenamiento establecida para la eliminación de datos duplicados no se produzca cuando el primer volumen puede seleccionarse. El servidor realiza comprobaciones adicionales para asegurarse de que se ha realizado una copia de seguridad de los datos de una agrupación de almacenamiento

configurada para la eliminación de los datos duplicados en una agrupación de almacenamiento de copia. Estas comprobaciones requieren más de una instancia de BACKUP STGPOOL antes de que el servidor reclame un volumen. Una vez que el servidor verifica que se ha realizado copia de seguridad de los datos, se reclama el volumen.

Puede cambiar esta opción dinámicamente con el comando SETOPT.

Atención: Para minimizar la posibilidad de que se produzca una pérdida de datos, no cambie el valor predeterminado de esta opción del servidor. Especifique el valor NO sólo si no tiene ninguna agrupación de almacenamiento de copia y no realiza copias de seguridad de agrupación de almacenamiento.

## Sintaxis

---

```
>>-DEDUPREQUIRESBACKUP---Yes+-----<<  
      '-No--'
```

## Parámetros

---

Yes

Especifica que debe realizarse la copia de seguridad de la agrupación de almacenamiento para que los volúmenes puedan reclamarse y para que los datos duplicados puedan descartarse. Este es el valor predeterminado.

No

Especifica que los volúmenes de las agrupaciones de almacenamiento de acceso secuencial primario configuradas para eliminación de datos duplicados se pueden reclamar y si no se realiza una copia de seguridad de las agrupaciones de almacenamiento, los datos duplicados pueden descartarse.

## Ejemplos

---

Especificar que no ha de realizarse la copia de seguridad de las agrupaciones de almacenamiento primarias de acceso secuencial que se han configurado para la eliminación de datos duplicados.

```
deduprequiresbackup no
```

## DEDUPTIER2FILESIZE

---

La opción DEDUPTIER2FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 2.

## Sintaxis

---

```
>>-DEDUPTIER2FILESIZE---nnn-----<<
```

## Parámetros

---

nnn

Especifica el tamaño de archivo, en gigabytes, a partir del cual el servidor de IBM Spectrum Protect empieza a utilizar el procesamiento de nivel 2 para la deduplicación de datos. Puede especificar un valor del 20 al 9999. El valor predeterminado es 100.

Nota: Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de la opción SERVERDEDUPTXNLIMIT, esta opción se ignora para la eliminación de datos duplicados del servidor. Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de CLIENTDEDUPTXNLIMIT, esta opción se ignora para la eliminación de duplicados de datos del cliente.

## Ejemplos

---

```
deduptier2filesize 550
```

## DEDUPTIER3FILESIZE

---

La opción DEDUPTIER3FILESIZE especifica con qué tamaño de archivo IBM Spectrum Protect empieza a utilizar la eliminación de datos duplicados de nivel 3.

## Sintaxis

---

```
>>-DEDUPTIER3FILESIZE--nnn-----<<
```

## Parámetros

---

nnn

Especifica el tamaño de archivo, en gigabytes, a partir del cual el servidor de IBM Spectrum Protect empieza a utilizar el procesamiento de nivel 3 para la deduplicación de datos. Puede especificar un valor del 90 al 9999. El valor predeterminado es 400.

- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de la opción SERVERDEDUPTXNLIMIT, esta opción se ignora para la eliminación de datos duplicados del servidor.
- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es mayor que el valor de CLIENTDEDUPTXNLIMIT, esta opción se ignora para la eliminación de duplicados de datos del cliente.
- Si el valor especificado o que se ha tomado como valor predeterminado para esta opción es menor que el valor especificado o que se ha tomado como valor predeterminado para DEDUPTIER2FILESIZE, el valor de DEDUPTIER2FILESIZE se utiliza para esta opción.

## Ejemplos

---

```
deduptier3filesize 1150
```

## DEVCONFIG

---

La opción DEVCONFIG especifica el nombre de un archivo en el que el usuario quiere que IBM Spectrum Protect almacene una copia de seguridad de la información de configuración del dispositivo.

IBM Spectrum Protect almacena la información siguiente en el archivo de configuración de dispositivos:

- Las definiciones de la clase de dispositivo creadas utilizando el mandato DEFINE DEVCLASS
- Definiciones de unidades creadas utilizando el mandato DEFINE DRIVE
- Definiciones de bibliotecas creadas utilizando el mandato DEFINE LIBRARY
- Información de inventario de biblioteca para las bibliotecas LIBTYPE=SCSI automatizadas
- Las definiciones de vía de acceso creadas utilizando el mandato DEFINE PATH
- Las definiciones de servidor creadas con el mandato DEFINE SERVER
- El nombre del servidor creado con el comando SET SERVERNAME
- La contraseña del servidor creada con el mandato SET SERVERPASSWORD

Nota:

- Solo se hace una copia de seguridad de las definiciones de vía de acceso con SRCTYPE=SERVER en el archivo de configuración del dispositivo. Las vías de acceso de SRCTYPE=DATAMOVER no se graban en el archivo.
- La información de la ubicación de volúmenes de biblioteca se almacena como comentarios (/...\*/) en el archivo de configuración de dispositivo siempre que se emitan los comandos CHECKIN LIBVOLUME, CHECKOUT LIBVOLUME y AUDIT LIBRARY para las bibliotecas SCSI.

Atención: Para restaurar la base de datos después de un siniestro, debe tener una copia del archivo de configuración del dispositivo actual. El archivo de configuración del dispositivo no se puede volver a crear.

Puede incluir una o varias opciones DEVCONFIG en el archivo de opciones de servidor. Si utiliza varias opciones DEVCONFIG, IBM Spectrum Protect actualiza y almacena automáticamente una copia de seguridad de la información de configuración del dispositivo en cada archivo especificado.

## Sintaxis

---

```
>>-DEVCONFig--nombre_archivo-----<<
```

## Parámetros

---

nombre\_archivo

Especifica el nombre del archivo en el que debe almacenarse una copia de seguridad de la información de configuración de dispositivos.

## Ejemplos

---

```
devconfig devices.sav
```

## DISABLEREORGTABLE

---

La opción DISABLEREORGTABLE especifica si está inhabilitada la reorganización de tabla para los nombres de tabla especificado en la lista de tablas.

Para utilizar la opción DISABLEREORGTABLE, debe detener el servidor, actualizar el archivo de opciones y, a continuación, reiniciar el servidor.

## Sintaxis

---

```
>>-DISABLEREORGTTable----tablelist-----><
```

## Parámetros

---

tablelist

Especifica una lista de nombres de tablas para la que está inhabilitada la reorganización de tabla. Si no especifica ningún nombre de tabla con la opción, o si la opción no está en el archivo de opciones, no hay ninguna tabla inhabilitada.

Restricción: Las tablas siguientes ya están excluidas del proceso de reorganización de tabla y no se pueden especificar para esta opción:

- STAGED\_EXPIRING\_OBJECTS
- STAGED\_OBJECT\_IDS
- BF\_DEREFERENCED\_CHUNKS
- BF\_QUEUED\_CHUNKS

## Ejemplo

---

```
DISABLEREORGTABLE BF_BITFILE_EXTENTS,REPLICATING_OBJECTS
```

## DISABLESCHEDS

---

La opción DISABLESCHEDS especifica si se desactivan las planificaciones de cliente y de administración durante una recuperación del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-DISABLEScheds---Yes+-----><  
      '-No--'
```

## Parámetros

---

Yes

Especifica que se desactivan las planificaciones de cliente y de administración.

No

Especifica que se activan las planificaciones de cliente y de administración.

## Ejemplos

---

```
disablescheds no
```

## DISPLAYLFINFO

---



La opción DISPLAYLFINFO especifica el modo en que los registros de contabilidad y las entradas de la tabla resumen informan sobre el nombre del nodo.

Cuando esta opción está activada, los registros de contabilidad y las entradas de la tabla resumen proporcionarán el valor node\_name(storage\_agent\_name) para el nombre del nodo. Si la opción no está activada, los registros de contabilidad y las entradas de la tabla resumen sólo proporcionarán node\_name para el nombre de nodo. El valor predeterminado es No.

## Sintaxis

---

```
>>-DISPLAYLFINFO---+Yes+-----<<
      '-No--'
```

## Parámetros

---

Yes

Especifica que los registros de contabilidad y las entradas de la tabla resumen informarán sobre el nombre del agente de almacenamiento

No

Especifica que los registros de contabilidad y las entradas de la tabla resumen no informarán sobre el nombre del agente de almacenamiento. Este es el valor predeterminado.

## Ejemplos

---

```
displaylfinfo yes
```

El resultado muestra el siguiente registro de contabilidad con el nombre de agente de almacenamiento visualizado (STA53):

```
5,0,ADSM,07/13/2004,15:35:14,COLIND-TUC(STA53),,WinNT,1,Tcp/Ip,1,0,0,0,
0,223,4063,0,0,222,7,8,3,1,4,0,0,0,0,3,0
```

La tabla resumen correspondiente también muestra el nombre del agente de almacenamiento:

```
HORA_INICIO: 2004-07-13 15:35:07.000000
END_TIME: 2004-07-13 15:35:14.000000
ACTIVITY: BACKUP
NUMBER: 8
ENTITY: COLIND-TUC (STA53)
COMMMETH: Tcp/Ip
ADDRESS: colind-tuc:2229
SCHEDULE_NAME:
EXAMINED: 0
AFFECTED: 223
FAILED: 0
BYTES: 4160875
IDLE: 8
MEDIAP: 1
PROCESSES: 1
SUCCESSFUL: YES
VOLUME_NAME:
DRIVE_NAME:
LIBRARY_NAME:
LAST_USE:
COMM_WAIT: 3
NUM_OFFSITE_VOLS:
```

## DNSLOOKUP

---

La opción DNSLOOKUP especifica si el servidor utiliza llamadas de API del sistema para determinar los nombres de servidor de nombres de dominio (DNS) de los sistemas que establecen contacto con el servidor.

## Sintaxis

---

```
>>-DNSLOOKUP---+Yes+-----<<
      '-No--'
```

## Parámetros

---

Yes

Especifica que el servidor obtiene los nombres DNS de los sistemas que establecen un contacto. El valor predeterminado es Yes.

No

Especifica que el servidor no obtiene los nombres DNS de los sistemas que establecen un contacto.

## Ejemplos

---

```
dnslookup yes
```

## DRIVEACQUIRERETRY

---

La opción DRIVEACQUIRERETRY le permite especificar el número de veces que el servidor reintentará la adquisición de una unidad en una biblioteca IBM® 349x. Si se comparte la biblioteca entre varias aplicaciones, puede parecer que sus unidades están disponibles en el servidor (mediante un proceso subordinado de sondeo), cuando en realidad no lo están.

Esta opción es válida solamente si ha especificado 3494SHARED YES en el archivo de opciones dsmserv.opt. Si ha especificado DRIVEACQUIRERETRY NEVER, debe supervisar el tiempo durante el que los archivos han estado esperando unidades y el tiempo durante el que el servidor ha estado sondeando las unidades. Puede que también tenga que comprobar el estado de estas unidades en los demás servidores de IBM Spectrum Protect. Puede haber cartuchos en las unidades y los demás servidores de IBM Spectrum Protect pueden haber marcado las unidades como *desactivadas*. Si éste es el caso, tendrá que marcar las unidades como *desactivadas* en el servidor de IBM Spectrum Protect que está sondeando las unidades. Si es necesario, cancele también los trabajos en espera.

## Sintaxis

---

```
>>-DRIVEACQuireretry--+-Forever-----+-----<<
                        +-Never-----+
                        '-número_de_reintentos-'
```

## Parámetros

---

Forever

La adquisición de una unidad se reintentará hasta que se ha adquirido una correctamente. Este es el valor predeterminado.

Never

El servidor no reintentará la adquisición de una unidad y cancela la operación.

número\_de\_reintentos

Especifica el número máximo de veces, de 1 a 9999, que el servidor reintentará la adquisición de una unidad.

## Ejemplos

---

Especificar que el servidor debe intentar 10 veces como máximo adquirir la unidad.

```
driveacquireretry 10
```

## ENABLENASDEDUP

---

La opción de servidor ENABLENASDEDUP especifica si el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos de almacenamiento conectado a red (NAS). Esta opción solo se aplica a los servidores de archivos NetApp.

Si el valor de la opción es NO, los datos almacenados mediante el servidor de archivos se omiten durante el proceso de identificación de duplicados. Si el valor de esta opción es YES, el valor del parámetro DEDUPLICATE en la definición de agrupación de almacenamiento debe ser YES.

## Sintaxis

---

```
>>-ENABLENASDEDUP--+-No--+-+-----<<
                        '-Yes-'
```

## Parámetros

---

Yes

Especifique que el servidor de IBM Spectrum Protect optimiza el almacenamiento de los datos almacenados por un servidor de archivos NetApp.

No

Especifica que el servidor no optimiza el almacenamiento de los datos almacenados mediante el servidor de archivos NetApp.

## Ejemplo

---

Especifique que el servidor optimiza el almacenamiento de los datos almacenados por un servidor de archivos NetApp.

```
enablenasdedup yes
```

## EVENTSERVER

---

La opción EVENTSERVER especifica si, en el momento del arranque, el servidor debe intentar establecer contacto con el servidor de eventos.

## Sintaxis

---

```
>>-EVENTSERVer--+-Yes-+-----><
                '-No--'
```

## Parámetros

---

Yes

Especifica que, en el momento del arranque, el servidor intenta establecer contacto con el servidor de eventos. El contacto se establece sólo si ya se ha emitido un comando DEFINE EVENTSERVER. Este es el valor predeterminado.

No

Especifica que, en el momento del arranque, el servidor no intenta establecer contacto con el servidor de eventos.

## Ejemplos

---

```
eventserver yes
```

## EXPINTERVAL

---

La opción EXPINTERVAL especifica el intervalo, en horas, que ha de transcurrir entre los procesos automáticos de caducidad de inventario que realiza IBM Spectrum Protect. El proceso de caducidad de inventario elimina las copias de seguridad y las copias archivadas del servidor, según se haya especificado mediante las clases de gestión a las que están vinculados los archivos del cliente. Si no se ejecuta periódicamente el proceso de caducidad, no se reclamará el espacio de agrupación de almacenamiento de los archivos del cliente caducados, y el servidor necesitará más espacio de almacenamiento del que necesita según la política.

También puede utilizar el comando EXPIRE INVENTORY para arrancar manualmente el proceso de caducidad de inventario. El proceso de caducidad puede poner espacio disponible en sus agrupaciones de almacenamiento para copias archivadas o copias de seguridad del cliente adicionales.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
                .-24----.
>>-EXPINterval--+-horas+-----><
```

## Parámetros

---

horas

Especifica el tiempo, en horas, entre procesos automáticos de caducidad de inventario. Puede especificar de 0 a 336 (14 días). El valor 0 significa que el proceso de caducidad debe iniciarse con el comando EXPIRE INVENTORY. El valor predeterminado es 24.

## Ejemplos

---

## EXPQUIET

---

La opción EXPQUIET especifica si IBM Spectrum Protect ha de enviar mensajes detallados durante el proceso de caducidad.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

### Sintaxis

---

```
>>-EXPQUIet---+- --No-+-----><
      '- --Sí-'
```

### Parámetros

---

No

Especifica que el servidor envía mensajes detallados. Este es el valor predeterminado.

Yes

Especifica que el servidor sólo envía mensajes mínimos. Estos mensajes se envían únicamente para los archivos que se han caducado según el grupo de copia de la clase de gestión predeterminada o del período de gracia de retención del dominio.

### Ejemplos

---

```
expquiet no
```

 Sistemas operativos Linux

## FASPBEGPORT

---

La opción FASPBEGPORT especifica el número inicial en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

Para definir el rango de números de puerto, especifique las opciones FASPBEGPORT y FASPENDDPORT.

### Sintaxis

---

```
      .-15100-----.
>>-FASPBEGPort--+- número_puerto_inicial-+-----><
```

### Parámetros

---

número\_puerto\_inicial

Especifica el número de puerto inicial para las comunicaciones de red que utilizan la tecnología Aspera FASP. El valor predeterminado es 15100.

Solicite al administrador de red que le ayude a definir el rango de números de puerto:

- Si no ha habilitado el protocolo SSL (capa de sockets seguros) para el par de servidores, asegúrese de que los puertos puedan utilizarse para sockets TCP (protocolo de control de transmisiones).
- Asegúrese de que los puertos puedan utilizarse para conexiones UDP (User Datagram Protocol).
- Asegúrese de que los puertos sean compatibles con las reglas de cortafuegos.

### Ejemplo


---

Si las reglas del cortafuegos requieren que los números de puerto sean mayores que 1800, debe especificar un número de puerto mínimo de 1801:

```
faspbegport 1801
```

**Referencia relacionada:**

FASPENDDPORT

 Sistemas operativos Linux

## FASPENDDPORT

---

La opción FASPENDDPORT especifica el número final en el rango de números de puerto que se utilizan para las comunicaciones de red con la tecnología Aspera Fast Adaptive Secure Protocol (FASP).

Para definir el rango de números de puerto, especifique las opciones FASPBEGPORT y FASPENDDPORT.

### Sintaxis

---

```
.-15199-----.  
>>-FASPENDDport--+número_puerto_final+-----<<
```

### Parámetros

---

número\_puerto\_final

Especifica el número de puerto final para las comunicaciones de red que utilizan la tecnología Aspera FASP. El valor predeterminado es 15199.

Solicite al administrador de red que le ayude a definir el rango de números de puerto:

- Si no ha habilitado el protocolo SSL (capa de sockets seguros) para el par de servidores, asegúrese de que los puertos puedan utilizarse para sockets TCP (protocolo de control de transmisiones).
- Asegúrese de que los puertos puedan utilizarse para conexiones UDP (User Datagram Protocol).
- Asegúrese de que los puertos sean compatibles con las reglas de cortafuegos.

### Ejemplo


---

Si las reglas de cortafuegos requiere números de puerto inferiores a 1900, debería especificar un número de puerto máximo de 1899:

```
faspndport 1899
```

**Referencia relacionada:**

FASPBEGPORT

 Sistemas operativos Linux

## FASPTARGETRATE

---

La opción FASPTARGETRATE especifica la tasa de destino para la transferencia de datos con la tecnología Aspera Fast Adaptive Secure Protocol (FASP) Si especifica la tasa de destino, limita el ancho de banda de cada conexión de red que utiliza la tecnología Aspera FASP. De este modo, puede asegurarse de que hay suficiente ancho de banda disponible para todas las conexiones de red.

### Sintaxis

---

```
.-250000-----.  
>>-FaspTargetRate--+tasa_destino+-----<<
```

### Parámetros

---

tasa\_destino

Especifica la tasa máxima, en kilobits por segundo, para la transferencia de datos durante una sesión. El valor predeterminado es 250000. Puede especificar valores en un rango de 100 - 100000000.

Por ejemplo, si emite el mandato PROTECT STGPOOL para ejecutar dos operaciones paralelas en la tasa de destino predeterminado, el rendimiento agregado no supera los 500.000 kbps. Si el sistema de archivos da soporte a dos operaciones para proteger las agrupaciones de datos en tasas mucho más altas que 500.000 kbps de rendimiento agregado, y está disponible el ancho de banda de red suficiente, puede aumentar la tasa de destino.

Para determinar la tasa de destino apropiada, consulte a su administrador de red.

### Ejemplos

---

Si el ancho de banda de red asignado es de 150.000 kbps, puede establecer la tasa de destino en 75.000 y utilizar el número de sesiones predeterminado (dos) para el mandato PROTECT STGPOOL.

```
fasptargetrate 75000
```

En una configuración blueprint de gran tamaño, si el ancho de red asignado es de 6.000,000 kbps, puede establecer la tasa de destino en 750.000 y utilizar ocho sesiones para el mandato PROTECT STGPOOL.

```
fasptargetrate 750000
```

## FFDCLOGLEVEL

---

La opción FFDCLOGLEVEL especifica el tipo de mensajes del servidor generales que se muestran en el registro FFDC (First Failure Data Capture).

El registro FFDC contiene tres categorías de mensajes generales del servidor. Si se establece la opción FFDCLOGLEVEL, las siguientes categorías resultan afectadas:

- FFDC\_GENERAL\_SERVER\_INFO
- FFDC\_GENERAL\_SERVER\_WARNING
- FFDC\_GENERAL\_SERVER\_ERROR

### Sintaxis

---

```
.-FFDCLOGLevel-----ALL-----.  
>>+-FFDCLOGLevel-----+ALL--+-----><  
      +-WARN--+  
      '-ERRor-'
```

### Parámetros

---

ALL

Especifica que todos los mensajes generales FFDC de registro del servidor están en el registro. Este es el valor predeterminado.

WARN

Especifica que aparecen los mensajes FFDC\_GENERAL\_SERVER\_WARNING y FFDC\_GENERAL\_SERVER\_ERROR en el registro.

ERRor

Especifica que solo aparecen los mensajes FFDC\_GENERAL\_SERVER\_ERROR en el registro.

### Ejemplo

---

```
ffdcloglevel warn
```

## FFDCLOGNAME

---

La opción FFDCLOGNAME especifica un nombre del registro FFDC (First Failure Data Capture).

El archivo de registro FFDC se utiliza para recopilar información de diagnóstico sobre el servidor. Cuando ocurre un error, los datos sobre el error se escriben en el archivo de registro FFDC. Esta información se puede proporcionar al soporte de IBM para ayudar a diagnosticar problemas. El archivo de registro FFDC se encuentra en el directorio de la instancia del servidor.

### Sintaxis

---

```
.-dsmffdc.log----.  
>>-FFDCLOGNAME--+nombre_archivo+-----><
```

### Parámetros

---

nombre\_archivo

Especifica un nombre de archivo para el archivo de registro FFDC. El nombre de archivo puede ser un nombre de archivo totalmente calificado o un nombre de archivo relativo al directorio de la instancia del servidor. El valor predeterminado es dsmffdc.log.

## Ejemplos

---

```
ffdclogname /tsminst1/tsmffdc.log
ffdclogname tsmffdc.log
ffdclogname c:\tsmserv1\tsmffdc.log
```

### Referencia relacionada:

FFDCMAXLOGSIZE  
FFDCNUMLOGS

## FFDCMAXLOGSIZE

---

La opción FFDCMAXLOGSIZE especifica el tamaño del archivo de registro FFDC (First Failure Data Capture).

El archivo de registro FFDC se utiliza para recopilar información de diagnóstico sobre el servidor. Cuando ocurre un error, los datos sobre el error se escriben en el archivo de registro FFDC. Esta información se puede proporcionar al soporte de IBM para ayudar a diagnosticar problemas.

## Sintaxis

---

```
          .-1024-----.
>>-FFDCMAXLOGSIZE--+-kilobytes+-----><
```

## Parámetros

---

kilobytes

Especifica el tamaño máximo en que puede crecer FFDC antes del reinicio. El valor mínimo es 500. El valor máximo es 2097151. El valor predeterminado es 1024.

Para permitir que el tamaño del archivo de registro crezca indefinidamente, especifique un valor de -1. Para inhabilitar el registro, establezca el valor en -1.

## Ejemplos

---

```
ffdcmaxlogsize 2000
```

### Referencia relacionada:

FFDCLOGNAME  
FFDCNUMLOGS

## FFDCNUMLOGS

---

La opción FFDCNUMLOGS especifica el número de archivos de registro que se pueden utilizar para el registro circular. El valor predeterminado es 10.

El registro circular utiliza un anillo de archivos de registro para proporcionar recuperación de las anomalías de transacción y de bloqueos del sistema. Por ejemplo, cuando el archivo dsmffcd.log es nulo, se renombra a dsmffdc.log.1. Si el archivo dsmffdc.log.1 existe, el archivo dsmffdc.log.1 se renombra a dsmffdc.log.2. Si existe dsmffdc.log.2, el archivo dsmffdc.log.2 se renombra a dsmffdc.log.3 y así sucesivamente hasta que se alcanza el valor de FFDCNUMLOGS. Si hay un archivo de registro que se renombra como el valor de FFDCNUMLOGS, dicho archivo de registro se suprime.

El valor mínimo es 1. El valor máximo es 100. El valor predeterminado es 10.

## Sintaxis

---

```
          .-10----.
>>-FFDCNUMLOGS--+-valor+-----><
```

## Parámetros

---

valor

Especifica el número de archivos de registro que se utilizan para el registro circular.

Si especifica el valor 1 y el tamaño del archivo de registro alcanza FFDCMAXLOGSIZE, el servidor continúa escribiendo el archivo de registro. Cualquier información de registro se sobrescribe y el servidor continúa escribiendo el archivo de registro.

## Ejemplos

---

```
ffdcnumlogs 20
```

## FILEEXIT

---

La opción FILEEXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es un registro del archivo.

## Sintaxis

---

```
>>-FILEEXIT--+-No--+-nombre_archivo--+-REPLACE--+------><
      '-Yes-'                +-APPEND---+
                              '-PRESERVE-'
```

## Parámetros

---

Yes

Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.

No

Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el comando BEGIN EVENTLOGGING.

nombre\_archivo

Especifica el nombre del archivo en el que se han de almacenar los eventos.

REPLACE

Especifica que si existe el archivo, se sobregabará.

APPEND

Especifica que si ya existe un archivo, se agregarán los datos al mismo.

PRESERVE

Especifica que si existe el archivo, no se sobregabará.

## Ejemplos

---

 Sistemas operativos Windows

```
fileexit yes \tsm\server\data replace
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
fileexit yes /tsm/server/data replace
```

## FILETEXTXIT

---

La opción FILETEXTXIT especifica el archivo al que se direccionan los eventos activados. Todo evento anotado cronológicamente es una línea con un tamaño fijo que puede leerse.

## Sintaxis

---

```
>>-FILETEXTXIT--+-No--+-nombre_archivo--+-REPLACE--+------><
      '-Yes-'                +-APPEND---+
                              '-PRESERVE-'
```



## Parámetros

---

Yes

Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.

No

Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el comando BEGIN EVENTLOGGING.

nombre\_archivo

Especifica el nombre del archivo en el que se han de almacenar los eventos.

REPLACE

Especifica que si existe el archivo, se sobregabará.

APPEND


Especifica que si existe el archivo, se agregarán los datos al mismo.

PRESERVE

Especifica que si existe el archivo, no se sobregabará.

## Ejemplos

---

 Sistemas operativos Windows

```
filetextexit yes \tsm\server\data replace
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
filetextexit yes /tsm/server/data replace
```

## FSUSEDTHRESHOLD

---

La opción FSUSEDTHRESHOLD especifica qué porcentaje del sistema de archivos puede llenar la base de datos antes emitir un mensaje de alerta.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

Si este valor se establece en un número bajo, las anotaciones de actividades pueden inundarse con mensajes que indiquen que el espacio de base de datos se ha llenado, incluso si todavía queda espacio disponible. Si el valor establecido es demasiado alto, el espacio de base de datos puede llenarse antes de poder agregar más espacio al sistema de archivos.

## Sintaxis

---

```
>>-FSUSEDThreshhold--percent-----<<
```

## Parámetros

---

porcentaje

Especifica el valor del espacio utilizado en la base de datos. Puede especificar un valor entre 0 y 100. El valor predeterminado es 90.

## Ejemplos

---

```
fsusedthreshold 70
```

## IDLETIMEOUT

---

La opción IDLETIMEOUT especifica el período de tiempo, en minutos, durante el que una sesión de cliente puede estar desocupada antes de que la cancele el servidor. Puede aumentar el valor de tiempo de espera para evitar que los clientes excedan el tiempo de espera si existe una gran carga en la red del entorno. Observe, sin embargo, que una gran cantidad de sesiones desocupadas puede impedir que otros usuarios puedan conectarse al servidor.

La opción de servidor IDLETIMEOUT se utiliza en las sesiones no administrativas. Consulte la opción ADMINIDLETIMEOUT para las sesiones de cliente administrativas.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el comando SETOPT.

## Sintaxis

---

```
.-15-----.  
>>-IDLETimeout--+-minutos+-----<<
```

## Parámetros

---

minutos

Especifica el número máximo de minutos que el servidor espera a un cliente desocupado. El valor predeterminado es de 15 minutos. El valor mínimo es de 1 minuto.

## Ejemplos

---

```
idletimeout 15
```

## KEEPALIVE

---

La opción KEEPALIVE especifica si la función keepalive del protocolo de control de transmisiones (TCP) está habilitada para los sockets TCP de salida. La función keepalive TCP envía una transmisión de un dispositivo a otro para comprobar que el enlace entre los dos dispositivos está operativo.

Si está utilizando la réplica de nodo, puede utilizar la opción KEEPALIVE en el servidor de réplica fuente para habilitar la función keepalive de TCP. La opción KEEPALIVE no es necesaria en el servidor de réplica de destino, a menos que especifique la réplica bidireccional, en cuyo caso el servidor de destino se convierte en el servidor de réplica fuente.

## Sintaxis

---

```
.-Yes-.  
>>-KEEPALIVE--+-No--<<
```

## Parámetros

---

Yes

Especifica que la función keepalive de TCP está habilitada para los sockets TCP de salida. Este es el valor predeterminado. Si la opción KEEPALIVE está habilitada, se utilizan los valores predeterminados para las opciones KEEPALIVETIME y KEEPALIVEINTERVAL.

No

Especifique que la función keepalive de TCP no está habilitada para los sockets TCP de salida. Si especifica un valor de NO, no afecta a las conexiones de socket TCP actuales que se han originado de solicitudes de conexión de salida mientras la opción KEEPALIVE estaba establecida en YES. El valor YES se aplica a estos sockets, hasta que la sesión relacionada finalizada y el socket se cierra.

## Ejemplo

---

Utilice el mandato SETOPT para habilitar la función keepalive sin inhabilitar o detener el servidor:

```
setopt keepalive yes
```

**Referencia relacionada:**

KEEPALIVEINTERVAL  
KEEPALIVETIME

## KEEPALIVETIME

---

La opción KEEPALIVETIME especifica la frecuencia con la que TCP envía una transmisión de estado activo cuando recibe una respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.

## Sintaxis

---

```
.-300-----.  
>>-KEEPALIVETIME--+-segundos-+-----<<
```

## Parámetros

---

seconds

Especifica la frecuencia con la que TCP envía transmisiones de estado activo para verificar que una conexión inactiva sigue activa. El valor se especifica en segundos.

Puede especificar un valor en el rango de 1 a 4294967. El valor predeterminado es 300 (5 minutos).

## Ejemplo

---

Establezca la opción KEEPALIVETIME en 120 segundos:

```
keepalivetime 120
```

**Referencia relacionada:**

KEEPALIVE

KEEPALIVEINTERVAL

## KEEPALIVEINTERVAL

---

La opción KEEPALIVEINTERVAL especifica la frecuencia con la que se envía una transmisión de estado activo, si no se recibe ninguna respuesta. Esta opción solo se aplica si establece la opción KEEPALIVE en YES.

## Sintaxis

---

```
.-30-----.  
>>-KEEPALIVEINTERVAL--+-segundos-+-----<<
```

## Parámetros

---

seconds

Especifica la longitud de tiempo, en segundos, entre las transmisiones de estado activo, cuando no se recibe ninguna respuesta. El valor se especifica en segundos.

Puede especificar un valor en el rango de 1 a 4294967. El valor predeterminado es 30 segundos.

## Ejemplo

---

Establezca la opción KEEPALIVEINTERVAL en 45 segundos:

```
keepaliveinterval 45
```

**Referencia relacionada:**

KEEPALIVE



KEEPALIVETIME


## LANGUAGE

---

La opción LANGUAGE controla la inicialización de los entornos nacionales. Un entorno nacional incluye el idioma y los formatos de fecha, hora y número que se han de utilizar para la consola y el servidor.

Si el cliente y el servidor se ejecutan en idiomas diferentes, es posible que los mensajes que se generen puedan ser incomprensibles cuando los mensajes se emiten desde el cliente al servidor o si el servidor envía la salida al cliente.

 Sistemas operativos AIX  Sistemas operativos Linux Si la inicialización del entorno nacional no se ejecuta correctamente, el servidor tomará, de forma predeterminada, el entorno correspondiente al inglés de Estados Unidos.

 Sistemas operativos Windows Si falla la inicialización del entorno nacional, el servidor toma de forma predeterminada el inglés americano y utiliza los formatos de fecha, hora y número que están establecidos mediante las opciones del servidor DATEFORMAT, TIMEFORMAT y NUMBERFORMAT.

```

(1)
>>-LANGUage--+-AMENG----->>
      |         (2)         |
      +-en_US-----+
      |         (3)         |
      '-entorno_local-----'


```

Notas:



1. AMENG sólo está disponible en HP-UX, Solaris, Windows.
2. en\_US sólo está disponible en AIX y Linux.
3. *entorno\_local* sólo está disponible en AIX, HP-UX, Solaris, Linux y Windows.

## Parámetros

 Sistemas operativos Windows AMENG

 Sistemas operativos Windows Especifica que se utilice el inglés americano como idioma predeterminado para el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux en\_US

 Sistemas operativos AIX  Sistemas operativos Linux Especifica que se utilice el inglés americano como idioma predeterminado para el servidor.

entorno\_local

Especifica el nombre del entorno local al que el servidor da soporte. Consulte las tablas siguientes para obtener información sobre los entornos nacionales soportados por el sistema operativo.

Nota: IBM Spectrum Protect ejecuta cualquier entorno nacional pero el valor predeterminado es inglés de EE.UU. Se dispone de soporte de idiomas para todos los entornos nacionales que figuran en la lista.


 Sistemas operativos AIX

Tabla 1. Idiomas del servidor para AIX

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
Chino, simplificado	Zh_CN
Chino, simplificado (UTF-8)	ZH_CN
Chino, tradicional (Big5)	Zh_TW
Chino, tradicional (UTF-8)	ZH_TW
Chino, tradicional (euc_tw)	zh_TW
Inglés	en_US
Inglés (UTF-8)	EN_US
Francés	fr_FR
Francés (UTF-8)	FR_FR
Alemán	de_DE
Alemán (UTF-8)	DE_DE
Italiano	it_IT
Italiano (UTF-8)	IT_IT
Japonés, EUC	ja_JP
Japonés, PC	Ja_JP
Japonés, UTF8	JA_JP
Coreano	ko_KR
Coreano (UTF-8)	KO_KR
Portugués, de Brasil	pt_BR
Portugués, de Brasil (UTF-8)	PT_BR

Idioma	Valor de la opción LANGUAGE
Ruso	ru_RU
Ruso (UTF-8)	RU_RU
Español	es_ES
Español (UTF-8)	ES_ES

Nota a pie de tabla: El sistema debe tener instalado el soporte para el entorno en\_US.


 Sistemas operativos Linux

Tabla 2. Idiomas del servidor para Linux

LANGUAGE	Valor de la opción LANGUAGE
Chino, simplificado	zh_CN
	zh_CN.gb18030
	zh_CN.utf8
Chino, tradicional	Big5 / Zh_TW
	zh_TW
	zh_TW.utf8
Inglés de Estados Unidos	en_US
	en_US.utf8
Francés	fr_FR
	fr_FR.utf8
Alemán	de_DE
	de_DE.utf8
Italiano	it_IT
	it_IT.utf8
Japonés	ja_JP
	ja_JP.utf8
Coreano	ko_KR
	ko_KR.utf8
Portugués, de Brasil	pt_BR
	pt_BR.utf8
Ruso	ru_RU
	ru_RU.utf8
Español	es_ES
	es_ES.utf8


 Sistemas operativos Windows

Tabla 3. Idiomas del servidor para Windows

Idioma	Valor de la opción LANGUAGE
Chino, simplificado	chs
Chino, tradicional	cht
Inglés	ameng
Francés	fra
Alemán	deu
Italiano	ita
Japonés	jpn
Coreano	kor

Idioma	Valor de la opción LANGUAGE
Portugués, de Brasil	ptb
Ruso	rus
Español	esp

## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux

lang ja\_JP

 Sistemas operativos Windows

lang jpn

## LDAPCACHEDURATION

La opción LDAPCACHEDURATION determina la cantidad de tiempo que el servidor IBM Spectrum Protect almacena en memoria caché la información de autenticación de contraseña LDAP.

Después de un enlace LDAP satisfactorio, el valor que introduce determina la cantidad de tiempo que la información sobre el servidor de directorios LDAP está disponible. Cuanto mayor sea el número, mejor será el rendimiento del servidor de directorios LDAP. Sin embargo, durante el periodo de caché, los cambios en el servidor de directorios LDAP o tienen efecto inmediato en el nodo. Por ejemplo, puede que las contraseñas antiguas estén disponibles durante algún tiempo, incluso después de que se cambiaran o bloquearan en el servidor LDAP.

Incluya la opción LDAPCACHEDURATION en un mandato SETOPT para que la opción surta efecto inmediatamente.

Restricción: La opción LDAPCACHEDURATION no se aplica a los agentes de almacenamiento.

## Sintaxis

```
>>-LDAPCACHEDURATION - minutos-----<<
```

## Parámetros

minutos

Especifica la cantidad máxima de tiempo después de un enlace LDAP correcto, que las sesiones posteriores para el mismo nodo o administrador se saltan para operaciones de enlace LDAP secundarias. El rango de valores va de cero a 360 minutos.

## Ejemplo: establecer el valor LDAPCACHEDURATION a 6 horas (máximo)

En el archivo dsmserv.opt , especifique el siguiente valor:

```
ldapcacheduration 360
```

Después de que un nodo o administrador se autentica con un servidor de directorio externo, se salta el enlace LDAP para 360 minutos en todas las sesiones.

## LDAPURL

La opción LDAPURL especifica la ubicación de un servidor LDAP (Lightweight Directory Access Protocol). Establezca la opción de LDAPURL después de configurar el servidor LDAP.

Consejo: La información de esta documentación corresponde al método de autenticación LDAP preferido para servidores IBM Spectrum Protect V7.1.7 o posteriores. Para obtener instrucciones sobre la utilización del método de autenticación LDAP anterior, consulte Gestión de contraseñas y procedimientos de inicio de sesión.

Se aplican las restricciones siguientes:

- La opción LDAPURL no se puede utilizar en combinación con el mandato SETOPT.
- La opción LDAPURL no se aplica a los agentes de almacenamiento.

## Sintaxis

---

```
>>-LDAPURL--ldap_url_value-----<<
```

## Parámetros

---

### ldap\_url\_value

Especifica la dirección URL de un servidor de directorios LDAP, o los URL de varios servidores LDAP. Puede entrar múltiples valores, con cada valor de URL de hasta 1024 caracteres. El número de puerto es opcional y tiene un valor predeterminado de 389. Cada valor de URL debe contener un nombre de servidor LDAP. Por ejemplo, el formato del nombre de servidor es `server1.storage.us.ibm.com` y el puerto LDAP es 341. El valor de la opción LDAPURL debe cumplir las especificaciones siguientes:

- Si especifica varios URL, cada uno debe estar en una línea diferente.
- Si especifica varios URL, cada URL debe apuntar a un directorio externo diferente y todos los directorios externos deben contener los mismos datos.
- Cada URL debe empezar por `ldap://`.

Restricción: La URL que designe no puede comenzar con `ldaps://`.

IBM Spectrum Protect soporta conexiones LDAP aseguradas con una operación LDAPv3 StartTLS estándar que establece un intercambio TLS (Transport Layer Security) en una conexión LDAP existente. La operación LDAP Simple Bind que utiliza IBM Spectrum Protect no protege la contraseña cuando se envía. Se necesita una conexión TLS segura para proteger la contraseña.

## Ejemplo: establecer el valor port para un servidor LDAP

---

En el archivo `dmserv.opt`, especifique el valor del puerto como 341 para un servidor LDAP:

```
ldapurl ldap://server1.storage.us.ibm.com:341/dc=storage,dc=us,dc=ibm,dc=com
```

## MAXSESSIONS

---

La opción MAXSESSIONS especifica el número máximo de sesiones cliente simultáneas que se pueden conectar con el servidor.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
.-25-----.  
>>-MAXSessions--+número_de_sesiones+-----<<
```

## Parámetros

---

### número\_de\_sesiones

Especifica el número máximo de sesiones cliente simultáneas. El valor predeterminado es de 25 sesiones cliente. El valor mínimo es de 2 sesiones clientes. El valor máximo está limitado únicamente por el tamaño de almacenamiento virtual disponible o por los recursos de comunicaciones.

## Ejemplos

---

```
maxsessions 25
```

## MESSAGEFORMAT

---

La opción MESSAGEFORMAT especifica si se visualiza un número de mensaje en todas las líneas de un mensaje de varias líneas.

## Sintaxis

---

```
>>-MESSagEformat--número-----<<
```

## Parámetros

---

número

Seleccione un número para especificar si se ha de visualizar un número de mensaje únicamente en la primera línea de un mensaje de varias líneas o si se ha de visualizar en todas las líneas.

1

El número del mensaje sólo se visualiza en la primera línea del mensaje. Este es el valor predeterminado.

2

El número del mensaje se visualiza en todas las líneas de un mensaje.

## Ejemplos

---

```
messageformat 2
```

## MIRRORLOGDIRECTORY

---

La opción MIRRORLOGDIRECTORY especifica el directorio para duplicar la vía de acceso de registro activo.

Todos los cambios realizados en el directorio de anotaciones activas también se grabarán en este directorio de duplicación. Esta opción se añade al archivo de opciones cuando se ejecuta el mandato DSMSERV FORMAT. Normalmente, no es necesario cambiar el directorio.

## Sintaxis

---

```
>>-MIRRorlogdirectory--dir_name-----<<
```

## Parámetros

---

nombre\_dir

Especifica un nombre de directorio cualificado al completo para la duplicación de anotaciones activas. El número máximo de caracteres es 175.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux

```
mirrorlogdirectory /tsm/mirrorlog
```

 Sistemas operativos Windows

```
mirrorlogdirectory c:\tsmserv1\mirrorlog
```

## MOVEBATCHSIZE

---

La opción MOVEBATCHSIZE especifica el número de archivos cliente que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Este movimiento de datos es el resultado de las operaciones de restauración y copia de seguridad de agrupaciones de almacenamiento, de migración, reclamación y MOVE DATA. Esta opción funciona con la opción MOVESIZETHRESH.

## Sintaxis

---

```
.-1000-----.  
>>-MOVEBatchsize--+número_de_archivos-+-----<<
```

## Parámetros

---

número\_de\_archivos

Especifica un número de archivos entre 1 y 1000. El valor predeterminado es 1000.

## Ejemplos

---



movebatchsize 100

## MOVESIZETHRESH

---

La opción MOVESIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos que se trasladarán y agruparán en un lote, dentro de la misma transacción del servidor. Cuando se alcance este umbral, no se agregarán más archivos al lote actual, y se arrancará una nueva transacción después de que se haya trasladado el lote actual.

### Sintaxis

---

```
.-4096-----.  
>>-MOVESizethresh--+ megabytes+-----<<
```

### Parámetros

---

megabytes

Especifica el número de megabytes como un entero comprendido entre 1 y 32.768. El valor predeterminado es 4096. Esta opción se utiliza con la opción MOVEBATCHSIZE.

### Ejemplos

---

```
movesizethresh 500
```

## MSGINTERVAL

---

La opción MSGINTERVAL especifica el tiempo, en minutos, entre los mensajes que solicitan a un operador que monte una cinta para el servidor.

### Sintaxis

---

```
.-1-----.  
>>-MSGINterval--+ minutos+-----<<
```

### Parámetros

---

minutos

Especifica el intervalo de tiempo en que el servidor solicita al operador que monte una cinta. El valor predeterminado es de 1 minuto. El valor mínimo es de 1 minuto.

### Ejemplos

---

```
msginterval 2
```

 Sistemas operativos Windows

## NAMEDPIPENAME

---

La opción NAMEDPIPENAME especifica un método de comunicaciones que permite que los procesos se comuniquen entre sí sin tener que saber dónde los procesos del emisor y remitente están ubicados. El nombre actúa como un alias, y conecta los dos procesos independientemente de si están en el mismo sistema o en otros dominios conectados.

### Sintaxis

---

```
>>-NAMEPipename-- nombre-----<<
```

### Parámetros

---




nombre

Especifica el nombre de Named Pipes que debe utilizar el servidor. El protocolo Named Pipes es ideal en el caso de que el cliente y el servidor estén en la misma máquina. No es necesario ningún tipo de software de comunicaciones ni configuración.

## Ejemplos

---

```
namedpipename \\.\PIPE\TSMPIPE
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## NDMPCONNECTIONTIMEOUT

---

La opción de servidor NDMPCONNECTIONTIMEOUT especifica el tiempo, en horas, que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante las operaciones de restauración NDMP a través de la LAN. Las operaciones de restauración NDMP de sistemas de archivos NAS de gran tamaño puede tener periodos prolongados de inactividad. El valor predeterminado es 6.

## Sintaxis

---

```
                .-6-----.  
>>-NDMPCONNECTIONTIMEOUT--+-horas+-----<<
```

## Parámetros

---

horas

El número de horas que espera el servidor de IBM Spectrum Protect para recibir las actualizaciones de estado durante una operación NDMP a través de la LAN. El valor predeterminado es 6. El mínimo es de 1 hora. El valor máximo es 48 horas.

## Ejemplo

---

Especifique un tiempo de espera de 10 horas antes de que la conexión NDMP exceda el tiempo de espera.

```
ndmpconnectiontimeout 10
```

## NDMPCONTROLPORT

---

La opción NDMPCONTROLPORT especifica el número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP (Network Data Management Protocol). El servidor de IBM Spectrum Protect no funciona como un servidor de cintas NDMP de uso general.

## Sintaxis

---

```
                .-10000-----.  
>>-NDMPControlport--+-número_puerto+-----<<
```

## Parámetros

---

número\_puerto

El número de puerto que se va a utilizar para comunicaciones internas para determinadas operaciones NDMP. El número de puerto debe oscilar entre 1024 y 32767. El valor predeterminado es 10000.

## Ejemplos

---

```
ndmpcontrolport 9999
```

## NDMPENABLEKEEPALIVE

---

La opción del servidor NDMPENABLEKEEPALIVE especifica si el servidor de IBM Spectrum Protect habilita el mantenido en actividad de TCP (Transmission Control Protocol) en las conexiones control NDMP (network data-management protocol) en dispositivos NAS (network-attached storage). El valor predeterminado es NO.

El estado activo TCP se implementa en el soporte de red de un sistema operativo. El estado activo TCP impide que una conexión inactiva, de ejecución larga, se cierre mediante el software de cortafuegos, que detecta y cierra conexiones inactivas. Restricción: Para evitar errores, no habilite el estado activo TCP en determinados tipos de entornos. Un ejemplo son los entornos en los que no existen cortafuegos entre el servidor de IBM Spectrum Protect y un dispositivo NAS. Otro ejemplo son los entornos con cortafuegos que toleran conexiones inactivas de ejecución larga. La habilitación del estado activo TCP en este tipo de entornos puede hacer que una conexión inactiva se cierre inadvertidamente si el socio de conexión no puede responder temporalmente a paquetes de estado activo TCP.

## Sintaxis

---

```
>>-NDMPENABLEKEEPALIVES--+NO--+-----<<
      '-YES-'
```

## Parámetros


---

NO

Inhabilitar el estado activo TCP en todas las conexiones de control NDMP. NO es el valor predeterminado.

YES

Habilitar el estado activo TCP en todas las conexiones de control NDMP. El tiempo de inactividad predeterminado antes de que se envíe el primer paquete de estado activo TCP es de 120 minutos.


 Para cambiar el tiempo de inactividad, utilice la opción de servidor NDMPKEEPIDLEMINUTES.

## Ejemplo

---

Habilitar el estado activo TCP en todas las conexiones de control NDMP de modo que las conexiones NDMP inactivas no se cierren:

```
ndmpenablekeepalive yes
```



## NDMPKEEPIDLEMINUTES

---

La opción de servidor NDMPKEEPIDLEMINUTES especifica la cantidad de tiempo, en minutos, antes de que el sistema operativo transmita el primer paquete de estado activo TCP (Transmission Control Protocol) en una conexión de control NDMP (Network Data-Management Protocol). El valor predeterminado son 120 minutos.

Requisito previo: Utilice esta opción sólo después de establecer el valor de la opción de servidor NDMPENABLEKEEPALIVES en YES.

## Sintaxis

---

```
      .-120-----.
>>-NDMPKEEPIDLEMINUTES--+minutes+-----<<
```

## Parámetros

---

minutos

El número de minutos de inactividad en conexiones de control NDMP antes de que se transmitan paquetes de estado activo TCP. El valor predeterminado es 120. El mínimo es 1 minuto. El máximo es de 600 minutos.

## Ejemplo

---

Especificar un tiempo de inactividad de 15 minutos antes de que se envíe el primer paquete de estado activo TCP:

```
ndmpkeepidleminutes 15
```

## NDMPPORTRANGE

---

La opción NDMPPORTRANGE especifica el rango de números de puerto por los que IBM Spectrum Protect pasa en secuencia para obtener un número de puerto para aceptar una sesión de un dispositivo NAS (almacenamiento conectado a red) para la transferencia de

datos. El valor predeterminado es 0,0, que significa que IBM Spectrum Protect deja que el sistema operativo proporcione un puerto (puerto efímero).

Si todos los puertos especificados están en uso cuando un dispositivo NAS intenta conectarse con el servidor, la operación no se ejecuta correctamente. Si se selecciona un único número de puerto (sin comas y sin ningún número de puerto para el valor alto), el valor predeterminado para el número de puerto alto es el número de puerto bajo más 100).

Cuando los datos NDMP (Network Data Management Protocol) se dirigen a una agrupación nativa de IBM Spectrum Protect, la comunicación puede iniciarse desde los sistemas NDMP o desde el servidor de IBM Spectrum Protect. Si existe un cortafuegos que separa el servidor y los dispositivos NAS, puede que sea necesario especificar números de puerto en las reglas del cortafuegos para permitir que fluya tráfico hasta y desde los dispositivos NAS. Los dispositivos NAS comunican al servidor de IBM Spectrum Protect los números de puerto que se utilizarán cuando se establezca contacto con el servidor. Los números de puerto del servidor se controlan con las opciones NDMPPortrange. El control del número de puerto para los dispositivos NAS es específico de los proveedores. Consulte la documentación del proveedor.

## Sintaxis

---

```
>>-NDMPPortrange--número_puerto_bajo+-----+---<  
                    '-,número_puerto_alto-'
```

## Parámetros

---

*número\_puerto\_bajo*

El número de puerto bajo desde el que IBM Spectrum Protect inicia el ciclo cuando necesita un número de puerto para aceptar una sesión de un dispositivo NAS para la transferencia de datos. El valor mínimo del número de puerto es 1024.

*número\_puerto\_alto*

El número de puerto alto hasta el que puede llegar IBM Spectrum Protect cuando necesita un número para aceptar una sesión de un dispositivo NAS para la transferencia de datos. El valor máximo del número de puerto es 32767. El número de puerto alto debe ser el mismo o más grande que el número de puerto bajo.

## Ejemplos

---

Especifique que IBM Spectrum Protect puede pasar por los números de puerto 1024 a 2024.

```
ndmpportrange 1024,2024
```

## NDMPREFDATAINTERFACE

---

Esta opción especifica la dirección IP que se asocia a la interfaz en la que desea que el servidor reciba todos los datos de copia de seguridad NDMP (Network Data Management Protocol).

Esta opción afectará a todas las operaciones de archivador a servidor NDMP posteriores, pero no afectará a las conexiones de control NDMP, que utilizan la interfaz de red predeterminada del sistema. El valor de esta opción es un nombre de host o una dirección IPV4 que se asocia a una de las interfaces de red activas del sistema en el que se ejecuta el servidor de IBM Spectrum Protect. Esta interfaz debe haberse activado para IPV4.

Puede actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor con el mandato SETOPT.

## Sintaxis

---

```
>>-NDMPREFDATAINTERFACE--dirección_ip-----<
```

## Parámetros

---

*dirección\_ip*

Especifique una dirección en formato decimal con puntos o en formato de nombre de host. Si especifica una dirección decimal con puntos, ésta no se verificará con un servidor de nombres de dominio. Si la dirección no es correcta, puede que se produzcan errores cuando el servidor intente abrir un socket durante el inicio de una copia de seguridad de archivador a servidor NDMP.

Las direcciones con formato de nombre de host se verifican con un servidor de nombres de dominio. No existe un valor predeterminado. Si no se establece ningún valor, todas las operaciones NDMP utilizan la interfaz de red del servidor de IBM

Spectrum Protect para recibir los datos de copia de seguridad durante las operaciones de copia de seguridad de archivador a servidor NDMP.

Para borrar el valor de la opción, especifique el comando SETOPT con un valor nulo, "".

## Ejemplos:

---

```
ndmpprefdatainterface net1.tucson.ibm.com
```

```
ndmpprefdatainterface 9.11.152.89
```

## NOPREEMPT

---

El servidor permite que determinadas operaciones tengan prioridad sobre otras operaciones para acceder a volúmenes y dispositivos. Puede especificar la opción NOPREEMPT para desactivar la prioridad. Cuando se desactiva la prioridad, ninguna operación puede tener prioridad sobre otra para acceder a un volumen, y únicamente una operación de copia de seguridad de base de datos puede tener prioridad sobre otra operación para acceder a un dispositivo.

Por ejemplo, una operación de restauración de datos de cliente tiene prioridad sobre una operación de copia de seguridad de datos cliente para utilizar un dispositivo específico o para acceder a un volumen específico.

## Sintaxis

---

```
>>-NOPREEMPT-----<
```

## Parámetros

---

Ninguno

## Ejemplos

---

No permitir que ninguna operación del servidor se adelante a otra:

```
nopreempt
```

## NORETRIEVEDATE

---

La opción NORETRIEVEDATE especifica que el servidor no actualiza la fecha de recuperación de un archivo en una agrupación de almacenamiento en disco cuando un cliente restaura o recupera el archivo. Esta opción y el parámetro MIGDELAY de agrupación de almacenamiento controlan cuándo el servidor migra los archivos.

Si no se especifica NORETRIEVEDATE, el servidor migra los archivos una vez han estado en la agrupación de almacenamiento el número de días que especifica el parámetro MIGDELAY. El número de días se cuenta a partir del día en que el archivo se almacenó en la agrupación de almacenamiento o un cliente lo recuperó, lo que sea más reciente. Si especifica NORETRIEVEDATE, el servidor no actualiza la fecha de recuperación de un archivo ni el número de días contados a partir del día en que el archivo entró en la agrupación de almacenamiento en disco.

Si se especifica esta opción y está activada la función de caché para una agrupación de almacenamiento de disco, las operaciones de reclamación de espacio en caché resultarán afectadas. Cuando se necesita espacio en una agrupación de almacenamiento de disco que contiene archivos en caché, el servidor obtiene el espacio borrando las copias en caché de forma selectiva. Los archivos que tienen las fechas de recuperación más antiguas y que ocupan la mayor cantidad de espacio son los que se seleccionan para suprimirlos. Cuando se especifica NORETRIEVEDATE, el servidor no actualiza la fecha de recuperación cuando se recupera un archivo. Esto puede ocasionar que se supriman las copias en caché aunque un cliente las haya recuperado recientemente.

## Sintaxis

---

```
>>-NORETRIEVEDATE-----<
```

## Parámetros

---

Ninguno.

## Ejemplos

---

Especificar que no se actualizan las fechas de recuperación de los archivos en las agrupaciones de almacenamiento en disco cuando los clientes restauran y recuperan archivos:

```
noretrieve date
```

 Sistemas operativos Windows

## NPAUDITFAILURE

---

La opción NPAUDITFAILURE especifica si ha de enviarse un evento a las anotaciones de eventos cuando un nodo se conecte con el servidor utilizando un nombre que se encuentra en el grupo de Windows pero que no coincide con el nombre de inicio de sesión de cuenta de Windows. Para garantizar que un nodo pueda acceder sólo a sus propios datos, el nombre del nodo y el nombre de cuenta Windows deben coincidir.

### Sintaxis

---

```
>>-NPAUDITFailure--+-Yes+-----<<  
          '-No--'
```

### Parámetros

---

Yes

Especifica que un evento se envía a las anotaciones de eventos cuando un nodo inicia una sesión en el servidor con un nombre que forma parte del grupo Windows. Sin embargo, este nombre no coincide con el nombre de inicio de sesión de la cuenta Windows con el que ha iniciado la sesión.

No

Especifica que no se enviará un evento de anomalía de auditoría a las anotaciones de eventos.

## Ejemplos

---

Especifique que se envíe un evento a las anotaciones de eventos cuando un nodo inicie una sesión en el servidor con un nombre que forme parte del grupo Windows. Sin embargo, este nombre no coincide con el nombre de inicio de sesión de la cuenta Windows con el que ha iniciado la sesión.

```
npauditfailure yes
```

 Sistemas operativos Windows

## NPAUDITSUCCESS

---

La opción NPAUDITSUCCESS especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPE.

### Sintaxis

---

```
>>-NPAUDITSuccess--+-Yes+-----<<  
          '-No--'
```

### Parámetros

---

Yes

Especifica que se envía un evento a las anotaciones de eventos cuando se autentica un usuario de nodo cliente para acceder al servidor mediante SECUREPIPES.

No

Especifica que no se envía un evento a las anotaciones de Windows.

## Ejemplos

---

Especificar que se envía un evento a las anotaciones de eventos cuando se autentica un nodo cliente para acceder al servidor.

npauditsuccess yes

 Sistemas operativos Windows

## NPBUFFERSIZE

---

La opción NPBUFFERSIZE especifica el tamaño del búfer de comunicaciones de Named Pipes.

### Sintaxis

---

```
..-8-----.  
>>-NPBUffersize--+-kilobytes-+-----><
```

### Parámetros

---

kilobytes

Especifica el tamaño, en kilobytes, del búfer de comunicaciones de Named Pipes. El valor predeterminado es 8.

### Ejemplos

---

Especificar un búfer de comunicaciones de Named Pipes de 16 KB:

```
npbuffersize 16
```

 Sistemas operativos Windows

## NUMBERFORMAT

---

La opción NUMBERFORMAT especifica el formato de numeración que el servidor utiliza para visualizar los números.

El valor de NUMBERFORMAT se altera temporalmente mediante la definición de formato numérico del entorno nacional si el entorno nacional se inicializa correctamente durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

### Sintaxis

---

```
>>-NUMberformat--número-----><
```

### Parámetros

---

número

Seleccione un número de 1 a 6 para identificar el formato de números que utiliza el servidor. El valor predeterminado es 1.

1	1,000.00
2	1,000,00
3	1 000,00
4	1 000.00
5	1.000,00
6	1'000,00

### Ejemplos

---

```
numberformat 4
```

## NUMOPENVOLSAALLOWED

---

La opción NUMOPENVOLSALLOWED especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.

Los volúmenes de entrada contienen datos que se deben leer durante operaciones de restauración de cliente y procesos de servidor, como reclamación y migración. Utilice esta opción para mejorar el rendimiento al reducir la frecuencia con la que se abren y cierran los volúmenes.

Cada sesión de un proceso de servidor u operación de cliente puede tener tantos volúmenes FILE como se especifiquen en esta opción. Una sesión la inicia una operación de cliente o un proceso de servidor. Se pueden iniciar varias sesiones en cada uno de ellos.

Durante una operación de restauración de cliente, los volúmenes permanecerán abiertos durante la duración de una operación de restauración de cliente y mientras una sesión de cliente esté activa. Durante una operación de restauración sin consulta, los volúmenes permanecerán abiertos hasta que se complete la restauración sin consulta. En ese momento, se cerrarán todos los volúmenes. Sin embargo, para operaciones de restauración clásicas iniciadas en modalidad interactiva, los volúmenes permanecerán abiertos al final de la operación de restauración. Los volúmenes se cerrarán y liberarán cuando se solicite la próxima operación de restauración clásica.

Establezca este valor en el archivo de opciones del servidor o utilice el mandato SETOPT.

Consejo: Esta opción puede aumentar significativamente el número de volúmenes y puntos de montaje en uso en cualquier momento. Para optimizar el rendimiento, siga estos pasos:

- Para establecer NUMOPENVOLSALLOWED, seleccione un valor de inicio (se recomienda el valor predeterminado). Supervise las sesiones de cliente y los procesos de servidor. Tenga en cuenta el número más alto de volúmenes abiertos para una única sesión o un único proceso. Aumente el valor de NUMOPENVOLSALLOWED si el número más alto de volúmenes abiertos es igual al valor especificado en NUMOPENVOLSALLOWED.
- Para evitar que las sesiones o los procesos tengan que esperar un punto de montaje, aumente el valor del parámetro MOUNTLIMIT en la definición de clase de dispositivo. Establezca el parámetro MOUNTLIMIT en un valor que sea lo suficientemente alto para que permita que todas las sesiones de cliente y todos los procesos de servidor que utilizan agrupaciones de almacenamiento con eliminación de duplicados abran el número de volumen especificado en la opción NUMOPENVOLSALLOWED. Para sesiones de cliente, compruebe el destino en la definición de grupo de copia para determinar cuántos nodos almacenan datos en la agrupación de datos con eliminación de duplicados. Para procesos de servidor, compruebe el número de procesos permitidos para cada proceso para la agrupación de almacenamiento.
- Puede producirse una situación en la que un nodo realice una copia de seguridad y restaure o archive y recupere al mismo tiempo en y desde una agrupación de almacenamiento desduplicada. Todos los puntos de montaje necesarios para estas operaciones aumentan el número total de puntos de montaje necesarios para el nodo.

Como consecuencia, es posible que el nodo no pueda iniciar sesiones de copia de seguridad adicionales si ya tiene más puntos de montaje abiertos de los que permite el parámetro MAXNUMMP de la definición del nodo de cliente. Esto puede suceder aunque el MOUNTLIMIT de la clase de dispositivo no se hubiera excedido.

Para, evitar que las operaciones de copia de seguridad y recuperación fallen, establezca el parámetro MAXNUMMP de la definición de nodo cliente en un valor que sea como mínimo igual de alto que la opción NUMOPENVOLSALLOWED. Aumente este valor si nota que el nodo no está realizando satisfactoriamente operaciones de copia de seguridad o recuperación porque se ha sobrepasado el valor de MAXNUMMP.

## Sintaxis

---

```
>>-NUMOPENVOLsallowed--número_volúmenes_abiertos-----><
```

## Parámetros

---

`número_volúmenes_abiertos`

Especifica el número de volúmenes FILE de entrada que pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado. El valor predeterminado es 10. El valor mínimo es 3 y el máximo es 999.

## Ejemplos

---

Especifique que hasta 5 volúmenes pueden estar abiertos a la vez en una agrupación de almacenamiento cuyos duplicados se han eliminado.

```
numopenvolsallowed 5
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## PUSHSTATUS

---



---

La opción PUSHSTATUS se utiliza en servidores de radio para asegurarse de que la información de estado se envía al servidor concentrador. No actualice esta opción a menos que deba restaurar la configuración del Centro de operaciones al estado preconfigurado donde los servidores de IBM Spectrum Protect no están definidos como servidores de concentrador o de radio.

Si debe restaurar la configuración del Centro de operaciones al estado preconfigurado, debe emitir el mandato siguiente en cada servidor de radio:

```
SETOPT PUSHSTATUS NO
```

## QUERYAUTH

---

La opción QUERYAUTH especifica el nivel de autorización de administración necesario para emitir los comandos QUERY o SQL SELECT. De forma predeterminada, cualquier administrador puede emitir los comandos QUERY y SELECT. Puede utilizar esta opción para restringir el uso de estos comandos.

### Sintaxis

---

```
>>-QUERYAuth--+-NOne-----+-----><
      +-System---+
      +-Policy---+
      +-Storage--+
      '-Operator-'
```

### Parámetros

---

#### NOne

Cualquier administrador puede emitir los comandos QUERY o SELECT sin que sea necesaria ninguna autorización de administración.

#### System

Los administradores deben tener autorización SYSTEM para emitir los comandos QUERY o SELECT.

#### Policy

Los administradores deben tener autorización POLICY sobre uno o varios dominios de políticas, o bien autorización SYSTEM para emitir los comandos QUERY o SELECT.

#### Storage

Los administradores deben tener autorización STORAGE sobre una o varias agrupaciones de almacenamiento, o bien autorización SYSTEM para emitir los comandos QUERY o SELECT.

#### Operator

Los administradores deben tener autorización OPERATOR o SYSTEM para emitir los comandos QUERY o SELECT.

### Ejemplos

---

Para restringir el uso de los comandos QUERY y SELECT a los administradores con autorización de sistema o almacenamiento, especifique lo siguiente:

```
queryauth storage
```

## RECLAIMDELAY

---

Esta opción retrasa la reclamación de un volumen SnapLock y permite que los datos restantes caduquen para que no haya necesidad de reclamar el volumen.

### Sintaxis

---

```
>>-RECLAIMDELAY--+-número_de_días-+-----><
      .-4-----.
```

### Parámetros

---

#### número\_de\_días

Especifica el número de días de retraso de la reclamación de un volumen SnapLock.

Antes de reclamar un volumen SnapLock, el servidor de IBM Spectrum Protect permite que transcurra el número de días especificado para que los archivos que queden en el volumen tengan la oportunidad de caducar. El periodo de retraso de reclamación predeterminado es de cuatro días, y los valores posibles son de 1 a 120 días.

## Ejemplos

Especifique que el número de días de retraso de la reclamación sea de 30 días:

```
reclaimdelay 30
```

## RECLAIMPERIOD

Esta opción permite definir el número de días para el periodo de reclamación de un volumen SnapLock.

### Sintaxis

```
.-30-----  
>>-RECLAIMPERIOD--+-número_de_días-+-----<<
```

### Parámetros

número\_de\_días

Especifica el número de días que se permiten para el periodo de reclamación de un volumen SnapLock.

Después de que caduque la retención de un volumen SnapLock, el servidor de IBM Spectrum Protect reclamará el volumen antes de que transcurra el número de días especificado si todavía quedan datos en el volumen. El periodo de reclamación predeterminado es de 30 días y puede establecerse en cualquier lugar y desde 7 a 365 días.

El periodo de reclamación no empieza hasta que ha caducado el periodo RECLAIMDELAY.

## Ejemplos

Especificar que el periodo de reclamación sea de 45 días:

```
reclaimperiod 45
```

## REORGBEGINTIME

La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor de IBM Spectrum Protect puede iniciar una reorganización de tabla o índice.

Planifique las reorganizaciones iniciadas por el servidor para que se inicien durante los periodos en los que la actividad del servidor es baja. Utilice esta opción conjuntamente con la opción REORGDURATION. REORGDURATION especifica un intervalo en el que puede empezar la reorganización.

### Sintaxis

```
>>-REORGBEGINTime--hh:mm-----<<
```

### Parámetros

hh:mm

Especifica la hora a la que el servidor puede iniciar una reorganización. La hora de inicio predeterminada es a las 6:00. Utilice un formato de 24 horas para especificar la hora.

Hora	Descripción	Valores
hh	La hora del día	Especifique un número de 1 a 23.
mm	El minuto de la hora	Especifique un número de 1 a 59.

## Ejemplos

---

Especificar las 6:00 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 06:00
```

Especificar las 20:30 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 20:30
```

Especificar el mediodía como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 12:00
```

Especificar las 15:30 como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 15:30
```

Especificar la medianoche como la hora más temprana a la que se puede iniciar una reorganización.

```
reorgbegintime 00:00
```

## REORGURATION

---

La opción REORGURATION especifica un intervalo en el que puede empezar la reorganización de tabla o índice iniciada por el servidor.

Planifique las reorganizaciones iniciadas por el servidor para que se inicien durante los periodos en los que la actividad del servidor es baja. Utilice esta opción conjuntamente con la opción REORGBEGINTIME. La opción REORGBEGINTIME especifica la hora más temprana a la que el servidor puede iniciar una reorganización.

### Sintaxis

---

```
>>-REORGURation--nn-----<<
```

### Parámetros

---

nn

Especifica el número de horas en las que puede iniciarse una reorganización. El valor mínimo es 1 y el máximo es 24. El valor predeterminado es 24.

### Ejemplo

---

Especifique un intervalo de cuatro horas en las que puede iniciarse una reorganización.

```
reorgduration 4
```

## REPORTRETRIEVE

---

La opción REPORTRETRIEVE genera informes sobre las operaciones de restauración o recuperación que realizan los nodos clientes o los administradores. El valor predeterminado es NO.

### Sintaxis

---

```
>>-REPORTRETRIEVE---YES+-----<<  
'-NO--'
```

### Parámetros

---

YES

Especifica que se emitirán mensajes en la consola del servidor y se almacenarán en las anotaciones de actividad cuando se restauren o recuperen los archivos desde el servidor de IBM Spectrum Protect. Los mensajes especificarán el nombre de los objetos que se están restaurando o recuperando e identificarán el nodo cliente o administrador que realice la operación.

NO

Especifica que no se emitirán mensajes.

## Ejemplos

---

Especificar que han de emitirse y almacenarse mensajes en las anotaciones de actividades siempre que se restauren o recuperen archivos desde el servidor de IBM Spectrum Protect:

```
reportretrieve yes
```

Se emite el siguiente mensaje para una sesión de cliente de administración:

```
ANR0411I Sesión 8 para el administrador COLIND-TUC iniciado como el nodo  
COLIND-TUC objeto de copia de seguridad restaurado o recuperado: nodo  
COLIND-TUC,  
espacio de archivos \\colind-tuc\c$,  
object\CODE\TESTDATA\ XXX.OUT
```

## REPLBATCHSIZE

---

La opción REPLBATCHSIZE especifica el número de archivos de cliente que se van a replicar en proceso por lotes, dentro de la misma transacción de servidor. Esta opción afecta únicamente a los procesos de réplica de nodo y funciona con la opción REPLSIZETHRESH para mejorar el proceso de réplica de nodo.

La opción REPLBATCHSIZE limita el número de ficheros en una transacción y la opción REPLSIZETHRESH limita el número de bytes en una transacción. La transacción finaliza cuando se alcanza el umbral de REPLBATCHSIZE o REPLSIZETHRESH.

## Sintaxis

---

```
.-4096-----.  
>>-REPLBatchsize---+number_of_files+-----<<
```

## Parámetros

---

número\_de\_archivos

Especifica un número de archivos entre 1 y 32768. El valor predeterminado es 4096.

## Ejemplos

---

```
replbatchsize 25000
```

## REPLSIZETHRESH

---

La opción REPLSIZETHRESH especifica, en megabytes, un umbral para la cantidad de datos replicados, dentro de la misma transacción del servidor.

La cantidad de datos se basa en el tamaño del archivo sin eliminación de duplicados, que es el tamaño original del archivo. La cantidad de datos que se replican está controlada por el umbral. Cuando la cantidad de datos supera el umbral, el servidor finaliza la transacción y no se agregan más archivos al lote actual. Se inicia una nueva transacción después de que se replica el lote actual. Esta opción se utiliza con la opción REPLBATCHSIZE.

Por ejemplo, supongamos que un archivo es de 10 MB y se almacena en una agrupación de almacenamiento que tiene habilitada la eliminación de duplicados de datos y sólo 2 MB del archivo se transfiere durante la réplica. La cantidad de datos replicados incluye el tamaño de 10 MB de archivo y excluye los 2 MB transferidos. Cuando la cantidad de datos duplicados supera el valor especificado para el umbral REPLSIZETHRESH, la transacción finaliza.

Consejo: Si está replicando datos desde un servidor de origen en la nube y recibe con frecuencia el mensaje de servidor ANR1880W en el servidor de destino, reduzca el valor de la opción REPLSIZETHRESH en el servidor de origen.

## Sintaxis

---

```
.-4096-----.  
>>-REPLSizethresh---+ megabytes+-----<<
```

## Parámetros

---

megabytes

Especifica el número de megabytes como un entero comprendido entre 1 y 32.768. El valor predeterminado es 4096.

## Ejemplos

---

```
replsizethresh 2000
```

## REQSYSAUTHOUTFILE

---

La opción REQSYSAUTHOUTFILE especifica si es necesaria la autorización del sistema para los comandos de administración que hacen que IBM Spectrum Protect realice una grabación en un archivo externo.

Esta opción se puede utilizar con los comandos siguientes:

- BACKUP DEVCONFIG con el parámetro FILENAMES
- BACKUP VOLHISTORY con el parámetro FILENAMES
- DEFINE BACKUPSET
- DELETE BACKUPSET
- GENERATE BACKUPSET
- MOVE DRMEDIA con el parámetro CMD
- MOVE MEDIA con el parámetro CMD
- QUERY DRMEDIA con el parámetro CMD
- QUERY MEDIA con el parámetro CMD
- QUERY SCRIPT con el parámetro OUTPUTFILE

## Sintaxis

---

```
>>-REQSYSauthoutfile--+-Yes-+-----<<  
                        '-No--'
```

## Parámetros

---

Yes

Especifica que es necesaria la autorización del sistema para los comandos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo.

No

Especifica que no es necesaria la autorización del sistema para los comandos de administración que ocasionan que IBM Spectrum Protect efectúe la grabación en un archivo externo. Es decir, no hay ningún cambio en el nivel de autorización necesario para emitir el comando.

## Ejemplos

---

```
reqsysauthoutfile no
```

## RESOURCETIMEOUT

---

La opción RESOURCETIMEOUT especifica el intervalo de tiempo que el servidor espera un recurso antes de cancelar la adquisición pendiente del recurso. Cuando se exceda el tiempo de espera, la petición del recurso se cancelará.

Nota: Al gestionar un conjunto de recursos de bibliotecas compartidos, como servidores designados como gestores y clientes de bibliotecas, plantéese la posibilidad de establecer esta opción en el mismo límite de tiempo para todos los participantes de la configuración compartida. En caso de recuperación de errores, IBM Spectrum Protect siempre aplazará la acción al límite de tiempo más largo.

## Sintaxis

---

```
                .-60-----.  
>>-RESOURCETimeout--+-minutos+-----<<
```

## Parámetros

---

minutos

Especifica el número máximo de minutos que el servidor espera un recurso. El valor predeterminado es de 60 minutos. El valor mínimo es de 1 minuto.

## Ejemplos

---

Especifica que el servidor esperará un recurso de servidor durante 15 minutos:

```
resourcetimeout 15
```

## RESTOREINTERVAL

---

La opción RESTOREINTERVAL especifica durante cuánto tiempo se puede guardar una sesión de restauración rearrancable en la base de datos del servidor. Siempre y cuando la sesión de restauración se haya guardado en la base de datos, se puede volver a arrancar desde el punto en el que se ha detenido.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
.-1440----.  
>>-RESTOREINTERVAL--+-minutos+-----<<
```

## Parámetros

---

minutos

Especifica el intervalo, en minutos, durante el cual una sesión de restauración rearrancable puede residir en la base de datos del servidor antes de que caduque. El valor mínimo es 0. El valor máximo es 10080 (una semana). El valor predeterminado es de 1440 minutos (24 horas). Si el valor se establece en 0 y la restauración se interrumpe o resulta anómala, de todos modos la restauración se continúa poniendo en estado rearrancable. Sin embargo, queda inmediatamente elegible para su caducidad.

## Ejemplos

---

```
restoreinterval 1440
```

## RETENTIONEXTENSION

---

La opción RETENTIONEXTENSION especifica el número de días que ha de ampliarse la fecha de retención de un volumen de SnapLock. Esta opción permite que el servidor amplíe la fecha de retención de un volumen de SnapLock para evitar las reclamaciones excesivas.

## Sintaxis

---

```
>>-RETENTIONEXTENSION--número_de_días-----<<
```

## Parámetros

---

número\_de\_días

Especifica el número de días para ampliar la fecha de retención de un volumen de SnapLock. El valor mínimo es 30 días; el valor máximo es 9999 días; el valor predeterminado es 365.

Si especifica un valor de 0 (cero) en el parámetro RETVER de un grupo de copia archivada, el valor real que se utiliza para RETVER es el valor de la opción RETENTIONEXTENSION, si se da una de las siguientes condiciones:



- La agrupación de almacenamiento de destino del grupo de copia archivada es una agrupación de almacenamiento SnapLock.
- La agrupación de almacenamiento de destino de una migración de agrupación de almacenamiento o de un mandato MOVE DATA o MOVE NODEDATA es una agrupación de almacenamiento SnapLock.

Si un volumen de SnapLock constituye el volumen de destino de los datos procedentes de otro volumen de SnapLock, y si la retención restante de los datos del volumen es menor que el valor especificado, la fecha de retención se definirá utilizando el valor especificado. De lo contrario, se utilizará la retención restante de los datos para definir la retención del volumen. Si un volumen de SnapLock ha introducido el período de reclamación pero el porcentaje del espacio reclamable del volumen no ha sobrepasado el umbral de reclamación de la agrupación de almacenamiento o bien el valor especificado en el parámetro THRESHOLD de un comando RECLAIM STGPOOL, la fecha de retención del volumen de SnapLock se ampliará en función del valor especificado en la opción RETENTIONEXTENSION.

## Ejemplos

Especificar que la fecha de retención se amplía en 60 días:

```
retentionextension 60
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## SANDISCOVERY

La opción SANDISCOVERY especifica si está activada la función de descubrimiento SAN de IBM Spectrum Protect.

Para utilizar el descubrimiento de SAN, todos los dispositivos de la SAN deben tener un número de serie de dispositivo exclusivo. Cuando se establece en ON, el servidor realiza el descubrimiento de SAN en las siguientes instancias:

- Cuando se ha cambiado la ruta de acceso del dispositivo
- Cuando se ha emitido el mandato QUERY SAN

Utilizando el descubrimiento de SAN, el servidor puede corregir automáticamente el nombre de archivo especial de un dispositivo si éste se ha cambiado para un dispositivo de cinta especificado.

El servidor de IBM Spectrum Protect no requiere un enlace permanente con la función de descubrimiento de SAN activada. Para mostrar una lista de los dispositivos detectados por el servidor, emita el mandato QUERY SAN.

## Sintaxis

```
.-SANDISCOVERY-----OFF-----
>>+-----+-----><
  '-SANDISCOVERY-----+ON-----'
    '-UNSCANNEDPATHOFF-'
```

## Parámetros

ON

Especifica que el servidor realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el mandato QUERY SAN.

OFF

Especifica que el servidor no realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el comando QUERY SAN. Si el servidor de IBM Spectrum Protect no puede abrir un dispositivo, se emite un mensaje pero la ruta asociada con el dispositivo no se pone fuera de línea. Este es el valor predeterminado.

UNSCANNEDPATHOFF

Especifica que el servidor no realiza descubrimiento de SAN cuando se cambia la ruta del dispositivo o cuando se emite el comando QUERY SAN. Si el servidor de IBM Spectrum Protect no puede abrir un dispositivo, se emite un mensaje y la ruta al dispositivo se pone fuera de línea.




## Ejemplos

```
sandiscovery on
```

## Comandos relacionados

Tabla 1. Mandatos relacionados con SANDISCOVERY

Comando	Descripción
PERFORM LIBACTION	Define todas las unidades y rutas de una biblioteca.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## SANDISCOVERYTIMEOUT

---

La opción SANDISCOVERYTIMEOUT especifica la cantidad de tiempo permitido para que respondan los adaptadores de bus de host si se consultan mediante el proceso de descubrimiento de SAN. Cuando se alcance el tiempo especificado en SANDISCOVERYTIMEOUT, el proceso excede el tiempo de espera.

### Sintaxis

---

```
>>-SANDISCOVERYTIMEOUT--valor-----<<
```

### Parámetros

---

valor

Especifica la cantidad de tiempo que transcurre antes de que el proceso de descubrimiento de SAN exceda el tiempo de espera. El rango es de 15 a 1800 segundos. El valor predeterminado son 15 segundos.

### Ejemplos

---

```
sandiscoverytimeout 45
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## SANREFRESHTIME

---

La opción SANREFRESHTIME especifica la cantidad de tiempo que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. La opción SANREFRESHTIME tiene un valor predeterminado de 0, que significa que no hay caché de descubrimiento de SAN. La información se obtiene directamente del adaptador de bus de host (HBA) cada vez que el servidor ejecuta una operación de descubrimiento de SAN.

Nota: El comando de servidor QUERY SAN siempre recibe información de la SAN en el momento de emitirse el comando y pasa por alto los valores que se han especificado para SANREFRESHTIME.

### Sintaxis

---

```
.-0----.  
>>-SANREFRESHTIME--+hora+-----<<
```

### Parámetros

---

hora

Cantidad de tiempo, en segundos, que debe transcurrir hasta que se renueva la información de descubrimiento de SAN en caché. El valor predeterminado es 0 y especifica que la información de descubrimiento de SAN no se guarda en la memoria caché. Si se especifica un valor que no sea 0, como por ejemplo 100 segundos, la información de descubrimiento de SAN se renueva 100 segundos después de la operación de descubrimiento de SAN anterior.

### Ejemplos

---

Renovar la información de descubrimiento de SAN transcurridos 100 segundos.

```
sanrefreshtime 100
```

Desactivar la colocación en caché de la información de descubrimiento de SAN.

```
sanrefreshtime 0
```

## SEARCHMPQUEUE

---

La opción SEARCHMPQUEUE especifica el orden en el que el servidor da respuesta a las peticiones de la cola de montaje. Si se especifica la opción, el servidor primero intenta satisfacer las peticiones de los volúmenes que ya están montados. Estas peticiones



pueden ser satisfechas antes que otras peticiones, aunque estas otras hayan estado esperando más tiempo el punto de montaje. Si no se especifica esta opción, el servidor satisface las peticiones en el orden en que éstas se reciben.

## Sintaxis

---

```
>>-SEARCHMPQUEUE-----<<
```

## Parámetros

---


Ninguno

## Ejemplos

---

Especificar que el servidor intenta primero satisfacer una petición de un volumen que ya está montado:

```
searchmpqueue
```

 Sistemas operativos Windows

## SECUREPIPES

---

Cuando se utiliza el protocolo Named Pipes, si se activa SECUREPIPES, el servidor se ve forzado a comprobar el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

El nombre del usuario y la contraseña definidos en el grupo Windows se utilizan para autenticar el nodo/usuario para acceder a los datos del servidor. El nodo/usuario también debe ser un nodo cliente de IBM Spectrum Protect registrado. Sin embargo, se pasa por alto la contraseña del nodo de cliente de IBM Spectrum Protect y se utiliza la contraseña de Windows asociada al usuario.

## Sintaxis

---

```
>>-SECUREPipes--+Yes-+-----<<
      '-No--'
```

## Parámetros

---

Yes

Especifica que IBM Spectrum Protect comprueba el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

No

Especifica que IBM Spectrum Protect no comprueba el grupo Windows designado por ADSMGROUPNAME a fin de autenticar un nodo/usuario cliente.

## Ejemplos

---

Especificar que IBM Spectrum Protect compruebe el grupo Windows para autenticar los nodos cliente.

```
securepipes yes
```

## SERVERDEDUPTXNLIMIT

---

La opción SERVERDEDUPTXNLIMIT especifica el tamaño máximo de los objetos que pueden tener optimización de almacenamiento en el servidor.

Cuando se usan proceso de identificación de duplicados (el mandato IDENTIFY DUPLICATES) para objetos de gran tamaño, puede producirse una actividad intensiva en la base de datos por las transacciones de ejecución larga necesarias para actualizar dicha base de datos. Unos niveles altos de actividad de la base de datos pueden producir los siguientes síntomas:

- Rendimiento reducido para las operaciones de copia de seguridad y de archivado del cliente
- Contienda de recursos debido a operaciones simultáneas del servidor
- Actividad excesiva del registro de recuperación

La medida en que se producen estos síntomas depende del número y del tamaño de los objetos que se procesan, de la intensidad y el tipo de las operaciones simultáneas que tienen lugar en el servidor de IBM Spectrum Protect y de la configuración de servidor de IBM Spectrum Protect.

Con la opción de servidor SERVERDEDUPTXNLIMIT es posible especificar un tamaño máximo, en gigabytes, para los objetos para los que se puede optimizar el almacenamiento. Si un objeto o un conjunto de objetos de una única transacción supera el límite especificado por SERVERDEDUPTXNLIMIT, los objetos no tienen optimización del almacenamiento por el servidor. Es posible especificar un valor de 32 a 102400 GB. El valor predeterminado es 5120 GB.

Aumentar el valor de esta opción hace que el servidor de IBM Spectrum Protect busque objetos aplazados anteriormente cuyo tamaño se encuentre por debajo del nuevo límite de transacción.

Recuerde: La búsqueda de objetos aplazados anteriormente puede llevar un tiempo. Tenga cuidado si aumenta el valor de SERVERDEDUPTXNLIMIT. Si se reduce el valor de esta opción, no se provoca que IBM Spectrum Protect busque objetos aplazados.

El valor adecuado para esta opción depende de la configuración de servidor de IBM Spectrum Protect y de la actividad simultánea del servidor. Es posible especificar un valor alto para esta opción si se minimiza la contienda de recursos. Para minimizar la contienda de recursos, realice operaciones como copia de seguridad, archivado, identificación de duplicados y reclamación en distintos momentos.

Para actualizar esta opción del servidor sin necesidad de detener y reiniciar el servidor, utilice el mandato SETOPT.

## Sintaxis

---

```
                .-5120-----.  
>>-SERVERDEDUPTXNlimit--+-gigabytes+-----<<
```

## Parámetros

---

**gigabytes**

Especifica el tamaño máximo, en gigabytes, de los objetos que se puede optimizar el almacenamiento en servidor. Es posible especificar un valor de 32 a 102400. El valor predeterminado es 5120.

## Ejemplos



---


Inhabilitar la optimización de almacenamiento de datos en el lado del servidor para todos los objetos de más de 120 GB:

```
serverdeduptxnlimit 120
```

## SHMPORT

---

 Sistemas operativos AIX  Sistemas operativos Linux La opción SHMPORT especifica la dirección del puerto TCP/IP de un servidor cuando se utiliza memoria compartida. Todas las comunicaciones de memoria compartida comienzan por una conexión TCP/IP.

 Sistemas operativos Windows La opción SHMPORT especifica el puerto en el que el servidor está a la escucha de conexiones de memoria compartida.

## Sintaxis




---

```
>>-SHMPort--número_puerto-----<<
```

## Parámetros

---

**número\_puerto**

Especifica el número de puerto.  Sistemas operativos AIX  Sistemas operativos Linux Puede especificar un valor de 1024 a 32767. El valor predeterminado es 1510.  Sistemas operativos Windows Puede especificar un valor de 1 a 32767. El valor predeterminado es 1.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux

```
shmport 1580
```

## SHREDDING

---

La opción SHREDDING especifica si la destrucción de datos confidenciales suprimidos se lleva a cabo automática o manualmente. La destrucción sólo se aplica a los datos de las agrupaciones de almacenamiento que se han configurado explícitamente para dar soporte a la destrucción.

### Sintaxis

---

```
>>-SHREdding--+-AUTOMatic+-----><  
      '-MANual-----'
```

### Parámetros

---

#### AUTOMatic

Especifica que la destrucción se produzca automáticamente cuando se supriman datos confidenciales. Utilice esta opción para destruir datos confidenciales lo antes posible después de suprimirlos. Si no se especifica la opción SHREDDING, éste es el comportamiento predeterminado. Si se produce un error de E/S durante la destrucción automática, se notifica un error y se detiene la destrucción del objeto actual. Si el error de E/S no puede corregirse, es posible sea necesario ejecutar la destrucción manualmente y utilizar la palabra clave IOERROR.

#### MANual

Especifica que la destrucción se produce manualmente, sólo cuando se invoca el comando SHRED DATA. Utilice esta opción para controlar cuando tiene lugar la destrucción para asegurarse de que no interfiera con otras actividades del servidor.

Consejo: Si especifica la destrucción manual, ejecute el comando SHRED DATA con regularidad, como mínimo con la frecuencia con la que realiza otras tareas de mantenimiento rutinarias del servidor (por ejemplo, la caducidad, la reclamación, etc.). Esta práctica puede evitar la degradación del rendimiento que podrían experimentar determinados procesos del servidor (en particular, la migración). Para obtener resultados óptimos, ejecute SHRED DATA después de cualquier operación que suprima archivos de una agrupación de destrucción (por ejemplo, la caducidad y la migración).

### Ejemplos

---

Especificar que IBM Spectrum Protect destruya automáticamente los datos de una agrupación de almacenamiento que se ha configurado para aplicar la destrucción tras haberse suprimido los datos:

```
shredding automatic
```

## SNMPHEARTBEATINTERVAL

---

La opción SNMPHEARTBEATINTERVAL especifica el intervalo en minutos entre consultas del servidor de IBM Spectrum Protect.

### Sintaxis

---

```
      .-5-----.  
>>-SNMPHEARTBEATINTERVAL--+-minutos+-----><
```

### Parámetros

---

#### minutos

Especifica el intervalo de consultas en minutos. Los valores válidos son de 0 a 1440 (un día). El valor predeterminado es de 5 minutos.

### Ejemplos

---

```
snmpheartbeatinterval 20
```

## SNMPMESSAGECATEGORY

---

La opción `SNMPMESSAGECATEGORY` especifica los tipos de detecciones que se utilizan cuando se envían los mensajes desde el servidor, a través del subagente SNMP (Simple Network Management Protocol), al gestor SNMP.

## Sintaxis

---

```
>>-SNMPMESSAGECATEGORY--+-SEVERITY---+-----<<
      '-INDIVIDUAL-'
```

## Parámetros

---

### SEVERITY

Especifica que existen cuatro tipos de detecciones basados en el nivel de gravedad de los mensajes.

- 1 Grave
- 2 Error
- 3 Aviso
- 4 Información

Este es el valor predeterminado.

### INDIVIDUAL

Especifica que se utiliza un tipo de detección (de condición de excepción) para cada mensaje. La parte numérica del identificador de mensaje indica el tipo de detección (de condición de excepción).

## Ejemplos

---

```
snmpmessagecategory individual
```

## SNMP SUBAGENT

---

La opción `SNMP SUBAGENT` especifica los parámetros necesarios para que el subagente de IBM Spectrum Protect se comunique con el daemon SNMP (Simple Network Management Protocol). Esta opción únicamente sirve para configurar el subagente SNMP para las comunicaciones con el agente SNMP; el servidor la ignora.

## Sintaxis

---

```
>>-SNMP SUBAGENT--+-+----->
      '-HOSTname -nombre_host-'

>--+-----+-----+-----<<
      '-COMMunityname -nombre_comunidad-' '-TIMEOUT -segundos-'
```

## Parámetros

---

### HOSTname nombre\_host

Especifica el nombre o número TCP/IP del host que ejecuta el agente SNMP con el que se conecta el subagente SNMP de IBM Spectrum Protect. Este parámetro es opcional. El nombre predeterminado es *localhost*.

### COMMunityname nombre\_comunidad

Especifica el nombre de comunidad configurado del sistema que se ejecuta en el agente SNMP. Este parámetro es opcional. El nombre predeterminado es *public*.

### TIMEOUT segundos

Especifica el tiempo, en segundos, en el que debe recibirse una petición. Este parámetro es opcional. El valor predeterminado es 600.

## Ejemplos

---

```
snmpsubagent hostname jimbo communityname public timeout 2600
```

## SNMPSUBAGENTHOST

---

La opción SNMPSUBAGENTHOST especifica la ubicación del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect. El valor predeterminado para esta opción es 127.0.0.1.

### Sintaxis

---

```
>>-SNMPSUBAGENTHOST--nombre_host-----<<
```

### Parámetros

---

**nombre\_host**  
Especifica el nombre o número del host TCP/IP en el que está ubicado el subagente SNMP de IBM Spectrum Protect. El subagente y el servidor deben estar en el mismo nodo.

### Ejemplos

---

```
snmpsubagenthost 9.116.23.450
```

## SNMPSUBAGENTPORT

---

La opción SNMPSUBAGENTPORT especifica el número de puerto del subagente SNMP (Simple Network Management Protocol) de IBM Spectrum Protect.

### Sintaxis

---

```
>>-SNMPSUBAGENTPORT--número_puerto-----<<
```

### Parámetros

---

**número\_puerto**  
Especifica el número de puerto del subagente SNMP de IBM Spectrum Protect. Los valores válidos son 1000 - 32767. El valor predeterminado es de 1521.

### Ejemplos

---

```
snmpsubagentport 1525
```

## SSLFIPSMODE

---

La opción SSLFIPSMODE especifica si se aplica la modalidad Estándar federal de procesamiento de información (FIPS) para la capa de sockets seguros (SSL). El valor predeterminado es NO.

Puesto que SSLv3 no está soportado por la modalidad FIPS, cuando se utiliza SSL con clientes de la versión 6.1 o V5.5, debe desactivar la modalidad FIPS.

### Sintaxis

---

```
.-SSLFIPSMODE-----No-----.  
>>+-----+-----<<  
'-SSLFIPSMODE-----+No--+'  
      '-Yes-'
```

### Parámetros

---

**No**  
Especifica que la modalidad FIPS SSL no está activa en el servidor. Este valor es necesario cuando se van a conectar al servidor versiones del cliente de archivado y copia de seguridad anteriores a IBM Spectrum Protect 6.3 con SSL.

Sí

Un valor YES indica que la modalidad FIPS SSL está activa en el servidor. Este valor restringe la negociación de sesiones SSL al uso de suites de cifrado aprobadas por FIPS. Se recomienda especificar YES cuando la comunicación SSL está habilitada y todos los clientes de archivado y copia de seguridad se encuentran en V6.3 o posterior.

Para desactivar la modalidad FIPS SSL en el servidor:

```
SSLFIPSMODE no
```

## SSLINITTIMEOUT

---

La opción SSLINITTIMEOUT especifica el tiempo, en minutos, que el servidor espera a que finalice la inicialización de una sesión SSL (capa de sockets seguros) antes de que cancelar la sesión.

Cuando especifica esta opción, la sesión SSL se cancela si un cliente, un servidor o un agente de almacenamiento no está configurado para SSL e intenta iniciar una sesión SSL. De forma parecida, la sesión SSL se cancela si la sesión SSL de cliente y el servidor no están configurados con la misma versión de TLS (seguridad de la capa de transporte). En estos casos, la sesión SSL no se inicializará completamente. El servidor cancela la sesión cuando se alcanza el tiempo de espera especificado.

### Sintaxis

---

```
.-2-----.  
>>-SSLINITTIMEout--+-minutos-+-----<<
```

### Parámetros

---

minutos

Especifica el número máximo de minutos que el servidor espera a que una sesión SSL finalice la inicialización. El valor predeterminado es 2 minutos. El valor mínimo es de 1 minuto.

### Ejemplo

---

```
sslinittimeout 1
```

## SSLTCPADMINPORT

---

La opción SSLTCPADMINPORT especifica la dirección del puerto en la que el controlador de comunicaciones TCP/IP del servidor espera peticiones solo de sesiones con SSL habilitado. Las sesiones son para el cliente de administración de línea de comandos.

Nota: A partir de IBM Spectrum Protect Versión 8.1.2, ya no es necesario utilizar la opción SSLTCPPOINT ni SSLTCPADMINPORT para permitir sesiones compatibles con SSL del cliente. El número de puerto especificado en la opción TCPPOINT o TCPADMINPORT escucha tanto a la sesión TCP/IP como a la sesión de cliente compatible con SSL.

Los siguientes tipos de sesiones no utilizan el protocolo de capa de sockets seguros (SSL):

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se establezcan números de puerto diferentes para las opciones SSLTCPADMINPORT y SSLTCPPOINT.

El controlador de comunicaciones TCP/IP debe estar activado con COMMETHOD TCPIP o COMMETHOD V6TCPIP.

### Sintaxis

---

```
>>-SSLTCPADMINPort--número_puerto-----<<
```

### Parámetros

---

número\_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. No existe un valor predeterminado.

## Ejemplos

---

```
ssltcpadminport 1543
```

## SSLTCPPOINT

---

La opción SSLTCPPOINT especifica el número de puerto de capa de sockets seguros (SSL) solo para las sesiones compatibles con SSL. La unidad de comunicación TCP/IP del servidor espera peticiones en este puerto para sesiones con SSL activada del cliente.

Importante: A partir de IBM Spectrum Protect Versión 8.1.2, ya no es necesario utilizar la opción SSLTCPPOINT ni SSLTCPADMINPORT para permitir sesiones compatibles con SSL del cliente. El número de puerto especificado en la opción TCPPOINT o TCPADMINPORT escucha tanto a la sesión TCP/IP como a la sesión de cliente compatible con SSL.

Los siguientes tipos de sesiones no utilizan SSL:

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se establezcan números de puerto diferentes para las opciones SSLTCPADMINPORT y SSLTCPPOINT.

Si especifica el mismo número de puerto para las opciones SSLTCPPOINT y TCPPOINT, solo se aceptarán conexiones SSL y se inhabilitarán las conexiones TCP/IP para el puerto.

El controlador de comunicaciones TCP/IP debe estar activado con COMMMETHOD TCPIP o COMMMETHOD V6TCPIP.

## Sintaxis

---

```
>>-SSLTCPPOINT--número_puerto-----<<
```

## Parámetros

---

número\_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. No existe un valor predeterminado.

## Ejemplos

---

```
ssltcpport 1542
```

## TCPADMINPORT

---

La opción TCPADMINPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las peticiones de sesiones compatibles con TCP/IP y SSL distintas de las sesiones de cliente. Esto incluye las sesiones de administración, las sesiones de servidor a servidor, las sesiones del agente de almacenamiento, las sesiones del cliente de biblioteca, las sesiones de servidor gestionado y las sesiones del servidor de eventos.

La utilización de números de puerto distintos para las opciones TCPPOINT y TCPADMINPORT le permite crear un conjunto de reglas de cortafuegos para las sesiones de cliente y otro conjunto para los otros tipos de sesiones anteriormente indicados. Utilizando el parámetro SESSIONINITIATION de los mandatos REGISTER NODE y UPDATE NODE, puede cerrar el puerto especificado por TCPPOINT en el cortafuegos y especificar los nodos cuyas sesiones planificadas se iniciarán desde el servidor. Si los dos números de puerto son diferentes, se usan diferentes hebras para las sesiones de cliente de servicio y los tipos de sesión. Si admite las dos opciones para usar el mismo número de puerto (de forma predeterminada o al configurarlos explícitamente al mismo número de puerto), se usa un solo hilo del servidor para dar servicio a todas las solicitudes de sesión.

Las sesiones de cliente que intenten utilizar el puerto que especifica TCPADMINPORT terminarán (si TCPPOINT y TCPADMINPORT especifican puertos distintos). Se permitirán sesiones de administración en cualquiera de ambos puertos (a menos que la opción ADMINONCLIENTPORT se establezca en NO), pero de forma predeterminada utilizarán el puerto especificado por TCPADMINPORT.

Las sesiones compatibles con SSL que utilicen la opción TCPADMINPORT, tienen las mismas limitaciones que la opción SSLTCPADMINPORT. Los siguientes tipos de sesiones no utilizan el protocolo de capa de sockets seguros (SSL):

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)

- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se especifiquen número de puerto diferentes para las opciones TCPADMINPORT y TCPSPORT.

## Sintaxis

---

```
>>-TCPADMINPort--número_puerto-----<<
```

## Parámetros

---

número\_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. El valor predeterminado es el valor de TCPSPORT.

## Ejemplos

---

```
tcpadminport 1502
```

 Sistemas operativos AIX  Sistemas operativos Linux

## TCPBUFSIZE

---

La opción TCPBUFSIZE especifica el tamaño del búfer utilizado para peticiones de envío TCP/IP. Durante una restauración, los datos de cliente se traspasan del componente de sesión IBM Spectrum Protect a un controlador de comunicaciones TCP. La opción TCPBUFSIZE determina si el servidor envía los datos directamente desde el búfer de la sesión o copia los datos en el búfer TCP. Un tamaño de búfer de 32 KB dará lugar a que servidor copie forzosamente los datos en su búfer de comunicaciones y al vaciado del búfer cuando éste esté lleno.

Nota: Esta opción no está relacionada con la opción TCPWINDOWSIZE.

## Sintaxis

---

```
>>-TCPBufsize--kilobytes-----<<
```

## Parámetros

---

kilobytes

Especifica el tamaño, en kilobytes, del búfer utilizado para peticiones de envío TCP/IP.

 Sistemas operativos AIX El rango de valores es de 1 a 64. El valor predeterminado es 32.

 Sistemas operativos Linux El rango de valores es de 1 a 64. El valor predeterminado es 16.

## Ejemplos

---

```
tcpbufsize 5
```

## TCPNODELAY

---

La opción TCPNODELAY especifica si el servidor inhabilita el retraso al enviar pequeños paquetes sucesivos en la red.

Cambie el valor predeterminado YES sólo en las condiciones siguientes:

- El representante del servicio le pide que cambie la opción.
- Comprende perfectamente las repercusiones del algoritmo Nagle TCP en las transmisiones por red. Si establece esta opción en NO, se habilitará el algoritmo Nagle, con lo que se retrasará el envío de pequeños paquetes sucesivos.

## Sintaxis

---

```
>>-TCPNodelay---+-Yes-+-----<<
```



## Parámetros

---

Yes

Especifica que el servidor permite el envío inmediato de pequeños paquetes sucesivos en la red. Si se establece esta opción en YES, el rendimiento de las redes de alta velocidad puede verse mejorado. El valor predeterminado es YES.

No

Especifica que el servidor no permite el envío inmediato de pequeños paquetes sucesivos en la red.

## Ejemplos

---

```
tcpnodelay no
```

## TCPPORT

---

La opción TCPPORT especifica el número de puerto en el que el controlador de comunicaciones TCP/IP del servidor ha de estar a la espera de las solicitudes de sesiones de cliente. El controlador de comunicación TCP/IP de servidor escucha este puerto tanto para las sesiones TCP/IP como para las sesiones compatibles con SSL desde el cliente.


La utilización de números de puerto distintos para las opciones TCPPORT y TCPADMINPORT le permite crear un conjunto de reglas de cortafuegos para las sesiones de cliente y otro conjunto para los otros tipos de sesiones (sesiones de administración, sesiones de servidor a servidor, sesiones del agente de almacenamiento, sesiones del cliente de biblioteca, sesiones de servidor gestionado y sesiones del servidor de eventos). Si dos números de puerto son diferentes, se usan diferentes hilos para dar servicio a las sesiones del cliente y los otros tipos de sesión. Si admite las dos opciones para usar el mismo número de puerto (de forma predeterminada o al configurarlos explícitamente al mismo número de puerto), se usa un solo hilo del servidor para dar servicio a todas las solicitudes de sesión.

Las sesiones de cliente compatibles con SSL que utilicen la opción TCPPORT, tienen las mismas limitaciones que la opción SSLTCPPOINT. Los siguientes tipos de sesiones no utilizan SSL:

- Protocolo de gestión de datos de redes (NDMP)
- Automated Cartridge System Library Software (ACSL)
- Operaciones de restauración de base de datos

Si la opción ADMINONCLIENTPORT está establecida en NO, las sesiones habilitadas para SSL para el cliente administrativo requieren que se especifiquen número de puerto diferentes para las opciones TCPADMINPORT y TCPPOINT.

Si especifica el mismo número de puerto para las opciones SSLTCPPOINT y TCPPOINT, solo se aceptarán conexiones SSL y se inhabilitarán las conexiones TCP/IP para el puerto.

 Sistemas operativos Windows Puede cambiar esta opción con el mandato SETOPT. Cuando cambia un puerto, el servidor de IBM Spectrum Protect inicia la escucha en el nuevo puerto de forma inmediata. Todas las conexiones permanecen en uso hasta que se cierran.

## Sintaxis

---

```
>>-TCPPOINT--número_puerto-----><
```

## Parámetros

---

número\_puerto

Especifica el número del puerto del servidor. Los valores válidos son 1024 - 32767. El valor predeterminado es 1500.



```
tcpport 1500
```

## TCPWINDOWSIZE

---

La opción TCPWINDOWSIZE especifica, en kilobytes, la cantidad de datos de recepción que se pueden almacenar en el búfer a la vez en una conexión TCP/IP. El host emisor no puede enviar más datos hasta que reciba una confirmación y una actualización de ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP anunciada en la conexión. Una ventana más grande permite que el emisor continúe enviando datos y puede mejorar el rendimiento de las comunicaciones, sobre todo en las redes rápidas con una latencia elevada.

Nota:

- Para mejorar el rendimiento de las copias de seguridad, aumente TCPWINDOWSIZE en el servidor. Para mejorar el rendimiento en las operaciones de restauración, aumente TCPWINDOWSIZE en el cliente.
- La ventana TCP actúa como búfer en la red.
- Una ventana más grande que el espacio del búfer en el adaptador de la red puede disminuir el rendimiento debido al reenvío de los paquetes que se habían perdido en el adaptador.
-  Sistemas operativos AIX  Sistemas operativos Linux La opción TCPWINDOWSIZE no está relacionada con la opción TCPBUFFSIZE ni con los búferes de envío y recepción asignados en la memoria del cliente o del servidor.

## Sintaxis

---

```
>>-TCPWindowsize--kilobytes-----<<
```

## Parámetros

---

kilobytes

Especifica el tamaño, en kilobytes, que desea utilizar para la ventana de posición TCP/IP de su nodo cliente. Puede especificar un valor de 0 a 2048. El valor predeterminado es 63. Si se especifica 0, el servidor utiliza el tamaño de ventana predeterminado que establece el sistema operativo. Los valores de 1 a 2048 indican que el tamaño de ventana se encuentra dentro del rango de 1 KB a 2 MB.

## Ejemplos

---

```
tcpwindowsize 63
```

## TECBEGINEVENTLOGGING

---

La opción TECBEGINEVENTLOGGING especifica si las anotaciones de eventos del receptor de TIVOLI deben empezar cuando se inicie el servidor. Si se especifica la opción TECHOST, TECBEGINEVENTLOGGING toma de forma predeterminada el valor YES.

## Sintaxis

---

```
>>-TECBegineventlogging--+-Yes+-----<<  
      '-No--'
```

## Parámetros

---

Yes

Especifica que la anotación de eventos se inicia al arrancar el servidor y si se ha especificado una opción TECHOST.

No

Especifica que cuando arranque el servidor no se iniciarán las anotaciones de eventos. Para iniciar más tarde las anotaciones de eventos en el receptor TIVOLI (si se ha especificado la opción TECHOST), debe emitir el comando BEGIN EVENTLOGGING.

## Ejemplos

---

```
tecbegineventlogging yes
```

## TECHOST

---

La opción TECHOST especifica el nombre de host o dirección IP del servidor de eventos de Tivoli.

## Sintaxis

---

```
>>-TECHost--nombre_host-----<<
```

## Parámetros

---

nombre\_host

Especifica el nombre de host o la dirección IP del servidor de eventos de Tivoli.

## Ejemplos

---

```
techost 9.114.22.345
```

## TECPORT

---

La opción TECPORT especifica la dirección de puerto TCP/IP en la que el servidor de eventos Tivoli está a la escucha. Esta opción sólo es necesaria si el servidor de eventos Tivoli se encuentra en un sistema que no tiene un servicio PortMapper en funcionamiento.

## Sintaxis

---



```
>>-TECPort--numero_puerto-----<<
```

## Parámetros

---

numero\_puerto

Especifica la dirección de puerto del servidor de eventos de Tivoli. El valor debe estar comprendido entre 0 y 32767.

 Sistemas operativos AIX  Sistemas operativos Linux Esta opción no es necesaria.

## Ejemplos

---

```
tecport 1555
```

## TECUTF8EVENT

---

La opción TECUTF8EVENT permite al administrador de IBM Spectrum Protect enviar información al servidor de Tivoli Enterprise Console (TEC) en formato de datos UTF-8. El valor predeterminado es No. Puede visualizar si esta opción está activada o no mediante la emisión del comando QUERY OPTION.

## Sintaxis

---

```
>>-TECUTF8event--+-Yes-+-----<<  
                '-No--'
```

## Parámetros

---

Yes

Especifica que el servidor de IBM Spectrum Protect codificará el evento TEC en formato UTF-8 antes de emitir el evento al servidor TEC.

No

Especifica que el servidor de IBM Spectrum Protect no codificará el evento TEC en formato UTF-8 y se enviará al servidor TEC en formato ASCII.

## Ejemplos

---

```
tecutf8event yes
```

## THROUGHPUTDATATHRESHOLD

---

La opción THROUGHPUTDATATHRESHOLD especifica un umbral de productividad que debe alcanzar una sesión de cliente para evitar que ésta se cancele después de que se haya alcanzado el umbral de tiempo.

Esta opción se utiliza junto con la opción del servidor THROUGHPUTTIMETHRESHOLD, que establece el valor del umbral de tiempo más el tiempo de espera de medios. El umbral de tiempo se inicia cuando el cliente empieza a enviar datos al servidor para almacenarlos (no cuando los configura o realiza el mantenimiento de los datos de la sesión).

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
>>-THROUGHPUTDatathreshold--kilobytes_por_segundo-----><
```

## Parámetros

---

kilobytes\_per\_second

Especifica la productividad que deben alcanzar las sesiones de cliente para evitar que se cancelen después de que hayan transcurrido THROUGHPUTTIMETHRESHOLD minutos. Este umbral no incluye el tiempo de espera de los montajes de medios. Un valor de 0 impide examinar las sesiones de cliente debido a una productividad insuficiente. La productividad se calcula sumando los recuentos de bytes enviados y recibidos y dividiendo el resultado por la duración de la sesión. La duración no incluye el tiempo de espera de los montajes de medios y se empieza a contar a partir del momento en que el cliente envía datos al servidor para su almacenamiento. El valor predeterminado es 0. El valor mínimo es 0; el valor máximo es 99999999.

## Ejemplos

---

Especificar que el servidor debe esperar hasta 90 minutos más el tiempo de espera del medio a partir del momento en que una sesión ha empezado a enviar datos antes de que el almacenamiento la examine como candidata a ser cancelada debido a una baja productividad. Si una sesión no alcanza una velocidad de transferencia de 50 KB por segundo, se cancelará.

```
throughputtimethreshold 90  
Throughputdatathreshold 50
```

## THROUGHPUTTIMETHRESHOLD

---

La opción THROUGHPUTTIMETHRESHOLD especifica el umbral de tiempo de una sesión a partir del cual puede ser cancelada por baja productividad.

Puede actualizar esta opción del servidor sin detener y reiniciar el servidor con el comando SETOPT. Consulte el apartado SETOPT (Establecer una opción de servidor para actualización dinámica).

## Sintaxis

---

```
>>-THROUGHPUTtimethreshold--minutos-----><
```

## Parámetros

---

minutos

Especifica el umbral para examinar sesiones de cliente y cancelarlas si no se alcanza el umbral de productividad de los datos (vea la opción de servidor THROUGHPUTDATATHRESHOLD). Este umbral no incluye el tiempo de espera de los montajes de medios. El umbral de tiempo se inicia cuando un cliente empieza a enviar datos al servidor para almacenarlos (no cuando los configura o realiza el mantenimiento de los datos de la sesión). El valor 0 impide examinar las sesiones de cliente debido a una baja productividad. El valor predeterminado es 0. El valor mínimo es 0; el valor máximo es 99999999.

## Ejemplos

---

Especificar que el servidor debe esperar hasta 90 minutos más el tiempo de espera del medio a partir del momento en que una sesión ha empezado a enviar datos antes de examinarla como candidata a ser cancelada. Si una sesión no alcanza una velocidad de transferencia de 50 mil bytes por segundo, se cancelará.

```
throughputtimethreshold 90  
Throughputdatathreshold 50
```

 Sistemas operativos Windows

## TIMEFORMAT

---

La opción TIMEFORMAT especifica el formato mediante el cual el servidor visualiza la hora.

El valor de TIMEFORMAT se altera temporalmente mediante la definición de formato de hora del entorno nacional si el entorno nacional se inicializa correctamente durante el arranque del servidor. El entorno nacional se especifica en la opción LANGUAGE.

## Sintaxis

---

```
>>-TIMEformat--número_formato-----><
```

## Parámetros

---

número\_formato

Seleccione un número de 1 a 4 para identificar el formato de hora que utiliza el servidor. El valor predeterminado es 1.

- |   |                     |
|---|---------------------|
| 1 | hh:mm:ss            |
| 2 | hh,mm,ss            |
| 3 | hh.mm.ss            |
| 4 | hh:mm:ss a.m o p.m. |
| 5 | a.m o p.m. hh:mm:ss |

## Ejemplos

---

```
timeformat 4
```

## TXNGROUPMAX

---

La opción TXNGROUPMAX especifica el número de objetos que se transferirán como un grupo entre un cliente y un servidor entre puntos de validación de transacciones. El valor mínimo es de 4 objetos y el valor máximo es de 65000 objetos. El valor predeterminado son 4096 objetos. Los objetos transferidos son directorios, archivos reales o ambos. El servidor cuenta cada archivo o directorio como un objeto.

El rendimiento de las operaciones de copia de seguridad del cliente, de archivado, de restauración y de recuperación puede mejorarse utilizando un valor más alto para esta opción:

1. Si incrementa el valor de la opción TXNGROUPMAX especificando una cantidad mayor, verifique los posibles efectos que ello puede tener en las anotaciones de recuperación. La especificación de un valor más alto para la opción TXNGROUPMAX puede incrementar la utilización de las anotaciones de recuperación, así como el tiempo necesario para la validación de una transacción. Si los efectos son lo suficientemente significativos, pueden dar lugar a problemas en el funcionamiento del servidor.
2. Si se aumenta el valor de la opción TXNGROUPMAX, es posible que aumente la productividad de las operaciones que almacenan los datos directamente en la cinta, especialmente cuando se almacenan muchos objetos. Sin embargo, un valor mayor de la opción TXNGROUPMAX también puede aumentar el número de objetos que deben volver a enviarse en caso de que la transacción se detenga debido a que un archivo de entrada ha cambiado durante la realización de la copia de seguridad o porque se necesitaba un nuevo volumen de almacenamiento. Cuanto mayor sea el valor de la opción TXNGROUPMAX, más datos se volverán a enviar.
3. El aumento del valor TXNGROUPMAX afectará a la sensibilidad de detención de la operación y es posible que el cliente tenga que esperar más tiempo para que se complete la transacción.

Puede modificar el valor de esta opción para nodos cliente individuales. Consulte el parámetro TXNGROUPMAX en la REGISTER NODE (Inscribir un nodo) y la UPDATE NODE (Actualizar atributos del nodo).

Esta opción está relacionada con la opción TXNBYTELIMIT del archivo de opciones del cliente. TXNBYTELIMIT controla el número de bytes, y no el de objetos, que se transfieren entre los puntos de validación de transacciones. Al finalizar la transferencia de un objeto, el cliente valida la transacción si el número de bytes transferidos durante la transacción alcanza o sobrepasa el valor de TXNBYTELIMIT, independientemente del número de objetos transferidos.

## Sintaxis

---

```
>>-TXNGroupmax--número_de_objetos-----><
```

## Parámetros

---

### number\_of\_objects

Especifica un número comprendido entre el 4 y el 65000 para el número máximo de objetos por transacción. El valor predeterminado es 4096.

## Ejemplos

---

```
txngroupmax 4096
```

## UNIQUETDPTEEVENTS

---

La opción UNIQUETDPTEEVENTS genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect, incluidos los mensajes del cliente, del servidor y del cliente de IBM Spectrum Protect. El valor predeterminado es No.

## Sintaxis

---

```
>>-UNIQUETDPteevents---+-Yes+-----<<  
                        '-No--'
```

## Parámetros

---

### Yes

Especifica que los mensajes exclusivos de IBM Spectrum Protect Data Protection se envían al servidor de eventos TEC. Establece dinámicamente UNIQUETEEvents en YES.

### No

Especifica que los mensajes generales se envían al servidor de eventos TEC.

## Ejemplos

---

```
uniquetdpcevents yes
```

## UNIQUETEEvents

---

La opción UNIQUETEEvents genera una clase de evento de Tivoli Enterprise Console (TEC) exclusiva para cada mensaje individual de IBM Spectrum Protect. El valor predeterminado es No.

## Sintaxis

---

```
>>-UNIQUETEEvents---+-Yes+-----<<  
                        '-No--'
```

## Parámetros

---

### Yes

Especifica que los mensajes exclusivos se envían al servidor de eventos TEC.

### No

Especifica que los mensajes generales se envían al servidor de eventos TEC.

## Ejemplos

---

```
uniqueteevents yes
```

## USEREXIT

---

La opción USEREXIT especifica la salida definida por el usuario a la que se otorgará control para poder gestionar un evento.

## Sintaxis

---

```

(1)          (2)
>>-USEREXIT---+Yes+---nombre_módulo-----nombre_DLL----->
      '-No--'

(3)
>--función-----><

```

Notas:

1. *nombre\_módulo* sólo está disponible en AIX, HP-UX, Linux, Solaris y z/OS.
2. *nombre\_DLL* sólo está disponible en Windows.
3. *función* sólo está disponible en Windows.

## Parámetros



---



Yes



Especifica que cuando arranque el servidor se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos.

No


Especifica que cuando arranque el servidor no se iniciarán automáticamente las anotaciones de eventos en el receptor de salida de archivos. Cuando se especifica este parámetro, debe comenzar la anotación manual de eventos emitiendo el comando BEGIN EVENTLOGGING.


 Sistemas operativos AIX  Sistemas operativos Linux *nombre\_módulo*


 Sistemas operativos AIX  Sistemas operativos Linux Especifica el nombre de módulo de la salida de usuario.

 Sistemas operativos AIX  Sistemas operativos Linux Es el nombre de una biblioteca compartida que contiene el programa de salida. El nombre de módulo puede ser un nombre de ruta totalmente calificado, o simplemente un nombre de módulo. Si se trata sólo del nombre de módulo, se carga desde el directorio actual.

 Sistemas operativos Windows *nombre\_DLL*

 Sistemas operativos Windows Especifica el nombre DLL que contiene la función de salida de usuario.

 Sistemas operativos Windows *función*

 Sistemas operativos Windows Especifica el nombre de la función de salida de usuario de la DLL.

## Ejemplos

---

 Sistemas operativos Windows

```
userexit yes dllname.dll dllmodulename
```

 Sistemas operativos AIX  Sistemas operativos Linux

```
userexit yes fevent.exit
```

## VERBCHECK

---

La opción VERBCHECK especifica que el servidor realizará una comprobación de errores adicional en la estructura de comandos que el cliente ha enviado. Esta opción sólo debe habilitarse cuando el cliente envía al servidor solicitudes con un formato incorrecto, lo que provoca que el servidor se cuelgue. Cuando esta opción está habilitada, obtendrá un error de protocolo en lugar de que el servidor se cuelgue.

## Sintaxis

---

```
>>-VERBCHECK-----><
```

## Parámetros

---

Ninguno

## Ejemplos

---

Habilita la comprobación de errores adicional de los comandos que envía el cliente:

## VOLUMEHISTORY

---

La opción VOLUMEHISTORY especifica los nombres de los archivos que se actualizarán automáticamente cada vez que se cambie la información histórica de volúmenes secuenciales del servidor. No existe un valor predeterminado para esta opción.

Puede incluir una o varias opciones VOLUMEHISTORY en el archivo de opciones del servidor. Cuando utiliza varias opciones VOLUMEHISTORY, automáticamente el servidor actualiza y almacena una copia de seguridad de la información histórica de volúmenes en cada archivo que especifique.

### Sintaxis

---

```
>>-VOLUMEHistory--nombre_archivo-----><
```

### Parámetros

---

nombre\_archivo

Especifica el nombre del archivo en el que desea que el servidor almacene una copia de seguridad de la información histórica de volúmenes que recoja.

### Ejemplos





---

```
volumehistory volhist.out
```



## Herramientas del servidor


---

Utilice las herramientas del servidor para realizar tareas especiales en el servidor mientras éste no está en ejecución.

-  Sistemas operativos Windows DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)  
Utilice el programa de utilidad DSMMAXSG para aumentar la longitud de transferencia máxima de los adaptadores de bus de host (HBA). Como resultado de ello, el tamaño de bloque que utiliza el servidor de IBM Spectrum Protect para la grabación de datos y para la obtención de datos de determinados tipos de unidades de cinta aumenta.
- DSMSERV (Iniciar el servidor)  
Utilice este programa de utilidad para iniciar el servidor de IBM Spectrum Protect.
-  Sistemas operativos AIX  Sistemas operativos Linux Script de inicio del servidor: rc.dsmserv  
Puede utilizar el script rc.dsmserv al arrancar el sistema para iniciar automáticamente una instancia de servidor con un ID de usuario específico.
-  Sistemas operativos Linux Script de inicio del servidor: dsmserv.rc  
Puede utilizar el script dsmserv.rc para detener una instancia del servidor o para iniciar manual o automáticamente un servidor.
- DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)  
Utilice este programa de utilidad para visualizar información sobre el espacio de almacenamiento definido para la base de datos. La salida de este programa de utilidad es la misma que la salida del mandato QUERY DBSPACE, pero puede utilizar este programa de utilidad cuando el servidor no se está ejecutando.
- DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)  
Utilice este programa de utilidad para visualizar información sobre anotaciones de recuperación, incluidas las anotaciones activas, la duplicación para las anotaciones activas, el directorio de recuperación de errores para las anotaciones de archivado y la ubicación de desbordamiento para las anotaciones. Utilice este programa de utilidad cuando el servidor no esté en ejecución.
- DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)  
Utilice este programa de utilidad para aumentar el espacio para la base de datos agregando directorios para que los utilice la base de datos. Este programa de utilidad realiza la misma función que el mandato EXTEND DBSPACE, pero puede utilizarlo cuando el servidor no esté ejecutándose.
- DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)  
Utilice el programa de utilidad DSMSERV FORMAT para inicializar las anotaciones de recuperación y de base de datos del servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.
- DSMSERV INSERTDB (Mover una base de datos de servidor a una base de datos vacía)  
Utilice el programa de utilidad DSMSERV INSERTDB para mover una base de datos del servidor a una nueva base de datos. La base de datos puede extraerse del servidor original e insertarse en una nueva base de datos del nuevo servidor con una conexión de red entre los dos servidores. La base de datos también puede insertarse a partir de los medios que contienen la base de datos extraída.



- DSMSERV LOADFORMAT (Formatear una base de datos)  
Utilice el programa de utilidad DSMSERV LOADFORMAT cuando actualice desde la Versión 5. El programa de utilidad formatea una base de datos vacía como preparación para insertar una base de datos extraída en la base de datos vacía.
- DSMSERV REMOVEDB (Eliminar una base de datos)  
Utilice el programa de utilidad DSMSERV REMOVEDB para eliminar una base de datos de servidor de IBM Spectrum Protect.
- DSMSERV RESTORE DB (Restaurar la base de datos)  
Utilice este programa de utilidad para restaurar una base de datos mediante una copia de seguridad de ésta.
-  Sistemas operativos Windows DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)  
Utilice este programa de utilidad para crear entradas de registro para una instancia de servidor de IBM Spectrum Protect si las entradas se han suprimido accidentalmente.
-  Sistemas operativos AIX DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)  
Utilice este comando para capturar mensajes de consola de servidor de IBM Spectrum Protect a un archivo de anotaciones de usuario. Puede especificar que IBM Spectrum Protect grabe mensajes a más de un archivo de anotaciones de usuario.

 Sistemas operativos Windows

## DSMMAXSG (Aumentar el tamaño de bloque para la grabación de datos)

Utilice el programa de utilidad DSMMAXSG para aumentar la longitud de transferencia máxima de los adaptadores de bus de host (HBA). Como resultado de ello, el tamaño de bloque que utiliza el servidor de IBM Spectrum Protect para la grabación de datos y para la obtención de datos de determinados tipos de unidades de cinta aumenta.

Con este programa de utilidad, el tamaño máximo de bloque que se puede especificar es de 256 KB. En función del entorno del sistema, el aumento del tamaño de bloque puede mejorar la velocidad a que IBM Spectrum Protect procesa datos en operaciones de copia de seguridad y restauración, y de archivado y recuperación. Sin embargo, el programa de utilidad no afecta a la generación de conjuntos de copias de seguridad.

Tan solo pueden utilizarse unidades de cintas que estén conectadas a los HBA SCSI o de canal de fibra y que tienen los siguientes tipos de dispositivo:

- 3590
- 3592
- DLT
- ECARTRIDGE
- LTO

El programa de utilidad se ejecuta automáticamente como parte de la instalación del servidor de IBM Spectrum Protect y del agente de almacenamiento. Sin embargo, si instala un nuevo HBA en el sistema después de instalar un servidor o un agente de almacenamiento, o si instala una nueva versión de un controlador de dispositivo HBA existente que restablezca el valor del tamaño máximo de transferencia, deberá ejecutar manualmente el programa de utilidad para aprovechar el tamaño de bloque mayor.

Cuando se ejecuta este programa de utilidad, se modifica una clave del registro para cada controlador HBA del sistema. El nombre de la clave es MaximumSGList.

Restricción: Si se realiza una operación de copia de seguridad o de archivado de datos en cinta utilizando el tamaño de bloque de 256 KB y el HBA no da soporte a ese tamaño de bloque, no podrá agregar datos a la cinta ni leer datos de ella. Por ejemplo, si utiliza un sistema Windows de 256 KB para realizar la copia de seguridad de los datos del cliente en el servidor de IBM Spectrum Protect, no podrá restaurar los datos con un sistema Windows que dé soporte a una longitud de transferencia distinta. Para agregar datos o leer datos desde una cinta grabada con una longitud de transferencia de 256 KB, debe instalar un HBA que dé soporte a transferencias de 256 KB.

### Sintaxis

```
>>-dsmmaxsg-----<<
```

### Ejemplo: incrementar el tamaño de bloque para la grabación de datos


Ejecutar el programa de utilidad DSMMAXSG para aumentar el tamaño de bloque que utiliza IBM Spectrum Protect.




```
dsmmaxsg
```

## DSMSERV (Iniciar el servidor)

Utilice este programa de utilidad para iniciar el servidor de IBM Spectrum Protect.

Restricciones:

- No entre más de 1022 caracteres en la interfaz de línea de mandatos de la consola DSMSERV. El texto que sobrepasa los 1022 caracteres se trunca.
-  Sistemas operativos Windows Los parámetros siguientes se excluyen entre sí:
  - NOEXPIRE
  - RUNFILE
  - MAINTENANCE




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Sintaxis



















```
>>-DSMSERV-----+----->
| (1) |
'|----- -u--nombre_usuario-'|
| |
| (2) .- -k--Server1-----.|
>+-----+-----+-----+----->
| (1) | | | | |
'|----- -i--dir_instancia-'| '|- -k--nombre_clave-''|
| |
| (1) | | (3) | |
'|----- -noexpire-'' '|-----NOEXPIRE-''|
| |
| '- -o--archivo_opciones-'' | (1) |
'|----- -quiet-'' |
| |
>+-----+-----+-----+-----<<
+-RUNFILE--nombre_archivo-+
| (4) |
'|-----MAINTenance-----'|
```

Notas:

1. Este parámetro se aplica solo a servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.
3. Este parámetro solo se aplica a los servidores Windows.
4. Este parámetro se aplica solo a servidores AIX, Linux, y Windows.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre\_usuario  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica el nombre de usuario al que cambiar antes de iniciar el servidor. Para iniciar el servidor desde el ID de usuario root, debe especificar el parámetro -u y seguir las instrucciones de Inicio del servidor desde el ID de usuario root.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir\_instancia  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. El directorio de instancia se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows-k nombre\_clave  
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es Server1.
-  Sistemas operativos AIX  Sistemas operativos Linux-noexpire  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica que el servidor no elimina archivos caducados de la base de datos de servidor. Los archivos no se suprimen del almacenamiento del servidor cuando se inicia el servidor.
-  Sistemas operativos WindowsNOEXPIRE  
 Sistemas operativos WindowsEspecifica que el servidor no elimina archivos caducados de la base de datos de servidor. Los archivos no se suprimen del almacenamiento del servidor cuando se inicia el servidor.
- o archivo\_opciones  
Especifica un archivo de opciones para utilizarlo.
-  Sistemas operativos AIX  Sistemas operativos Linux-quiet

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Especifica que se suprimen los mensajes para la consola.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows **MAINTenance**

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Especifica que el servidor se ha iniciado en modalidad de mantenimiento y que las planificaciones de mandatos administrativos, las planificaciones de cliente, las sesiones de cliente, la reclamación de espacio de almacenamiento, la caducidad del inventario y la migración de la agrupación de almacenamiento están inhabilitadas.

Consejo: La modalidad de mantenimiento es el método preferido para ejecutar el servidor durante las tareas de mantenimiento o reconfiguración. Cuando se ejecuta el servidor en modalidad de mantenimiento, las operaciones que pueden interrumpir las tareas de mantenimiento o reconfiguración se inhabilitan automáticamente.

**RUNFILE** Nombre\_archivo

Especifica el nombre de un archivo que debe ejecutarse en el servidor. El archivo contiene una lista de mandatos de servidor.

Atención: Cuando se utiliza el parámetro RUNFILE, el servidor se detiene cuando se completa el proceso. Debe reiniciar el servidor utilizando el programa de utilidad DSMSERV.

## Ejemplo: iniciar el servidor

---

Inicie el servidor para un funcionamiento normal. Emita el siguiente mandato en una sola línea:

Sistemas operativos AIX

```
LDR_CNTRL=TEXTPSIZE=64K@DATAPSIZE=64K@STACKPSIZE=64K@SHMPSIZE=64K  
usr/bin/dsmserv
```

Sistemas operativos AIX asegúrese de incluir un espacio después de `SHMPSIZE=64K`. Al iniciar el servidor con este comando, puede habilitar 64 KB de páginas de memoria para el servidor. Este valor permite optimizar el rendimiento del servidor.

Sistemas operativos Linux

```
/opt/tivoli/tsm/server/bin/dsmserv
```

Sistemas operativos Windows

```
C:\Archivos de programa\Tivoli\TSM\bin\dsmserve -k server2
```

Sistemas operativos Windows

## Ejemplo: iniciar otro servidor

---

Inicie un servidor adicional utilizando la clave de registro denominada SERVER2.

```
dsmserv -k server2
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows

## Ejemplo: cargar el script de ejemplo

---

Cargar el archivo de script de ejemplo que se proporciona con el servidor.

```
dsmserv  
runfile scripts.smp
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows

## Ejemplo: iniciar el servidor en modalidad de mantenimiento

---

Antes de iniciar las tareas de mantenimiento o reconfiguración, inicie el servidor en modalidad de mantenimiento.

```
dsmserv maintenance
```

### Tareas relacionadas:

Inicio del servidor en modalidad de mantenimiento

Sistemas operativos AIX

## Script de inicio del servidor: rc.dsmserve

---

Puede utilizar el script `rc.dsmserve` al arrancar el sistema para iniciar automáticamente una instancia de servidor con un ID de usuario específico.

## Sintaxis

---



```
>>-rc.dsmsserv--+ -u--nombre_usuario+----->
                '- -U--nombre_usuario-'
>--+-----+-----<
    '- -i--dir_instancia-'
```

## Parámetros

---

- u nombre\_usuario  
Especifica el ID de usuario de la instancia para la cual se ha configurado el entorno. El servidor se ejecutará con este ID de usuario.
- U nombre\_usuario  
Especifica el ID de usuario de la instancia para la cual se ha configurado el entorno. El servidor se ejecutará con el ID de usuario del invocador del mandato.
- i dir\_instancia  
Especifica un directorio de instancia, que se convierte en el directorio de trabajo del servidor.

### Tareas relacionadas:

-  AIX: Inicio automático de servidores
-  Sistemas operativos Linux

## Script de inicio del servidor: dsmsserv.rc

---

Puede utilizar el script dsmsserv.rc para detener una instancia del servidor o para iniciar manual o automáticamente un servidor.

## Requisitos previos

---

Antes de emitir el mandato DSMSSERV.RC, complete los pasos siguientes:

1. Asegúrese de que la instancia de servidor se ejecuta bajo un ID de usuario no root con el mismo nombre que el propietario de la instancia.
2. Copie el script dsmsserv.rc en el directorio /etc/rc.d/init.d. El script dsmsserv.rc está en el directorio de instalación del servidor, por ejemplo, /opt/tivoli/tsm/server/bin.
3. Cambie el nombre del script de modo que coincida con el nombre del propietario de la instancia de servidor, por ejemplo, tsminst1.
4. Si el directorio de instancia de servidor no es directorio\_inicio/tsminst1, localice la siguiente línea en la copia del script:

```
instance_dir="${instance_home}/tsminst1"
```

Cambie la línea para que apunte al directorio de instancia de servidor, por ejemplo:

```
instance_dir="/tsminst1"
```

5. En la copia del script, localice la línea siguiente:

```
# pidfile: /var/run/dsmsserv_instancename.pid
```

Cambie el valor del nombre de instancia por el nombre del propietario de la instancia del servidor. Por ejemplo, si el propietario de la instancia del servidor es tsminst1, actualice la línea como se muestra:

```
# pidfile: /var/run/dsmsserv_tsminst1.pid
```

6. Utilice herramientas como el programa de utilidad CHKCONFIG para configurar el nivel de ejecución en el que se inicia automáticamente el servidor. Especifique un valor que corresponda con una modalidad multiusuario, con el uso de redes habilitado. Generalmente, el nivel de ejecución que se utilizará es 2, 3 o 5, en función del sistema operativo y de su configuración. Para obtener más detalles sobre los niveles de ejecución, consulte la documentación de su sistema operativo.

## Sintaxis

---

```
>>-dsmsserv.rc--+-----<
                +-start---+
                +-stop----+
                +-estado---
```

```
'-restart-'
```

## Parámetros

---


**start**  
Inicia el servidor.

**stop**  
Detiene el servidor.

**status**  
Muestra el estado del servidor. Si el estado es *iniciado*, el ID de proceso del proceso de servidor también se conoce.

**restart**  
Detiene el servidor y lo inicia de nuevo.

### Tareas relacionadas:

 [Linux: Inicio automático de servidores en sistemas Linux](#)

## DSMSERV DISPLAY DBSPACE (Visualizar información sobre espacio de almacenamiento de base de datos)

---

Utilice este programa de utilidad para visualizar información sobre el espacio de almacenamiento definido para la base de datos. La salida de este programa de utilidad es la misma que la salida del mandato QUERY DBSPACE, pero puede utilizar este programa de utilidad cuando el servidor no se está ejecutando.

## Sintaxis

---





```
>>-DSMSERV -+-----+----->
              | (1)                                     |
              '----- -u--nombre_usuario-'
              (2) .- -k--Server1-----
>--+-----+-----+-----+-----+----->
              | (1)                                     |   '- -k -nombre_clave-'
              '----- -i--dir_instancia-'
>--+-----+-----+-----+-----+----->
              '- -o--archivo_opciones-'   '- -noexpire-'   '- -quiet-'
>--DISPlay DBSPace-----<<
```





### Notas:



1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros

---

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)-u nombre\_usuario  
 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor.

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)-i dir\_instancia  
 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)Especifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.

 [Sistemas operativos Windows](#)-k nombre\_clave  
 [Sistemas operativos Windows](#)Especifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo cuando exista más de un servidor en el mismo sistema. El valor predeterminado es SERVER1.

-o archivo\_opciones  
Especifica un archivo de opciones para utilizarlo.

-noexpire  
Especifica que el proceso de caducidad se suprime durante el inicio.

-quiet  
Especifica que se suprimen los mensajes para la consola.


## Ejemplo: visualizar información acerca del espacio de base de datos

Visualizar información acerca del espacio de almacenamiento de la base de datos. Consulte la publicación Descripciones de los campos para obtener detalles sobre la información que aparece en la salida. Emita el comando.

```
dsmserv display dbspace
```

 Sistemas operativos AIX  Sistemas operativos Linux

Ubicación	Espacio total (MB)	Espacio utilizado (MB)	Espacio libre (MB)
/tsmdb001	46.080,00	20.993,12	25.086,88
/tsmdb002	46.080,00	20.992,15	25.087,85

 Sistemas operativos Windows

Ubicación	Espacio total (MB)	Espacio utilizado (MB)	Espacio libre (MB)
d:\tsm\db001	46.080,00	20.993,12	25.086,88
d:\tsm\db002	46.080,00	20.993,15	25.087,85

## Descripciones de los campos

### Ubicación

Directorio o ruta que se utiliza para almacenar la base de datos



### Espacio total (MB)

Número total de megabytes de la ubicación

### Espacio utilizado (MB)

Número de megabytes en uso en la ubicación

### Espacio libre (MB)

 Sistemas operativos AIX  Sistemas operativos Linux Espacio que queda en el sistema de archivos en el que se encuentra la ruta

 Sistemas operativos Windows Espacio que queda en la unidad en la que se encuentra el directorio

## DSMSERV DISPLAY LOG (Visualizar información de anotaciones de recuperación)

Utilice este programa de utilidad para visualizar información sobre anotaciones de recuperación, incluidas las anotaciones activas, la duplicación para las anotaciones activas, el directorio de recuperación de errores para las anotaciones de archivado y la ubicación de desbordamiento para las anotaciones. Utilice este programa de utilidad cuando el servidor no esté en ejecución.

## Sintaxis

```
>>-DSMSERV -+-----+----->
      | (1) |
      '-u--nombre_usuario-'

      (2) .- -k--Server1-----.
>+-----+-----+-----+----->
      | (1) | | '- -k--nombre_clave-'
      '-i--dir_instancia-'







>+-----+-----+-----+----->
      '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'

>--DISPLAY LOG-----<<
```

### Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros


-  Sistemas operativos Linux-u nombre\_usuario  
 Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor.
-  Sistemas operativos Linux-i dir\_instancia  
 Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows-k nombre\_clave  
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. Utilice este parámetro sólo cuando exista más de un servidor en el mismo sistema. El valor predeterminado es SERVER1.
- o archivo\_opciones  
 Especifica un archivo de opciones para utilizarlo.
- noexpire  
 Especifica que el proceso de caducidad se suprime durante el inicio.
- quiet  
 Especifica que se suprimen los mensajes para la consola.

## Ejemplo: visualizar información de las anotaciones de recuperación

---


Visualizar información acerca de las anotaciones de recuperación. Consulte la publicación Descripciones de los campos para obtener detalles sobre la información que aparece en la salida.

```
dsmserv display log
```

 Sistemas operativos Linux

```

Espacio total(MB): 38.912
Espacio utilizado(MB): 401.34
Espacio libre(MB): 38.358,65
Directorio anotaciones activas: /activelog
Directorio anotaciones archivado: /archivelog
Directorio anotaciones duplicadas: /mirrorlog
Directorio anotac. recuperación errores archivado: /archfailoverlog
```

 Sistemas operativos Windows

```

Espacio total(MB): 38.912
Espacio utilizado(MB): 401.34
Espacio libre(MB): 38.358,65
Directorio anotaciones activas: h:\tsm\activelog
Directorio anotaciones archivado: k:\tsm\archivelog
Directorio anotaciones duplicadas: i:\tsm\mirrorlog
Directorio de anotaciones de recuperación de errores de archivado: j:\tsm\archfailoverlog
```

## Descripciones de los campos

---

- Espacio total  
 Especifica el tamaño máximo de las anotaciones activas.
- Espacio utilizado  
 Especifica la cantidad total del espacio de anotaciones activas que utiliza actualmente la base de datos, en megabytes.
- Espacio libre  
 Especifica la cantidad de espacio de anotaciones activas en la base de datos que no se utiliza para transacciones sin validar, en megabytes.
- Directorio de anotaciones activas  
 Especifica la ubicación donde se guardan los archivos de anotaciones activas. Cuando cambie el directorio de anotaciones activas, el servidor moverá todas las anotaciones archivadas al directorio de anotaciones de archivado y todas las anotaciones activas a un nuevo directorio de anotaciones activas.
- Directorio anotaciones duplicadas  
 Especifica la ubicación en la que se mantiene la duplicación de las anotaciones activas.
- Directorio de anotaciones de recuperación de errores de archivado  
 Especifica la ubicación en la que el servidor guarda las anotaciones de archivado si las anotaciones no se pueden archivar en el destino de las anotaciones de archivado.

## DSMSERV EXTEND DBSPACE (Incrementar el espacio para la base de datos)

---

Utilice este programa de utilidad para aumentar el espacio para la base de datos agregando directorios para que los utilice la base de datos. Este programa de utilidad realiza la misma función que el mandato EXTEND DBSPACE, pero puede utilizarlo cuando el servidor





## Ejemplo: aumentar el espacio para la base de datos

Añadir un directorio denominado stg1 en el directorio tsm\_db para el espacio de almacenamiento de base de datos y, a continuación, redistribuir los datos y reclamar espacio emitiendo el mandato siguiente:

```
dsmserv extend dbSPACE /tsm_db/stg1
```

 Sistemas operativos Windows

## Ejemplo: aumentar el espacio para la base de datos

Añadir la unidad D al espacio de almacenamiento para la base de datos y luego redistribuir los datos y reclamar almacenamiento emitiendo el mandato siguiente:

```
dsmserv extend dbSPACE D:
```


### Referencia relacionada:


EXTEND DBSPACE (Incrementar el espacio para la base de datos)

## DSMSERV FORMAT (Dar formato a la base de datos y a las anotaciones)

Utilice el programa de utilidad DSMSERV FORMAT para inicializar las anotaciones de recuperación y de base de datos del servidor. No se permite ninguna otra actividad del servidor durante la inicialización de las anotaciones de recuperación y la base de datos.

Los directorios que se especifican en este programa de utilidad han de corresponder a almacenamiento rápido y fiable. No sitúe los directorios en sistemas de archivos que podrían quedarse sin espacio. Si determinados directorios (por ejemplo, el directorio de anotaciones activas), dejan de estar disponibles o se llenan, el servidor se detendrá.

 **Sistemas operativos Windows** Restricción: Si está utilizando una tabla de asignación de archivos (FAT o FAT32) o un formato New Technology File System (NTFS), no puede especificar el directorio raíz de dicho sistema como la ubicación de un directorio de base de datos o un directorio de registros. En su lugar, debe crear uno o varios subdirectorios dentro del directorio raíz. A continuación, cree los directorios de bases de datos y directorios de registros dentro de los subdirectorios.

 **Sistemas operativos Windows** Importante: El programa de instalación crea un conjunto de claves de registro. Una de estas claves señala al directorio en el que se crea el servidor predeterminado, denominado SERVER1. Para instalar un servidor adicional, cree un directorio y utilice el programa de utilidad DSMSERV FORMAT, con el parámetro -k, desde dicho directorio. Ese directorio se convierte en la ubicación del servidor. El registro realiza un seguimiento de los servidores instalados.

Cuando se crea un servidor inicialmente, con el programa de utilidad DSMSERV FORMAT o con el asistente de configuración, se crean una base de datos de servidor y un registro de recuperación. Asimismo, se crean archivos para mantener la información de base de datos que utiliza el gestor de bases de datos.

## Sintaxis





```
>>>DSMSERV -+-----+----->
          | (1) |
          +----- -u--nombre_usuario-'
          (2) .- -k--Server1-----.
>+-----+-----+-----+----->
  | (1) | | '- -k--nombre_clave-'
  +----- -i--dir_instancia-'
>+-----+-----+-----+----->
  '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'
          .-,-----
          v |
>--FORMAT--+-DBDir-----directorio+-+----->
            '-DBFile-----archivo-----'
          .-ACTIVELOGSize-----16384-----
>+-----+-----+-----+----->
  '-ACTIVELOGSize-----megabytes-'
>--ACTIVELOGDirectory-----directory----->
>--ARCHLogdirectory-----directory----->
>+-----+-----+-----+----->
```





```
'-ARCHFailoverlogdirectory---directory-'
>-----<
'-MIRRorlogdirectory---directory-'
```



**Notas:**

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros

 **Sistemas operativos AIX**  **Sistemas operativos Linux-u nombre\_usuario**  
 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor. Este parámetro es opcional.

 **Sistemas operativos AIX**  **Sistemas operativos Linux-i dir\_instancia**  
 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.

 **Sistemas operativos Windows-k nombre\_clave**  
 **Sistemas operativos Windows** Especifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo para instalar servidores adicionales en el mismo sistema. Después de instalar un servidor mediante este parámetro, siempre debe iniciarlo con el valor de este parámetro. Este parámetro es opcional. El valor predeterminado es SERVER1.  
 Restricción: Las instancias adicionales del servidor IBM Spectrum Protect que se ejecuten en el mismo sistema competirán por los recursos y tendrán un impacto en el rendimiento general de cada servidor IBM Spectrum Protect.

-o archivo\_opciones  
 Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.

-noexpire  
 Especifica que el proceso de caducidad se suprime durante el inicio. Este parámetro es opcional.

-quiet  
 Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.

DBDir  
 Especifica los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. Los nombres de directorio deben separarse mediante comas pero sin espacios. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

DBFile  
 Especifica el nombre de un archivo que contiene los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. El nombre de directorio de cada volumen debe estar en una línea aparte. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

ACTIVELOGSize  
 Especifica el tamaño del archivo de anotaciones activas en megabytes. Este parámetro es opcional. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16384 MB.

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Obligatorio)  
 Especifica el directorio en el que el servidor graba y almacena los archivos de registro activo. Sólo existe una ubicación de anotaciones activas. El nombre debe ser un nombre de directorio cualificado al completo. El directorio debe existir, debe estar vacío, y debe ser accesible mediante el ID de usuario del gestor de base de datos. El número máximo de caracteres es 175.

ARCHLogdirectory (Obligatorio)  
 Especifica el directorio para los archivos de anotaciones de archivado. El nombre debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

## ARCHFailoverlogdirectory

Especifica el directorio que se utilizará como ubicación de almacenamiento alternativa si el directorio ARCHLOGDIRECTORY se llena. Este parámetro es opcional. El número máximo de caracteres es 175.


## MIRRORlogdirectory

Especifica el directorio en el que el servidor duplicará las anotaciones activas (los archivos en el directorio ACTIVELOGDIRECTORY). Este parámetro es opcional. El directorio debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

## Ejemplo: formatear una base de datos

 Sistemas operativos AIX  Sistemas operativos Linux

```
dsmserv format dbdir=/tsmdb001 activelogsiz=8192
activelogdirectory=/activelog archlogdirectory=/archlog
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

 Sistemas operativos Windows

```
dsmserv -k server2 format dbdir=d:\tsm\db001 activelogsiz=8192
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

## DSMSERV INSERTDB (Mover una base de datos de servidor a una base de datos vacía)

Utilice el programa de utilidad DSMSERV INSERTDB para mover una base de datos del servidor a una nueva base de datos. La base de datos puede extraerse del servidor original e insertarse en una nueva base de datos del nuevo servidor con una conexión de red entre los dos servidores. La base de datos también puede insertarse a partir de los medios que contienen la base de datos extraída.

Antes de utilizar el programa de utilidad DSMSERV INSERTDB, complete las tareas de planificación y preparación, tales como realizar la copia de seguridad de la base de datos y guardar la información de la configuración. Asegúrese de que cumple todos los requisitos previos antes de mover la base de datos del servidor.

## Requisitos para la inserción empleando medios

Antes de ejecutar el programa de utilidad para insertar la base de datos de servidor en una base de datos vacía, asegúrese de que el sistema satisface los requisitos siguientes.

- Debe disponerse del archivo de manifiesto de la operación DSMUPGRD EXTRACTDB.
- Si el archivo de manifiesto no contiene información de configuración de dispositivo, o si especifica el parámetro CONFIGINFO=DEVCONFIG, deben cumplirse las siguientes sentencias:
  - El archivo de opciones de servidor debe contener una entrada para el archivo de configuración de dispositivo.
  - El archivo de configuración de dispositivo debe contener información acerca de la clase de dispositivo que se especifica en el archivo de manifiesto.
- Los medios que contienen la base de datos extraída deben estar disponibles para el servidor V8. Asimismo, deben establecerse los permisos para garantizar el acceso a los medios a los ID de usuarios propietarios de la instancia del servidor V8.

## Sintaxis

```
>>-DSMSERV -+-----+----->
          | (1)                               |
          '----- -u--nombre_usuario-'
                                     (2) .- -k--Server1-----
>-+-----+-----+-----+----->
          | (1)                               |   '- -k--nombre_clave-'
          '----- -i--dir_instancia-'
>-+-----+-----+-----+----->
          '- -o--archivo_opciones-' '- -noexpire-' '- -quiet-'
>--INSERTDB---+| A: Inserción empleando medios |-----+----->
               '-| B: Inserción por medio de una red |-
               .-PREview----No-----
>-+-----+-----+-----+-----<
          '-PREview----+Yes-+-'
```

```
'-No--'
```

A: Inserción empleando medios

```
|---+-----+----->
  '-DEVclass---nombre_clase_dispositivo-'
  .-CONFiginfo---MANifest-----
>---+-----+---MANifest---file_name---|
  '-CONFiginfo---+MANifest-+-'
      '-DEVconfig-'
```











B: Inserción por medio de una red

```
.-SESSWait---60-----
|---+-----+-----|
  '-SESSWait---minutos-'
```

Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre\_usuario  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor. Este parámetro es opcional.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir\_instancia  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.
-  Sistemas operativos Windows-k nombre\_clave  
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. Este parámetro es opcional. El valor predeterminado es SERVER1.
- o archivo\_opciones  
Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.
- noexpire  
Especifica que el proceso de caducidad se suprime durante el inicio. Este parámetro es opcional.
- quiet  
Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.
- DEVclass  
Especifica una clase de dispositivo de acceso secuencial. Puede especificar cualquier clase de dispositivo excepto la clase de dispositivo DISK. La definición de la clase de dispositivo debe existir en el archivo de manifiesto o el archivo de configuración de dispositivo.  
Este parámetro es opcional y se utiliza sólo cuando la base de datos que desea insertar en la base de datos V8 vacía se ha extraído en medios. Si la base de datos se encuentra en un medio y no especifica una clase de dispositivo, se utiliza la clase de dispositivo identificada en el archivo de manifiesto.  
Restricción: No puede utilizar una clase de dispositivo con un tipo de dispositivo NAS o CENTERA.
- MANifest  
Especifica la ubicación del archivo de manifiesto. Utilice un nombre de archivo cualificado al completo o indique un directorio local. Por ejemplo: ./manifest.txt  
  
Este parámetro es necesario cuando la base de datos que desea insertar en la base de datos V8 vacía se ha extraído en medios.
- CONFiginfo  
Especifica el origen de la información de configuración de dispositivo que ha utilizado la operación DSMSEV INSERTDB. El valor predeterminado para este parámetro es MANIFEST. Los valores posibles son los siguientes:
- MANifest  
Especifica que la información de configuración de dispositivo se lee desde el archivo manifiesto. Si el archivo de manifiesto no tiene información de configuración de dispositivo, en su lugar se utiliza el archivo de configuración de dispositivo.
- DEVConfig  
Especifica que la información de configuración de dispositivo se lee desde el archivo de configuración de dispositivo.
- SESSWait  
Especifica el número de minutos que el servidor V8 esperará a ser contactado por el servidor original. El valor predeterminado es de 60 minutos.

Utilice este parámetro sólo si los datos que se insertan en la base de datos V8 vacía se transmiten desde el servidor de origen con una conexión de red.

#### PREview

Especifica si se obtiene una vista previa de la operación de inserción. Este parámetro es opcional. El valor predeterminado es NO.

Utilice el parámetro PREVIEW=YES para probar una base de datos. Si utiliza este parámetro, la operación incluye todos los pasos del proceso, salvo la inserción real de datos en la nueva base de datos. Si ve una vista previa de la operación de inserción, puede verificar rápidamente que la base de datos de origen se puede leer. También puede identificar el incumplimiento de las restricciones de datos que pueden evitar que una base de datos actualizada se ponga en producción.

## DSMSERV LOADFORMAT (Formatear una base de datos)

Utilice el programa de utilidad DSMSERV LOADFORMAT cuando actualice desde la Versión 5. El programa de utilidad formatea una base de datos vacía como preparación para insertar una base de datos extraída en la base de datos vacía.











### Sintaxis

```
>>-DSMSERV -+-----+----->
          | (1)
          |----- -u--nombre_usuario-|
          |
          | (2) .- -k--Server1----- .
>+-----+-----+-----+----->
          | (1)
          |----- -i--dir_instancia-|
          |
          |----- -o--archivo_opciones-|
          |----- -noexpire-|
          |----- -quiet-|
          |
          |----- .- ,----- .
          |----- v----- |
>--LOADFORMAT--+-DBDir-----directorio+----->
          |----- -DBFile-----archivo-----|
          |
          |----- .-ACTIVELOGSize-----16384----- .
>+-----+-----+-----+----->
          |----- -ACTIVELOGSize-----megabytes-|
          |
>--ACTIVELOGDirectory-----directory----->
          |
>--ARCHLogdirectory-----directory----->
          |
>+-----+-----+-----+----->
          |----- -ARCHFailoverlogdirectory-----directory-|
          |
>+-----+-----+-----+-----<
          |----- -MIRRORlogdirectory-----directory-|
          |
```

#### Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

### Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux-u nombre\_usuario  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor. Este parámetro es opcional.
-  Sistemas operativos AIX  Sistemas operativos Linux-i dir\_instancia  
 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Este directorio se convierte en el directorio de trabajo actual del servidor. Este parámetro es opcional.
-  Sistemas operativos Windows-k nombre\_clave  
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows que se utiliza para almacenar información sobre este servidor. Utilice este parámetro sólo para instalar servidores adicionales en el mismo sistema. Después de instalar un servidor mediante este parámetro, siempre debe iniciarlo con el valor de este parámetro. El valor predeterminado es SERVER1.

-o archivo\_opciones

Especifica un archivo de opciones para utilizarlo. Este parámetro es opcional.

-noexpire

Especifica que el proceso de caducidad se suprime cuando se inicia el servidor. Este parámetro es opcional.

-quiet

Especifica que se suprimen los mensajes para la consola. Este parámetro es opcional.

DBDir

Especifica los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. Los nombres de directorio deben separarse mediante comas pero sin espacios. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

DBFile

Especifica el nombre de un archivo que contiene los nombres de ruta relativa de uno o más directorios que se utilizan para almacenar objetos de base de datos. El nombre de directorio de cada volumen debe estar en una línea aparte. Puede especificar hasta 128 nombres de directorio. Debe especificar el parámetro DBDIR o el parámetro DBFILE.

ACTIVELOGSize

Especifica el tamaño del archivo de anotaciones activas en megabytes. Este parámetro es opcional. El valor mínimo es de 2048 MB (2 GB) y el máximo de 524,288 MB (512 GB). Si se especifica un número impar, el valor se redondea hasta el siguiente número par. El valor predeterminado es 16384 MB.

El tamaño de un archivo de registro está basado en el valor de la opción ACTIVELOGSIZE. Las directrices para los requisitos de espacio las encontrará en la tabla siguiente:

Tabla 1. Cómo calcular los requisitos de volumen y de espacio de archivos

Valor de la opción ACTIVELOGSize	Reserve esta cantidad de espacio libre en el directorio de registros activos, además del espacio ACTIVELOGSize
16 GB - 128 GB	5120 MB
129 GB - 256 GB	10240 MB
257 GB - 512 GB	20480 MB

ACTIVELOGDirectory (Obligatorio)

Especifica el directorio en el que el servidor graba y almacena los archivos de registro activo. Sólo existe una ubicación de anotaciones activas. El nombre debe ser un nombre de directorio cualificado al completo. El directorio debe existir, debe estar vacío, y debe ser accesible mediante el ID de usuario del gestor de base de datos. El número máximo de caracteres es 175.

ARCHLogdirectory (Obligatorio)

Especifica el directorio para los archivos de anotaciones de archivado. El nombre debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

ARCHFailoverlogdirectory

Especifica el directorio que se utilizará como ubicación de almacenamiento alternativa si el directorio ARCHLOGDIRECTORY se llena. Este parámetro es opcional. El número máximo de caracteres es 175.

MIRRORlogdirectory

Especifica el directorio en el que el servidor duplicará las anotaciones activas (los archivos en el directorio ACTIVELOGDIRECTORY). Este parámetro es opcional. El directorio debe ser un nombre de directorio cualificado al completo. El número máximo de caracteres es 175.

## Ejemplo: formatear una base de datos

 Sistemas operativos AIX  Sistemas operativos Linux

```
dsmserv loadformat dbdir=/tsmdb001 activelogsiz=8192  
activelogdirectory=/activelog archlogdirectory=/archlog  
archfailoverlogdirectory=/archfaillog mirrorlogdirectory=/mirrorlog
```

 Sistemas operativos Windows

```
dsmserv -k server2 loadformat dbdir=d:\tsm\db001 activelogsiz=8192  
activelogdirectory=e:\tsm\activelog archlogdirectory=f:\tsm\archlog  
archfailoverlogdirectory=g:\tsm\archfaillog mirrorlogdirectory=h:\tsm\mirrorlog
```

## DSMSERV REMOVEDB (Eliminar una base de datos)

Utilice el programa de utilidad DSMSERV REMOVEDB para eliminar una base de datos de servidor de IBM Spectrum Protect.

Cuando ejecuta este programa de utilidad, se suprime la base de datos del servidor, los archivos de registro activo y los archivos de duplicación de registro activo. Sin embargo, los archivos de registro de archivado y archivos de registro de migración tras error del registro de archivado se suprimen sólo después de iniciar una restauración de base de datos en un punto en el tiempo.

El servidor de IBM Spectrum Protect debe detenerse antes de emitir este mandato.











## Sintaxis

```
>>-DSMSERV -+-----+----->
          | (1) |
          |----- -u--nombre_usuario-|
          |-----|
          |----- (2) .- -k--Server1-----|
>+-----+----->
          | (1) | | | -k--nombre_clave-|
          |----- -i--dir_instancia-|
          |-----|
          |-----+-----+-----+----->
          | -o--archivo_opciones-| | -noexpire-| | -quiet-|
          |-----|
          |----- .- -force---No-----|
>--REMOVEDB--nombre_basedatos-+-----+-----><
          |-----|
          |----- -force---No---+|
          |-----|
          |----- -Yes-|
```

### Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros

-  Sistemas operativos AIX  Sistemas operativos Linux -u nombre\_usuario  
 Sistemas operativos AIX  Sistemas operativos Linux Especifica un nombre de usuario al cual conmutar antes de inicializar el servidor.
-  Sistemas operativos AIX  Sistemas operativos Linux -i dir\_instancia  
 Sistemas operativos AIX  Sistemas operativos Linux Especifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.
-  Sistemas operativos Windows -k nombre\_clave  
 Sistemas operativos Windows Especifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.
- o archivo\_opciones  
Especifica un archivo de opciones para utilizarlo.
- noexpire  
Especifica que el proceso de caducidad se suprime durante el inicio.
- quiet  
Especifica que se suprimen los mensajes para la consola.
- nombre\_basedatos  
El nombre de base de datos que se especificó durante la instalación. Si la base de datos se formateó manualmente, este es el parámetro de nombre de base de datos del programa de utilidad DSMSERV FORMAT o DSMSERV LOADFORMAT. Este nombre de base de datos también puede encontrarse en el archivo dsmserv.opt. Este parámetro es necesario.
- force  
Especifica si se elimina la base de datos cuando hay conexiones abiertas. El valor predeterminado es No. Este parámetro es opcional. Los valores son los siguientes:
- Yes  
Especifica que la base de datos se elimine independientemente de las conexiones abiertas.
- No  
Especifica que la base de datos se elimine sólo cuando estén cerradas todas las conexiones.

## Ejemplo: eliminar una base de datos

Eliminar la base de datos de servidor de IBM Spectrum Protect TSMDB1 y todas sus referencias.

```
dsmserv removedb TSMDB1
```

## Ejemplo: eliminar una base de datos con el parámetro force

Elimine la base de datos de servidor de IBM Spectrum Protect TSMDB1 y todas sus referencias, aunque haya conexiones abiertas:

```
dsmserve removedb TSMDB1 force=yes
```

## DSMSERV RESTORE DB (Restaurar la base de datos)

Utilice este programa de utilidad para restaurar una base de datos mediante una copia de seguridad de ésta.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

La operación de restauración utiliza copias de seguridad de base de datos creadas con el mandato BACKUP DB.

Importante: Tras una operación de restauración a un punto en el tiempo específico, emita el mandato AUDIT VOLUME para auditar todos los volúmenes de DISK y resolver cualquier incoherencia entre la información de la base de datos y los volúmenes de agrupación de almacenamiento. Antes de restaurar la base de datos, examine el archivo histórico de volúmenes para averiguar los volúmenes de agrupaciones de almacenamiento de acceso secuencial que se suprimieron o reutilizaron desde el momento en el que se restauró la base de datos.

- DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)  
Utilice el programa de utilidad DSMSERV RESTORE DB para restaurar una base de datos a su estado más actualizado cuando se dan determinadas condiciones.
- DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)  
Utilice este mandato para restaurar una base de datos a momento anterior. Un archivo de historial de volumen y un archivo de configuración de dispositivo deben estar disponibles.

## DSMSERV RESTORE DB (Restaurar una base de datos a su estado más actualizado)

Utilice el programa de utilidad DSMSERV RESTORE DB para restaurar una base de datos a su estado más actualizado cuando se dan determinadas condiciones.

Deben satisfacerse las condiciones siguientes:

- Existe un archivo histórico de volúmenes intacto disponible.
- Las anotaciones de recuperación están disponibles.
- Existe un archivo de configuración de dispositivo con la información de dispositivo aplicable disponible.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

IBM Spectrum Protect solicita que los montajes de volúmenes carguen la serie de copias de seguridad más reciente y, a continuación, utiliza las anotaciones de recuperación para actualizar la base de datos a su estado más actual.

Las copias de seguridad de instantáneas de la base de datos no pueden utilizarse para restaurar una base de datos a su estado más actual.

## Sintaxis

```
>>-DSMSERV -+-----+----->
                | (1) |
                +----- -u--nombre_usuario-'
                (2) .- -k--Server1-----.
>+-----+-----+-----+----->
    | (1) | | '- -k--nombre_clave-'
    +----- -i--dir_instancia-'
>+-----+-----+-----+-----RESTORE DB----->
    '- -o--archivo_opciones-' | (1) |
                           +----- -quiet-'
```



```

>-----+----->
  '-RECOVerydir----directorio-'

>-----+----->
  '-ACTIVELOGDir----directorio-'

>-----+----->
  '-ON----archivo_directorio_destino-'

.-PReview-----No----- .-RESTOREKeys-----No-----
>-----+----->
  '-PReview----+Yes-+-'  '-RESTOREKeys-----+No-+-'
                '-No--'                      +-YES--+
                                                '-ONLY-'

>-----+-----<
  '-PASSword----nombre_contraseña-'

```

Notas:

1. Este parámetro solo se aplica a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.

## Parámetros

---

Sistemas operativos AIX Sistemas operativos Linux-u nombre\_usuario  
 Sistemas operativos AIX Sistemas operativos LinuxEspecifica un nombre de usuario al cual conmutar antes de inicializar el servidor.

Sistemas operativos AIX Sistemas operativos Linux-i dir\_instancia  
 Sistemas operativos AIX Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Este directorio de instancia se convierte en el directorio de trabajo actual del servidor.

Sistemas operativos Windows-k nombre\_clave  
 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.

-o archivo\_opciones  
Especifica un archivo de opciones para utilizarlo.

Sistemas operativos AIX Sistemas operativos Linux-quiet  
 Sistemas operativos AIX Sistemas operativos LinuxEspecifica que se suprimen los mensajes para la consola.

RECOVerydir  
Especifica un directorio donde almacenar la información de anotaciones de recuperación a partir de los soportes de copia de seguridad de la base de datos. Este directorio debe tener espacio suficiente para contener la información de recuperación de transacciones y debe ser un directorio vacío. Si no se especifica este parámetro, el valor predeterminado es el directorio especificado por uno de los parámetros siguientes en el programa de utilidad DSMSERV FORMAT o DSMSERV LOADFORMAT:

- ARCHFAILOVERLOGDIRECTORY, si se especifica
- ARCHLOGDIRECTORY, si no se ha especificado ARCHFAILOVERLOGDIRECTORY

ACTIVELOGDir

Especifica un directorio donde almacenar los archivos de anotaciones que se utilizan para rastrear las operaciones de la base de datos activas. Este directorio sólo debe especificarse si se tiene la intención de cambiar a un directorio de registros activos diferente del que ya se ha configurado.

On

Especifica un archivo que contiene un listado de los directorios en los que se restaurará la base de datos. Especifique cada directorio en una línea separada del archivo. Por ejemplo, el parámetro ON especifica el archivo restorelist.txt que contiene la lista siguiente: Sistemas operativos AIX Sistemas operativos Linux

```

/tsmdb001
/tsmdb002
/tsmdb003

```

Sistemas operativos Windows

```

e: \tsm\db001
f: \tsm\db002
g: \tsm\db003

```

Si no se especifica este parámetro, se utilizarán los directorios originales que se registraron en la copia de seguridad de la base de datos.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

#### PReview

Especifica que los archivos de historial de volumen se examinarán y que los volúmenes de copia de seguridad de base de datos del archivo de historial de volumen se evaluarán.

1. ¿Qué conjunto de volúmenes de copia de seguridad de base de datos cumple mejor los criterios más actualizados que se han especificado para el proceso de restauración? La información de historial de volumen proporciona detalles sobre el ID de serie de copias de seguridad, el ID de operación (completo, incremental 1, incremental 2, etc.), la fecha de la copia de seguridad de la base de datos, y la clase de dispositivo. Esta información y los parámetros especificados en el comando DSMSEV RESTORE DB determinan qué se utiliza para realizar la restauración. El archivo de historial de volumen se examina para buscar la copia de seguridad de base de datos más reciente y restaurar los datos utilizando esa copia de seguridad.
2. ¿Hay disponibles datos autodescriptivos para el conjunto seleccionado de volúmenes de copia de seguridad de base de datos? Coteje la información de historial de volumen para esta serie de copias de seguridad. La reconciliación notifica qué contienen los datos autodescriptivos comparados con los datos obtenidos de las entradas del historial de volumen. El cotejo implica montar uno o varios de los volúmenes indicados en el historial de volumen. A continuación, utilizando los datos autodescriptivos que se han incluido en los volúmenes de copia de seguridad de base de datos, esa información se reconcilia con los datos del historial de volumen de la copia de seguridad de base de datos. Si la información del archivo de historial de volumen es incoherente con los datos autodescriptivos, se emiten mensajes para identificar el problema. Por ejemplo, no todos los valores se han especificado y están disponibles, y no se encuentran datos autodescriptivos.



Si la información del historial de volumen es coherente con los datos autodescriptivos de la copia de seguridad de base de datos, se emite un mensaje indicando que la copia de seguridad de base de datos puede utilizarse para procesos de restauración.




Si la información del historial de volumen no es coherente con los datos autodescriptivos de la copia de seguridad de base de datos o si no se encuentran datos autodescriptivos para la copia de seguridad, se emiten mensajes de error indicando qué se ha comprobado y qué faltaba.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y si el historial de volumen y los datos autodescriptivos de la copia de seguridad de la base de datos son coherentes, la restauración continúa.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y la reconciliación y la validación fallan, no se realiza la restauración de la base de datos. Haga que haya más volúmenes disponibles y haga referencia a ellos desde el archivo de historial de volumen, o elimine la operación o la serie de copias de seguridad para que el servidor de IBM Spectrum Protect seleccione una operación o serie preferida diferente y continúe el proceso.

Si el parámetro PREVIEW está definido en YES, el proceso solo ejecuta la evaluación del archivo de historial de volumen y la reconciliación y validación con la copia de seguridad de base de datos seleccionada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows RESTOREKeys

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica si se debe restaurar la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento cuando se restaura la base de datos. Este parámetro es opcional y solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno en la nube. Si la clave maestra de servidor está protegida cuando se restaura la base de datos, el valor predeterminado es YES. Si la clave maestra de servidor no está protegida cuando se restaura la base de datos, el valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No




Especifica que la clave maestra de servidor no se restaura cuando se restaura la base de datos.




Yes

Especifica que la clave maestra de servidor se restaura cuando se restaura la base de datos. Debe especificar una contraseña con este parámetro.

Only

Especifica que sólo se restaura la clave maestra del servidor. La base de datos no se restaura.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows PASSWORD

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. Este parámetro solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno de nube. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos. Debe utilizar una contraseña si especifica el parámetro RESTOREKEYS=YES o RESTOREKEYS=ONLY.

## Ejemplo: restaurar la base de datos a su estado más actualizado

Restaurar la base de datos a su estado más actual utilizando el directorio de registro activo que ya está configurado.

```
dsmserv restore db
```

## Ejemplo: Restaurar la clave maestra del servidor sin restaurar la base de datos

Para restaurar la clave maestra del servidor sin restaurar la base de datos, emita el siguiente comando:

```
dsmserv restore db restorekeys=only
```

## DSMSERV RESTORE DB (Restaurar una base de datos a un instante específico)

Utilice este mandato para restaurar una base de datos a momento anterior. Un archivo de historial de volumen y un archivo de configuración de dispositivo deben estar disponibles.

Restricción: No se puede restaurar una base de datos del servidor si el nivel de release de la copia de seguridad de la base de datos del servidor es diferente del nivel de release del servidor que se está restaurando. Por ejemplo, se produce un error si se restaura una base de datos versión 7.1.3 y se está utilizando un servidor de IBM Spectrum Protect versión 8.1.

Las copias de seguridad de bases de datos completas e incrementales o las copias de seguridad de instantáneas de bases de datos pueden utilizarse para restaurar una base de datos a un punto en el tiempo específico.

Consejo: Cuando se restaura una base de datos del servidor de IBM Spectrum Protect V7 o posterior a un punto específico en el tiempo, el método preferido es emitir el mandato DSMSERV REMOVE DB antes de emitir el mandato DSMSERV RESTORE DB. De este modo se garantiza que el sistema está en un estado limpio. El sistema elimina y descataloga la base de datos en segundo plano. Al restaurar datos a un punto específico en el tiempo, todos los registros necesarios y la imagen de base de datos se recuperan de los medios de copia de seguridad.

## Sintaxis

```
>>-DSMSERV -+-----+----->
              | (1) |
              '----- -u--nombre_usuario-'
              (2) .- -k--Server1-----.
>-+-----+-----+----->
  | (1) | | ' -k--nombre_clave-'
  '----- -i--dir_instancia-'
>-+-----+-----+-----RESTORE DB----->
  '- -o--archivo_opciones-' | (1) |
                          '----- -quiet-'
                          .-TOTime----23:59:59-.
>-TODate----fecha----->
                          '-TOTime----hora-----'
                          .-Source----DBBackup-----.
>-+-----+-----+----->
  '-Source----+DBBackup---+'
  '-DBSnapshot-'
>-+-----+-----+----->
  '-RECOVerydir----directorio-'
>-+-----+-----+----->
  '-ACTIVELOGDir----directorio-'
>-+-----+-----+----->
  '-ON----archivo_directorio_destino-'
  .-Preview----No----- .-RESTOREKeys----No----- .
>-+-----+-----+----->
  '-Preview----+Yes-+' '-RESTOREKeys----+No---+'
  '-No--' '+-YES--+'
  '+-ONLY-'
>-+-----+-----+-----><
```



'-PASSWORD-----nombre\_contraseña-'



#### Notas:



1. Este parámetro se aplica solo a los servidores AIX y Linux.
2. Este parámetro solo se aplica a los servidores Windows.



## Parámetros


---


 Sistemas operativos AIX  Sistemas operativos Linux-u nombre\_usuario

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un nombre de usuario al que cambiar antes de iniciar el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux-i dir\_instancia

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica un directorio de instancia para utilizarlo. Se convierte en el directorio de trabajo actual del servidor.



 Sistemas operativos Windows-k nombre\_clave

 Sistemas operativos WindowsEspecifica el nombre de la clave de registro de Windows de la que ha de recuperarse información acerca del servidor. El valor predeterminado es SERVER1.

-o archivo\_opciones

Especifica un archivo de opciones para utilizarlo.

 Sistemas operativos AIX  Sistemas operativos Linux-quiet

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica que se suprimen los mensajes para la consola.

TODate (Obligatorio)

Especifica la fecha en la que debe restaurarse la base de datos. Son posibles los valores siguientes:

MM/DD/AAAA

Especifica que desea restaurar una base de datos utilizando la última serie de copias de seguridad creada antes de la fecha especificada.

TODAY

Especifica que desea restaurar una base de datos utilizando la serie de copias de seguridad más reciente creada antes de hoy.

TODAY-número\_días o -número\_días

Especifica que desea restaurar una base de datos utilizando la serie de copias de seguridad más reciente que fue creado en el número de días especificado antes de la fecha actual.

TOTime

Especifica el momento del día en el que debe restaurarse la base de datos. Este parámetro es opcional. El valor predeterminado es el final del día (23:59:59). Los valores posibles son:

HH:MM:SS

Especifica que desea restaurar la base de datos utilizando la última serie de copias de seguridad creada en el momento especificado o antes en la fecha que se especifica en el parámetro TODATE.

NOW

Especifica que desea restaurar la base de datos utilizando una serie de copias de seguridad creada en el momento especificado o antes en la fecha que se especifica en el parámetro TODATE.

Por ejemplo, si emite el programa de utilidad DSMSEV RESTORE DB a las 9:00 con TOTIME=NOW, la base de datos se restaura utilizando la última serie de copias de seguridad creada a las 9:00 o antes en la fecha especificada en el parámetro TODATE.

NOW-número\_horas:número\_minutos o -número\_horas:número\_minutos

Especifica que desea restaurar la base de datos utilizando una serie de copias de seguridad creada en el momento actual o antes menos un número especificado de horas y, opcionalmente, minutos en la fecha que se especifica en el parámetro TODATE.

Por ejemplo, si emite el programa de utilidad DSMSEV RESTORE DB a las 9:00 con TOTIME=NOW-3:30, la base de datos se restaura utilizando la última serie de copias de seguridad creada a las 5:30 o antes en la fecha especificada en el parámetro TODATE.

Source

Especifica si la base de datos se restaura mediante volúmenes de copia de seguridad incrementales o completas de la base de datos o mediante volúmenes de instantánea de base de datos. Este parámetro es opcional. El valor predeterminado es DBBackup. Son posibles los valores siguientes:

DBBackup

Especifica que la base de datos se restaure del siguiente modo:

1. Lee el archivo histórico de volúmenes para localizar los volúmenes de copia de seguridad incremental y completa de la base de datos necesarios.
2. Solicita montajes y carga datos de los volúmenes de copia de seguridad incremental y completa de la base de datos que necesarios para restaurar el volumen de base de datos al momento especificado.

#### DBSnapshot

Especifica que la base de datos se restaure del siguiente modo:

1. Lee el archivo histórico de volúmenes para localizar los volúmenes de instantánea de base de datos necesarios,
2. Solicita montajes y carga datos de los volúmenes de instantánea de base de datos que necesita para restaurar el volumen al momento especificado.

#### RECOVdir

Especifica un directorio donde almacenar la información de anotaciones de recuperación a partir de los soportes de copia de seguridad de la base de datos. Esta información de anotaciones se utiliza para establecer la coherencia de las transacciones de la base de datos del servidor como parte del proceso de recuperación. Este directorio debe tener espacio suficiente para contener la información de recuperación de transacciones y debe ser un directorio vacío. Si el parámetro no se especifica, el valor predeterminado es el directorio especificado por uno de los parámetros siguientes en el programa de utilidad DSMSERV FORMAT o DSMSERV LOADFORMAT:

- ARCHFAILOVERLOGDIRECTORY, si se especifica
- ARCHLOGDIRECTORY, si no se ha especificado ARCHFAILOVERLOGDIRECTORY

#### ACTIVELOGDir

Especifica un directorio donde almacenar los archivos de anotaciones que se utilizan para rastrear las operaciones de la base de datos activas. Especifique este directorio sólo si se tiene intención de conmutar a un directorio de anotaciones activas diferente del que ya se ha configurado.

#### On

Especifica un archivo que contiene un listado de los directorios en los que se restaurará la base de datos. Especifique cada directorio en una línea separada del archivo. Por ejemplo, el parámetro ON especifica el archivo restorelist.txt que contiene la lista siguiente:

```
/tsmdb001  
/tsmdb002  
/tsmdb003
```

 Sistemas operativos Windows

```
e: \tsm\db001  
f: \tsm\db002  
g: \tsm\db003
```

Si no se especifica este parámetro, se utilizarán los directorios originales que se registraron en la copia de seguridad de la base de datos.

Consejo: Si especifica varios directorios, asegúrese de que los sistemas de archivos subyacentes son de tamaño igual para garantizar un grado coherente de paralelismo para las operaciones de la base de datos. Si uno o más directorios de la base de datos son más pequeños que los demás, reducen el potencial de precarga y distribución en paralelo optimizada de la base de datos.

#### Preview

Especifica que los archivos de historial de volumen se examinarán y que los volúmenes de copia de seguridad de base de datos del archivo de historial de volumen se evaluarán.

1. ¿Qué conjunto de volúmenes de copia de seguridad de base de datos cumple mejor los criterios de instante específico que se han especificado para el proceso de restauración? La información de historial de volumen proporciona detalles sobre el ID de serie de copias de seguridad, el ID de operación (completo, incremental 1, incremental 2, etc.), la fecha de la copia de seguridad de la base de datos, y la clase de dispositivo. Esta información y los parámetros especificados en el comando DSMSERV RESTORE DB determinan qué se utiliza para realizar la restauración. El archivo de historial de volumen se examina para buscar la copia de seguridad de base de datos que mejor cumpla los criterios de instante específico y realizar a continuación la restauración utilizando esa copia de seguridad.
2. ¿Hay disponibles datos autodescriptivos para el conjunto seleccionado de volúmenes de copia de seguridad de base de datos? Coteje la información de historial de volumen para esta serie de copias de seguridad. La reconciliación notifica qué contienen los datos autodescriptivos comparados con los datos obtenidos de las entradas del historial de volumen. El cotejo implica montar uno o varios de los volúmenes indicados en el historial de volumen. A continuación, utilizando los datos autodescriptivos que se han incluido en los volúmenes de copia de seguridad de base de datos, esa información se reconcilia con los datos del historial de volumen de la copia de seguridad de base de datos. Si la información del archivo de historial de volumen es incoherente con los datos autodescriptivos, se emiten mensajes para identificar el problema. Por ejemplo, no todos los valores se han especificado y están disponibles, y no se encuentran datos autodescriptivos.




Si la información del historial de volumen es coherente con los datos autodescriptivos de la copia de seguridad de base de datos, se emite un mensaje indicando que la copia de seguridad de base de datos puede utilizarse para procesos de restauración.




Si la información del historial de volumen no es coherente con los datos autodescriptivos de la copia de seguridad de base de datos o si no se encuentran datos autodescriptivos para la copia de seguridad, se emiten mensajes de error indicando qué se ha comprobado y qué faltaba.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y si el historial de volumen y los datos autodescriptivos de la copia de seguridad de la base de datos son coherentes, la restauración continúa.

Si no se especifica el parámetro PREVIEW o si está definido en NO, y la reconciliación y la validación fallan, no se realiza la restauración de la base de datos. Haga que haya más volúmenes disponibles y haga referencia a ellos desde el archivo de historial de volumen, o elimine la operación o la serie de copias de seguridad para que el servidor de IBM Spectrum Protect seleccione una operación o serie preferida diferente y continúe el proceso.

Si el parámetro PREVIEW está definido en YES, el proceso solo ejecuta la evaluación del archivo de historial de volumen y la reconciliación y validación con la copia de seguridad de base de datos seleccionada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **RESTOREKeys**

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica si se debe restaurar la clave de cifrado maestra de servidor que se utiliza para cifrar datos de agrupación de almacenamiento cuando se restaura la base de datos. Este parámetro es opcional y solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno en la nube. Si la clave maestra de servidor está protegida cuando se restaura la base de datos, el valor predeterminado es YES. Si la clave maestra de servidor no está protegida cuando se restaura la base de datos, el valor predeterminado es NO. Puede especificar uno de los siguientes valores:

No




Especifica que la clave maestra de servidor no se restaura cuando se restaura la base de datos.




Yes

Especifica que la clave maestra de servidor se restaura cuando se restaura la base de datos. Debe especificar una contraseña con este parámetro.

Only

Especifica que sólo se restaura la clave maestra del servidor. La base de datos no se restaura.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows **PASSword**

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica la contraseña que se utiliza para proteger la copia de seguridad de base de datos. Este parámetro solo se aplica si está utilizando agrupaciones de almacenamiento de contenedores cifradas en un entorno de nube. Si especifica una contraseña para la copia de seguridad de base de datos, debe especificar la misma contraseña en el mandato RESTORE DB para restaurar la base de datos. Debe utilizar una contraseña si especifica el parámetro RESTOREKEYS=YES o RESTOREKEYS=ONLY.

## Ejemplo: restaurar la base de datos a un instante específico

---

Restaurar la base de datos al estado que tenía el 12 de mayo de 2011 a las 14:25 horas.

```
dsmserv restore db todate=05/12/2011 totime=14:45
```

## Ejemplo: Restaurar la clave maestra del servidor sin restaurar la base de datos

---

Para restaurar la clave maestra del servidor sin restaurar la base de datos, emita el siguiente comando:

```
dsmserv restore db restorekeys=only
```

 Sistemas operativos Windows

## DSMSERV UPDATE (Crear entradas de registro para una instancia de servidor)

---

Utilice este programa de utilidad para crear entradas de registro para una instancia de servidor de IBM Spectrum Protect si las entradas se han suprimido accidentalmente.

Ejecute este programa de utilidad del directorio de instancia para la base de datos (donde archivos tales como dsmserv.dsk se almacenan para el servidor). El programa de utilidad vuelve a crear las entradas de registro originales para el servidor.

## Sintaxis

---

```
      .- -k--Server1-----.  
>>-DSMSERV--+-+-----+--UPDATE----->>  
      '- -k--nombre_clave-'
```

## Parámetros

-k nombre\_clave

Especifica el nombre de la clave de registro de Windows en la que ha de almacenarse información acerca del servidor. El valor predeterminado es Server1.

## Ejemplo: volver a crear entradas de registro para una instancia de servidor

Ejecute el programa de utilidad para volver a crear entradas de registro para la instancia de servidor, Server2.

```
"c:\Archivos de programa\Tivoli\TSM\server\bin\dsmserve" -k server2 update
```

 Sistemas operativos AIX  Sistemas operativos Linux

## DSMULOG (Capturar mensajes de servidor de IBM Spectrum Protect en un archivo de anotaciones de usuario)

Utilice este comando para capturar mensajes de consola de servidor de IBM Spectrum Protect a un archivo de anotaciones de usuario. Puede especificar que IBM Spectrum Protect grabe mensajes a más de un archivo de anotaciones de usuario.

Importante: No coloque las anotaciones de usuario en los sistemas de archivos usr/ u /opt porque existen restricciones de espacio en el sistema de archivos que pueden impedir que el servidor se inicie.

## Sintaxis

```
>>-DSMULOG--+-+-----+----->>  
      | .-,-----|  
      | v          |  
      '---nombre_archivo_anotaciones--+'
```

## Parámetros

nombre\_archivo\_anotaciones (Necesario)

Especifica el nombre de uno o varios archivos de anotaciones de usuario en los que IBM Spectrum Protect guarda mensajes de consola del servidor. Cuando especifique varios nombres de archivo, se graba en cada archivo durante un día y, a continuación, el servidor se mueve al siguiente archivo para capturar mensajes de anotaciones. Cuando todos los archivos de la lista se hayan grabado, el servidor comenzará a escribir en el primer archivo de nuevo y todos los mensajes contenidos en él se sobrescribirán.

## Ejemplo: Capturar mensajes de la consola en un archivo de anotaciones de usuario




Utilice el comando DSMULOG para registrar mensajes de la consola en un archivo de anotaciones de usuario. Especifique los archivos de anotaciones de usuario en los que desee registrar los mensajes de la consola.


```
dsmulog /u/admin/log1 /u/admin/log2 /u/admin/log3
```

## Programas de utilidad de dispositivos de servidor de IBM Spectrum Protect

Puede utilizar los programas de utilidad de dispositivo para las tareas relacionadas con la configuración de dispositivos de almacenamiento para el servidor.

## Programas de utilidad de dispositivo

-  Sistemas operativos AIXtsmdlst (Visualizar información sobre dispositivos)
-  Sistemas operativos Linuxautoconf (dispositivos de configuración automática)
-  Sistemas operativos Windowstsmldst (Visualizar información sobre dispositivos)

 Sistemas operativos AIX

## tsmdlst (Visualizar información sobre dispositivos)

Use el programa de utilidad tsmdlst para ver los nombres del dispositivo y otra información acerca del conmutador de medios y los dispositivos de cinta controlados por el controlador del dispositivo IBM Spectrum Protect.


El programa de utilidad tsmdlst forma parte del paquete de controlador del dispositivo IBM Spectrum Protect que es igual para el servidor y para el agente de almacenamiento. Debe instalar el controlador del dispositivo IBM Spectrum Protect para ejecutar el programa de utilidad tsmdlst para el agente de almacenamiento.

Después de que se configuren los dispositivos, puede ejecutar la herramienta tsmdlst para mostrar la información de dispositivos. La herramienta guarda esta información en archivos que se pueden recuperar. Los archivos se denominan lbinfo para los dispositivos del conmutador de soporte y mtinfo para los dispositivos de cinta. Después de que se añada o se vuelva a configurar un dispositivo, puede actualizar estos archivos ejecutando la herramienta tsmdlst de nuevo.

La herramienta tsmdlst y los archivos de salida que genera se encuentran en el directorio devices/bin, que de forma predeterminada es /opt/tivoli/tsm/devices/bin. Antes de ejecutar la herramienta tsmdlst, asegúrese de que se haya detenido el servidor de IBM Spectrum Protect o que se hayan detenido todas las actividades de los dispositivos. Si un dispositivo está siendo utilizado por el servidor de IBM Spectrum Protect cuando se ejecuta la herramienta tsmdlst, se emite un error de dispositivo ocupado.

### Opciones

- /t Muestra los mensajes de rastreo para el programa de utilidad tsmdlst.
- /? Muestra la información de utilización de tsmdlst y sus parámetros.

 Sistemas operativos AIX

### Ejemplo: Visualizar información sobre todos los dispositivos

Visualice información sobre todos los dispositivos que ha configurado el controlador de dispositivo de IBM Spectrum Protect:

```
tsmdlst
```

TSM Device Name	Vendor	Product ID	Firmware	World Wide Name	Serial Number
/dev/lb4	ATL	P3000	0100	N/A	1651639999
TSM Device Name	Vendor	Product ID	Firmware	World Wide Name	Serial Number
/dev/mt0	QUANTUM	DLT-S4	2A2A	50:0e:09:e0:00:16:ca:47	QD0619AMD00052
/dev/mt1	QUANTUM	DLT-S4	2A2A	50:0e:09:e0:00:16:cd:e5	QD0624AMD00184
/dev/mt22	QUANTUM	DLT7000	0100	N/A	1651639000
/dev/mt23	QUANTUM	DLT7000	0100	N/A	1651639002

 Sistemas operativos Linux

## autoconf (dispositivos de configuración automática)

Utilice el programa de utilidad autoconf para configurar los dispositivos para su uso con el servidor de IBM Spectrum Protect.

La herramienta autoconf realiza las siguientes tareas:

- Carga el controlador en el kernel
- Crea los archivos necesarios para el controlador de dispositivo de IBM Spectrum Protect
- Crea archivos de información de dispositivo para bibliotecas y dispositivos de cinta

La herramienta autoconf se incluye en el paquete de controlador de dispositivo y se instala en el directorio /opt/tivoli/tsm/devices/bin.

### Opciones

- a Añade permisos de lectura y grabación a los archivos de dispositivo de IBM Spectrum Protect para permitir a todos los usuarios el acceso a los dispositivos. Especifique este valor para configurar los dispositivos si un usuario no root inicia el servidor de IBM Spectrum Protect.
- g



Añade permisos de lectura y grabación a los archivos de dispositivo de IBM Spectrum Protect para permitir que cualquiera que esté en el mismo grupo que un usuario root utilice los dispositivos.

-t

Habilita el rastreo de la herramienta autoconf.


-?

Muestra información sobre la herramienta autoconf y sus parámetros.

## Ejemplo: Configurar dispositivos utilizando la herramienta autoconf

Ejecute el programa de utilidad autoconf para configurar los dispositivos de IBM Spectrum Protect:

```
> /opt/tivoli/tsm/devices/bin/autoconf
```

 Sistemas operativos Linux

## Ejemplo: Para un servidor que se inicia mediante un ID de usuario no root, configurar dispositivos utilizando el programa de utilidad autoconf

Ejecute autoconf para configurar los dispositivos de IBM Spectrum Protect. Utilice la opción `-a` porque el servidor se ha iniciado mediante un ID de usuario que no es el usuario root.

```
> /opt/tivoli/tsm/devices/bin/autoconf -a
```

```
Added the read and write permissions for all users to /dev/sg4.
Added the read and write permissions for all users to /dev/sg5.
Added the read and write permissions for all users to /dev/sg6.
Added the read and write permissions for all users to /dev/sg7.
Added the read and write permissions for all users to /dev/sg8.
Added the read and write permissions for all users to /dev/sg9.
Added the read and write permissions for all users to /dev/sg10.
Added the read and write permissions for all users to /dev/sg11.
Added the read and write permissions for all users to /dev/sg12.
Added the read and write permissions for all users to /dev/sg13.
Added the read and write permissions for all users to /dev/sg14.
Added the read and write permissions for all users to /dev/sg15.
Added the read and write permissions for all users to /dev/sg16.
Added the read and write permissions for all users to /dev/sg17.
Added the read and write permissions for all users to /dev/sg18.
Added the read and write permissions for all users to /dev/sg19.
Added the read and write permissions for all users to /dev/sg20.
Added the read and write permissions for all users to /dev/sg21.
Added the read and write permissions for all users to /dev/sg22.
Added the read and write permissions for all users to /dev/sg23.
Added the read and write permissions for all users to /dev/sg24.
Added the read and write permissions for all users to /dev/sg25.
Added the read and write permissions for all users to /dev/sg26.
Added the read and write permissions for all users to /dev/sg27.
Added the read and write permissions for all users to /dev/sg28.
Added the read and write permissions for all users to /dev/sg29.
```

Tape Drives:

=====

Index	Minor	Host	CHN	ID	LUN	Type	Vendor_ID	Device_Serial_Number	Product_ID	Rev.
000	004	003	000	004	000	001	IBM	1068000439	ULTRIUM-HH5	C5X1
001	007	003	000	008	001	001	HP	01UbWSD-04	Ultrium 2-SCSI	R210
002	008	003	000	008	002	001	HP	01UbWSD-05	Ultrium 2-SCSI	R210
003	010	003	000	008	004	001	HP	01UbWSD-07	Ultrium 3-SCSI	R210
004	012	003	000	008	006	001	HP	01UbWSD-01	Ultrium 3-SCSI	R210
005	013	003	000	008	007	001	HP	01UbWSD-02	Ultrium 3-SCSI	R210
006	014	003	000	008	008	001	HP	01UbWSD-08	Ultrium 3-SCSI	R210
007	015	003	000	008	009	001	HP	01UbWSD-09	Ultrium 3-SCSI	R210
008	016	003	000	008	010	001	HP	01UbWSD-0a	Ultrium 3-SCSI	R210
009	017	003	000	008	011	001	HP	01UbWSD-0b	Ultrium 3-SCSI	R210
010	018	003	000	008	012	001	HP	01UbWSD-0c	Ultrium 3-SCSI	R210
011	019	003	000	008	013	001	HP	01UbWSD-0d	Ultrium 3-SCSI	R210
012	020	003	000	005	000	001	IBM	1068000913	ULTRIUM-HH5	C5X1
013	022	003	000	009	001	001	QUANTUM	01UbWSD-0f	SDLT320	R210
014	023	003	000	009	002	001	QUANTUM	01UbWSD-0g	SDLT320	R210
015	024	003	000	009	003	001	QUANTUM	01UbWSD-0h	SDLT320	R210
016	025	003	000	009	004	001	QUANTUM	01UbWSD-0i	SDLT320	R210
017	026	003	000	006	000	001	IBM	1068001573	ULTRIUM-HH4	B5Q1
018	027	003	000	007	000	001	IBM	1068001545	ULTRIUM-HH4	B5Q1
019	028	003	000	010	000	001	HP	HU19477PAE	Ultrium 5-SCSI	I65W

#### Medium Changer Devices:

=====

Index	Minor	Host	CHN	ID	LUN	Type	Vendor_ID	Device_Serial_Number	Product_ID	Rev.
000	005	003	000	004	001	008	NEC	2Y11BB0023	LL-2B01	0004
001	006	003	000	008	000	008	HP	01UbWSD-03	VLS	1.00
002	009	003	000	008	003	008	HP	01UbWSD-06	ThinStor AutoLdr	T133
003	011	003	000	008	005	008	HP	01UbWSD-00	ESL E-Series	2.00
004	021	003	000	009	000	008	HP	01UbWSD-0e	MSL6000 Series	0430
005	029	003	000	010	001	008	HP	3615-0101	MSL G3 Series	1120

 Sistemas operativos Windows

## tsmdlst (Visualizar información sobre dispositivos)

Utilice el programa de utilidad tsmdlst para ver nombres de dispositivo y otra información sobre el conmutador de soporte o dispositivos de cintas en el sistema.

### Opciones

Después de que se configuren los dispositivos, puede ejecutar la herramienta tsmdlst para mostrar la información de dispositivos. El programa de utilizada está en el directorio del servidor de dispositivos, que está en \Program Files\Tivoli\TSM\server por defecto.

`/computer=computer_name`

Especifica el nombre del sistema para el que se enumeran los dispositivos. El valor predeterminado es el sistema local.

`/detail`

Muestra los detalles de los dispositivos en la lista. De manera predeterminada, se muestra un resumen.

`/all`

Muestra información sobre todos los tipos de dispositivos. De manera predeterminada, en los resultados sólo se incluyen las unidades de cinta y las bibliotecas de cinta.

`/nogenerictapecheck`

Omite los pasos para abrir unidades detectadas para ver si son compatibles para el tipo de dispositivo de IBM Spectrum Protect GENERICTAPE.

`/nohbatcheck`

Omite los pasos para la detección de la API del adaptador de bus de host (HBA), que podría acelerar el proceso. Esta opción puede ser útil cuando se necesita depuración.

`/trace`

Se utiliza con fines de diagnóstico. Almacena la salida de rastreo en el archivo tsmdlst\_trace.txt.

`/?`

Muestra la información de utilización de tsmdlst y sus parámetros.

`/xinqury`

Proporciona una forma alternativa para obtener la información del número de serie y del nombre de ámbito mundial. Esta opción sólo se utiliza para los dispositivos que son compatibles con el controlador de dispositivos de cinta de IBM®. Los parámetros siguientes son específicos a la opción /xinqury:

`/processAll`

Indica que el proceso entra en bucle hasta que se procesan todos los dispositivos.

`/maxRetries=#`

Indica el número máximo de intentos para abrir cada unidad. Esta opción requiere la opción /processAll.

`/genpathfile`

Utilice esta opción para generar una lista de dispositivos y números de serie. El archivo tsmdlst\_pathfile.txt se escribe con información para las opciones /genmacropathsyntax y /genmacropathoffline.

`/includelib`

Si este parámetro se ha especificado con la opción /genpathfile, la lista de dispositivos incluye bibliotecas además de unidades.

`/genmacropathsyntax`

Genera un macro para sincronizar las vías de acceso de IBM Spectrum Protect para el agente de almacenamiento basándose en el número de serie. Una unidad debe tener un número de serie que esté definido en IBM Spectrum Protect para que esta opción funcione.

`/genmacropathoffline`

Genera un macro para actualizar las vías de acceso de IBM Spectrum Protect para el agente de almacenamiento al estado en línea o fuera de línea basándose en la accesibilidad de la unidad. Es posible acceder a una unidad si una llamada abierta de sistema operativo tiene como resultado: ERROR\_SUCCESS, ERROR\_BUSY o ERROR\_ACCESS\_DENIED. Esta opción solo funciona para dispositivos que utilizan el controlador de dispositivo de IBM. Para abrir un nombre de dispositivo se precisa un nombre simbólico, por ejemplo, \\.\tape0.

Las opciones siguientes solo se utilizan con las opciones /genmacropathsyntax y /genmacropathoffline:

`/server=servername`  
Especifica el nombre del servidor que utiliza el agente de almacenamiento.

`/stagent=stagentname`  
Especifica el nombre del agente de almacenamiento.

`/tcps=address`  
Especifica la dirección del servidor de IBM Spectrum Protect.

`/tcpport=port`  
Especifica el puerto del servidor de IBM Spectrum Protect. El valor predeterminado es 1500.

`/id=id`  
Especifica el identificador administrativo de IBM Spectrum Protect.

`/pass=password`  
Especifica la contraseña administrativa de IBM Spectrum Protect.

`/devicetype=drivetype`  
Especifica el tipo de dispositivo de la unidad, por ejemplo, LTO. Esta opción distingue entre mayúsculas y minúsculas y es opcional.

`/libraryname=libname`  
Filtros en el nombre de biblioteca de la unidad, por ejemplo LTO3584. Esta opción distingue entre mayúsculas y minúsculas y es opcional.

`/execmacropathsync`  
Emite la macro de sincronización de vías de acceso al servidor de IBM Spectrum Protect.

`/execmacropathoffline`  
Emite la macro fuera de línea de vías de acceso al servidor de IBM Spectrum Protect.

`/addpaths`  
Añade sentencias para definir y actualizar vías de acceso. Esta opción se utiliza con la opción `/genmacropathsync`.

`/verbose`  
Lista la información de la unidad y, también, de la vía de acceso devuelta del servidor IBM Spectrum Protect y el contenido del archivo de la vía de acceso.

`/encodednames`  
Si una vía de acceso se establece en `online=no`, el nombre de dispositivo codifica la indicación de tiempo, el error y el dispositivo como el nombre del dispositivo actualizado.

## Ejemplo: visualizar información sobre dispositivos

Visualizar información sobre dispositivos de cinta y bibliotecas de cintas para un sistema local, WANTON, ejecutando la herramienta `tsmdlst`:

```
tsmdlst
```

El nombre de dispositivo que se visualiza es el nombre de alias que se puede utilizar en el mandato `DEFINE PATH` y el mandato `UPDATE PATH`. El nombre de alias no es el nombre real del dispositivo.

```
Computer Name:      WANTON
OS Version:         6.2
OS Build #:         9200
Controlador de dispositivo de TSM: TSMScsi - No activo
```

```
4 HBAs were detected.
```

Manufacturer	Model	Driver	Version	Firmware	NodeWWN	Description
QLogic Corporation	QLE2562	ql2300.sys	9.1.11.28	7.03.00	20000024FF25F846	QLogic QLE2562 Fibre Channel Adapter
QLogic Corporation	QLE2562	ql2300.sys	9.1.11.28	7.03.00	20000024FF25F847	QLogic QLE2562 Fibre Channel Adapter
QLogic Corporation	QLE2562	ql2300.sys	9.1.11.28	7.03.00	20000024FF25F7FE	QLogic QLE2562 Fibre Channel Adapter
QLogic Corporation	QLE2562	ql2300.sys	9.1.11.28	7.03.00	20000024FF25F7FF	QLogic QLE2562 Fibre Channel Adapter

Nombre	TSM ID	LUN	Bus	Puerto	SSN	WWN	TSM	Tipo	Controlador	Dispositivo	Identificador
mt0.0.0.7	0	0	0	7	000001327176	5005076300566011	3592	IBM	IBM		
03592E06	2883										
lb0.1.0.7	0	1	0	7	0000013400480405	5005076300566011	LIBRARY	IBM	IBM		
03584L22	E01q										
mt1.0.0.7	1	0	0	7	000001327147	5005076300566012	3592	IBM	IBM		
03592E06	2883										
mt2.0.0.7	2	0	0	7	000001327349	5005076300566013	3592	IBM	IBM		

03592E06	2883												
mt3.0.0.7	3	0	0	7	000001327140	5005076300566014	3592		IBM	IBM			
03592E06	2883												
mt4.0.0.7	4	0	0	7	1068000254	500507630F51FA05	LTO		IBM	IBM			
ULT3580-TD5	D8D4												
lb4.1.0.7	4	1	0	7	0000078216780402	500507630F51FA05	LIBRARY		IBM	IBM			
03584L32	C460												
mt5.0.0.7	5	0	0	7	1068000039	500507630F51FA06	LTO		IBM	IBM			
ULT3580-TD5	D8D4												
mt6.0.0.7	6	0	0	7	1068000047	500507630F51FA07	LTO		IBM	IBM			
ULT3580-TD5	D8D4												
mt7.0.0.7	7	0	0	7	1068000017	500507630F51FA08	LTO		IBM	IBM			
ULT3580-TD5	D8D4												

## Scripts de servidor y macros para automatización

Puede automatizar tareas administrativas comunes creando scripts de servidor y macros de cliente administrativas de IBM Spectrum Protect. Los scripts de servidor se almacenan en la base de datos del servidor y se pueden planificar para ejecutar con un mandato de planificación administrativa. Las macros de cliente administrativo se almacenan como archivos en el cliente de administración. Las macros no se pueden distribuir entre servidores y no se pueden planificar en el servidor.

- **Scripts de servidor**  
Puede automatizar tareas administrativas comunes con scripts que se almacenan en la base de datos del servidor. Puede planificar un script para su proceso mediante el planificador de mandatos de administración en el servidor.
- **Macros de cliente administrativo**  
Una macro es un archivo que contiene uno o más mandatos de cliente de administración. Sólo puede ejecutar una macro desde el cliente administrativo en la modalidad de proceso por lotes o en la modalidad interactiva. Las macros se almacenan como archivos en el cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

## Scripts de servidor

Puede automatizar tareas administrativas comunes con scripts que se almacenan en la base de datos del servidor. Puede planificar un script para su proceso mediante el planificador de mandatos de administración en el servidor.

Los scripts de IBM Spectrum Protect admiten las siguientes prestaciones y sentencias:

- Sustitución de parámetros de mandatos.
- Mandatos SELECT que se especifican al procesar el script.
- Control de la ejecución de mandatos, como las opciones de proceso PARALLEL y SERIAL.
- Sentencias de flujo lógico condicional. Estas sentencias de flujo lógicas incluyen las siguientes sentencias:
  - La cláusula IF; esta cláusula determina cómo debe continuar el proceso en función del valor del código de retorno actual.
  - La sentencia EXIT; esta sentencia finaliza el proceso del script.
  - Las sentencias GOTO y LABEL. Estas sentencias indican que el flujo lógico continúa el proceso con la línea que empieza por la etiqueta especificada.
- Línea de comentarios.

Se proporcionan scripts de ejemplo en el archivo scripts.smp. Los scripts de ejemplo tienen un orden de ejecución de ejemplo para la planificación de mandatos de administración.

Si uno de los mandatos especificados en el script no se procesa correctamente, los demás mandatos no se procesan.

- **Definición de un script de servidor**  
Se puede definir un script de servidor línea a línea, crear un archivo que contenga las líneas de mandatos o copiar un script ya existente.
- **Actualización de un script**  
Puede actualizar un script para cambiar una línea de mandatos o para añadir una línea de mandatos a un script.
- **Consulta de un script de servidor para crear otro script de servidor**  
Se pueden crear más scripts de servidor consultando un script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene se puede utilizar como entrada de otro script sin tener que crear un script línea a línea.
- **Ejecución de un script del servidor**  
Para procesar un script, emita el mandato RUN. Se puede ejecutar un script que contenga variables de sustitución especificándolas junto con el mandato RUN.

## Definición de un script de servidor

Se puede definir un script de servidor línea a línea, crear un archivo que contenga las líneas de mandatos o copiar un script ya existente.

## Acerca de esta tarea

---

Restricción: No se puede redirigir la salida de un mandato dentro de un script de servidor. En su lugar, ejecute el script y, a continuación, especifique la redirección de mandatos. Por ejemplo, para dirigir la salida de script1 al directorio c:\temp\test.out, ejecute el script y especifique la redirección de mandatos como en el ejemplo siguiente:

```
run script1 > c:\temp\test.out
```

## Procedimiento

---

1. Defina un script con el mandato DEFINE SCRIPT. Se puede definir inicialmente la primera línea del script con este mandato. Por ejemplo:

```
define script qaixc "select node_name from nodes where platform='aix'"  
desc='Visualizar clientes AIX'
```

En este ejemplo se define el script como QAIXC. Al ejecutar el script, se visualizan todos los clientes AIX.

2. Defina más líneas en el script con el mandato UPDATE SCRIPT. Por ejemplo, para añadir un mandato QUERY SESSION, entre:

```
update script qaixc "query session *"
```

3. Opcional: Puede especificar un parámetro WAIT con el mandato DEFINE CLIENTACTION. Utilizando este parámetro, puede especificar que la acción del cliente se debe completar antes de que se procese el paso siguiente en el script de mandato o la macro.
4. Opcional: Para ayudarle a determinar cuándo hay un problema en un mandato en un script, utilice el mandato ISSUE MESSAGE.

- Ejecución de mandatos en paralelo o en serie  
Tiene la posibilidad de ejecutar mandatos en serie, en paralelo o en serie y en paralelo. También puede hacerlo utilizando los mandatos de script SERIAL o PARALLEL del parámetro COMMAND\_LINE de DEFINE y UPDATE SCRIPT. Por lo tanto, es posible ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente.
- Continuación de mandatos a través de varias líneas de mandatos  
Los mandatos largos se pueden continuar en varias líneas de mandatos especificando el carácter de continuación (-) como el último carácter de un mandato que continúa.
- Inclusión de las variables de sustitución en un script  
En un script se pueden incluir variables de sustitución. Las variables de sustitución se especifican con el carácter \$ seguido de un número que representa la posición del parámetro al procesarse el script.
- Inclusión de sentencias de flujo lógico en un script  
Se pueden utilizar sentencias de flujo lógico condicional en función de los códigos de retorno emitidos en el proceso de mandatos anterior. Utilizando estas sentencias lógicas, puede procesar los scripts según el resultado de ciertos mandatos. Se pueden utilizar las sentencias IF, EXIT, o GOTO (etiqueta).
- Utilización de mandatos SELECT en un script  
Un script de IBM Spectrum Protect es uno o varios mandatos almacenados como un objeto en la base de datos. Puede definir un script que contenga uno o más mandatos SELECT.

## Ejecución de mandatos en paralelo o en serie

---

Tiene la posibilidad de ejecutar mandatos en serie, en paralelo o en serie y en paralelo. También puede hacerlo utilizando los mandatos de script SERIAL o PARALLEL del parámetro COMMAND\_LINE de DEFINE y UPDATE SCRIPT. Por lo tanto, es posible ejecutar varios mandatos en paralelo y esperar a que finalicen antes de proceder con el mandato siguiente.

## Acerca de esta tarea

---

La ejecución de mandatos en serie en un script garantiza que cualquier mandato precedente haya finalizado antes de continuar y garantiza que los mandatos siguientes se ejecuten en serie. Cuando se inicia un script, todos los mandatos se ejecutan en serie hasta que aparece un mandato PARALLEL. Varios mandatos que se ejecutan en paralelo y que acceden a recursos comunes, como las unidades de cintas, pueden ejecutarse en serie.

Los códigos de retorno de script siguen siendo los mismos antes y después de que se ejecute un mandato PARALLEL. Cuando aparece un mandato SERIAL, el código de retorno de script se establece en el código de retorno máximo de todos los mandatos anteriores ejecutados en paralelo.

Al utilizar mandatos de servidor que admiten el parámetro WAIT después de un mandato PARALLEL, el comportamiento es el siguiente:

- Si especifica (o utiliza el valor predeterminado) WAIT=NO, un script no espera hasta la finalización del mandato cuando aparece un mandato SERIAL posterior. El código de retorno de dicho mandato refleja el proceso sólo hasta el punto en el que el mandato inicia un proceso subordinado. El código de retorno final del mandato no está disponible para el script.
- Si especifica WAIT=YES, su script espera hasta la finalización del mandato cuando aparece un mandato SERIAL posterior. El código de retorno de dicho mandato refleja el proceso de todo el mandato.

En la mayoría de los casos, puede utilizar WAIT=YES en los mandatos que se ejecutan en paralelo.

Restricción: Si el mandato inicia un proceso en segundo plano que no tiene el parámetro WAIT, el mandato se considera completado después de que se inicie la hebra de fondo. Por lo tanto, el mandato sólo puede ejecutarse en paralelo.

El ejemplo siguiente ilustra el modo en que se utiliza el mandato PARALLEL para realizar una copia de seguridad, migrar y reclamar agrupaciones de almacenamiento.

```
/*run multiple commands in parallel and wait for
them to complete before proceeding*/
PARALLEL
/*back up four storage pools simultaneously*/
BACKUP STGPOOL PRIMPOOL1 COPYPOOL1 WAIT=YES
BACKUP STGPOOL PRIMPOOL2 COPYPOOL2 WAIT=YES
BACKUP STGPOOL PRIMPOOL3 COPYPOOL3 WAIT=YES
BACKUP STGPOOL PRIMPOOL4 COPYPOOL4 WAIT=YES
/*wait for all previous commands to finish*/
SERIAL
/*after the backups complete, migrate stgpools
simultaneously*/
PARALLEL
MIGRATE STGPOOL PRIMPOOL1 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL2 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL3 DURATION=90 WAIT=YES
MIGRATE STGPOOL PRIMPOOL4 DURATION=90 WAIT=YES
/*wait for all previous commands to finish*/
SERIAL
/*after migration completes, relcaim storage
pools simultaneously*/
PARALLEL
RECLAIM STGPOOL PRIMPOOL1 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL2 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL3 DURATION=120 WAIT=YES
RECLAIM STGPOOL PRIMPOOL4 DURATION=120 WAIT=YES
```

**Referencia relacionada:**

DEFINE SCRIPT (definir un script de servidor)  
UPDATE SCRIPT (actualizar un script de servidor)

## Continuación de mandatos a través de varias líneas de mandatos

---

Los mandatos largos se pueden continuar en varias líneas de mandatos especificando el carácter de continuación (-) como el último carácter de un mandato que continúa.

### Acerca de esta tarea

---

En el ejemplo siguiente se continúa una sentencia SQL en varias líneas de mandatos:

```
/*-----*/
/* Ejemplo de continuación */
SELECT-
* FROM-
NODE WHERE-
PLATFORM='win32'
```

Cuando se procesa este mandato, se ejecuta el siguiente mandato:

```
select * from nodes where platform='win32'
```

## Inclusión de las variables de sustitución en un script

---

En un script se pueden incluir variables de sustitución. Las variables de sustitución se especifican con el carácter \$ seguido de un número que representa la posición del parámetro al procesarse el script.

## Acerca de esta tarea

---

En el ejemplo siguiente, el script SQLSAMPLE especifica las variables de sustitución \$1 y \$2:

```
/*-----*/
/* Ejemplo de sustitución          */
/* -----*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM='$2'
```

Al ejecutar el script, debe especificar dos valores, uno para \$1 y otro para \$2. Por ejemplo:

```
run sqlsample
nombre_nodo aix
```

El mandato que se procesa cuando se ejecuta el script SQLSAMPLE es el siguiente:

```
select nombre_nodo from nodes where
platform='aix'
```

## Inclusión de sentencias de flujo lógico en un script

---

Se pueden utilizar sentencias de flujo lógico condicional en función de los códigos de retorno emitidos en el proceso de mandatos anterior. Utilizando estas sentencias lógicas, puede procesar los scripts según el resultado de ciertos mandatos. Se pueden utilizar las sentencias IF, EXIT, o GOTO (etiqueta).

A medida que cada mandato se procesa en un script, el código de retorno se guarda para su posible evaluación antes de procesarse el siguiente mandato. El código de retorno puede ser de tres clases de gravedad: OK (correcto), WARNING (aviso) o ERROR (error). Consulte Códigos de devolución para utilizar en scripts para obtener una lista de códigos de devolución válidos y niveles de gravedad.

- Especificación de la cláusula IF  
La cláusula IF se puede utilizar al principio de una línea de mandatos para determinar cómo debe continuar el proceso del script en función del valor de código de retorno actual. En la cláusula IF se especifica la gravedad o el valor simbólico del código de retorno.
- Especificación de la sentencia EXIT  
Utilice la sentencia EXIT para finalizar un proceso de script.
- Especificación de la sentencia GOTO  
La sentencia GOTO se utiliza conjuntamente con una sentencia de etiqueta. La sentencia de etiqueta es el destino de la sentencia GOTO. La sentencia GOTO dirige el proceso del script a la línea que contiene la sentencia de etiqueta para que el proceso se reanude desde ese punto.

## Especificación de la cláusula IF

---

La cláusula IF se puede utilizar al principio de una línea de mandatos para determinar cómo debe continuar el proceso del script en función del valor de código de retorno actual. En la cláusula IF se especifica la gravedad o el valor simbólico del código de retorno.

## Acerca de esta tarea

---

El servidor establece inicialmente el código de retorno al principio del script en RC\_OK. Cada mandato procesado actualiza el código de retorno. Si el código de retorno actual del mandato procesado es igual que alguno de los códigos de retorno o gravedades que hay en la cláusula IF, se procesará el resto de la línea. Si el código de retorno actual es distinto de uno de los valores listados, se salta la línea.

En el ejemplo siguiente de script, se hace una copia de seguridad de la agrupación de almacenamiento BACKUPPOOL sólo si no hay ninguna sesión que esté accediendo al servidor en la actualidad. La copia de seguridad continúa sólo si se recibe el código de retorno RC\_NOTFOUND:

```
/* Hacer una copia de seguridad de las agrupaciones de          */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* No hay sesiones si se recibe rc_notfound */
if(rc_notfound) backup stg backuppool copypool
```

En el ejemplo siguiente de script, se hace una copia de seguridad de la agrupación de almacenamiento BACKUPPOOL si se detecta un código de retorno con gravedad de aviso:

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* No hay sesiones si se recibe rc_notfound */
if(warning) backup stg backuppool cypool
```

## Especificación de la sentencia EXIT

---

Utilice la sentencia EXIT para finalizar un proceso de script.

### Acerca de esta tarea

---

En el ejemplo siguiente, se utiliza la cláusula IF junto con RC\_OK para determinar si los clientes están accediendo al servidor. Si se recibe un código de retorno RC\_OK, indica que las sesiones de cliente están accediendo al servidor. El script continúa con la sentencia exit y no se inicia la copia de seguridad.

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* Hay sesiones si se recibe rc_ok */
if(rc_ok) exit
backup stg backuppool cypool
```

## Especificación de la sentencia GOTO

---

La sentencia GOTO se utiliza conjuntamente con una sentencia de etiqueta. La sentencia de etiqueta es el destino de la sentencia GOTO. La sentencia GOTO dirige el proceso del script a la línea que contiene la sentencia de etiqueta para que el proceso se reanude desde ese punto.

### Acerca de esta tarea

---

La sentencia de etiqueta siempre va seguida de dos puntos (:) y puede tener un espacio en blanco después de los dos puntos. En el ejemplo siguiente, se utiliza la sentencia GOTO para hacer una copia de seguridad de la agrupación de almacenamiento sólo si no hay ninguna sesión que esté accediendo al servidor en la actualidad. En este ejemplo, el código de retorno RC\_OK indica que hay clientes accediendo al servidor. La sentencia GOTO dirige el proceso a la etiqueta done: que contiene la sentencia EXIT que finaliza el proceso del script:

```
/* Hacer una copia de seguridad de las agrupaciones de */
/* almacenamiento si los clientes no están accediendo al servidor */
select * from sessions
/* Hay sesiones si se recibe rc_ok */
if(rc_ok) goto done
backup stg backuppool cypool
done:exit
```

## Utilización de mandatos SELECT en un script

---

Un script de IBM Spectrum Protect es uno o varios mandatos almacenados como un objeto en la base de datos. Puede definir un script que contenga uno o más mandatos SELECT.

### Acerca de esta tarea

---

Un script puede ejecutarse desde un cliente de administración o la consola del servidor. También lo puede incluir como una planificación de mandatos de administración para que se ejecuten automáticamente. Consulte el apartado Scripts de servidor para obtener más detalles.

IBM Spectrum Protect se distribuye con un archivo que contiene diversos scripts a modo de ejemplo. El archivo, scripts.smp, se encuentra en el directorio del servidor. Para crear y guardar los scripts como objetos en la base de datos del servidor, emita el mandato DSMSERV RUNFILE durante la instalación:

```
> dsmserv runfile scripts.smp
```

También puede ejecutar el archivo como una macro desde un cliente de línea de mandatos de administración:

```
macro scripts.smp
```



El archivo de scripts de ejemplo contiene mandatos. Estos mandatos suprimen los scripts que tienen los mismos nombres que los que se van a definir y, a continuación, definen los scripts. La mayor parte de los ejemplos crean mandatos SELECT, pero otros llevan a cabo otras tareas tales como hacer copias de seguridad de agrupaciones de almacenamiento. También puede copiar y modificar el archivo de scripts de ejemplo para crear sus propios scripts.

A continuación se incluyen algunos ejemplos del archivo de scripts de ejemplo:

```
def script q_inactive_days /* -----*/
upd script q_inactive_days /* Nombre de script: Q_INACTIVE */
upd script q_inactive_days /* Descripción: Muestra nodos que no han */
upd script q_inactive_days /* accedido al servidor de seguridad durante */
upd script q_inactive_days /* un número especificado de días */
upd script q_inactive_days /* Parámetro 1: días */
upd script q_inactive_days /* Ejemplo: run q_inactive_days 5 */
upd script q_inactive_days /* -----*/
upd script q_inactive_days "select node_name,lastacc_time from nodes where -"
upd script q_inactive_days " cast((current_timestamp-lastacc_time)days as -"
upd script q_inactive_days " decimal) >= $1 "

/* Muestra mensajes en las anotaciones de actividades de gravedad X o Y */

def script q_msg_sev desc='Muestra mensajes en las anotaciones de gravedad X o Y'
upd script q_msg_sev /* -----*/
upd script q_msg_sev /* Nombre de script: Q_MSG_SEV */
upd script q_msg_sev /* Descripción: Muestra mensajes en las */
upd script q_msg_sev /* anotaciones de actividades con una */
upd script q_msg_sev /* de las gravedades especificadas. */
upd script q_msg_sev /* Parámetro 1: gravedad 1 */
upd script q_msg_sev /* Parámetro 2: gravedad 2 */
upd script q_msg_sev /* donde la gravedad es I, W, E, S, o D */
upd script q_msg_sev /* Ejemplo: ejecute q_msg_sev S E */
upd script q_msg_sev /* -----*/
upd script q_msg_sev "select date_time,msgno,message from actlog -"
upd script q_msg_sev " where severity=upper('$1') or severity=upper('$2')"
```

## Actualización de un script

Puede actualizar un script para cambiar una línea de mandatos o para añadir una línea de mandatos a un script.

- **Añadir un nuevo mandato**  
Para agregar una línea de mandatos a un script ya existente, emita el mandato UPDATE SCRIPT sin el parámetro LINE=. La línea de mandatos agregada recibe un número de línea de cinco unidades más que el último número de línea de mandatos de la secuencia de líneas de mandatos. Por ejemplo, si el script acaba con la línea 010, a la línea de mandatos agregada se le asigna el número de línea 015.
- **Sustitución de un mandato existente**  
Puede cambiar una línea de mandatos existente especificando el parámetro LINE=.
- **Adición de un mandato y un número de línea**  
Puede cambiar un script existente añadiendo líneas nuevas.
- **Supresión de un mandato de un script del servidor**  
Se puede suprimir una línea de mandatos concreta de un script. Al especificar un número de línea, sólo se suprime del script la línea de mandatos correspondiente.

## Añadir un nuevo mandato

Para agregar una línea de mandatos a un script ya existente, emita el mandato UPDATE SCRIPT sin el parámetro LINE=. La línea de mandatos agregada recibe un número de línea de cinco unidades más que el último número de línea de mandatos de la secuencia de líneas de mandatos. Por ejemplo, si el script acaba con la línea 010, a la línea de mandatos agregada se le asigna el número de línea 015.

## Acerca de esta tarea

A continuación, se presenta un ejemplo del script QSTATUS. El script tiene las líneas 001, 005 y 010 según se indica:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
```

Para añadir el mandato QUERY SESSION al final del script, emita el mandato siguiente:

```
update script qstatus "query session"
```

El mandato QUERY SESSION recibe el número de línea de mandatos 015 y el script actualizado queda del siguiente modo:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY PROCESS
015 QUERY SESSION
```

## Sustitución de un mandato existente

---

Puede cambiar una línea de mandatos existente especificando el parámetro LINE=.

### Acerca de esta tarea

---

El número de línea 010 del script QSTATUS contiene un mandato QUERY PROCESS. Para sustituir el mandato QUERY PROCESS por el mandato QUERY STGPOOL, especifique el parámetro LINE= según se indica:

```
update script qstatus "query stgpool" line=10
```

El script QSTATUS se actualiza para contener las líneas siguientes:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
010 QUERY STGPOOL
015 QUERY SESSION
```

## Adición de un mandato y un número de línea

---

Puede cambiar un script existente añadiendo líneas nuevas.

### Acerca de esta tarea

---

Para añadir el mandato QUERY NODE como la nueva línea 007 del script QSTATUS, emita el mandato siguiente:

```
update script qstatus "query node" line=7
```

El script QSTATUS se actualiza para contener las líneas siguientes:

```
001 /* Éste es el script QSTATUS */
005 QUERY STATUS
007 QUERY NODE
010 QUERY STGPOOL
015 QUERY SESSION
```

## Supresión de un mandato de un script del servidor

---

Se puede suprimir una línea de mandatos concreta de un script. Al especificar un número de línea, sólo se suprime del script la línea de mandatos correspondiente.

### Acerca de esta tarea

---

Por ejemplo, para suprimir la línea de mandatos 007 del script QSTATUS, emita el mandato siguiente:

```
delete script qstatus line=7
```

## Consulta de un script de servidor para crear otro script de servidor

---

Se pueden crear más scripts de servidor consultando un script y especificando los parámetros FORMAT=RAW y OUTPUTFILE. La salida que se obtiene se puede utilizar como entrada de otro script sin tener que crear un script línea a línea.

### Acerca de esta tarea

---

El ejemplo siguiente muestra cómo consultar el script SRTL2 y dirigir la salida a newscript.script:

```
query script srtl2 format=raw outputfile=newscript.script
```

A continuación, puede editar el archivo `newsript.script` con un editor del que disponga el sistema. Para crear un nuevo script utilizando la salida editada de la consulta, emita:

```
define script srtnew file=newscript.script
```

## Ejecución de un script del servidor

---

Para procesar un script, emita el mandato `RUN`. Se puede ejecutar un script que contenga variables de sustitución especificándolas junto con el mandato `RUN`.

### Acerca de esta tarea

---

Para detener el script que se está ejecutando, el administrador deberá parar el servidor. No puede cancelar un script después de iniciarlo utilizando un mandato de IBM Spectrum Protect.

### Procedimiento

---

- Obtenga una vista previa de los mandatos de un script para evaluar este antes de ejecutarlo. Para previsualizar el script sin ejecutar los mandatos, escriba el mandato `RUN` con el parámetro `PREVIEW=YES`. Si el script contiene variables de sustitución, los mandatos se muestran con las variables sustituidas.
- Ejecute un mandato que no tenga ninguna variable especificando el siguiente mandato: `run qaixc` donde `qaixc` es el nombre del script.
- Ejecute un script que contenga variables de sustitución especificando los valores variables con el mandato. Contenido del script:

```
/*-----*/
/* Ejemplo de continuación y sustitución      */
/* -----*/
SELECT-
$1 FROM-
NODES WHERE-
PLATFORM=' $2 '
```

Para ejecutar este script, introduzca el siguiente mandato:

```
run qaixc nombre_nodo aix
```

Donde `node_name` es el valor de la variable `$1` y `aix` es el valor de la variable `$2`.

#### Referencia relacionada:

`RUN` (ejecutar un script de servidor)

## Macros de cliente administrativo

---

Una macro es un archivo que contiene uno o más mandatos de cliente de administración. Sólo puede ejecutar una macro desde el cliente administrativo en la modalidad de proceso por lotes o en la modalidad interactiva. Las macros se almacenan como archivos en el cliente de administración. Las macros no se distribuyen a través de los servidores y no se pueden planificar en el servidor.

Las macros pueden incluir los elementos siguientes:

- mandatos de servidor administrativo
- Comentarios.
- Caracteres de continuación.
- Variables.

El nombre de una macro debe ajustarse a los convenios de denominación del cliente de administración que ejecuta el sistema operativo.

En una macro que contenga varios mandatos, utilice los mandatos `COMMIT` y `ROLLBACK` para controlar el proceso de los mandatos en la macro.

Puede incluir el mandato `MACRO` dentro de un archivo de macros para llamar a otras macros, hasta un máximo de 10 niveles de profundidad. La macro a la que se llama desde la línea de mandatos del cliente de administración se denomina macro de nivel superior. Las macros a las que se llama desde dentro de la macro de nivel superior se denominan macros *anidadas*.

- Grabación de mandatos en una macro  
Añada mandatos administrativos a una macro. El cliente de administración no tiene en cuenta las líneas en blanco que contiene la macro. No obstante, una línea completamente en blanco termina un mandato continuo (con un carácter de continuación).

- Grabación de comentarios en una macro  
Añada comentarios al archivo de macro para describir la finalidad o los mandatos incluidos en él.
- Inclusión de caracteres de continuación en una macro  
Puede utilizar caracteres de continuación en un archivo de macro cuando desee ejecutar un mandato que sea más largo que el ancho de la pantalla o de la ventana.
- Inclusión de las variables de sustitución en un macro  
Puede utilizar variables de sustitución en una macro para que, al ejecutar la macro, pueda proporcionar valores para elementos como parámetros de mandato. Al emplear variables de sustitución, puede utilizar una macro una y otra vez, siempre que necesite llevar a cabo la misma tarea para objetos distintos o con valores de parámetros diferentes.
- Ejecución de una macro  
Utilice el mandato MACRO cuando desee ejecutar una macro. Puede entrar el mandato MACRO en la modalidad de proceso por lotes o en la modalidad interactiva.
- Proceso de mandatos en una macro  
Cuando emita un mandato MACRO, el servidor procesa todos los mandatos del archivo de macros por orden, incluidos los mandatos que están contenidos en las macros anidadas. El servidor compromete todos los mandatos de una macro una vez finalizado correctamente el proceso de la macro de nivel superior.

## Grabación de mandatos en una macro

---

Añada mandatos administrativos a una macro. El cliente de administración no tiene en cuenta las líneas en blanco que contiene la macro. No obstante, una línea completamente en blanco termina un mandato continuo (con un carácter de continuación).

### Acerca de esta tarea

---

A continuación figura un ejemplo de una macro denominada REG.MAC que registra un nuevo administrador y le concede autorización:

```
register admin pease mypasswd -
  contact='david pease, x1234'
grant authority pease -
  classes=policy,storage -
  domains=domain1,domain2 -
  stgpools=stgpool1,stgpool2
```

Este ejemplo utiliza caracteres de continuación en el archivo de macros. Para obtener más información acerca de los caracteres de continuación, consulte el apartado Inclusión de caracteres de continuación en una macro.

Una vez creado un archivo de macros, puede actualizar la información que contiene el mismo y volver a utilizarlo. También puede copiar el archivo de macro. Después de copiar un archivo de macro, puede modificar y ejecutar la copia.

## Grabación de comentarios en una macro

---

Añada comentarios al archivo de macro para describir la finalidad o los mandatos incluidos en él.

### Acerca de esta tarea

---

Para escribir un comentario:

- Escriba una barra inclinada y un asterisco (/\*) para indicar el principio del comentario.
- Escriba el comentario.
- Escriba un asterisco y una barra inclinada (\*/) para indicar el final del comentario.

Puede escribir un comentario en una línea dedicada únicamente a comentarios o colocarlo en una línea que contiene un mandato o parte de un mandato.

Por ejemplo, para utilizar un comentario para identificar la finalidad de una macro, escriba la línea siguiente:

```
/* auth.mac-inscribir nuevos nodos */
```

O puede escribir un comentario para explicar algo acerca de un mandato o parte de un mandato:

```
domain=domain1          /* asignar nodo a domain1 */
```

Los comentarios no pueden anidarse y no pueden fragmentar líneas. Cada línea de un comentario debe contener los delimitadores de comentarios.

## Inclusión de caracteres de continuación en una macro

---

Puede utilizar caracteres de continuación en un archivo de macro cuando desee ejecutar un mandato que sea más largo que el ancho de la pantalla o de la ventana.

## Acerca de esta tarea

---

Sin caracteres de continuación, puede especificar hasta 256 caracteres. Con los caracteres de continuación, este límite se amplía a 1500 caracteres. En el mandato MACRO, los valores de las variables de sustitución se incluyen en el recuento de caracteres.

Para utilizar un carácter de continuación, entre un guión o una barra inclinada invertida al final de la línea que desea a continuación. Con los caracteres de continuación, puede continuar las líneas siguientes de una macro.

## Ejemplos

---

- Continúe un mandato, por ejemplo:

```
register admin pease mypasswd -  
contact="david, ext1234"
```

- Continúe una lista de valores especificando un guión o una barra inclinada invertida, sin ningún espacio en blanco precedente, después de la última coma de la lista que especifique en la primera línea. A continuación, entre los elementos de la lista restantes en la línea siguiente sin anteponer ningún espacio en blanco. En el ejemplo siguiente, una lista de nombres de agrupación de almacenamiento continúa entre líneas:

```
stgpools=stg1, stg2, stg3, -  
stg4, stg5, stg6
```

- Continúe una serie de valores que está especificada entre comillas entrando la primera parte de la serie entre comillas, seguida por un guión o una barra inclinada invertida al final de la línea. A continuación, entre el resto de la serie en la línea siguiente. Cierre el resto de la serie en el mismo tipo de comillas. El ejemplo siguiente muestra una serie que continúa entre líneas:

```
contact="david pease, bldg. 100, room 2b, san jose," -  
"ext. 1234, alternate contact-norm pass, ext 2345"
```

Las dos series se concatenan sin ningún espacio en blanco. Debe utilizar este método sólo para continuar una serie de valores entre comillas en más de una línea.

## Inclusión de las variables de sustitución en un macro

---

Puede utilizar variables de sustitución en una macro para que, al ejecutar la macro, pueda proporcionar valores para elementos como parámetros de mandato. Al emplear variables de sustitución, puede utilizar una macro una y otra vez, siempre que necesite llevar a cabo la misma tarea para objetos distintos o con valores de parámetros diferentes.

## Acerca de esta tarea

---

Una variable de sustitución consta de un signo de porcentaje (%), seguido de un número exclusivo que identifica la variable de sustitución. Cuando ejecute el archivo con el mandato MACRO, debe especificar los valores de las variables.

Restricciones:

- Si el sistema utiliza el signo de porcentaje como carácter comodín, el cliente administrativo interpreta una expresión coincidente con el patrón de una macro en que el signo de porcentaje va inmediatamente seguido de un dígito numérico como variable de sustitución.
- Las variables de sustitución no se pueden delimitar mediante comillas. Sin embargo, un valor proporcionado como sustitución de la variable puede ser una serie entrecomillada.

## Ejemplo

---

Cree una macro denominada AUTH.MAC para registrar nodos nuevos. La macro tiene cuatro variables de sustitución para parámetros en el mandato:

```
/* inscribir nuevos nodos */  
register node %1 %2 - /* contraseña de ID de usuario */  
contact=%3 - /* 'nombre, número teléfono' */  
domain=%4 /* dominio de políticas */
```

Cuando ejecute la macro, debe entrar los valores que desea pasar al servidor para procesar el mandato.

Por ejemplo, para utilizar la macro para registrar el nodo denominado DAVID con una contraseña de DAVIDPW, incluir el nombre y el número de teléfono como información de contacto y asignarlo al dominio de políticas DOMAIN1, entre el siguiente mandato:

```
macro auth.mac david davidpw "david pease, x1234" domain1
```

## Ejecución de una macro

---

Utilice el mandato MACRO cuando desee ejecutar una macro. Puede entrar el mandato MACRO en la modalidad de proceso por lotes o en la modalidad interactiva.

### Acerca de esta tarea

---

Si la macro no contiene variables de sustitución, ejecute la macro especificando el mandato MACRO con el nombre del archivo de macro. Por ejemplo:

```
macro reg.mac
```

Si la macro contiene variables de sustitución, incluya los valores que desea suministrar tras el nombre de la macro. Los distintos valores se delimitan mediante un espacio. Por ejemplo:

```
macro auth.mac pease mypasswd "david pease, x1234" domain1
```

Si el número de valores que especifica es inferior al de variables de sustitución que hay en la macro, el cliente de administración sustituye las variables restantes por series nulas.

Si desea omitir uno o más valores entre los valores, especifique una cadena nula ("" ) para cada uno de los valores omitidos. Por ejemplo, para omitir la información de contacto en el ejemplo anterior, escriba:

```
macro auth.mac pease mypasswd "" domain1
```

#### Referencia relacionada:

MACRO (Invocar una macro)

## Proceso de mandatos en una macro

---

Cuando emita un mandato MACRO, el servidor procesa todos los mandatos del archivo de macros por orden, incluidos los mandatos que están contenidos en las macros anidadas. El servidor compromete todos los mandatos de una macro una vez finalizado correctamente el proceso de la macro de nivel superior.

Si se produce un error en algún mandato de la macro o de alguna de las macros anidadas, el servidor termina el proceso y retrotrae los cambios originados por todos los mandatos anteriores.

Si especifica la opción ITEMCOMMIT al introducir el mandato DSMADMC, el servidor compromete uno a uno cada uno de los mandatos en un script o en una macro, una vez finalizado correctamente el proceso de cada uno de ellos. Si se produce algún error, el servidor continúa con el proceso y sólo retrotrae los cambios provocados por el mandato erróneo.

Puede controlar con precisión cuándo se comprometen los mandatos con el mandato COMMIT. Si se produce un error al procesar los mandatos de una macro, el servidor termina el proceso de la macro y retrotrae los cambios no comprometidos. Los cambios no comprometidos son los mandatos que se han procesado desde el último mandato COMMIT. Asegúrese de que la sesión del cliente de administración no se esté ejecutando con la opción ITEMCOMMIT si desea controlar el proceso de mandatos con el mandato COMMIT.

Puede probar una macro antes de implementarla mediante el mandato ROLLBACK. Puede introducir los mandatos (excepto el mandato COMMIT) que desea emitir en la macro e introducir ROLLBACK como último mandato. A continuación, puede ejecutar la macro para verificar que todos los mandatos se procesen correctamente. El mandato ROLLBACK que ha incluido al final retrotrae los cambios efectuados en la base de datos como consecuencia de los mandatos. No olvide eliminar el mandato ROLLBACK antes de poner la macro a disposición para su uso real. Asimismo, compruebe que la sesión del cliente de administración no se esté ejecutando con la opción ITEMCOMMIT si desea controlar el proceso de mandatos con el mandato ROLLBACK.

Consejo: Los mandatos que inician procesos de fondo no pueden retrotraerse.

Si tiene una serie de mandatos que se procesan correctamente en la línea de mandatos pero no al emitirse dentro de una macro, es probable que existan dependencias entre los mandatos. Puede suceder que un mandato emitido dentro de una macro no pueda procesarse correctamente hasta que se haya comprometido un mandato anterior emitido dentro de la misma macro. Lleve a cabo alguna de las acciones siguientes para que estos mandatos se procesen correctamente dentro de una macro:

- Inserte un mandato COMMIT antes del mandato que depende de un mandato anterior. Por ejemplo, si COMMAND C depende de COMMAND B, inserte un mandato COMMIT antes de COMMAND C.

```

command a
command b
commit
command c/

```

- Inicie la sesión del cliente de administración utilizando la opción ITEMCOMMIT. Esta opción hace que todos los mandatos de una macro se confirmen antes de que se procese el mandato siguiente.

**Referencia relacionada:**

COMMIT (controlar la validación de mandatos en una macro)  
 ROLLBACK (Retrotraer cambios no validados en una macro)

## Códigos de retorno de los scripts para IBM Spectrum Protect

Puede escribir scripts de IBM Spectrum Protect que utilizan códigos de retorno para determinar cómo continúa el proceso de script. Los códigos de retorno pueden ser de una de estas tres gravedades: OK, WARNING, ERROR.

Los scripts de IBM Spectrum Protect utilizan el código de retorno simbólico para el procesamiento, no el valor numérico. El cliente de administración muestra los valores numéricos cuando se ejecuta un mandato. Los códigos de retorno se muestran en la tabla siguiente.

Tabla 1. Códigos de retorno

Código de retorno	Gravedad	Valor numérico	Descripción
RC_OK	Aceptar	0	El mandato se ha completado satisfactoriamente.
RC_UNKNOWN	ERROR	2	El mandato no se ha encontrado; no se reconoce el mandato.
RC_SYNTAX	ERROR	3	El mandato es válido, pero uno o más parámetros no se han especificado correctamente.
RC_ERROR	ERROR	4	Un error interno ha impedido que el mandato se completara correctamente.
RC_NOMEMORY	ERROR	5	El mandato no se ha podido completar porque no hay memoria suficiente en el servidor.
RC_NOLOG	ERROR	6	El mandato no se ha podido completar porque no hay espacio de registro de recuperación suficiente en el servidor.
RC_NODB	ERROR	7	El mandato no se puede completar porque no hay espacio de base de datos suficiente en el servidor.
RC_NOSTORAGE	ERROR	8	El mandato no se puede completar porque no hay espacio de almacenamiento suficiente en el servidor.
RC_NOAUTH	ERROR	9	El mandato ha fallado porque el administrador no está autorizado para emitir este mandato.
RC_EXISTS	ERROR	10	El mandato ha fallado porque el objeto especificado ya existe en el servidor.
RC_NOTFOUND	AVISO	11	Devuelto por un mandato QUERY o SQL SELECT cuando no se encuentran objetos que coincidan con las especificaciones.
RC_INUSE	ERROR	12	El mandato ha fallado porque el objeto con el que se va a operar estaba en uso.
RC_ISREFERENCED	ERROR	13	El mandato ha fallado porque el objeto en el que se iba a operar todavía está siendo referenciado por otro servidor en construcción.
RC_NOTAVAILABLE	ERROR	14	El mandato ha fallado porque el objeto con el que se va a operar no está disponible.
RC_IOERROR	ERROR	15	El mandato ha fallado porque ha encontrado un error de entrada/salida (E/S) en el servidor.

Código de retorno	Gravedad	Valor numérico	Descripción
RC_NOTXN	ERROR	16	El mandato ha fallado porque la transacción de una base de datos ha fallado en el servidor.
RC_NOLOCK	ERROR	17	El mandato ha fallado porque se ha producido un conflicto de bloqueo en la base de datos del servidor.
RC_NOTHREAD	ERROR	19	El mandato no se ha podido completar porque no hay memoria suficiente en el servidor.
RC_LICENSE	ERROR	20	El mandato ha fallado porque el servidor no cumple con la licencia.
RC_INVDEST	ERROR	21	El mandato ha fallado porque el valor de destino no es válido.
RC_IFILEOPEN	ERROR	22	El mandato ha fallado porque el archivo de entrada necesario no se ha podido abrir.
RC_OFILEOPEN	ERROR	23	El mandato ha fallado porque no ha podido abrir el archivo de salida necesario.
RC_OFILEWRITE	ERROR	24	El mandato ha fallado porque no ha podido grabarse correctamente en un archivo de salida necesario.
RC_INVADMIN	ERROR	25	El mandato falló porque el administrador no se había definido.
RC_SQLERROR	ERROR	26	Se ha detectado un error de SQL durante la consulta de sentencia SELECT.
RC_INVALIDUSE	ERROR	27	El mandato ha fallado porque se ha emitido de manera no válida.
RC_NOTABLE	ERROR	28	El mandato ha fallado debido a un nombre de tabla desconocido de SQL.
RC_FS_NOTCAP	ERROR	29	El mandato ha fallado debido a los tipos de nombres de espacio de archivo no compatibles.
RC_INVALIDADDR	ERROR	30	El mandato ha fallado porque hay una dirección de alto nivel o una dirección de bajo nivel incorrectas.
RC_INVALIDCG	ERROR	31	El mandato ha fallado porque la clase de gestión no tiene un grupo de copia de archivado.
RC_OVERSIZE_VOL	ERROR	32	El mandato ha fallado porque el tamaño del volumen supera el máximo permitido.
RC_DEFVOL_FAIL	ERROR	33	El mandato ha fallado porque los volúmenes no se pueden definir en las agrupaciones de almacenamiento de RECLAMATIONTYPE=SNAPLOCK.
RC_DELVOL_FAIL	ERROR	34	El mandato ha fallado porque los volúmenes no se pueden suprimir en las agrupaciones de almacenamiento de RECLAMATIONTYPE=SNAPLOCK.
RC_CANCELED	AVISO	35	El mandato se ha cancelado.
RC_INVPOLICY	ERROR	36	El mandato ha fallado porque hay una definición no válida en el dominio de políticas.
RC_INVALIDPW	ERROR	37	El mandato ha fallado porque hay una contraseña no válida.
RC_UNSUPP_PARM	AVISO	38	El mandato ha fallado porque el mandato o el parámetro no es compatible.

**Referencia relacionada:**

DEFINE SCRIPT (definir un script de IBM Spectrum Protect)

UPDATE SCRIPT (actualizar un script de IBM Spectrum Protect)



## Documentación de servidor en archivos PDF

Hay disponibles archivos PDF predefinidos de la documentación de IBM Spectrum Protect para su descarga.

Consejo: A partir de la V7.1.3, la *Guía de usuario del administrador* queda obsoleta. Utilice las guías de la solución para implementar y gestionar una solución de disco de un solo sitio y una solución de disco de varios sitios. Los procedimientos para realizar las tareas de administración del sistema están disponibles en los siguientes temas:

- Configuración y gestión del entorno de almacenamiento
- Soluciones de protección de datos IBM Spectrum Protect

Para completar las tareas siguientes, consulte los archivos PDF en los enlaces siguientes.

Tarea	Componentes	Enlaces
Información sobre conceptos de producto y soluciones	<ul style="list-style-type: none"> <li>• Servidor</li> <li>• Centro de operaciones</li> </ul>	Introducción a las soluciones de protección de datos
Despliegue de una solución de mejores prácticas	<ul style="list-style-type: none"> <li>• Servidor</li> <li>• Centro de operaciones</li> </ul>	<ul style="list-style-type: none"> <li>• Guía de solución de disco con un solo sitio</li> <li>• Guía de solución de disco con varios sitios</li> <li>• Guía de soluciones de cintas</li> </ul>
Instalación de componentes	<ul style="list-style-type: none"> <li>• Servidor</li> <li>• Centro de operaciones</li> </ul>	<ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>
Actualización de componentes	<ul style="list-style-type: none"> <li>• Servidor</li> </ul>	<ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>
Uso de mandatos y opciones	<ul style="list-style-type: none"> <li>• Servidor</li> </ul>	<ul style="list-style-type: none"> <li>• AIX</li> <li>• Linux</li> <li>• Windows</li> </ul>
Uso de mensajes y códigos de error	<ul style="list-style-type: none"> <li>• Servidor</li> </ul>	Todos los sistemas operativos

## IBM Spectrum Protect clientes de archivado y copia de seguridad

Para guardar copias de archivos y directorios en estaciones de trabajo y servidores de archivos, utilice el cliente de archivado y copia de seguridad de IBM Spectrum Protect para almacenar los datos en el servidor de IBM Spectrum Protect. En caso de que los archivos originales queden dañados o se pierdan, podrá recuperar estas copias. Dependiendo de sus motivos para guardar los datos, puede hacer una copia de seguridad o archivar los datos.

- Novedades de los clientes de archivado y copia de seguridad IBM Spectrum Protect  
Leer sobre las características nuevas y modificadas. Revise las notas del release antes de instalar el producto.
- Protección para estaciones de trabajo y servidores de archivos  
IBM Spectrum Protect es un producto de cliente/servidor con licencia que proporciona servicios de gestión de almacenamiento en un entorno de sistemas multiplataforma.
- Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)  
El cliente de archivado y copia de seguridad de IBM Spectrum Protect le ayuda a proteger la información de las estaciones de trabajo.
- Configuración de clientes de copia de seguridad/archivado  
Puede configurar el cliente de archivado y copia de seguridad para utilizar muchas de las características de cliente disponibles. Se proporciona información para configurar los clientes de copia de seguridad/archivado.
- Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad  
Si quiere guardar una copia de un archivo desde su ordenador al IBM Spectrum Protect servidor, utilice la función *copia de seguridad*. Si en alguna ocasión se daña o se pierde el archivo original, puede *restaurar* la versión de copia de seguridad del servidor.
- Archivar y recuperar datos con clientes de archivado y copia de seguridad  
Si desea guardar una copia de un archivo en un almacenamiento a largo plazo en el servidor de IBM Spectrum Protect utilice la función *archive*.

- Planificar operaciones para clientes de archivado y copia de seguridad  
Pueden planificarse las operaciones de copia de seguridad que protegen los datos del cliente para garantizar que esas operaciones se ejecuten regularmente.
- Políticas de gestión de almacenamiento  
Las políticas de gestión de almacenamiento son reglas que el administrador define con el fin de gestionar las copias de seguridad y las copias archivadas en el servidor.
- Opciones y mandatos del cliente de copia de seguridad/archivado  
Utilice las opciones del cliente para ajustar el proceso de cliente de archivado y copia de seguridad para que se adapte a sus necesidades. Utilice la interfaz de línea de mandatos de cliente (CLI) como alternativa a la interfaz gráfica de usuario (GUI). Se proporciona información de referencia para las opciones, mandatos y otra información adicional del cliente.
- Mensajes ANS 0000-9999

**Tareas relacionadas:**

Desarrollo de soluciones con la interfaz de programación de aplicaciones

**Referencia relacionada:**

Archivos PDF para imprimir

## Novedades de los clientes de archivado y copia de seguridad IBM Spectrum Protect




















Leer sobre las características nuevas y modificadas. Revise las notas del release antes de instalar el producto.






- Actualizaciones del cliente de archivado y copia de seguridad  
Descubra las nuevas características y actualizaciones del cliente de archivado y copia de seguridad en IBM Spectrum Protect Versión 8.1.
- Notas del release para IBM Spectrum Protect Backup-Archive Client Versión 8.1  
Ya está disponible IBM Spectrum Protect Backup-Archive Client V8.1. Lea este documento para obtener información importante sobre la instalación. También puede obtener información sobre actualizaciones de producto, problemas de compatibilidad limitaciones y problemas conocidos.
- Archivos léame para los fixpacks del cliente de archivado y copia de seguridad de IBM Spectrum Protect Versión 8.1  
Los archivos léame para los fixpacks del cliente de archivado y copia de seguridad de IBM Spectrum Protect V8.1 están disponibles en la base de conocimiento de soporte cuando hay una actualización del fix pack.
- Últimas actualizaciones de la documentación  
Se pueden realizar actualizaciones de la documentación del cliente de archivado y copia de seguridad de IBM Spectrum Protect tras la publicación de la documentación en IBM® Knowledge Center.













## Actualizaciones del cliente de archivado y copia de seguridad





Descubra las nuevas características y actualizaciones del cliente de archivado y copia de seguridad en IBM Spectrum Protect Versión 8.1.


















Release	Nuevas características y actualizaciones
8.1.2	<p>Proteja el cliente con una configuración de seguridad mejorada</p> <p>A partir de IBM Spectrum Protect Versión 8.1.2 se han introducido diversos cambios en el cliente de archivado y copia de seguridad para su uso con el servidor de IBM Spectrum Protect V8.1.2, que proporciona mejoras para una mayor seguridad de las comunicaciones entre cliente y el servidor.</p> <p>Tras la actualización del servidor de IBM Spectrum Protect a V8.1.2, su configuración con el protocolo de seguridad mejorado y la actualización del cliente de archivado y copia de seguridad a V8.1.2, se deben configurar los valores de seguridad del cliente para su utilización con las mejoras de seguridad en el servidor. Para obtener más información sobre cómo configurar el cliente para los distintos escenarios de seguridad, consulte Configuración de los valores de seguridad del cliente para la conexión al servidor de IBM Spectrum Protect versión 8.1.2 y posterior.</p> <p>En este release están disponibles los cambios siguientes:</p> <p>Nueva opción <code>sslacceptcertfromserv</code>, cambios en tres opciones existentes relacionadas con SSL</p> <p>Para simplificar el proceso de distribución de certificados de servidor, ahora IBM Spectrum Protect incluye una nueva opción <code>sslacceptcertfromserv</code> para controlar si el cliente de archivado y copia de seguridad o la aplicación de la API acepta y confía en el certificado público SSL (Secure Sockets Layer) del servidor de IBM Spectrum Protect la primera vez que se conectan.</p>






Release	Nuevas características y actualizaciones
	<p>Además, tres opciones relacionadas con SSL <code>ssl</code>, <code>ssldisablelegacytls</code> y <code>sslrequired</code> han cambiado. Su funcionamiento varía en función de si operan con un servidor IBM Spectrum Protect V8.1.2 o con un servidor IBM Spectrum Protect V8.1.1 o V8 anterior, y con V7.1.7 y niveles anteriores.</p> <p>Para obtener una descripción de estos valores de opción e información de versión importante, consulte <code>Sslacceptcertfromserv</code>, <code>Ssl</code>, <code>Ssldisablelegacytls</code> y <code>Sslrequired</code>.</p> <p>La ubicación de la contraseña de IBM Spectrum Protect ha cambiado A partir de V8.1.2, se utilizan los almacenes de claves de IBM® Global Security Kit (GSKit) para almacenar todas las contraseñas de IBM Spectrum Protect. Cuando se actualiza al cliente de archivado y copia de seguridad de IBM Spectrum Protect V8.1.2, las contraseñas existentes se migran automáticamente a nuevas ubicaciones en el sistema cliente.</p> <p>Para obtener más información sobre la nueva ubicación de contraseña y consideraciones relacionadas, consulte Almacenamiento seguro de contraseñas.</p> <p>Hay disponible una nueva forma de importar certificados de servidor con el programa de utilidad <code>dsmcert</code>. Para obtener información sobre la importación de certificados de servidor, consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer.</p> <p>Debido a la utilización del nuevo almacenamiento seguro de contraseñas, hay disponibles nuevos procedimientos para otorgar acceso a contraseñas a usuarios no administrativos.</p> <p> Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Para los clientes UNIX y Linux, consulte Permitir que los usuarios no root gestionen sus propios datos.</p> <p> Sistemas operativos Windows Para los clientes Windows, consulte Derechos de seguridad y operaciones del cliente de archivado y copia de seguridad.</p> <p>Despliegue automático de actualizaciones de cliente de archivado y copia de seguridad El administrador del servidor de IBM Spectrum Protect puede utilizar mandatos de servidor para planificar actualizaciones para uno o más clientes de archivado y copia de seguridad. Las actualizaciones pueden ser fixpacks o releases nuevos. Esta característica estaba disponible en releases anteriores de IBM Spectrum Protect, pero hay disponible un procedimiento mejorado para V8.1.2. Para obtener más información, consulte Planificación de actualizaciones automáticas para los clientes de archivado y copia de seguridad.</p> <p>Funciones en desuso Las funciones siguientes están en desuso en este release:</p> <p>Opciones <code>lanfreessl</code> y <code>replsslport</code> Dos opciones relacionadas con SSL, <code>lanfreessl</code> y <code>replsslport</code>, están en desuso y no están disponibles si se conecta a un servidor de IBM Spectrum Protect V8.1.2 y posterior. Estas opciones todavía son válidas y están disponibles si se conecta a una servidor IBM Spectrum Protect V8.1.1 o V8 anterior, y V7.1.7 o anterior.</p> <p> Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Trusted Communications Agent (TCA)  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Trusted Communications Agent (TCA), utilizado anteriormente por los usuarios no root en los clientes de V8.1.0, V7.1.6 y anteriores, ya no está disponible. Los usuarios root pueden utilizar otros métodos para permitir que los usuarios no root gestionen sus archivos. Para obtener más información, consulte:</p> <ul style="list-style-type: none"> <li>• Trusted Communications Agent ya no está disponible</li> <li>• Permitir que los usuarios no root gestionen sus propios datos</li> </ul> <p>Cliente web de IBM Spectrum Protect Ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior. Sin embargo, aún puede utilizar el cliente web para conectarse a los servidores de IBM Spectrum Protect V8.1.1, V8.1.0, V7.1.7 o anteriores. Para obtener más información, consulte Utilización del cliente web en el nuevo entorno de seguridad.</p> <p> Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Operaciones del cliente web y línea de mandatos de NDMP  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Si se conecta al servidor de IBM Spectrum Protect V8.1.2 o posterior, ya no puede utilizar la</p>

Release	Nuevas características y actualizaciones
	<p>interfaz de línea de mandatos del cliente o el cliente web para hacer copia de seguridad o restaurar servidores de archivos NAS utilizando Network Data Management Protocol (NDMP). Como alternativa, puede utilizar mandatos del servidor de IBM Spectrum Protect con el cliente de línea de mandatos administrativo (dsmadm) para restaurar datos de NDMP. Para obtener más información, consulte la información de NDMP en Utilización del cliente web en el nuevo entorno de seguridad.</p> <p><b>Inscripción abierta</b> Si el cliente se conecta a un servidor de IBM Spectrum Protect V8.1.2 o posterior, la característica de inscripción abierta ya no está disponible. Para conectarse al servidor de IBM Spectrum Protect, debe utilizar la inscripción cerrada. Para obtener más información, consulte el apartado <b>Inscripción cerrada</b>. La inscripción abierta aún está disponible si el cliente se conecta a servidores de IBM Spectrum Protect V8.1.1, V8.1.0, V7.1.7 o anteriores.</p> <p>Para obtener más información sobre las mejoras de seguridad en el servidor, consulte Protección del entorno de almacenamiento con un protocolo de seguridad mejorado.</p> <p> Sistemas operativos Windows Soporte mejorado para Data Protection for Microsoft Hyper-V ejecutándose en Windows Server 2016</p> <p> Sistemas operativos Windows</p> <p><b>Copia de seguridad de las máquinas virtuales utilizando RCT (Resilient Change Tracking - Seguimiento de cambios resistentes)</b> Para mejorar la escalabilidad y el rendimiento de las copias de seguridad de máquina virtual (VM), se utiliza RCT (Resilient Change Tracking) para todas las operaciones de copia de seguridad de máquina virtual de hosts Hyper-V que se ejecutan en el sistema operativo Microsoft Windows Server 2016. Para obtener más información, consulte Copias de seguridad de máquinas virtuales con RCT.</p> <p> Sistemas operativos Windows</p> <p><b>Ejercer más control sobre las operaciones de copia de seguridad en las máquinas virtuales con discos físicos</b> Puede controlar si las copias de seguridad de máquina virtual Hyper-V RCT se procesan si la VM tiene uno o más discos físicos (discos de paso a través) suministrados. Para obtener más información, consulte las opciones siguientes:</p> <ul style="list-style-type: none"> <li>• Vmprocessvmwithphysdisks</li> <li>• Vmskipphysdisks</li> </ul> <p><b>Especificar el número de intentos de instantánea y el nivel de coherencia de datos para operaciones de copia de seguridad</b> Para determinar el número total de intentos de instantánea a realizar para una máquina virtual que falla durante el proceso de copia de seguridad debido a un error de instantánea, utilice la opción INCLUDE.VMSNAPSHOTATTEMPTS. Puede optar por intentar instantáneas coherentes con la aplicación o coherentes con respecto a bloqueos. Para obtener más información, consulte INCLUDE.VMSNAPSHOTATTEMPTS.</p> <p><b>Excluir discos de máquina virtual de las operaciones de copia de seguridad o incluirlos en dichas operaciones</b> Puede utilizar el exclude.vmdisk opción para excluir un disco de máquina virtual (VHDX) de las operaciones de copia seguridad de máquina virtual o utilizar la opción include.vmdisk para incluir un disco de máquina virtual en operaciones de copia de seguridad de máquina virtual. Para obtener más información consulte los siguientes temas:</p> <ul style="list-style-type: none"> <li>• Exclude.vmdisk</li> <li>• Include.vmdisk</li> <li>• Domain.vmfull</li> <li>• Backup VM</li> </ul> <p> Sistemas operativos Windows Soporte mejorado para Data Protection for Microsoft Hyper-V ejecutándose en Windows Server 2012 y 2012 R2</p> <p> Sistemas operativos Windows</p> <p>Se ha mejorado la escalabilidad y fiabilidad de las copias de seguridad de máquinas virtuales Las máquinas virtuales se agrupan de forma lógica en una sola instantánea para reducir o eliminar los conflictos de instantánea a nivel de host Hyper-V. El proceso de reintento de instantánea mejorado</p>

Release	Nuevas características y actualizaciones
	<p>simplifica la planificación y mejora la fiabilidad entre nodos de clúster.</p> <ul style="list-style-type: none"> <li>• Para controlar el número de máquinas virtuales en una instantánea, utilice la opción vmmxpersnapshot. Para obtener más información, consulte Vmmxpersnapshot.</li> <li>• Para controlar el número de reintentos de instantánea, utilice la opción vmmxsnapshotretry. Para obtener más información, consulte Vmmxsnapshotretry.</li> </ul> <p>Utilice estas mejoras de agrupación y reintentos junto con la opción vmmxparallel para mejorar el rendimiento.</p> <p>Para obtener información, consulte Ajuste de copias de seguridad de máquina virtual planificadas para clústeres de Windows Server 2012 y 2012 R2.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Soporte de VVOL (Enhanced Virtual Volumes)</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Se ha mejorado del soporte de VVOL para incluir instantáneas persistentes en el almacenamiento de hardware y protección de aplicación. Para obtener más información sobre las nuevas características de VVOL, consulte, IBM Spectrum Protect for Virtual Environments: Data Protection for VMware updates.</p> <p>Para utilizar las características mejoradas de VVOL, utilice las opciones que se describen en las secciones siguientes:</p> <p>Especifique la ubicación para las operaciones de restauración y copia de seguridad de máquina virtual: local y/o servidor</p> <p>Para máquinas virtuales alojadas en almacenes de datos VVOL, ahora puede especificar una de las siguientes ubicaciones de copia de seguridad para operaciones de copia de seguridad y restauración: local y/o servidor. Una copia de seguridad local es una instantánea persistente en el almacenamiento de hardware.</p> <p>Para especificar la ubicación de copia de seguridad para el mandato Backup VM o Restore VM, utilice la opción vmbackuplocation. Para obtener más información, consulte Vmbackuplocation.</p> <p>También puede especificar la ubicación o las ubicaciones de copia de seguridad que desea consultar cuando ejecuta el mandato Query VM. Para obtener más información, consulte Query VM.</p> <p>Los códigos de Gestión de copia de seguridad local (IBM Spectrum Protect) están disponibles para copias de seguridad locales. Para obtener más información, consulte Códigos de protección de datos admitidos.</p> <p><b>Crear un grupo de planificación</b></p> <p>Puede utilizar la opción schedgroup para crear un grupo que contenga varias planificaciones. A continuación, puede utilizar la Plug-in de cliente de IBM Spectrum Protect vSphere para asignar el grupo de planificación a un objeto en el cliente web de VMware vSphere en lugar de hacerlo a una planificación individual. Un ejemplo de la utilización de esta opción es agrupar varias planificaciones de copia de seguridad local diaria con una única planificación de copia de seguridad de servidor de IBM Spectrum Protect.</p> <p>Para obtener más información, consulte Schedgroup.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Restaurar varios discos virtuales simultáneamente</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Puede utilizar el cliente de IBM Spectrum Protect para restaurar varios discos virtuales simultáneamente en los sistemas operativos Microsoft Windows y Linux utilizando la opción vmmxrestoreparalleldisks.</p> <p>Para obtener instrucciones sobre los valores de la opción, consulte Vmmxrestoreparalleldisks.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Se ha añadido la opción de cliente snapdiffchangelogdir para operaciones de copia de seguridad diferencial de instantánea</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Las copias de seguridad diferenciales de instantánea ya no utilizan la opción stagingdirectory para almacenar los archivos de registro de cambios diferenciales de instantánea. A partir de V8.1.2, utilice la nueva opción snapdiffchangelogdir para especificar la ubicación donde el cliente almacena registros de cambios persistentes para las copias de seguridad diferenciales de instantánea.</p> <p>Para obtener una descripción de los valores de esta opción e información importante acerca de la migración desde versiones de cliente anteriores, consulte Snapdiffchangelogdir.</p>
8.1.0	IBM Tivoli Storage Manager es ahora IBM Spectrum Protect

Release	Nuevas características y actualizaciones
	<p>IBM Spectrum Protect versión 8.1 es la siguiente generación de Tivoli Storage Manager. Esta nueva versión va más allá de un simple cambio de nombre en la documentación y la interfaz de usuario. Se trata de una evolución hacia un nuevo nivel de protección de datos, diseñado para satisfacer las complejas demandas del mundo actual.</p> <p>Para obtener más información, consulte la publicación Conozca IBM Spectrum Protect.</p> <p>Ya no se crea de forma predeterminada un ID de usuario de administración con el mandato de servidor REGISTER NODE</p> <p>A partir de IBM Spectrum Protect V8.1, el mandato de servidor REGISTER NODE no crea automáticamente un ID de usuario de administración que coincide con el nombre de nodo. Esta actualización de producto se ha diseñado para optimizar la autenticación de usuario en un servidor LDAP (Lightweight Directory Access Protocol).</p> <p>Esta actualización del producto no afecta a los nodos existentes del producto, pero puede afectar al proceso de registro de nuevos nodos de cliente, incluidos, entre otros, los nodos para clientes de archivado y copia de seguridad de IBM Spectrum Protect. En algunos casos, es posible que tenga que crear un ID de usuario de administración al registrar un nodo. Puede crear el ID de usuario de administración emitiendo el mandato REGISTER NODE y especificando el parámetro USERID. Para obtener información sobre los tipos de clientes afectados, consulte la nota técnica 7048963.</p> <p>Si tiene previsto utilizar el cliente web, tiene que crear manualmente un ID de usuario de administración al registrar el nodo nuevo. Para obtener más información, consulte el apartado Registrar la estación de trabajo en un servidor.</p> <p>Ejecute el cliente web independientemente del navegador web</p> <p>En lugar de ejecutar el cliente web IBM Spectrum Protect como un applet de Java™, el cliente web se suministra como una aplicación de inicio de Java Web, que se puede iniciar y gestionar de forma independiente del navegador web.</p> <p>Para obtener más información sobre cómo iniciar el cliente web, consulte el apartado Inicio de una sesión de cliente web.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows La gestión de copias de seguridad incluye mejoras, como nuevos códigos de protección de datos, para el soporte a la codificación</p> <p> Sistemas operativos Linux  Sistemas operativos Windows</p> <p>Hay nuevos códigos de protección de datos disponibles para el soporte a la codificación</p> <p>Se han añadido nuevos códigos de protección de datos para ayudarle a gestionar las operaciones de copia de seguridad de máquina virtual con la Plug-in de cliente de IBM Spectrum Protect vSphere en el cliente web de VMware vSphere. Además de utilizar códigos para excluir máquinas virtuales de operaciones de copia de seguridad planificada y asignar clases de gestión o retención, introducidas en la V7.1.6, puede asignar los nuevos códigos a los objetos de inventario de vSphere para ejecutar las tareas siguientes:</p> <ul style="list-style-type: none"> <li>• Incluir máquinas virtuales en operaciones de seguridad planificadas</li> <li>• Asignar un transportador de datos a una máquina virtual</li> <li>• Especificar una lista de discos virtuales de los que se debe realizar una copia de seguridad</li> <li>• Asignar una planificación de copia de seguridad a máquinas virtuales en un contenedor</li> <li>• Especificar la coherencia de datos que conseguir en los intentos de instantánea durante las operaciones de seguridad de máquina virtual</li> <li>• Proporcionar protección de aplicaciones a las máquinas virtuales que ejecutan software de Microsoft SQL Server o Microsoft Exchange Server</li> </ul> <p>Para obtener más información, consulte Códigos de protección de datos admitidos.</p> <p>Definición de un transportador de datos predeterminado para la codificación</p> <p>Puede definir un transportador de datos predeterminado para proteger las máquinas virtuales en los objetos de inventario de vSphere que se han codificado con códigos de protección de datos. El transportador de datos predeterminado es el que realiza la copia de seguridad de las nuevas máquinas virtuales que se añaden al contenedor codificado y están protegidas por una planificación, pero que no tienen un código de transportador de datos.</p> <p>Para obtener más información, consulte Vmtagdefaultdatamover.</p>

Release	Nuevas características y actualizaciones
	<p>Los códigos de protección de datos se pueden heredar desde objetos de inventario de vSphere de un nivel superior</p> <p>Puede utilizar la herencia de códigos para gestionar la protección de datos de máquinas virtuales en el inventario de vSphere.</p> <p>Para obtener más información, consulte Herencia de valores de protección de datos.</p> <p>Se pueden añadir máquinas virtuales a una planificación de copia de seguridad utilizando la Plug-in de cliente de IBM Spectrum Protect vSphere</p> <p>Puede seleccionar una planificación de copia de seguridad para máquinas virtuales desde la Plug-in de cliente de IBM Spectrum Protect vSphere del cliente web de VMware vSphere. La planificación de copia de seguridad especifica con qué frecuencia y cuándo realizar una copia de seguridad automática de las máquinas virtuales en un objeto de inventario de vSphere.</p> <p>Para obtener más información, consulte la publicación Selección de una planificación para realizar la copia de seguridad de máquinas virtuales.</p> <p>También puede ver y gestionar planificaciones de copia de seguridad desde la Plug-in de cliente de IBM Spectrum Protect vSphere. Para obtener más información, consulte la publicación Gestión de planificaciones de copia de seguridad en el vCenter.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows La copia de seguridad diferencial de instantánea ya no se admite en AIX</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Ya no puede ejecutar copias de seguridad diferenciales de instantánea de volúmenes de gestor de archivos NetApp en el cliente de archivado y copia de seguridad en el sistema operativo IBM AIX. Puede ejecutar copias de seguridad diferenciales de instantánea sólo en clientes Linux y Microsoft Windows.</p> <p>Funciones que se han dejado de mantener</p> <p>En este release, han dejado de mantenerse las siguientes funciones:</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Ejecución de operaciones de máquina virtual en el cliente de archivado y copia de seguridad</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Las operaciones de máquina virtual sólo están disponibles si utiliza el cliente como un transportador de datos para los productos IBM Spectrum Protect for Virtual Environments (Data Protection for VMware o Data Protection for Microsoft Hyper-V).</p> <p>Ya no puede ejecutar operaciones de máquina virtual sin instalar IBM Spectrum Protect for Virtual Environments.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows La API de VMware vStorage ya no forma parte de la instalación de cliente</p> <p> Sistemas operativos Linux  Sistemas operativos Windows El componente de archivos de ejecución de la API de VMware vStorage utilizado para operaciones de VMware ya no forma parte de la instalación del cliente de archivado y copia de seguridad. Está instalado como parte del paquete de instalación de Data Protection for VMware.</p> <p> Sistemas operativos Linux  Sistemas operativos Windows Operaciones de máquina virtual que se han dejado de mantener para el transportador de datos</p> <p> Sistemas operativos Linux  Sistemas operativos Windows</p> <p>Copias de seguridad de máquina virtual a nivel de archivos</p> <p>Ya no se pueden ejecutar copias de seguridad de máquinas virtuales VMware a nivel de archivo en el transportador de datos. En su lugar, utilice operaciones de copia de seguridad completa incremental-constante o copia de seguridad incremental-constante-incremental.</p> <p>Copias de seguridad completas y copias de seguridad incrementales periódicas</p> <p>Ya no es posible ejecutar copias de seguridad completas ni copias de seguridad incrementales periódicas de máquinas virtuales en el transportador de datos. En su lugar, utilice operaciones de copia de seguridad completa incremental-constante o copia de seguridad incremental-constante-incremental.</p> <p>Soporte a vCloud Director de VMware</p> <p>Ya no puede realizar copias de seguridad ni restaurar vCloud vApps con el transportador de datos. Para realizar copias de seguridad o restauraciones de vApps, tiene que utilizar Data Protection for VMware V7.1.</p> <p> Sistemas operativos Windows Restauraciones de estado del sistema en línea</p>

Release	Nuevas características y actualizaciones
	<p> <b>Sistemas operativos Windows</b> Ya no puede restaurar el estado del sistema en un sistema en línea. En lugar de ello, utilice el método de recuperación basado en ASR (Automated System Recovery) para restaurar el estado del sistema a la modalidad fuera de línea de Windows Preinstallation Environment (PE).</p> <p>Para obtener más información, consulte:</p> <ul style="list-style-type: none"> <li>• Restaurar el sistema operativo de Windows con Automated System Recovery</li> <li>• Restore Systemstate</li> </ul> <p> <b>Sistemas operativos Windows</b> Copia de seguridad adaptable de subarchivos</p> <p> <b>Sistemas operativos Windows</b> Se han dejado de mantener las operaciones de copia de seguridad adaptable de subarchivos, pero aún puede restaurar datos de copia de seguridad de subarchivos existentes.</p> <p>Cifrado de datos DES (Data Encryption Standard) de 56 bits</p> <p>Para aumentar la seguridad, utilice el cifrado de datos AES (Advanced Encryption Standard) de 128 bits o 256 bits para las operaciones de copia de seguridad y archivado.</p> <p>Para obtener más información, consulte Encryptiontype.</p> <p> <b>Sistemas operativos Windows</b> El soporte GPFS para el cliente Windows</p> <p> <b>Sistemas operativos Windows</b> El cliente de archivado y copia de seguridad de Windows ya no puede realizar copias de seguridad de archivos, ni restaurarlos, en un clúster GPFS solo Windows. Sin embargo, aún puede utilizar el cliente de archivado y copia de seguridad de AIX o Linux para proteger datos en clústeres GPFS que contengan nodos mixtos, que pueden ser de AIX, Linux y Windows.</p> <p>Plug-in de Data Protection for IBM Domino</p> <p>El plug-in de Data Protection for IBM Domino se ha estabilizado en la V7.1.0 y ya no es compatible con el cliente de archivado y copia de seguridad. Si se ha instalado y configurado el plug-in de Data Protection for IBM Domino en el mismo servidor que IBM Domino Server y el cliente de archivado y copia de seguridad V8.1, ya no podrá realizar procesos de copia de seguridad o restauración de bases de datos y archivos de registro de transacciones de IBM Domino con el cliente web.</p> <p>La opción guitreeviewafterbackup</p> <p>La opción guitreeviewafterbackup ya no se admite en este release y se ha eliminado del editor de preferencias. Si esta opción está presente en el archivo de opciones de cliente cuando se ejecuta el cliente, la opción se omite y no se visualiza ningún mensaje de error.</p> <p>Soporte suspendido para los sistemas operativos de cliente</p> <p>Para aprovechar las nuevas características del producto, instale la versión 8.1 del cliente de archivado y copia de seguridad en uno de los sistemas operativos compatibles. Para ver la lista actualizada de sistemas operativos compatibles, consulte la nota técnica 1243309.</p> <p>Los sistemas operativos siguientes ya no son compatibles con el cliente de archivado y copia de seguridad:</p> <ul style="list-style-type: none"> <li>• Sistemas operativos Windows de 32 bits (cliente y API).</li> <li>• Sistemas operativos Windows Server 2008, Windows Server 2008 R2, Windows 7 y Windows 8.</li> <li>• Sistemas operativos HP-UX. Aún puede utilizar la API de IBM Spectrum Protect en un sistema operativo HP-UX.</li> <li>• Linux on Power Systems (big endian). Aún puede utilizar la API de IBM Spectrum Protect en Linux on Power Systems (big endian).</li> <li>• Sistemas operativos Solaris SPARC. Todavía puede utilizar la API de IBM Spectrum Protect en sistemas operativos Solaris SPARC.</li> </ul>

**Información relacionada:**

Protección para estaciones de trabajo y servidores de archivos

## Notas del release para IBM Spectrum Protect Backup-Archive Client Versión 8.1

Ya está disponible IBM Spectrum Protect Backup-Archive Client V8.1. Lea este documento para obtener información importante sobre la instalación. También puede obtener información sobre actualizaciones de producto, problemas de compatibilidad limitaciones y problemas conocidos.

### Contenido



- Descripción
- Anuncio
- Compatibilidad con versiones anteriores
- Requisitos del sistema
- Instalación del cliente de copia de seguridad/archivado
- Actualizaciones, limitaciones y problemas conocidos

## Descripción

---

IBM Spectrum Protect es un producto de cliente/servidor con licencia que proporciona servicios de gestión de almacenamiento en un entorno de sistemas multiplataforma. El cliente de archivado y copia de seguridad se puede utilizar para realizar copias de seguridad y archivar archivos desde estaciones de trabajo o servidores de archivos a almacenamiento y para restaurar y recuperar versiones de copias de seguridad y copias archivadas de archivos a estaciones de trabajo locales.

Para obtener una lista de los APAR arreglados en esta versión, consulte la nota técnica 1993247.

## Anuncio

---

El anuncio de la familia de productos de IBM Spectrum Protect V8.1 incluye la información siguiente:

- Descripción detallada del producto, incluida una descripción de las funciones nuevas
- Declaración de posicionamiento del producto
- Detalles sobre pedidos y embalajes
- Información sobre compatibilidad internacional

Para buscar el anuncio del producto, siga estos pasos:

1. Vaya al sitio web del anuncio del producto.
2. En el campo Search for, escriba el identificador del producto (PID) para su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Information Type, seleccione Announcement letters y pulse en Search.
4. En la lista Search in, seleccione Product Number.
5. Opcional: En el panel Refine Your Search en la parte izquierda de la ventana, seleccione el país en el que reside.
6. En la sección Sort by, seleccione Newest first.

## Compatibilidad con versiones anteriores

---

For compatibility with earlier versions, see IBM Spectrum Protect Server/Client Compatibility and Upgrade Considerations.

## Requisitos del sistema

---

Para obtener información sobre sobre la compatibilidad con el hardware y el software, consulte el documento de requisitos detallados del sistema en los sitios web siguientes:

Requisitos de clientes Apple Macintosh

Nota técnica 1053584

IBM® AIX requisitos de clientes

Nota técnica 1052226

Requisitos del cliente de Linux on Power Systems

Nota técnica 1169963

Requisitos de clientes Linux x86\_64

Nota técnica 1052223

Requisitos del cliente de Linux on z Systems

Nota técnica 1066436

Requisitos de clientes de Microsoft Windows

Nota técnica 1197133

Requisitos del cliente de Oracle Solaris x86\_64

Nota técnica 1232956

## Instalación del cliente de copia de seguridad/archivado

---

Si descarga el producto desde IBM Passport Advantage, siga las indicaciones del documento de descarga en la nota técnica 4042940.

Para obtener instrucciones de instalación, consulte el apartado Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows).

## Actualizaciones, limitaciones y problemas conocidos

---

Las actualizaciones de documentación, limitaciones y problemas conocidos se documentan como notas técnicas en la base de conocimiento de soporte en IBM Support Portal for IBM Spectrum Protect. IBM Software Support actualiza las bases de datos de conocimientos a medida que se detectan y resuelven problemas. Buscando en esta base de datos podrá encontrar métodos alternativos o soluciones para los problemas.

### Limitaciones y problemas conocidos

En el momento de la publicación, las limitaciones y los problemas conocidos se documentan en las siguientes notas técnicas:

- En el caso de sistemas operativos AIX, Linux, Mac OS X y Oracle Solaris, consulte la nota técnica 1993251.
- En el caso de sistemas operativos Windows, consulte la nota técnica 1993250.

### Actualizaciones de la documentación

Para obtener información que no estaba disponible en el momento de la publicación, hay disponibles actualizaciones de la documentación en las notas técnicas siguientes:

- En el caso de sistemas operativos AIX, Linux, Mac OS X y Oracle Solaris, consulte la nota técnica 7048955.
- En el caso de sistemas operativos Windows, consulte la nota técnica 7048956.

## Archivos léame para los fixpacks del cliente de archivado y copia de seguridad de IBM Spectrum Protect Versión 8.1

---

Los archivos léame para los fixpacks del cliente de archivado y copia de seguridad de IBM Spectrum Protect V8.1 están disponibles en la base de conocimiento de soporte cuando hay una actualización del fix pack.

Ver archivos léame del fixpack del cliente de archivado y copia de seguridad de IBM Spectrum Protect V8.1

## Últimas actualizaciones de la documentación

---

Se pueden realizar actualizaciones de la documentación del cliente de archivado y copia de seguridad de IBM Spectrum Protect tras la publicación de la documentación en IBM® Knowledge Center.

Las últimas actualizaciones de la documentación están disponibles en los siguientes documentos en el Portal de soporte de IBM:

- Para los clientes AIX, Linux, Mac OS X y Oracle Solaris, consulte la Nota técnica 7048955.
- Para los clientes Windows, consulte la Nota técnica 7048956.

## Protección para estaciones de trabajo y servidores de archivos




---

IBM Spectrum Protect es un producto de cliente/servidor con licencia que proporciona servicios de gestión de almacenamiento en un entorno de sistemas multiplataforma.

El programa cliente de archivado y copia de seguridad permite a los usuarios realizar copias de seguridad de archivos o archivarlos desde las estaciones de trabajo o servidores de archivos y restaurar y recuperar versiones de copia de seguridad y copias archivadas de archivos en las estaciones de trabajo locales.




Además del cliente de copia de seguridad/archivado, IBM Spectrum Protect incluye los siguientes componentes:




- Un programa de servidor que actúa como servidor de archivado y copia de seguridad para las estaciones de trabajo distribuidas y los servidores de archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El programa servidor también proporciona servicios de gestión de almacenamiento jerárquico (HSM), y permite que los sistemas actúen como un servidor de migración.





- Un programa del cliente administrativo que puede acceder desde un navegador web o desde una línea de mandatos. El programa permite que el administrador de IBM Spectrum Protect controle y supervise las actividades del servidor, defina políticas de gestión de almacenamiento para servicios de gestión de espacio, copias de seguridad y archivado, y establezca planificaciones para ejecutar dichos servicios en intervalos regulares.
- Una interfaz de programas de aplicación (API) que puede utilizar para mejorar una aplicación existente con los servicios de gestión de almacenamiento. Cuando se inscribe una aplicación con un servidor como nodo cliente, la aplicación puede realizar copias de seguridad, restaurar, archivar y recuperar objetos del almacenamiento.


- Un cliente de archivado y copia de seguridad que permite que un administrador autorizado, el personal de help desk y otros usuarios lleven a cabo copias de seguridad, restauración archivado y servicios de recuperación utilizando un navegador web en un sistema remoto.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los programas de cliente de IBM Spectrum Protect for Space Management e IBM Spectrum Protect HSM for Windows están asociados a IBM Spectrum Protect, pero se venden por separado. Estos productos migran automáticamente los archivos elegibles al almacenamiento para conservar niveles de espacio libre en los sistemas de archivos locales y recuperan los archivos migrados cuando se accede a éstos. Además, permite a los usuarios migrar y recuperar archivos específicos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los términos *gestión de almacenamiento jerárquico* y *gestión del espacio* tienen el mismo significado en esta publicación.

#### Conceptos relacionados:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Planificación de las copias de seguridad

 Sistemas operativos Windows Planificación de las copias de seguridad (Windows)

Actualizaciones del cliente de archivado y copia de seguridad

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

#### Tareas relacionadas:

Configuración de clientes de copia de seguridad/archivado

Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad

Archivar y recuperar datos con clientes de archivado y copia de seguridad

 Sistemas operativos AIX  sistemas operativos Mac OS X  Sistemas operativos Linux  Sistemas operativos Oracle Solaris





 Sistemas operativos Windows

## Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

El cliente de archivado y copia de seguridad de IBM Spectrum Protect le ayuda a proteger la información de las estaciones de trabajo.

Puede conservar versiones de copia de seguridad de los archivos que puede restaurar si los archivos originales se pierden o resultan dañados. También puede archivar archivos usados con poca frecuencia, mantenerlos en su estado actual y recuperarlos cuando los necesite.





El cliente de copia de seguridad y archivado funciona conjuntamente con el servidor de IBM Spectrum Protect. Póngase en contacto con el administrador del servidor de IBM Spectrum Protect para obtener acceso a las copias de seguridad y copias archivadas en el servidor o consulte las publicaciones del servidor para obtener información sobre la instalación y configuración del servidor de IBM Spectrum Protect.

- Actualización del cliente de archivado y copia de seguridad  
En los siguientes apartados se explica qué debe hacer si desea realizar una actualización a la versión 8.1.2 del cliente de archivado y copia de seguridad de IBM Spectrum Protect desde una versión anterior.
- Requisitos del entorno del cliente  
Cada uno de los clientes de IBM Spectrum Protect tiene requisitos de hardware y software.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Requisitos de soporte para NDMP (sólo Extended Edition)  
Utilice el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad y restaurar sistemas de archivos NAS en bibliotecas o unidades de cintas que están conectadas localmente a los servidores de archivos NAS de Network Appliance y EMC Celerra.
-  Sistemas operativos Linux  Sistemas operativos Windows Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack  
Antes de poder realizar una copia de seguridad o archivado de los datos del cliente de FastBack, tiene que instalar el software necesario.
-  Sistemas operativos Windows Asistente para la configuración del cliente para Tivoli Storage Manager FastBack  
El cliente de archivado y copia de seguridad proporciona un asistente para configurar el cliente de archivado y copia de seguridad de Tivoli Storage Manager FastBack.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Instalar los clientes de archivado y copia de seguridad UNIX y Linux  
En este apartado se proporcionan instrucciones para instalar y configurar clientes de IBM Spectrum Protect UNIX y Linux.
-  Sistemas operativos Windows Visión general de la instalación del cliente de copia de seguridad y archivado de Windows  
Puede instalar el cliente de archivado y copia de seguridad IBM Spectrum Protect de Windows desde el soporte de instalación.
-  Sistemas operativos Linux  Sistemas operativos Windows Instalación del servicio de gestión de cliente para recopilar información de diagnóstico


Puede instalar los servicios de gestión de clientes de IBM Spectrum Protect para recopilar información de diagnóstico sobre el cliente de archivado y copia de seguridad. El servicio de gestión de cliente hace que la información esté disponible para IBM Spectrum Protect Operations Center, para poder realizar una supervisión básica.

#### Conceptos relacionados:

Actualizaciones del cliente de archivado y copia de seguridad

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

Planificación de las copias de seguridad

 Sistemas operativos Windows Planificación de las copias de seguridad (Windows)

#### Tareas relacionadas:

Configuración de clientes de copia de seguridad/archivado

Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad

Archivar y recuperar datos con clientes de archivado y copia de seguridad

## Actualización del cliente de archivado y copia de seguridad

---

En los siguientes apartados se explica qué debe hacer si desea realizar una actualización a la versión 8.1.2 del cliente de archivado y copia de seguridad de IBM Spectrum Protect desde una versión anterior.


- **Actualización de la vía de acceso para clientes y servidores**  
Los clientes y los servidores de IBM Spectrum Protect se pueden actualizar en momentos diferentes. La combinación de servidores y clientes que despliega debe ser compatible.
- **Información adicional sobre la actualización**  
Cuando actualiza un cliente de copia de seguridad y archivado, hay información adicional que debe tenerse en cuenta antes de utilizar el nuevo software de cliente.
- **Despliegue automático del cliente de copia de seguridad y archivado**  
El administrador del servidor de IBM Spectrum Protect puede desplegar de forma automática un cliente de archivado y copia de seguridad para las estaciones de trabajo que ya tienen instalado el cliente de archivado y copia de seguridad.

## Actualización de la vía de acceso para clientes y servidores

---

Los clientes y los servidores de IBM Spectrum Protect se pueden actualizar en momentos diferentes. La combinación de servidores y clientes que despliega debe ser compatible.

Para evitar interrupciones de las actividades de archivado y copia de seguridad mientras actualiza de un release a otro, siga las directrices de compatibilidad para los clientes y servidores de IBM Spectrum Protect en la nota técnica 1053218.




 Sistemas operativos AIX Para obtener información sobre cómo actualizar las configuraciones de AIX IBM® PowerHA SystemMirror, consulte Migración de configuraciones de AIX IBM PowerHA SystemMirror antiguas.


## Información adicional sobre la actualización

---

Cuando actualiza un cliente de copia de seguridad y archivado, hay información adicional que debe tenerse en cuenta antes de utilizar el nuevo software de cliente.

Tenga en cuenta la información siguiente al actualizar un cliente de archivado y copia de seguridad:

-  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si está actualizando desde el cliente de archivado y copia de seguridad de IBM® Tivoli Storage Manager Versión 7.1.2 o anterior en el sistema operativo Oracle Solaris, tiene que desinstalar los paquetes de idioma previamente instalados para poder continuar con la actualización.
-  Sistemas operativos Mac OS X Para usuarios de Mac, las actualizaciones realizadas en el cliente de Mac OS X contenidas en IBM Spectrum Protect V6.3 o versiones más nuevas, requieren que tenga en cuenta los siguientes artículos:
  - Cuando utilice el cliente de Mac OS X que se proporciona en esta versión, asegúrese de que los archivos `dsm.sys` y `dsm.opt` se codifican mediante Unicode (UTF-8). La codificación UTF-8 permite el uso de caracteres de cualquier idioma en los archivos de opciones. Si los archivos `dsm.sys` o `dsm.opt` se codificaron anteriormente como MacRoman (o cualquier otro distinto a UTF-8), ábralos en un editor como TextEdit y guárdelos con la codificación UTF-8, y sin la extensión `.txt`. Las listas `include-exclude` se pueden codificar bien como UTF-8 o UTF-16. Para obtener más información sobre el uso de Unicode, consulte Consideraciones sobre los clientes habilitados para Unicode.
  - Los espacios de archivos del servidor de IBM Spectrum Protect que se crearon mediante clientes de Mac OS 9 no se pueden gestionar mediante el cliente de Mac OS X que se proporcionó en IBM Spectrum Protect V6.3. Utilice `q file nodo f=d` en el servidor para listar archivos almacenados para un nodo. Los archivos de plataforma Mac que no empiezan por una barra inclinada (/) los ha creado probablemente un cliente Mac más antiguo. No puede restaurar ni gestionar estos archivos mediante el cliente de Mac OS X que se proporciona en esta versión. Puede gestionar estos archivos, pero tiene que utilizar un cliente de Mac que esté instalado en un nodo de cliente de la versión 6.2.2 o anterior.

-  Sistemas operativos Windows El tamaño del búfer para guardar las notificaciones que cambian para un sistema de archivos diario particular (DirNotifyBufferSize) ha cambiado. El valor predeterminado es 16 KB.
- Para obtener una lista de mensajes nuevos y cambiados desde la versión anterior de IBM Spectrum Protect, consulte el archivo client\_message.chg en el paquete del clúster.

## Despliegue automático del cliente de copia de seguridad y archivado

---

El administrador del servidor de IBM Spectrum Protect puede desplegar de forma automática un cliente de archivado y copia de seguridad para las estaciones de trabajo que ya tienen instalado el cliente de archivado y copia de seguridad.

El servidor de IBM Spectrum Protect se puede configurar para actualizar automáticamente los clientes de archivado y copia de seguridad en las estaciones de trabajo de cliente. Los clientes de archivado y copia de seguridad existentes debe ser de la versión 6.4.3 o posterior.

Para obtener más información sobre cómo desplegar automáticamente actualizaciones de cliente desde el servidor, consulte los documentos siguientes:

- Para servidores de IBM Spectrum Protect 8.1.2 o posteriores, consulte la Nota técnica 2004596.
- Para los servidores de IBM® Tivoli Storage Manager V7.1 y los servidores de IBM Spectrum Protect V8.1.0 y V8.1.1, consulte la Nota técnica 1673299.

Restricciones: Se aplican las restricciones siguientes al despliegue automático de cliente:

- El entorno de servicios en clúster de Windows no está admitido.
- El cliente de archivado y copia de seguridad únicamente se puede desplegar desde el servidor de IBM Spectrum Protect. Otros productos relacionados como IBM Spectrum Protect for Space Management, IBM Spectrum Protect HSM for Windows, IBM Spectrum Protect for Virtual Environments y otros productos de Data Protection no están soportados. Si se intenta un despliegue de un producto no soportado, el proceso de despliegue se detiene con un mensaje de error.
- No planifique despliegues de cliente automáticos en estaciones de trabajo que ya tengan una aplicación de IBM Spectrum Protect for ERP instalada.

Cuando el administrador del servidor planifica despliegues automáticos de cliente de archivado y copia de seguridad, los paquetes del cliente actualizados (que incluyen los componentes del cliente y la biblioteca de API) se instalan en las estaciones de trabajo que los reciben. El programa de instalación del cliente realiza una comprobación de dependencias para asegurarse de que la biblioteca API no entra en conflicto con el paquete del cliente instalado actualmente.

Las aplicaciones de IBM Spectrum Protect for ERP no utilizan la misma tecnología de instalación que el programa de instalación del cliente. Por lo tanto, la comprobación de dependencias de la instalación del cliente no detecta si la biblioteca de API que utilizan las aplicaciones de IBM Spectrum Protect for ERP es compatible con la biblioteca de API que instalarán los despliegues automáticos del cliente. Si un paquete de cliente se despliega e instala automáticamente en una estación de trabajo, la biblioteca API instalada podría no ser compatible con la biblioteca API que haya sido instalada por la aplicación de IBM Spectrum Protect for ERP. La biblioteca de API recién desplegada puede hacer que fallen las aplicaciones de IBM Spectrum Protect for ERP.

## Cómo la opción autodeploy del cliente puede afectar al despliegue del cliente

---

Puede utilizar la opción autodeploy para habilitar condicionalmente el despliegue automático del cliente, si el despliegue no necesita un reinicio de la estación de trabajo del cliente.

La opción autodeploy está habilitada de forma predeterminada y la estación de trabajo cliente se reinicia en caso necesario.

Para utilizar el despliegue automático pero no reiniciar el sistema, especifique la opción autodeploy noreboot.

Para desactivar el despliegue automático del cliente, añada autodeploy no al archivo de opciones del cliente.

Puede establecer la opción autodeploy en las ubicaciones siguientes:

- En una definición de planificación en el servidor de IBM Spectrum Protect. Las definiciones de planificación que despliegan las actualizaciones de software del cliente tienen una sentencia `action=deploy`. En esas planificaciones, puede incluir la opción autodeploy como parte del mandato que incluye en la sentencia `-postnschedulecmd`.
- En el nodo del cliente, en un archivo de opciones asociado con el planificador del cliente o el aceptador de cliente. El gestor de despliegue detecta los archivos de opciones que están asociados con el planificador o el aceptador de cliente. Si hay varios procesos de planificadores o de aceptador de cliente en ejecución simultáneamente en la misma máquina y los procesos utilizan distintos archivos de opciones, el gestor de despliegue utiliza el valor de la opción autodeploy establecido en uno de los archivos de opciones.
- En el cliente, en el archivo de opciones del cliente (dsm.opt). La opción autodeploy que se define en el archivo de opciones del cliente sustituye a cualquier otro ajuste de autodeploy.

**Referencia relacionada:**  
Autodeploy








## Requisitos del entorno del cliente

---





Cada uno de los clientes de IBM Spectrum Protect tiene requisitos de hardware y software.

En la lista siguiente se muestra la ubicación de los requisitos previos de entorno para cada plataforma admitida.

Para obtener la información actual sobre los requisitos previos de entorno de cliente para todas las plataformas de cliente de copia de seguridad y archivado admitidas, consulte la nota técnica 1243309.

-  **Sistemas operativos AIX**Entorno del cliente AIX  
Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para la plataforma AIX.
- Entorno de la API de HP-UX Itanium 2  
Revise la información sobre el entorno de la API, los componentes instalables y los requisitos de hardware y software de la plataforma de HP-UX Itanium 2.
-  **Sistemas operativos Linux**Entorno de clientes de Linux on Power Systems  
Esta sección contiene información de entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para las plataformas de cliente de Linux on Power Systems.
-  **Sistemas operativos Linux**Entorno de cliente Linux x86\_64  
Esta sección contiene información sobre el entorno del cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para Linux on Intel (Linux x86\_64) .
-  **Sistemas operativos Linux**Entorno de cliente Linux on System z  
Esta sección contiene información sobre el entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y de software para la plataforma Linux on System z.
-  **sistemas operativos Mac OS X**Entorno del cliente Mac OS X  
Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para el cliente de Mac OS X .
-  **Sistemas operativos Oracle Solaris**Entorno de cliente Oracle Solaris  
Revise la información sobre el entorno de cliente, los componentes de cliente y los requisitos de hardware y software para la plataforma Oracle Solaris.
-  **Sistemas operativos Windows**Requisitos del entorno de cliente Windows  
Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software de las plataformas Windows admitidas.





### Conceptos relacionados:


 **Sistemas operativos AIX**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Windows**Requisitos de soporte para NDMP (sólo Extended Edition)  
 **Sistemas operativos AIX**

## Entorno del cliente AIX

---

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para la plataforma AIX.

-  **Sistemas operativos AIX**Componentes instalables del cliente AIX  
El cliente de archivado y copia de seguridad consta de varios componentes instalables.
-  **Sistemas operativos AIX**Requisitos de sistema para el cliente de AIX  
Los clientes de IBM Spectrum Protect AIX requieren un mínimo de hardware, espacio de disco, memoria y software.
-  **Sistemas operativos AIX**Métodos de comunicación del cliente AIX  
Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad AIX.
-  **Sistemas operativos AIX**Funciones de cliente de archivado y copia de seguridad disponibles en AIX  
En esta lista se muestran las funciones admitidas en AIX.

 **Sistemas operativos AIX**

## Componentes instalables del cliente AIX


---

El cliente de archivado y copia de seguridad consta de varios componentes instalables.

Los componentes instalables para el cliente AIX son los siguientes:

- Cliente de línea de mandatos de copia de seguridad/archivado
- Cliente de administración
- Interfaz gráfica de usuario de cliente de archivado y copia de seguridad, que utiliza tecnología Oracle Java™
- Cliente web de archivado y copia de seguridad
- API de 64 bits de IBM Spectrum Protect

La API se puede instalar de forma separada. Los demás componentes se instalan todos cuando se instala el paquete AIX (tivoli.tsm.client.api.64bit).

 Sistemas operativos AIX

## Requisitos de sistema para el cliente de AIX

Los clientes de IBM Spectrum Protect AIX requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones admitidas de los clientes de AIX, incluidos los fixpacks más recientes, consulte la nota técnica 1052226.

 Sistemas operativos AIX


## Métodos de comunicación del cliente AIX

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad AIX.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.2 AIX:

Tabla 1. Métodos de comunicación del cliente AIX

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con plataformas AIX admitidas)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con plataformas AIX admitidas)	AIX

 Sistemas operativos AIX

## Funciones de cliente de archivado y copia de seguridad disponibles en AIX

En esta lista se muestran las funciones admitidas en AIX.

Tabla 1. Funciones admitidas en AIX

Funciones	¿Admitidas en AIX?
Línea de mandatos y GUI de copia de seguridad y archivado	sí
Copia de seguridad con registro por diario	sí
Operaciones fuera de la LAN	sí
Copia de seguridad de imagen activada	sí
Copia de seguridad de imagen fuera de línea	sí

## Entorno de la API de HP-UX Itanium 2

Revise la información sobre el entorno de la API, los componentes instalables y los requisitos de hardware y software de la plataforma de HP-UX Itanium 2.

- Componente instalable de la API de HP-UX Itanium 2  
Solo puede instalar la API de HP-UX Itanium 2 en IBM Spectrum Protect versión 8.1.2.
- Requisitos del sistema para la API de HP-UX Itanium 2  
La API de HP-UX Itanium 2 de IBM Spectrum Protect requiere un mínimo de hardware, espacio de disco, memoria y software.
- Métodos de comunicación de la API de HP-UX Itanium 2  
Los métodos de comunicación de memoria compartida y TCP/IP están disponibles para la API de HP-UX Itanium 2.

## Componente instalable de la API de HP-UX Itanium 2

Solo puede instalar la API de HP-UX Itanium 2 en IBM Spectrum Protect versión 8.1.2.

## Requisitos del sistema para la API de HP-UX Itanium 2

La API de HP-UX Itanium 2 de IBM Spectrum Protect requiere un mínimo de hardware, espacio de disco, memoria y software.


Para conocer los requisitos de software y hardware de todas las versiones soportadas de la API de HP-UX Itanium 2, incluidos los fixpacks más recientes, consulte la nota técnica 1197146.

## Métodos de comunicación de la API de HP-UX Itanium 2

Los métodos de comunicación de memoria compartida y TCP/IP están disponibles para la API de HP-UX Itanium 2.




Tabla 1. Métodos de comunicación de la API de HP-UX Itanium 2

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con HP-UX)	AIX, Linux, Windows

 Sistemas operativos Linux

## Entorno de clientes de Linux on Power Systems

Esta sección contiene información de entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para las plataformas de cliente de Linux on Power Systems.

-  Sistemas operativos Linux Componentes instalables de cliente de Linux on Power Systems  
La línea de mandatos del cliente de copia de seguridad y archivado, la GUI de Java™, el archivado y copia de seguridad web y la API constan de los componentes instalables de cliente de archivado y copia de seguridad de Linux on Power Systems.
-  Sistemas operativos Linux Requisitos de sistema para clientes en Linux en Power Systems  
Los clientes de IBM Spectrum Protect en Linux en Power Systems necesitan una cantidad mínima de hardware, espacio de disco, memoria y software.
-  Sistemas operativos Linux Métodos de comunicación de cliente de Linux on Power Systems  
Los clientes de archivado y copia de seguridad en Linux on Power Systems pueden utilizar TCP/IP o la memoria compartida como método de comunicaciones para las comunicaciones de cliente-servidor.

 Sistemas operativos Linux

## Componentes instalables de cliente de Linux on Power Systems

La línea de mandatos del cliente de copia de seguridad y archivado, la GUI de Java™, el archivado y copia de seguridad web y la API constan de los componentes instalables de cliente de archivado y copia de seguridad de Linux on Power Systems.

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.2:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API (64 bits) de IBM Spectrum Protect

 Sistemas operativos Linux

## Requisitos de sistema para clientes en Linux en Power Systems

Los clientes de IBM Spectrum Protect Linux en Power Systems necesitan una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes de en Linux en Power Systems, incluidos los fixpacks más recientes, consulte nota técnica 1169963.



## Métodos de comunicación de cliente de Linux on Power Systems

Los clientes de archivado y copia de seguridad en Linux on Power Systems pueden utilizar TCP/IP o la memoria compartida como método de comunicaciones para las comunicaciones de cliente-servidor.




Tabla 1 lista los métodos de comunicaciones de cliente de Linux on Power Systems disponibles y los sistemas operativos de servidor de IBM Spectrum Protect con los que los puede utilizar.

Tabla 1. Métodos de comunicación de cliente de Linux on Power Systems

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux en Power Systems

## Entorno de cliente Linux x86\_64

Esta sección contiene información sobre el entorno del cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y software para Linux on Intel (Linux x86\_64).

-  **Componentes instalables del cliente Linux x86\_64**  
La línea de mandatos del cliente de copia de seguridad y archivado, la GUI de Java™, el archivado y copia de seguridad web, el cliente de administración y la API son los componentes instalables del cliente de copia de seguridad y archivado de Linux on Intel (Linux x86\_64).
-  **Requisitos de sistema para clientes Linux x86\_64**  
Los clientes IBM Spectrum Protect Linux x86\_64 requieren un mínimo de hardware, espacio de disco, memoria y software.
-  **Métodos de comunicación del cliente Linux x86\_64**  
Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad de Linux on Intel (Linux x86\_64).

## Componentes instalables del cliente Linux x86\_64

La línea de mandatos del cliente de copia de seguridad y archivado, la GUI de Java™, el archivado y copia de seguridad web, el cliente de administración y la API son los componentes instalables del cliente de copia de seguridad y archivado de Linux on Intel (Linux x86\_64).

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.2:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

## Requisitos de sistema para clientes Linux x86\_64

Los clientes IBM Spectrum Protect Linux x86\_64 requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes de Linux x86\_64, incluidos los fixpacks más recientes, consulte la nota técnica 1052223.


## Métodos de comunicación del cliente Linux x86\_64

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad de Linux on Intel (Linux x86\_64).

Puede utilizar los siguientes métodos de comunicación con el cliente de IBM Spectrum Protect versión 8.1.2 Linux en Intel (Linux x86\_64)




Tabla 1. Métodos de comunicación del cliente Linux on Intel x86\_64

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux x86_64

 Sistemas operativos Linux

## Entorno de cliente Linux on System z

Esta sección contiene información sobre el entorno de cliente, los componentes del cliente de copia de seguridad y archivado y los requisitos de hardware y de software para la plataforma Linux on System z.

-  **Sistemas operativos Linux** Componentes instalables del cliente Linux on System z  
La línea de mandatos del cliente de copia de seguridad y archivado, el cliente administrativo, el cliente de archivado y copia de seguridad web y la API son los componentes instalables del cliente de archivado y copia de seguridad de Linux on System z.
-  **Sistemas operativos Linux** Requisitos de sistema para clientes Linux on System z  
Los clientes de IBM Spectrum Protect Linux System z requieren una cantidad mínima de hardware, espacio de disco, memoria y software.
-  **Sistemas operativos Linux** Métodos de comunicación del cliente Linux on System z  
Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Linux on System z.

 Sistemas operativos Linux

## Componentes instalables del cliente Linux on System z

La línea de mandatos del cliente de copia de seguridad y archivado, el cliente administrativo, el cliente de archivado y copia de seguridad web y la API son los componentes instalables del cliente de archivado y copia de seguridad de Linux on System z.

Puede instalar los siguientes componentes con IBM Spectrum Protect Versión 8.1.2:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

 Sistemas operativos Linux

## Requisitos de sistema para clientes Linux on System z

Los clientes de IBM Spectrum Protect Linux System z requieren una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de hardware y software para todas las versiones soportadas de los clientes de Linux System z, incluidos los fixpacks más recientes, consulte la nota técnica 1066436.

 Sistemas operativos Linux


## Métodos de comunicación del cliente Linux on System z

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Linux on System z.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.2 Linux en System z:




Tabla 1. Métodos de comunicación del cliente Linux on System z


Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Linux)	AIX, Linux, Windows
Memoria compartida	TCP/IP (estándar con Linux)	Linux on System z

 sistemas operativos Mac OS X

## Entorno del cliente Mac OS X

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software para el cliente de Mac OS X.

-  sistemas operativos Mac OS X Componentes instalables del cliente Mac OS X  
 La línea de mandatos del cliente de copia de seguridad y archivado, la GUI Java™, el archivado y copia de seguridad web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad Mac OS X.
-  sistemas operativos Mac OS X Requisitos de sistema para clientes Mac OS X  
 Los clientes Mac OS X de IBM Spectrum Protect requieren un mínimo de hardware, espacio de disco, memoria y software.
-  sistemas operativos Mac OS X Métodos de comunicación del cliente Mac OS X  
 Existen métodos de comunicación TCP/IP para el cliente de archivado y copia de seguridad Mac OS X.

 sistemas operativos Mac OS X

## Componentes instalables del cliente Mac OS X


La línea de mandatos del cliente de copia de seguridad y archivado, la GUI Java™, el archivado y copia de seguridad web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad Mac OS X.

Los componentes siguientes se instalan con IBM Spectrum Protect Versión 8.1.2:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado

Consejo: El archivo de script de shell `dsmj` para la GUI Java está instalado en la siguiente ubicación:


```
/Library/Application Support/tivoli/tsm/client/ba/bin
```

 sistemas operativos Mac OS X

## Requisitos de sistema para clientes Mac OS X

Los clientes Mac OS X de IBM Spectrum Protect requieren un mínimo de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de software y hardware para todas las versiones soportadas de los clientes Mac OS X, incluidos los fixpacks más recientes, consulte la nota técnica 1053584.

 sistemas operativos Mac OS X

## Métodos de comunicación del cliente Mac OS X

Existen métodos de comunicación TCP/IP para el cliente de archivado y copia de seguridad Mac OS X.

Utilice los siguientes métodos de comunicación con el cliente IBM Spectrum Protect Versión 8.1.2 Mac OS X:

Tabla 1. Métodos de comunicación del cliente Mac OS X




Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Mac OS X)	AIX, Linux, Windows

## Entorno de cliente Oracle Solaris

---

Revise la información sobre el entorno de cliente, los componentes de cliente y los requisitos de hardware y software para la plataforma Oracle Solaris.

A partir de IBM Spectrum Protect Versión 8.1.0, el cliente de archivado y copia de seguridad de Oracle Solaris está disponible sólo en la plataforma Oracle Solaris x86\_64. La API de Oracle Solaris está disponible en las plataformas Oracle Solaris x86\_64 y Oracle Solaris SPARC.

-  **Sistemas operativos Oracle Solaris**Componentes instalables del cliente Oracle Solaris  
La línea de mandatos de IBM Spectrum Protect, la GUI Java™, la copia de seguridad y archivado web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad de Solaris.
-  **Sistemas operativos Oracle Solaris**Requisitos de sistema para clientes Oracle Solaris  
Los clientes Oracle Solaris de IBM Spectrum Protect requieren una cantidad mínima de hardware, espacio de disco, memoria y software.
-  **Sistemas operativos Oracle Solaris**Métodos de comunicación del cliente Oracle Solaris  
Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Oracle Solaris.

## Componentes instalables del cliente Oracle Solaris

---

La línea de mandatos de IBM Spectrum Protect, la GUI Java™, la copia de seguridad y archivado web y la API constituyen los componentes instalables del cliente de archivado y copia de seguridad de Solaris.

Puede instalar los siguientes componentes del cliente en Oracle Solaris x86\_64:

- Cliente de archivado y copia de seguridad
- Cliente de administración
- Interfaz gráfica de usuario (GUI) de Java de copia de seguridad y archivado
- Cliente Web de copia de seguridad/archivado
- API de IBM Spectrum Protect

Puede instalar la API de IBM Spectrum Protect en Oracle Solaris SPARC.

## Requisitos de sistema para clientes Oracle Solaris

---

Los clientes Oracle Solaris de IBM Spectrum Protect requieren una cantidad mínima de hardware, espacio de disco, memoria y software.

Para conocer los requisitos de hardware y software de todas las versiones soportadas de clientes de IBM Spectrum Protect Oracle Solaris, incluidos los fixpacks más recientes, consulte las siguientes páginas de soporte de IBM®:

- Para conocer los requisitos de cliente de Oracle Solaris x86\_64, consulte la nota técnica 1232956.
- Para conocer los requisitos de la API de Oracle Solaris SPARC, consulte la nota técnica 1052211.

## Métodos de comunicación del cliente Oracle Solaris

---

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Oracle Solaris.






Utilice los siguientes métodos de comunicación con el cliente Oracle Solaris:

Tabla 1. Métodos de comunicación del cliente Oracle Solaris

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con Solaris)	AIX, Linux, Windows

## Requisitos del entorno de cliente Windows

Este apartado contiene información sobre el entorno de cliente, sobre los componentes del cliente de copia de seguridad y archivado y sobre los requisitos de hardware y de software de las plataformas Windows admitidas.

-  **Sistemas operativos Windows Componentes instalables del cliente Windows**  
El cliente de archivado y copia de seguridad consta de varios componentes instalables.
-  **Sistemas operativos Windows Requisitos de sistema para clientes Windows**  
El cliente de copia de seguridad y archivado de Windows necesita una cantidad mínima de espacio de disco para la instalación y un sistema operativo admitido.
-  **Sistemas operativos Windows Métodos de comunicación del cliente Windows**  
Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Windows.
-  **Sistemas operativos Windows Funciones de cliente de archivado y copia de seguridad disponibles en las plataformas de Windows**  
En este tema se muestran las funciones que están admitidas y las que no en las diferentes plataformas de Windows.
-  **Sistemas operativos Windows Sistemas de archivos compatibles con Windows**  
El cliente de archivado y copia de seguridad Windows de IBM Spectrum Protect se admite en diversos sistemas de archivos.

## Componentes instalables del cliente Windows

El cliente de archivado y copia de seguridad consta de varios componentes instalables.

Los componentes instalables para el cliente de copia de seguridad y archivado de Windows son los siguientes:

- Cliente de línea de mandatos de copia de seguridad y archivado
- Cliente de administración
- Interfaz gráfica de usuario de cliente de archivado y copia de seguridad, que utiliza tecnología Oracle Java™
- Cliente web de archivado y copia de seguridad
- API (64 bits) de IBM Spectrum Protect

## Requisitos de sistema para clientes Windows

El cliente de copia de seguridad y archivado de Windows necesita una cantidad mínima de espacio de disco para la instalación y un sistema operativo admitido.

Para conocer los requisitos de software y hardware para todas las versiones admitidas de los clientes de Windows, incluidos los fixpacks más recientes, consulte la nota técnica 1197133.

## Métodos de comunicación del cliente Windows

Existen métodos de comunicación de memoria compartida y TCP/IP para el cliente de archivado y copia de seguridad Windows.

Puede utilizar los siguientes métodos de comunicación con el cliente de copia de seguridad y archivado de Windows:

Tabla 1. Métodos de comunicación del cliente Windows

Para utilizar este método de comunicación:	Instale este software:	Para conectarse a estos servidores de IBM Spectrum Protect:
TCP/IP	TCP/IP (estándar con todas las plataformas Windows)	AIX, Linux, Windows
Named Pipes	Named Pipes (estándar con todas las plataformas Windows admitidas)	Windows
Memoria compartida	TCP/IP (estándar con todas las plataformas Windows admitidas)	Windows


# Funciones de cliente de archivado y copia de seguridad disponibles en las plataformas de Windows

En este tema se muestran las funciones que están admitidas y las que no en las diferentes plataformas de Windows.

Tabla 1 muestra las características soportadas y no soportadas en las diferentes plataformas Windows.

Tabla 1. Funciones admitidas en las plataformas Windows

Funciones	Windows 10	Windows Server 2012 Windows Server 2012 R2 Windows Server 2016
Copia de seguridad con registro por diario	sí	sí
Copia de seguridad de imagen activada	sí	sí
Copia de seguridad de imagen fuera de línea	sí	sí
Soporte de estado del sistema con servicios de duplicación de volúmenes (VSS)	sí	sí
Operaciones fuera de la LAN	sí	sí
Recuperación automática del sistema (ASR)	sí	BIOS: yes UEFI: yes
Soporte de archivos abiertos (OFS)	sí	sí




 Sistemas operativos Windows

## Sistemas de archivos compatibles con Windows

El cliente de archivado y copia de seguridad Windows de IBM Spectrum Protect se admite en diversos sistemas de archivos.

El cliente de archivado y copia de seguridad de Windows admite los siguientes tipos de sistemas de archivos:

- Tabla de asignación de archivos (FAT y FAT32)
- Microsoft New Technology File System (NTFS)
- Microsoft Resilient File System (ReFS). ReFS se introdujo en sistemas de Windows Server 2012.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Requisitos de soporte para NDMP (sólo Extended Edition)

Utilice el protocolo NDMP (Network Data Management Protocol) para realizar copias de seguridad y restaurar sistemas de archivos NAS en bibliotecas o unidades de cintas que están conectadas localmente a los servidores de archivos NAS de Network Appliance y EMC Celerra.

*El soporte de NDMP solo está disponible en IBM Spectrum Protect Extended Edition.*

El soporte para NDMP requiere el hardware y software siguiente:

- IBM Spectrum Protect Edición ampliada
- Unidad de cintas y biblioteca de cintas. Para conocer las combinaciones admitidas, consulte: Información del producto

 Sistemas operativos Linux  Sistemas operativos Windows

## Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack

Antes de poder realizar una copia de seguridad o archivado de los datos del cliente de FastBack, tiene que instalar el software necesario.

Debe instalar el siguiente software:

- Tivoli Storage Manager FastBack Versión 6.1






- Cliente de Tivoli Storage Manager V6.1.3.x (donde x es 1 o superior) o V6.2 o posterior
- Servidor de Tivoli Storage Manager V6.1.3 o superior
- Tivoli Storage Manager Administration Center V6.1.3
  - Solo es necesario si quiere utilizar Tivoli Storage Manager FastBack integrado - administración.

A partir de la versión 7.1, el componente del Centro de administración ya no se distribuye con Tivoli Storage Manager o IBM Spectrum Protect. Los usuarios de FastBack que tengan un Centro de administración de una versión de servidor anterior pueden seguir utilizándolo para crear y modificar planificaciones de FastBack. Si no tiene instalado el Centro de administración, puede descargar la versión anterior de <ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/>. Si no tiene instalado el Centro de administración, tiene que crear y modificar las planificaciones de FastBack en el servidor de IBM Spectrum Protect. Para obtener información sobre la creación de planificaciones en el servidor, consulte la documentación del servidor IBM Spectrum Protect.

El entorno de Tivoli Storage Manager FastBack debe estar en ejecución. Para obtener información sobre cómo instalar y configurar Tivoli Storage Manager FastBack, consulte la información sobre el producto en Tivoli Storage Manager FastBack.

Para obtener información sobre cómo integrar IBM Spectrum Protect y Tivoli Storage Manager FastBack, consulte Integración de Tivoli Storage Manager FastBack y IBM Spectrum Protect.

Podrá instalar el cliente de IBM Spectrum Protect de una de estas maneras:

-  Sistemas operativos Windows Instale el cliente de copia de seguridad y archivado en una estación de trabajo que tenga instalado el servidor de FastBack. En este caso, los requisitos previos son: servidor de FastBack, shell de FastBack y montaje de FastBack.
-  Sistemas operativos Linux Instale el cliente de copia de seguridad y archivado en una estación de trabajo que tenga instalado FastBack Disaster Recovery Hub. En este caso, los requisitos previos son: configuración de FastBack Disaster Recovery Hub y shell de FastBack.
-  Sistemas operativos Windows Instale el cliente de copia de seguridad y archivado en una estación de trabajo que tenga instalado FastBack Disaster Recovery Hub. En este caso, los requisitos previos son: configuración de FastBack Disaster Recovery Hub, shell de FastBack y montaje de FastBack.
-  Sistemas operativos Linux Instale el cliente de copia de seguridad y archivado en una estación de trabajo que no tenga instalado el servidor de FastBack ni FastBack Disaster Recovery Hub. En este caso, el shell de FastBack sigue siendo necesario.
-  Sistemas operativos Windows Instale el cliente de copia de seguridad y archivado en una estación de trabajo que no tenga instalado el servidor de FastBack ni FastBack Disaster Recovery Hub. En este caso, asegúrese de que el shell de FastBack y el montaje de FastBack estén instalados.

#### Conceptos relacionados:

Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

 Sistemas operativos Windows

## Asistente para la configuración del cliente para Tivoli Storage Manager FastBack





---

El cliente de archivado y copia de seguridad proporciona un asistente para configurar el cliente de archivado y copia de seguridad de Tivoli Storage Manager FastBack.

Este asistente se encuentra disponible en una aplicación remota (el cliente web) y en una aplicación local (GUI Java™). El asistente le ayudará a establecer las opciones para enviar datos de cliente de FastBack al servidor de IBM Spectrum Protect de forma programada.

#### Conceptos relacionados:

Configuración del cliente de copia de seguridad y archivado para proteger datos del cliente FastBack

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X


## Instalar los clientes de archivado y copia de seguridad UNIX y Linux

---

En este apartado se proporcionan instrucciones para instalar y configurar clientes de IBM Spectrum Protect UNIX y Linux.

Nota: Debe iniciar la sesión como usuario root para instalar el cliente de copia de seguridad y archivado en una estación de trabajo UNIX o Linux.


Aquí figuran los clientes de UNIX y Linux soportados y la ubicación de las instrucciones de instalación de cada cliente.

-  Sistemas operativos AIX Instalación del cliente AIX  
Puede instalar el cliente de archivado y copia de seguridad de AIX desde el soporte de instalación del producto.

-  **Sistemas operativos AIX** Desinstalación del cliente AIX  
Utilice los siguientes procedimientos para desinstalar el cliente de copia de seguridad y archivado AIX de IBM Spectrum Protect.
- **Instalación de la API de HP-UX Itanium 2**  
Puede instalar la API de HP-UX Itanium 2 desde el soporte de instalación del producto.
- **Desinstalación de la API de HP-UX Itanium 2**  
Puede utilizar los procedimientos siguientes para desinstalar la API de IBM Spectrum Protect HP-UX Itanium 2.
-  **Sistemas operativos Linux** Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)  
Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)  
Puede desinstalar el IBM Spectrum Protect cliente en Linux on Power Systems (Little Endian).
-  **Sistemas operativos Linux** Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)  
Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación del cliente en Ubuntu Linux on Power Systems (Little Endian)  
Puede desinstalar el cliente de copia de seguridad y archivado de IBM Spectrum Protect en Ubuntu Linux on Power Systems (Little Endian).
-  **Sistemas operativos Linux** Instalación de la API en Linux on Power Systems (Big Endian)  
Puede instalar la API de IBM Spectrum Protect desde el soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación de la API en Linux on Power Systems (Big Endian)  
Puede desinstalar la API de IBM Spectrum Protect en IBM Spectrum Protect Linux on Power Systems (Big Endian).
-  **Sistemas operativos Linux** Instalación del cliente Linux x86\_64  
Puede instalar el cliente de archivado y copia de seguridad de Linux x86\_64 desde el soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación del cliente Linux x86\_64  
Utilice el siguiente procedimiento para desinstalar el cliente IBM Spectrum Protect Linux x86\_64.
-  **Sistemas operativos Linux** Instalación del cliente Ubuntu Linux x86\_64  
Puede instalar el cliente de archivado y copia de seguridad de Ubuntu Linux de 64 bits desde el soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación del cliente Ubuntu Linux x86\_64  
Puede utilizar el siguiente procedimiento para desinstalar el cliente de IBM Spectrum Protect Ubuntu Linux de 64 bits.
-  **Sistemas operativos Linux** Instalación del cliente Linux on System z  
Puede instalar el cliente de archivado y copia de seguridad de Linux on System z desde el soporte de instalación del producto.
-  **Sistemas operativos Linux** Desinstalación del cliente de Linux on System z  
Utilice los siguientes procedimientos para desinstalar el cliente de IBM Spectrum Protect Linux on System z.
-  **sistemas operativos Mac OS X** Instalación del cliente Mac OS X  
Puede instalar el cliente de archivado y copia de seguridad Mac OS X de IBM Spectrum Protect desde el soporte de instalación del producto.
-  **sistemas operativos Mac OS X** Desinstalación del cliente Mac OS X  
Puede desinstalar el cliente de IBM Spectrum Protect Mac OS X si ya no lo necesita.
-  **Sistemas operativos Oracle Solaris** Instalación del cliente de Oracle Solaris x86\_64  
Puede instalar el cliente de archivado y copia de seguridad de Oracle Solaris x86\_64 de IBM Spectrum Protect desde el soporte de instalación del producto.
-  **Sistemas operativos Oracle Solaris** Desinstalación del cliente Oracle Solaris x86\_64  
Puede desinstalar todos los paquetes que están relacionados con el cliente Oracle Solaris x86\_64 de IBM Spectrum Protect, incluidos los componentes línea de mandatos, GUI, GUI web y cliente de administración.
-  **Sistemas operativos Oracle Solaris** Instalación de la API de Oracle SPARC  
Puede instalar la API de Oracle Solaris SPARC de IBM Spectrum Protect desde el soporte de instalación del producto.
-  **Sistemas operativos Oracle Solaris** Desinstalación de la API de Oracle Solaris SPARC  
Puede desinstalar todos los paquetes que están relacionados con la API de Oracle Solaris SPARC de IBM Spectrum Protect.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **sistemas operativos Mac OS X**  **Sistemas operativos Oracle Solaris**  
Actualizaciones de software  
Las actualizaciones de software deben estar disponibles periódicamente mediante IBM® para su descarga.

#### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 **Sistemas operativos AIX**

## Instalación del cliente AIX

---

Puede instalar el cliente de archivado y copia de seguridad de AIX desde el soporte de instalación del producto.

### Acerca de esta tarea

---



En IBM Spectrum Protect Versión 8.1.2 se facilita una versión de 64 bits del cliente AIX en las bibliotecas de distribución. No puede actualizar un cliente AIX de 32 bits previamente instalado al nuevo cliente AIX de 64 bits. Si tiene un cliente de 32 bits instalado desde una versión anterior de IBM Spectrum Protect, puede utilizar SMIT para llevar a cabo las siguientes tareas:

1. Desinstale el cliente de 32 bits (tivoli.tsm.client.ba).
2. Desinstale todos los archivos de idioma nacional que se hayan instalado anteriormente.
3. Desinstale la API (tivoli.tsm.client.api.32bit).

A continuación, utilice SMIT para instalar los siguientes paquetes en las bibliotecas de distribución de IBM Spectrum Protect V8.1.2, siguiendo el orden indicado:

1. Instale la API de 64 bits (tivoli.tsm.client.api.64bit).
2. Instale el cliente de 64 bits (tivoli.tsm.client.ba.64bit).

Si ya tiene instalado el cliente IBM Spectrum Protect V6.3 de 64 bits (o más nuevo), puede actualizar el cliente en vez de desinstalarlo y volver a instalarlo.

Si tiene un cliente de 64 bits de una versión anterior de IBM Spectrum Protect instalado (por ejemplo, versión 6.1 o V6.2) debe desinstalar el cliente, los paquetes de idiomas y la API. A continuación, instale la API y el cliente de IBM Spectrum Protect nuevos.

Todos los paquetes necesarios para instalar el cliente se incluyen en el paquete del cliente AIX y se grabarán encima de cualquier aplicación en tiempo de ejecución anterior del sistema durante la instalación. Se requiere el LibC (C Set ++ ) en tiempo de ejecución.

Cuando utilice el mandato installp para instalar este cliente, no cambie los valores de campo predeterminados de las dos opciones siguientes:

- ¿Instalar AUTOMÁTICAMENTE el software de requisito?
- ¿SOBREGABAR las mismas versiones o las más recientes?

La inhabilitación o el cambio de los valores permite a un componente del cliente de nivel inferior instalar sobre un componente de nivel superior instalado actualmente. En tales circunstancias, puede que las llamadas a función entre los componentes de distintos niveles dejen de ser válidas.

Instale los siguientes paquetes. Todos se proporcionan en los medios de instalación. Necesitará la edición ampliada, Extended Edition, para poder utilizar el cliente de NAS.

Los archivos siguientes se listan en orden de dependencia. Por ejemplo, la API depende de Global Security Kit (GSKit). Cuando instale cualquiera de ellos mediante SMIT, puede seleccionarlos (F7) en cualquier orden.

GSKit8.gskcrypt64.ppc.rte y GSKit8.gskssl64.ppc.rte

IBM® GSKit de 64 bits (necesario para la API del cliente de 64 bits).

tivoli.tsm.client.api.64bit

Instala la API de 64 bits.

tivoli.tsm.client.ba.64bit

Instala los siguientes archivos del cliente de 64 bits:

- Cliente de archivado y copia de seguridad de Java™ (GUI)
- Cliente web de archivado y copia de seguridad
- Cliente de copia de seguridad NAS

tivoli.tsm.filepath\_aix

Instala la extensión de kernel de vía de acceso de archivo que es necesaria para la copia de seguridad basada en el diario.

tivoli.tsm.client.jbb.64bit

Instala el componente de copia de seguridad con registro por diario.

Cada paquete se instala en el siguiente directorio de instalación predeterminado:

- Los archivos de copia de seguridad-archivado, de cliente web y de cliente administrativo (dsmadm) de 64 bits se instalan en el directorio /usr/tivoli/tsm/client/ba/bin64.
- Los archivos de la API de 64 bits de IBM Spectrum Protect se instalan en el directorio /usr/tivoli/tsm/client/api/bin64.
- El archivo de opciones del sistema de ejemplo, dsm.sys.smp, se ubica en el directorio de instalación.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.

- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Si está copiando primero los archivos de cliente en un directorio local, el mandato `installp` crea automáticamente un archivo a `.toc`. Para crear manualmente un archivo `.toc`, ejecute `/usr/sbin/inutoc` en el directorio local en el que se ha copiado la imagen de IBM Spectrum Protect. En la línea de mandatos de AIX, escriba:

```
/usr/sbin/inutoc /usr/sys/inst.images
```

Se creará un archivo `.toc` en ese directorio.

## Procedimiento

---

1. Inicie la sesión como el usuario `root`.
2. Monte el volumen desde el que está realizando la instalación.
3. Desde la línea de mandatos de AIX, escriba `smitty install` y pulse Intro.
4. Seleccione Instalar y actualizar software y pulse Intro.
5. Seleccione Instalar y actualizar desde todo el software disponible y pulse Intro.
6. En el indicador `INPUT device/directory for software`, pulse la tecla F4, especifique el directorio que contiene las imágenes de ilustración y pulse Intro.
7. En el indicador `SOFTWARE a instalar`, pulse la tecla F4. Seleccione los juegos de archivos de IBM Spectrum Protect que desee instalar pulsando la tecla F7. Después, pulse la tecla Intro.
8. En el panel Instalar y actualizar desde todo el software disponible, pulse la tecla F4 para cambiar cualquiera de los campos de entrada o bien utilice los campos predeterminados. Pulse Intro dos veces para iniciar la instalación.
9. Cuando finalice la instalación, pulse F10 para salir.

## Resultados

---

Cuando se instalan juegos de archivos, estos se validan automáticamente en el sistema. La versión anterior del software del cliente de copia de seguridad y archivado se sustituye por la versión que acaba de instalarse.

Los archivos del cliente de copia de seguridad y archivado se instalan en el directorio `/usr/tivoli/tsm/client/ba/bin64`. Si traspasa los archivos del cliente a otro directorio, deberá realizar los siguientes pasos:

1. Asegúrese de que no han cambiado los permisos de los archivos instalados.
2. Actualice los vínculos simbólicos para los archivos instalados en los siguientes directorios:
  - El directorio `/usr/bin`
  - El directorio `/usr/lib` para las bibliotecas de IBM Spectrum Protect
3. Asegúrese de que todos los usuarios del cliente de copia de seguridad y archivado definen la variable de entorno `DSM_DIR` en el directorio recién instalado.


## Qué hacer a continuación

---

Una vez finalizada la instalación, consulte el apartado Configurar el cliente de IBM Spectrum Protect para obtener información sobre la realización de tareas obligatorias y opcionales antes de utilizar el cliente de copia de seguridad y archivado.

Nota:

- Las particiones de carga de trabajo de AIX (WPAR) están soportadas como sigue:
  - Soportadas en entornos globales
  - Soportadas con las WPAR de sistemas no compartidos
  - Soportadas con las WPAR de sistemas compartidos (los archivos de configuración y los registros del cliente de copia de seguridad y archivado se deben definir en ubicaciones no predeterminadas)
  - Sin soporte para las WPAR de aplicación
  - Sin soporte para copia de seguridad de imágenes
  - Sin soporte para restauración de conjunto de copias de seguridad desde cinta
- En AIX versión 6.1, si va a utilizar sistemas de archivos cifrados (EFS) con el cliente de copia de seguridad y archivado, y si la contraseña del almacén de claves de usuario de EFS difiere de la contraseña de inicio de sesión de usuario, el almacén de claves de EFS no se abrirá automáticamente cuando se inicie una sesión. Si el almacén de claves de EFS no se abre al iniciar sesión, es posible que el cliente no restaure un archivo que no sea EFS en un sistema de archivos EFS. Podrá evitar el problema de restauración del sistema de archivos EFS de una de las siguientes maneras:
  - Inicie el cliente de copia de seguridad y archivado mediante el mandato `efskeymgr -o`. Por ejemplo: `efskeymgr -o ./dsmj`
  - Sincronice la contraseña de almacén de claves con la contraseña de inicio de sesión utilizando el mandato `efskeymgr -n`. Por ejemplo: `efskeymgr -n`

 Sistemas operativos AIX

## Desinstalación del cliente AIX

Utilice los siguientes procedimientos para desinstalar el cliente de copia de seguridad y archivado AIX de IBM Spectrum Protect.

### Antes de empezar

Los módulos y los componentes del cliente de IBM Spectrum Protect están estrechamente integrados, y los juegos de archivos instalados se validan automáticamente. No existe la opción de retrotracción de componentes desinstalados.

### Procedimiento

1. Escriba el siguiente mandato de AIX: `smitty remove`.
2. Pulse la tecla Intro.
3. En el campo del nombre de SOFTWARE, pulse F4 para que se muestre una lista de los juegos de archivos de IBM Spectrum Protect que desea desinstalar; pulse la tecla Intro.
4. Seleccione los juegos de archivos de IBM Spectrum Protect que desea desinstalar; pulse la tecla Intro.  
Nota: La característica de copia de seguridad con registro por diario está en dos conjuntos de archivos. Seleccione `tivoli.tsm.client.jbb.64bit` y `tivoli.tsm.filepath_aix`. Si desinstala los conjuntos de archivos de uno en uno, desinstale primero el conjunto de archivos `tivoli.tsm.client.jbb.64bit`.
5. En el campo PREVIEW only? (la operación de eliminación no tendrá lugar), seleccione No; pulse la tecla Intro.

## Instalación de la API de HP-UX Itanium 2

Puede instalar la API de HP-UX Itanium 2 desde el soporte de instalación del producto.

### Acerca de esta tarea

Los siguientes paquetes de origen están disponibles en los medios de instalación:

`tsmcli/hp11ia64/gskcrypt64-8.x.x.x.hpux.ia64.tar.Z` and `tsmcli/hp11ia64/gskssl64-8.x.x.x.hpux.ia64.tar.Z`  
Contiene el GSKit. Si tiene una versión anterior de GSKit, desinstálela antes de instalar la nueva versión.

`tsmcli/hp11ia64/TIVsmCapi64`

En este paquete, el nombre de selección de software utilizado por `swlist` para el nombre de producto de nivel superior es `TIVsm64`. Bajo `TIVsm64` se encuentra el componente `TIVsm.CLIENT_API64`.

#### Directorios de instalación predeterminados

A continuación, figuran los directorios predeterminados donde se almacenan determinados archivos como parte de la instalación del cliente:

- Los archivos de la API de IBM Spectrum Protect están instalados en el directorio `/opt/tivoli/tsm/client/api/bin64`.
- El archivo de opciones del sistema de ejemplo, `dsm.sys.smp`, se ubica en el directorio de instalación.

Para eliminar las versiones anteriores del cliente de copia de seguridad y archivado, conéctese como usuario `root` y escriba el mandato siguiente:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```

Si ha instalado idiomas adicionales en un cliente de la Versión 7.1.2 o anterior, ejecute el mandato siguiente para eliminarlos:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64.CLIENT_msg_idioma
```

Sustituya *idioma* por el código de idioma adecuado de la Tabla 1.

Tabla 1. Cliente de HP-UX  
Itanium 2: códigos de idioma  
para paquetes de instalación

Idioma	Código de idioma
Chino simplificado	ZH_CN
Chino tradicional	ZH_TW
Checo	CS_CZ
Francés	FR_FR

Idioma	Código de idioma
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués de Brasil	PT_BR
Ruso	RU_RU
Español	ES_ES

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

## Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Para instalar GSKit: Si tiene instalada una versión anterior de GSKit, elimínela antes de instalar la nueva versión. Extraiga el contenido de gskcrypt64-8.x.x.x.hpux.ia64.tar.Z y gskssl64-8.x.x.x.hpux.ia64.tar.Z en un directorio del disco duro. Escriba los siguientes mandatos para instalar los paquetes:

```
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskcrypt64 gskcrypt64
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`
/gskssl64 gskssl64
```

4. Si lo ha descargado del FTP, vaya al directorio donde se encuentra la imagen instalable. Especifique el siguiente mandato:

```
/usr/sbin/swinstall -x mount_all_filesystems=false -v -s `pwd`/TIVsmCapi64 TIVsm64
```

Puede utilizarse `pwd` en lugar del nombre absoluto del directorio actual.

- Aumento del límite predeterminado del tamaño de segmento de datos  
El límite predeterminado del tamaño de los segmentos de datos de un proceso en HP-UX 11i v2 es de 64 MB. Si realiza copias de seguridad de grandes sistemas de archivos, es posible que la API supere este límite y se quede sin memoria.

### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

## Desinstalación de la API de HP-UX Itanium 2

Puede utilizar los procedimientos siguientes para desinstalar la API de IBM Spectrum Protect HP-UX Itanium 2.

### Antes de empezar

Importante: Asegúrese de que desinstala los paquetes en el orden que se muestra.

### Procedimiento

1. Para eliminar el conjunto de archivos CLIENT\_API, escriba el siguiente mandato:

```
/usr/sbin/swremove -x mount_all_filesystems=false -v TIVsm64
```

2. Para eliminar Global Security Kit (GSKit), escriba los siguientes mandatos:

```
/usr/sbin/swremove -x mount_all_filesystems=false gskssl64
/usr/sbin/swremoveswremove -x mount_all_filesystems=false gskcrypt64
```

## Qué hacer a continuación

Después de desinstalar la API de HP-UX, varios directorios vacíos permanecen en el sistema de archivos, por ejemplo los directorios siguientes:

- El directorio de licencia (/opt/tivoli/tsm/license)
- Uno o varios directorios de idioma (/opt/tivoli/tsm/client/ba/bin/xx\_XX), donde xx\_XX representa uno de los siguientes códigos de idioma: cs\_CZ, de\_DE, es\_ES, it\_IT, fr\_FR, hu\_HU, ja\_JP, ko\_KR, pl\_PL, pt\_BR, ru\_RU, zh\_CN and zh\_TW
- /opt/tivoli/tsm/client/ba/bin/cit
- /opt/tivoli/tsm/client/ba/bin/images
- /opt/tivoli/tsm/client/ba/bin/plugin

Si desea eliminar estos directorios vacíos, puede eliminarlos manualmente.

 Sistemas operativos Linux

## Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)

Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.

### Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

### Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.ppc64le.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas y los ejemplos de la API de IBM Spectrum Protect.	/opt/tivoli/tsm/client/api/bin64

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-BA.ppc64le.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Normalmente este directorio es el directorio de instalación predeterminado para muchos archivos de cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no establece la variable de entorno DSM_DIR, el archivo ejecutable dsms, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.</p> <p>Si no establece la variable de entorno DSM_CONFIG, el archivo de opciones de usuario de cliente debe estar en este directorio.</p> <p>Si no establece la variable de entorno DSM_LOG, el cliente de copia de seguridad y archivado graba mensajes en los archivos dsmserror.log y dsmsched.log en el directorio de trabajo actual.</p>
TIVsm-APIcit.ppc64le.rpm TIVsm-BAcit.ppc64le.rpm	Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Estos archivos son opcionales. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	<p>APIcit está instalado en /opt/tivoli/tsm/client/api/bin64/cit</p> <p>BAcit está instalado en /opt/tivoli/tsm/client/ba/bin/cit</p>
TIVsm-filepath-source.tar.gz TIVsm-JBB.ppc64le.rpm	Archivos necesarios para las copias de seguridad basadas en diarios.	<p>Los paquetes filepath y TIVsm-JBB solo son necesarios si tiene previsto utilizar copias de seguridad basadas en el diario.</p> <p>Filepath se instala en /opt/filepath</p> <p>El paquete TIVsm-JBB.ppc64le.rpm se instala en /opt/tivoli/tsm/client/ba/bin.</p>

## Procedimiento

1. Monte el volumen desde el que vaya a instalar los paquetes.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En el ejemplo de mandato siguiente, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.ppcle.rpm gskssl64-8.x.x.x.linux.ppcle.rpm
```

4. Instale la API de IBM Spectrum Protect y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

a. Necesario: Instale la API:

```
rpm -ivh TIVsm-API64.ppc64le.rpm
```

b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -ivh TIVsm-APIcit.ppc64le.rpm
```

Consejo: Si está actualizando la API y los paquetes de Common Inventory Technology se han instalado previamente, debe actualizar tanto la API como los paquetes de Common Inventory Technology. Por ejemplo, ejecute el mandato siguiente:

```
rpm -U TIVsm-API64.ppc64le.rpm TIVsm-APIcit.ppc64le.rpm
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

a. Instale los componentes del cliente de archivado y copia de seguridad.

```
rpm -ivh TIVsm-BA.ppc64le.rpm
```

b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.

```
rpm -ivh TIVsm-BAcit.ppc64le.rpm
```

6. Opcional: Si desea utilizar las copias de seguridad basadas en diarios, instale los paquetes necesarios para el componente de la vía de acceso de archivos y las copias de seguridad basadas en diarios.

a. Extraiga TIVsm-filepath-source.tar.gz y vea el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel de Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).

b. Instale el paquete de copia de seguridad basada en el diario:

```
rpm -ivh TIVsm-JBB.ppc64le.rpm
```

**Conceptos relacionados:**

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)

---

Puede desinstalar el IBM Spectrum Protect Linux on Power Systems (Little Endian).

### Antes de empezar

---

Debe haber iniciado la sesión como usuario root para desinstalar el producto. Debe desinstalar los paquetes en el orden que se muestra, de lo contrario la desinstalación fallará.

### Procedimiento

---

Para desinstalar el cliente de copia de seguridad y archivado, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de archivado y copia de seguridad, la API y el IBM Global Security Kit (GSKit).

Consejo: El número de versión de los paquetes no es necesario.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos rpm -e diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
rpm -e TIVsm-BA
```

3. Desinstale los paquetes del cliente de archivado y copia de seguridad:
  - a. Si ha instalado el paquete de inventario común (TIVsmBAcit), desinstálo:

```
rpm -e TIVsm-BAcit
```

- b. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
rpm -e TIVsm-BA
```

4. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Siga las instrucciones de los productos dependientes de la API para determinar qué necesita realizar para evitar la pérdida de datos al desinstalar y volver a instalar los productos.

5. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

6. Desinstale los paquetes de la API:

- a. Si ha instalado el paquete de inventario común de la API (TIVsm-APIcit), desinstálo:

```
rpm -e TIVsm-APIcit
```

- b. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

7. Desinstale GSKit entrando el mandato siguiente:

```
rpm -e gskcrypt64 gskssl64
```

#### Tareas relacionadas:

Instalación del cliente de copia de seguridad y archivado en Linux on Power Systems (Little Endian)

 Sistemas operativos Linux

## Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)

Puede instalar el cliente de archivado y copia de seguridad del soporte de instalación del producto.

### Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

### Acerca de esta tarea

Los siguientes paquetes de instalación están disponibles en el soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64_8.x.x.ppc64el.deb	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
gskssl64_8.x.x.ppc64el.deb		



Nombre del paquete	Contenido	Directorio predeterminado
tivsm-api64.ppc64el.deb	Interfaz de programación de aplicaciones (API), que contiene la biblioteca compartida y los ejemplos de la API de IBM Spectrum Protect.	/opt/tivoli/tsm/client/api/bin64
tivsm-ba.ppc64el.deb	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	/opt/tivoli/tsm/client/ba/bin  Normalmente este directorio es el directorio de instalación predeterminado para muchos archivos de cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio.  Si no establece la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.  Si no establece la variable de entorno DSM_CONFIG, el archivo de opciones de usuario de cliente debe estar en este directorio.  Si no establece la variable de entorno DSM_LOG, el cliente de copia de seguridad y archivado graba mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.
TIVsm-filepath-source.tar.gz tivsm-jbb.ppc64el.deb	Archivos necesarios para las copias de seguridad basadas en diarios.	El paquete TIVsm-filepath-source.tar.gz se instala en el directorio /opt/filepath.  El paquete tivsm-jbb.ppc64el.rpm se instala en el directorio /opt/tivoli/tsm/client/ba/bin.

## Procedimiento

1. Monte el volumen desde el que vaya a instalar los paquetes.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En el siguiente ejemplo de mandato, los caracteres "8.x.x.x" representan la versión de GSKit:

```
dpkg -i gskcrypt64_8.x.x.x.ppc64el.deb gskssl64_8.x.x.x.ppc64el.deb
```

4. Instale la API de IBM Spectrum Protect:

```
dpkg -i tivsm-api64.ppc64el.deb
```

Si solo necesita instalar la API, puede detenerse aquí. Siga los pasos siguientes para instalar el cliente de copia de seguridad y archivado y los paquetes que se necesitan para ejecutar copias de seguridad basadas en el registro de diario.

5. Instale el cliente de archivado y copia de seguridad:


```
dpkg -i tivsm-ba.ppc64el.deb
```

6. Opcional: Si desea utilizar copias de seguridad con registro por diario, instale los paquetes siguientes:
  - a. Extraiga TIVsm-filepath-source.tar.gz y revise el archivo README para ver instrucciones sobre cómo compilar e instalar el software. El módulo de kernel de Linux Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).
  - b. Instale el paquete de copia de seguridad basada en el diario:

```
dpkg -i tivsm-jbb.ppc64el.deb
```

### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación del cliente en Ubuntu Linux on Power Systems (Little Endian)

Puede desinstalar el cliente de copia de seguridad y archivado de IBM Spectrum Protect en Linux on Power Systems (Little Endian).

## Antes de empezar

Debe haber iniciado la sesión como usuario root para desinstalar el producto.

Requisito: Debe desinstalar los paquetes en el orden que se muestra, de lo contrario la desinstalación fallará.

## Procedimiento

Para desinstalar el cliente de copia de seguridad y archivado, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el cliente de archivado y copia de seguridad, la API de IBM Global Security Kit (GSKit). Las instrucciones para desinstalar el componente Filepath se proporcionan junto con el código fuente de Filepath al obtener el software de IBM®.

Consejo: El número de versión de los paquetes no es necesario.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine tivsm-jbb y los paquetes de la vía de acceso al archivo. El paquete tivsm-jbb depende del paquete Filepath. Primero desinstale el paquete tivsm-jbb.

- a. `dpkg -r tivsm-jbb`
- b. `dpkg -r TIVsm-filepath`

2. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
dpkg -r tivsm-ba
```

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail.

Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Siga las instrucciones de los productos dependientes de la API para determinar qué necesita realizar para evitar la pérdida de datos al desinstalar y volver a instalar los productos.

4. Desinstale el paquete de API emitiendo el mandato siguiente:

```
dpkg -r tivsm-api64
```

5. Elimine los paquetes de GSKit:

```
dpkg -r gskcrypt64 gskssl64
```

### Tareas relacionadas:

Instalación de la API del cliente de copia de seguridad y archivado en Ubuntu Linux on Power Systems (Little Endian)

 Sistemas operativos Linux

## Instalación de la API en Linux on Power Systems (Big Endian)

Puede instalar la API de IBM Spectrum Protect desde el soporte de instalación del producto.

## Antes de empezar

Debe haber iniciado la sesión como usuario root para instalar el producto.

## Acerca de esta tarea

Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínela (`rpm -e`) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.

Si tiene IBM Spectrum Protect versión 6.3 (o más reciente) instalado, puede utilizar la opción de actualización `rpm (rpm -U)` o la opción de renovación `rpm (rpm -F)` para actualizar el software existente a una versión más reciente. El mandato `rpm -U` se puede utilizar para instalar nuevos paquetes o actualizar paquetes existentes; `rpm -F` sólo puede actualizar paquetes que ya estén instalados.

Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect. Si está ejecutando un cliente de la Versión 7.1.2 o anterior, debe desinstalar los paquetes de idioma antes de continuar con la actualización.

Tabla 1 muestra las opciones de instalación disponibles en paquetes no comprimidos del soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
--------------------	-----------	---------------------------

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.ppc64.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64
TIVsm-APIcit.ppc64.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	APIcit está instalado en /opt/tivoli/tsm/client/api/bin64/cit

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

## Procedimiento

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.ppc.rpm gskssl64-8.x.x.x.linux.ppc.rpm
```

4. Instale la API de IBM Spectrum Protect y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (processor value unit - value unit de procesador).
  - a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.ppc64.rpm
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.


```
rpm -i TIVsm-APIcit.ppc64.rpm
```

Consejo: Si está actualizando la API y los paquetes de Common Inventory Technology se han instalado previamente, debe actualizar tanto la API como los paquetes de Common Inventory Technology. Por ejemplo, ejecute el mandato siguiente:

```
rpm -U TIVsm-API64.ppc64.rpm TIVsm-APIcit.ppc64.rpm
```

### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación de la API en Linux on Power Systems (Big Endian)

Puede desinstalar la API de IBM Spectrum Protect en IBM Spectrum Protect Linux on Power Systems (Big Endian).

### Antes de empezar

Debe haber iniciado sesión como root para desinstalar el producto. Desinstale los paquetes en el orden que se muestra.

### Procedimiento

Para desinstalar un paquete de IBM Spectrum Protect previamente instalado, introduzca los mandatos siguientes para eliminar los paquetes de la copia de seguridad basada en el diario, el componente de la vía de acceso, el cliente de archivado y copia de seguridad (si corresponde), la API y el Global Security Kit (GSKit) de IBM.

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

1. Complete este paso si se ha instalado previamente una versión 7.1 o anterior del cliente.

Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos rpm -e diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Si se había instalado previamente una versión 7.1 o anterior del cliente, desinstale los paquetes del cliente de archivado y copia de seguridad.

- a. si ha instalado el paquete TIVsmBACit opcional, desinstálo utilizando el siguiente mandato:

```
rpm -e TIVsm-BACit
```

- b. Desinstale el paquete de cliente de archivado y copia de seguridad:

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya xx\_xx por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 1.

```
rpm -e TIVsm-BA.msg.xx_xx
```

Tabla 1. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN

Idioma	Identificador de idioma
Chino tradicional Big5	ZH_TW

- Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo tras instalar una versión más reciente del paquete de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.
- Si instala el paquete de inventario común de la API opcional (TIVsm-APIcit), utilice el siguiente mandato para desinstalar el paquete:

```
rpm -e TIVsm-APIcit
```

- Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

- Desinstale GSKit con el mandato siguiente:

```
rpm -e gskcrypt64 gskssl64
```

#### Tareas relacionadas:

Instalación de la API en Linux on Power Systems (Big Endian)

 Sistemas operativos Linux

## Instalación del cliente Linux x86\_64

Puede instalar el cliente de archivado y copia de seguridad de Linux x86\_64 desde el soporte de instalación del producto.

### Antes de empezar

- Debe haber iniciado la sesión como root para instalar el producto.
- Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínala (rpm -e) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.
- Si tiene IBM Spectrum Protect versión 6.3 (o posterior) instalado, puede utilizar la opción de actualización rpm (rpm -U) o la opción de renovación rpm (rpm -F) para actualizar el software existente a una versión más reciente. El mandato rpm -U se puede utilizar para instalar paquetes nuevos o actualizar paquetes existentes solo si no ha instalado anteriormente ningún paquete de idioma. El mandato rpm -F solo puede actualizar paquetes que ya están instalados.
- Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect.
- Si se han instalado paquetes de idioma, tiene que desinstalarlos antes de instalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect.

### Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.x86_64.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-BA.x86_64.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	<p>/opt/tivoli/tsm/client/ba/bin</p> <p>Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsms, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.</p> <p>Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio.</p> <p>Si no define DSM_LOG, escribe mensajes en los archivos dsmserror.log y dsmsched.log en el directorio de trabajo actual.</p>
TIVsm-APIcit.x86_64.rpm TIVsm-BACit.x86_64.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	<p>APIcit está instalado en /opt/tivoli/tsm/client/api/bin64/cit/</p> <p>BACit está instalado en /opt/tivoli/tsm/client/ba/bin/cit/</p>
TIVsm-filepath-source.tar.gz TIVsm-JBB.x86_64.rpm	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	<p>Filepath se instala en /opt/filepath</p> <p>JBB se instala en /opt/tivoli/tsm/client/ba/bin</p>
TIVsm_BAhdw.x86_64.rpm	Proporciona soporte para la copia de seguridad incremental de instantáneas para servidores de archivos NetAPP y N-Series.	/opt/tivoli/tsm/client/ba/bin/plugins

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

## Procedimiento

Para instalar el cliente de copia de seguridad y archivado Linux x86\_64, complete los siguientes pasos:

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.x86_64.rpm gskssl64-8.x.x.x.linux.x86_64.rpm
```

4. Instale la API de IBM Spectrum Protect y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
  - a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.x86_64.rpm
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -i TIVsm-APIcit.x86_64.rpm
```

Consejo: Si está actualizando la API y los paquetes de Common Inventory Technology se han instalado previamente, debe actualizar tanto la API como los paquetes de Common Inventory Technology. Por ejemplo, ejecute el mandato siguiente:

```
rpm -U TIVsm-API64.x86_64.rpm TIVsm-APIcit.x86_64.rpm
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
  - a. Instale los componentes del cliente de archivado y copia de seguridad.

```
rpm -i TIVsm-BA.x86_64.rpm
```

- b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.


```
rpm -i TIVsm-BAcit.x86_64.rpm
```

6. Opcional: Si desea utilizar copias de seguridad basadas en el diario, debe compilar e instalar el componente filepath que coincide con el kernel de Linux en el sistema de cliente. Extraiga TIVsm-filepath-source.tar.gz y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel filepath de Linux tiene licencia en conformidad con los términos de la "GPL" (General Public License) de GNU.
7. Para instalar la copia de seguridad incremental por diferencia de instantánea para los servidores de archivos de NetApp y N-Series, especifique el siguiente mandato:

```
rpm -i TIVsm-BAhdw.x86_64.rpm
```

#### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación del cliente Linux x86\_64

---

Utilice el siguiente procedimiento para desinstalar el cliente IBM Spectrum Protect Linux x86\_64.

### Antes de empezar

---

Debe haber iniciado sesión como root para desinstalar el producto. Desinstale los paquetes en el orden que se muestra.

### Procedimiento

---

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de copia de seguridad y archivado, la API y el IBM Global Security Kit (GSKit).

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete de vía de acceso. Si utiliza dos mandatos rpm -e diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale los paquetes del cliente de archivado y copia de seguridad:

- a. Si ha instalado el paquete TIVsm-BAcit opcional, desinstálo antes de desinstalar el cliente.

```
rpm -e TIVsm-BAcit
```

- b. Desinstale el cliente de archivado y copia de seguridad.

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya xx\_xx por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 1.

```
rpm -e TIVsm-msg.xx_xx
```

Tabla 1. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN
Chino tradicional Big5	ZH_TW

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.

- a. Si ha instalado el paquete de inventario común de la API opcional (TIVsm-APIcit), desinstálo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:

```
rpm -e TIVsm-APIcit
```

- b. Desinstale el paquete de la API mediante el mandato siguiente:


```
rpm -e TIVsm-API64
```

4. Para eliminar el paquete de GSKit de 64 bits, escriba el siguiente mandato:

```
rpm -e gskcrypt64 gskssl64
```

#### Tareas relacionadas:

Instalación del cliente Linux x86\_64

 Sistemas operativos Linux

## Instalación del cliente Ubuntu Linux x86\_64



Puede instalar el cliente de archivado y copia de seguridad de Ubuntu Linux de 64 bits desde el soporte de instalación del producto.

## Acerca de esta tarea

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
tivsm-api64.amd64.deb	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64
tivsm-ba.amd64.deb	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	/opt/tivoli/tsm/client/ba/bin  Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.  Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio.  Si no define DSM_LOG, escribe mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.
tivsm-apicit.amd64.deb tivsm-bacit.amd64.deb	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	APIcit está instalado en /opt/tivoli/tsm/client/api/bin64/cit  BACit está instalado en /opt/tivoli/tsm/client/ba/bin/cit

Nombre del paquete	Contenido	Directorio predeterminado
tivsm-filepath-source.tar.gz tivsm-jbb.amd64.deb	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	Los paquetes filepath y tivsm-jbb solo son obligatorios si tiene previsto utilizar copias de seguridad con registro por diario.  El paquete tivsm-jbb.x86_64.deb se instala en /opt/tivoli/tsm/client/ba/bin.
tivsm-bahdw.amd64.deb	Proporciona soporte para la copia de seguridad incremental de instantáneas para servidores de archivos NetAPP y N-Series.	/opt/tivoli/tsm/client/ba/bin/plugins

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

## Procedimiento

Para instalar el cliente de copia de seguridad y archivado Ubuntu Linux x86\_64, complete los siguientes pasos.

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes de instalación.
3. Instale los paquetes de GSKit de 64 bits.

```
sudo dpkg -i gskcrypt64_8.0-50.40.linux.x86_64.deb gskssl64_8.0-50.40.linux.x86_64.deb
```

4. Instale la API de IBM Spectrum Protect y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
  - a. Necesario: Instale la API:

```
sudo dpkg -i tivsm-api64.amd64.deb
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
sudo dpkg -i tivsm-apicit.amd64.deb
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y, opcionalmente, instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).
  - a. Instale los componentes del cliente de archivado y copia de seguridad.

```
sudo dpkg -i tivsm-ba.amd64.deb
```

- b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.


```
sudo dpkg -i tivsm-bacit.amd64.deb
```

6. Opcional: Realice este paso solo si piensa utilizar copias de seguridad basadas en el diario.
  - a. Extraiga tivsm-filepath-source.tar.gz y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel de Filepath tiene licencia de conformidad con los términos de la "GPL" (GNU General Public License).
  - b. Instale el paquete de copia de seguridad con registro por diario: `dpkg -i tivsm-jbb.amd64.deb`.
7. Para instalar la copia de seguridad incremental por diferencia de instantánea para los servidores de archivos de NetApp y N-Series, especifique el siguiente mandato:

```
sudo dpkg -i tivsm-bahdw.amd64.deb
```

**Conceptos relacionados:**

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación del cliente Ubuntu Linux x86\_64

Puede utilizar el siguiente procedimiento para desinstalar el cliente de IBM Spectrum Protect Linux de 64 bits.

### Procedimiento

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el cliente de archivado y copia de seguridad, la API y el IBM Global Security Kit (GSKit). Las instrucciones para desinstalar el componente Filepath se proporcionan junto con el código fuente de Filepath al obtener el software de IBM®.

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine el componente tivsm-jbb y el componente Filepath. El paquete tivsm-jbb depende del paquete Filepath. Primero desinstale el paquete tivsm-jbb.

- a. `sudo dpkg -r tivsm-jbb`
- b. `sudo dpkg -r tivsm-filepath`

2. Desinstale los paquetes del cliente de archivado y copia de seguridad:

- a. Si ha instalado el paquete tivsm-bacit opcional, desinstálo antes de desinstalar el cliente.

```
sudo dpkg -r tivsm-bacit
```

- b. Desinstale el cliente de archivado y copia de seguridad.

```
sudo dpkg -r tivsm-ba
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya xx-xx por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 1.

```
dpkg -r tivsm-msg.xx-xx
```

Tabla 1. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	cs-cz
Francés	fr-fr
Alemán	de-de
Húngaro	hu-hu
Italiano	it-it
Japonés	ja-jp
Coreano	ko-kr
Polaco	pl-pl
Portugués	pt-br
Ruso	ru-ru
Español	es-es
Chino tradicional (EUC)	zh-cn
Chino tradicional Big5	zh-tw

3. Desinstale los productos que dependan de la API, como por ejemplo los productos de IBM Spectrum Protect Data Protection. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.

- a. Si ha instalado el paquete de inventario común de la API opcional (tivsm-apicit), desinstálo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:

```
sudo dpkg -r tivsm-apicit
```

b. Desinstale el paquete de la API mediante el mandato siguiente:

```
sudo dpkg -r tivsm-api64
```

4. Para eliminar los paquetes de GSKit de 64 bits, escriba el siguiente mandato:

```
sudo dpkg -r gskcrypt64 gskssl64
```

**Tareas relacionadas:**

Instalación del cliente Ubuntu Linux x86\_64

 Sistemas operativos Linux

## Instalación del cliente Linux on System z

---

Puede instalar el cliente de archivado y copia de seguridad de Linux on System z desde el soporte de instalación del producto.

### Antes de empezar

---

Debe haber iniciado la sesión como root para instalar el producto.

### Acerca de esta tarea

---

Si tiene IBM Spectrum Protect versión 6.2 (o una versión anterior) instalada, elimínela (rpm -e) y cualquier otro programa de software dependiente antes de instalar una versión más reciente.

Si tiene IBM Spectrum Protect versión 6.3 (o más reciente) instalado, puede utilizar la opción de actualización rpm (rpm -U) o la opción de renovación rpm (rpm -F) para actualizar el software existente a una versión más reciente. El mandato rpm -U se puede utilizar para instalar nuevos paquetes o actualizar paquetes existentes; rpm -F sólo puede actualizar paquetes que ya estén instalados.

Detenga los procesos del cliente en ejecución antes de desinstalar o actualizar la API o el cliente de archivado y copia de seguridad de IBM Spectrum Protect. Si está ejecutando un cliente de la Versión 7.1.2 o anterior, debe desinstalar los paquetes de idioma antes de continuar con la actualización.

Las siguientes opciones de instalación están disponibles en paquetes no comprimidos en el soporte de instalación.

Tabla 1. Nombres de paquetes, contenido y directorio predeterminado

Nombre del paquete	Contenido	Directorio predeterminado
gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm	Paquetes de Global Security Kit (GSKit) de 64 bits	/usr/local/ibm/gsk8
TIVsm-API64.s390x.rpm	Interfaz de programación de aplicaciones (API), que contiene las bibliotecas compartidas de la API de IBM Spectrum Protect y ejemplos.	/opt/tivoli/tsm/client/api/bin64

Nombre del paquete	Contenido	Directorio predeterminado
TIVsm-BA.s390x.rpm	Cliente de archivado y copia de seguridad (línea de mandatos y GUI), cliente administrativo (dsmadm) y el cliente web.	<p>/opt/tivoli/tsm/client/ba</p> <p>Este directorio se considera como el directorio de instalación predeterminado para muchos archivos del cliente de archivado y copia de seguridad. El archivo de opciones del sistema de ejemplo (dsm.sys.smp) se graba en este directorio. Si no se ha establecido la variable de entorno DSM_DIR, el archivo ejecutable dsmc, los archivos de recursos y el archivo dsm.sys se almacenan en este directorio.</p> <p>Si no se ha establecido DSM_CONFIG, el archivo de opciones de usuario del cliente debe estar en este directorio.</p> <p>Si no define DSM_LOG, el cliente de copia de seguridad y archivado escribe mensajes en los archivos dsmerror.log y dsmsched.log en el directorio de trabajo actual.</p>
TIVsm-APIcit.s390x.rpm TIVsm-BAcit.s390x.rpm	Opcional. Estos archivos proporcionan los componentes de Common Inventory Technology que puede utilizar para obtener información acerca del número de dispositivos de número de clientes y servidores conectados al sistema, y la utilización de las unidades de valor de procesador (PVU) mediante los dispositivos del servidor. Para obtener más información sobre las PVU, consulte Estimación de las unidades de valor de procesador en la documentación del servidor de IBM Spectrum Protect.	<p>APIcit está instalado en /opt/tivoli/tsm/client/api/bin64/cit</p> <p>BAcit está instalado en /opt/tivoli/tsm/client/ba/bin/cit</p>
TIVsm-filepath-source.tar.gz TIVsm-JBB.s390x.rpm	Los archivos deben ser compatibles con las copias de seguridad basadas en diarios.	<p>Filepath se instala en /opt/filepath</p> <p>JBB se instala en /opt/tivoli/tsm/client/ba/bin</p>

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

## Procedimiento

1. Monte el volumen desde el que está realizando la instalación.
2. Cambie el directorio en el que se guardan los paquetes.
3. Instale los paquetes de GSKit de 64 bits. En este ejemplo, los caracteres "8.x.x.x" representan la versión de GSKit:

```
rpm -U gskcrypt64-8.x.x.x.linux.s390x.rpm gskssl64-8.x.x.x.linux.s390x.rpm
```

4. Instale la API de IBM Spectrum Protect y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (processor value unit - value unit de procesador).

- a. Necesario: Instale la API:

```
rpm -i TIVsm-API64.s390x.rpm
```

- b. Opcional: Instale el paquete de Common Inventory Technology que utiliza la API. Este paquete depende de la API, por lo que debe instalarse una vez que se instale el paquete de la API.

```
rpm -i TIVsm-APIcit.s390x.rpm
```

Consejo: Si está actualizando la API y los paquetes de Common Inventory Technology se han instalado previamente, debe actualizar tanto la API como los paquetes de Common Inventory Technology. Por ejemplo, ejecute el mandato siguiente:

```
rpm -U TIVsm-API64.s390x.rpm TIVsm-APIcit.s390x.rpm
```

Si solo necesita instalar la API, puede detenerse aquí. El resto de los pasos de este procedimiento describen cómo instalar los componentes del cliente de archivado y copia de seguridad y un paquete del cliente opcional que sólo es necesario si desea que el cliente envíe métricas de PVU al servidor. En los pasos subsiguientes también se describe la instalación de los paquetes que son necesarios si desea realizar copias de seguridad basadas en el diario.

5. Instale el cliente de archivado y copia de seguridad y opcionalmente instale el paquete de Common Inventory Technology que se necesita para soportar los cálculos de PVU (value unit de procesador).

- a. Instale los componentes del cliente de archivado y copia de seguridad.

```
rpm -i TIVsm-BA.s390x.rpm
```


- b. Opcional: Instale el paquete de tecnología común de inventario que el cliente utiliza para enviar medidas de PVU al servidor. Este paquete depende del paquete del cliente, por lo que debe instalarse una vez que se instale el paquete del cliente.

```
rpm -i TIVsm-BAcit.s390x.rpm
```

6. Opcional: Si desea utilizar copias de seguridad basadas en el diario, debe compilar e instalar el componente filepath que coincide con el kernel de Linux en el sistema de cliente. Extraiga TIVsm-filepath-source.tar.gz y consulte el archivo README para obtener instrucciones de compilación e instalación. El módulo de kernel filepath de Linux tiene licencia en conformidad con los términos de la "GPL" (General Public License) de GNU.

#### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Linux

## Desinstalación del cliente de Linux on System z

---

Utilice los siguientes procedimientos para desinstalar el cliente de IBM Spectrum Protect Linux on System z.

### Antes de empezar

---

Debe haber iniciado la sesión como root para instalar el producto. Desinstale los paquetes en el orden que se muestra.

### Acerca de esta tarea

---

Para desinstalar un paquete de cliente de IBM Spectrum Protect instalado anteriormente, entre los mandatos siguientes para eliminar los paquetes para la copia de seguridad basada en el diario, el componente de vía de acceso de archivo, el cliente de copia de seguridad y archivado, la API y IBM® Global Security Kit (GSKit).

Consejo: Para la desinstalación no se necesita el número de versión de los paquetes.

### Procedimiento

---

1. Para desinstalar sólo los componentes de la copia de seguridad con registro por diario, elimine ambos paquetes (vía de acceso y copia de seguridad con registro por diario). El paquete TIVsm-JBB depende del paquete filepath. Si utiliza dos mandatos rpm -e diferentes para desinstalar los componentes de uno en uno, desinstale antes el paquete TIVsm-JBB.

```
rpm -e TIVsm-JBB TIVsm-filepath
```

2. Desinstale los paquetes del cliente de archivado y copia de seguridad:
  - a. Si ha instalado el paquete TIVsm-BAcit opcional, desinstálelo antes de desinstalar el cliente.

```
rpm -e TIVsm-BAcit
```

b. Desinstale el cliente de archivado y copia de seguridad.

```
rpm -e TIVsm-BA
```

Nota: Si hay paquetes de idioma instalados en un cliente de la Versión 7.1.2 o anterior, debe eliminarlos antes de eliminar el paquete de API. Escriba el siguiente mandato y sustituya xx\_xx por el código de idioma para cada idioma adicional que haya instalado. Para obtener una lista de identificadores de códigos de idioma, consulte Tabla 1.

```
rpm -e TIVsm-msg.xx_xx
```

Tabla 1. Identificadores del paquete de idioma

Idioma	Identificador de idioma
Checo	CS_CZ
Francés	FR_FR
Alemán	DE_DE
Húngaro	HU_HU
Italiano	IT_IT
Japonés	JA_JP
Coreano	KO_KR
Polaco	PL_PL
Portugués	PT_BR
Ruso	RU_RU
Español	ES_ES
Chino tradicional (EUC)	ZH_CN
Chino tradicional Big5	ZH_TW

3. Desinstale los productos que dependan de la API, como por ejemplo IBM Spectrum Protect for Databases y IBM Spectrum Protect for Mail. Cualquier producto dependiente de la API debe desinstalarse antes de desinstalar el paquete de la API. Si desinstala un producto dependiente de la API, tendrá que volver a instalarlo después de instalar una versión más reciente de los paquetes de cliente de archivado y copia de seguridad y de la API. Consulte la documentación del producto dependiente para determinar lo que necesita hacer para evitar pérdidas de datos al desinstalar y volver a instalar los productos.

a. Si ha instalado el paquete de inventario común de la API opcional (TIVsm-APIcit), desinstálo antes de desinstalar el paquete de la API. Utilice el mandato siguiente para desinstalar el paquete:

```
rpm -e TIVsm-APIcit
```

b. Desinstale el paquete de la API mediante el mandato siguiente:

```
rpm -e TIVsm-API64
```

4. Para eliminar el paquete de GSKit de 64 bits, escriba el siguiente mandato:

```
rpm -e gskcryp64 gskssl64
```

#### Tareas relacionadas:

Instalación del cliente Linux on System z

 sistemas operativos Mac OS X

## Instalación del cliente Mac OS X

Puede instalar el cliente de archivado y copia de seguridad Mac OS X de IBM Spectrum Protect desde el soporte de instalación del producto.

### Antes de empezar

Debe ser administrador del sistema para instalar el cliente de copia de seguridad y archivado.

### Acerca de esta tarea

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Para clientes de MAC OS X, puede utilizar un asistente de instalación que le solicitará información mientras se instala el producto o puede instalar el cliente desde la línea de mandatos. Cuando instala el cliente mediante el procedimiento de instalación de la línea de mandatos, la instalación se ejecuta sin la interacción del cliente. El procedimiento de la línea de mandatos es útil si desea ejecutar el script de instalación en muchos nodos o si debe instalar el software en un sistema que no tiene un monitor.

## Procedimiento


Seleccione un método de instalación e instale el cliente. Utilice bien el método del asistente de instalación o instale el cliente desde la línea de mandatos.

Método de instalación	Procedimiento
Asistente de instalación	a. Pulse dos veces el archivo 8.1.2.0.0-TIV-TSMBAC-Mac.dmg para montar la imagen de disco. b. Pulse dos veces el icono del paquete de instalación de IBM Spectrum Protect y siga las solicitudes para completar la instalación.
Línea de mandatos	a. Cambie los directorios a la ubicación del instalador de IBM Spectrum Protect. b. Instale el paquete de instalación personalizada con el siguiente mandato:  <pre>/usr/sbin/installer -pkg "/Volumes/IBM Spectrum Protect/ IBM Spectrum Protect.pkg" -target /</pre>

## Qué hacer a continuación

Un ejemplo de archivo de opciones de sistema del cliente, denominado `dsm.sys.smp`, se crea en el directorio de instalación. Puede copiar el archivo y modificarlo para crear el archivo de opciones del sistema del cliente para su nodo. El nombre predeterminado para el archivo de opciones del cliente es `dsm.sys`.

Después de instalar el cliente, es posible que necesite definir las variables de entorno antes de utilizarlo. Para obtener más información sobre cómo establecer las variables de entorno, consulte Definir variables de entorno de proceso.

 sistemas operativos Mac OS X

## Desinstalación del cliente Mac OS X

Puede desinstalar el cliente de IBM Spectrum Protect Mac OS X si ya no lo necesita.

### Antes de empezar

Si el planificador de IBM Spectrum Protect está configurado como elemento de inicio, utilice las herramientas de IBM Spectrum Protect para la función de administradores, o el script de shell de `StopCad.sh` para detener y desinstalar el planificador antes de comenzar el procedimiento.

### Acerca de esta tarea

Puede utilizar el script de shell para desinstalar el cliente de archivado y copia de seguridad. El nombre del script de shell es `uninstall.sh` y está en el directorio de instalación predeterminado, que es `/Library/Application Support/tivoli/tsm/client/ba/bin`. Utilice el mandato `sudo` para ejecutar el script.

También, puede completar los siguientes pasos en lugar de utilizar el script:

## Procedimiento

1. Mueva las siguientes carpetas a la papelera:



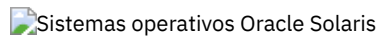
- o /Applications/IBM Spectrum Protect
  - o /Library/Application Support/tivoli
2. Elimine los siguientes enlaces simbólicos:
- o /usr/bin/dsmc
  - o /usr/bin/dsmcad
  - o /usr/bin/dsmadm
  - o /usr/bin/dsmtrace
  - o /usr/bin/dsmagent
  - o /usr/lib/libxmlutil-6.2.0.dylib
  - o /usr/lib/libtsm620xerces-c1\_6\_0.dylib
3. Opcional: Elimine los archivos de registro y los archivos de opciones si no quiere conservarlos. El proceso de desinstalación los deja en el disco, así que los ajustes se retienen en caso de que vuelva a instalar el producto más tarde.

Es posible que el cliente de copia de seguridad y archivado haya creado archivos de registro en estas ubicaciones:

- a. /Library/Logs/tivoli
- b. ~/Library/Logs/tivoli

Los archivos de opciones del cliente (dsm.opt and dsm.sys) se encuentran en las siguientes ubicaciones:

- a. /Library/Preferences/Tivoli Storage Manager
- b. ~/Library/Preferences/Tivoli Storage Manager



## Instalación del cliente de Oracle Solaris x86\_64

Puede instalar el cliente de archivado y copia de seguridad de Oracle Solaris x86\_64 de IBM Spectrum Protect desde el soporte de instalación del producto.

### Antes de empezar

A partir de IBM Spectrum Protect Versión 8.1.0, el cliente de archivado y copia de seguridad de Oracle Solaris está disponible sólo en la plataforma Oracle Solaris x86\_64. El cliente de archivado y copia de seguridad ya no está disponible en la plataforma Oracle Solaris SPARC; sólo la API de IBM Spectrum Protect está disponible en Oracle Solaris SPARC. Para obtener información sobre cómo instalar la API de Solaris SPARC, consulte Instalación de la API de Oracle SPARC.

### Acerca de esta tarea

Si se ha instalado una versión anterior del cliente de copia de seguridad y archivado, elimínela antes de instalar una versión nueva. Para obtener más información sobre cómo eliminar los paquetes del cliente Solaris anterior, consulte Desinstalación del cliente Oracle Solaris x86\_64.

Se utiliza el archivo de administración de la instalación de IBM Spectrum Protect (tsmadmin) en lugar del archivo de administración predeterminado (/var/sadm/install/admin), de forma que no se le preguntan los valores de `setuid` ni `setgid`, ni se le pide permiso de superusuario durante la instalación. Si desea utilizar el archivo de administración predeterminado, quite la opción `-a ./tsmadmin` de los mandatos que se muestran y responda a las preguntas sobre los valores `setuid` y `setgid`, o sobre el permiso de superusuario durante la instalación con `Y`.

Tabla 1. Nombres y descripciones de los paquetes de instalación

Paquete	Nombre del paquete	Descripción del paquete
IBM® Global Security Kit (GSKit) de 64 bits	gsk8cry64.pkg y gsk8ssl64.pkg	Contiene el GSKit de IBM que proporciona cifrado de datos de 64 bits Secure Sockets Layer (SSL) entre el cliente IBM Spectrum Protect y el servidor.
Interfaz de programación de aplicaciones (API) de IBM Spectrum Protect	TIVsmCapi.pkg	Contiene los ejemplos y las bibliotecas compartidas de la API de 64 bits de IBM Spectrum Protect.

Paquete	Nombre del paquete	Descripción del paquete
Cliente de archivado y copia de seguridad	TIVsmCba.pkg	<p>Contiene los siguientes componentes de 64 bits:</p> <ul style="list-style-type: none"> <li>• Cliente de copia de seguridad/archivado (línea de mandatos y GUI)</li> <li>• Cliente de administración (línea de mandatos)</li> <li>• Cliente Web de copia de seguridad/archivado</li> </ul> <p>Nota:</p> <ol style="list-style-type: none"> <li>1. Como métodos de comunicación, se admiten el protocolo TCP/IP y la memoria compartida.</li> <li>2. El cliente web es una parte del paquete de cliente de archivado y copia de seguridad y no se puede instalar sin él.</li> </ol>

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Instale los paquetes en el orden que se muestra; algunos paquetes dependen de la presencia de otros. Por ejemplo, GSKit es un requisito previo de la API y la API es un requisito previo del paquete del cliente de archivado y copia de seguridad.

## Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Cambie el directorio en el que se guardan los paquetes.
4. El GSKit IBM; es un requisito previo del paquete de la API de IBM Spectrum Protect. Instale el GSKit utilizando los siguientes mandatos:

```
pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
```

Nota: En Solaris 10, estos mandatos instalan el GSKit de 64 bits en la zona global y en todas las zonas no globales en ejecución. Para instalar el cliente sólo en una zona no global esparcida-raíz, GSKit debe instalarse primero en la zona global. En Solaris 11, los paquetes sólo se instalan en la zona en la que se ejecutan estos mandatos.

5. Utilice el mandato siguiente para instalar la API de IBM Spectrum Protect:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
```

Nota: En Solaris 10, este mandato instala la API de IBM Spectrum Protect de 64 bits en la zona global y en todas las zonas no globales en ejecución. Si desea instalarla sólo en la zona global, utilice el parámetro -G del mandato pkgadd. En Solaris 11, la API sólo se instala en la zona en la que se ejecuta este mandato.

6. Utilice el siguiente mandato para instalar el cliente de archivado y copia de seguridad:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCba.pkg TIVsmCba
```

Nota: En Solaris 10, este mandato instala los componentes del cliente de archivado y copia de seguridad en la zona global y en todas las zonas no globales en ejecución. Si desea instalarlos sólo en la zona global, utilice el parámetro -G del mandato pkgadd. En Solaris 11, los componentes de cliente sólo deben instalarse en la zona en la que se ejecuta este mandato.


## Resultados

Importante: Para una zona no global de la raíz de archivos esparcidos de Solaris 10, el sistema de archivos `/usr` suele montarse como sistema de archivos de sólo lectura (LOFS) desde la zona global, y tienen aplicación las condiciones siguientes:

- Si no se ha instalado el cliente en la zona global, aparecerá un mensaje de aviso al final de la instalación. El mensaje solicitará al administrador global que cree los enlaces necesarios que se suministran como parte de los mensajes de aviso.
- Si ya se ha instalado el cliente en la zona global, no será necesario crear los vínculos. Los enlaces ya están disponibles y hacen referencia a las bibliotecas y archivos ejecutables correctos.

#### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Oracle Solaris

## Desinstalación del cliente Oracle Solaris x86\_64

---

Puede desinstalar todos los paquetes que están relacionados con el cliente Oracle Solaris x86\_64 de IBM Spectrum Protect, incluidos los componentes línea de mandatos, GUI, GUI web y cliente de administración.

### Acerca de esta tarea

---

Importante: Asegúrese de desinstalar los paquetes en el orden especificado.

Se utiliza el archivo de administración de instalación de IBM Spectrum Protect (`tsmadmin`) en lugar del archivo de administración predeterminado (`/var/sadm/install/admin`), para que no se le hagan preguntas sobre el permiso de superusuario, `setuid` o `setgid` durante la instalación. Si desea utilizar el archivo de administración predeterminado, elimine la opción `-a` `./tsmadmin` de los mandatos siguientes y haga las preguntas sobre el permiso de superusuario, `setuid` o `setgid` durante la instalación con `y`.

### Procedimiento

---

1. Especifique el mandato siguiente para desinstalar el cliente de archivado y copia de seguridad:

```
pkgrm -n -a ./tsmadmin TIVsmCba
```

Este mandato desinstala todos los componentes del cliente de archivado y copia de seguridad (línea de mandatos, GUI, cliente web y el cliente administrativo). No puede desinstalar componentes individuales de este paquete (por ejemplo, el cliente de línea de mandatos).

Nota: Si se instalan uno o más paquetes de mensajes de idioma en clientes de la Versión 7.1.2 o anteriores, elimínelos antes de eliminar el paquete de API. Entre el mandato siguiente como usuario `root`:

```
pkgrm -n -a ./tsmadmin TIVsmClCs TIVsmClDe TIVsmClEs TIVsmClFr \  
TIVsmClHu TIVsmClIt TIVsmClJa TIVsmClKo \  
TIVsmClPl TIVsmClPt TIVsmClRu TIVsmClSc TIVsmClTc
```

2. Especifique el mandato siguiente para desinstalar la API de IBM Spectrum Protect:

```
pkgrm -n -a ./tsmadmin TIVsmCapi
```

No se puede eliminar la API si está instalado el cliente de copia de seguridad y archivado. Se debe eliminar primero el cliente de archivado y copia de seguridad.

3. Especifique los siguientes mandatos para desinstalar el GSKit:

```
pkgrm -n -a ./tsmadmin gsk8ss164  
pkgrm -n -a ./tsmadmin gsk8cry64
```

 Sistemas operativos Oracle Solaris

## Instalación de la API de Oracle SPARC

---

Puede instalar la API de Oracle Solaris SPARC de IBM Spectrum Protect desde el soporte de instalación del producto.

### Acerca de esta tarea

---

Si se ha instalado una versión anterior de la API, elimínela antes de instalar una nueva versión. Para obtener información sobre cómo eliminar los paquetes de la API de Solaris anteriores, consulte Desinstalación de la API de Oracle Solaris SPARC.

Se utiliza el archivo de administración de la instalación de IBM Spectrum Protect (tsmadmin) en lugar del archivo de administración predeterminado (/var/sadm/install/admin), de forma que no se le preguntan los valores de `setuid` ni `setgid`, ni se le pide permiso de superusuario durante la instalación. Si desea utilizar el archivo de administración predeterminado, quite la opción `-a ./tsmadmin` de los mandatos que se muestran y responda a las preguntas sobre los valores `setuid` y `setgid`, o sobre el permiso de superusuario durante la instalación con `Y`.

Tabla 1. Nombres y descripciones de los paquetes de instalación

Paquete	Nombre del paquete	Descripción del paquete
IBM® Global Security Kit (GSKit) de 64 bits	gsk8cry64.pkg y gsk8ssl64.pkg	Contiene el GSKit de IBM que proporciona cifrado de datos de 64 bits Secure Sockets Layer (SSL) entre la API y el servidor de IBM Spectrum Protect.
Interfaz de programación de aplicaciones (API) de IBM Spectrum Protect	TIVsmCapi.pkg	Contiene los ejemplos y las bibliotecas compartidas de la API de 64 bits de IBM Spectrum Protect.

Este procedimiento de instalación puede utilizarse para instalar nuevas distribuciones o actualizaciones del soporte de instalación descargado. Es posible que los archivos descargados que se utilizan para instalar el cliente estén comprimidos. En función del formato de archivo de paquete, copie o extraiga los archivos en el disco y utilice estas instrucciones para instalar los componentes.

Puede descargar el archivo de paquete correspondiente de uno de los siguientes sitios web:

- Descargue el paquete de cliente de Passport Advantage o de Fix Central.
- Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.

Instale los paquetes en el orden que se muestra.

## Procedimiento

1. Inicie la sesión como el usuario root.
2. Monte el volumen desde el que está realizando la instalación.
3. Cambie el directorio en el que se guardan los paquetes.
4. El GSKit IBM; es un requisito previo del paquete de la API de IBM Spectrum Protect. Instale el GSKit utilizando los siguientes mandatos:

```
pkgadd -n -a ./tsmadmin -d ./gsk8cry64.pkg gsk8cry64
pkgadd -n -a ./tsmadmin -d ./gsk8ssl64.pkg gsk8ssl64
```

Nota: En Solaris 10, estos mandatos instalan el GSKit de 64 bits en la zona global y en todas las zonas no globales en ejecución. Para instalar la API sólo en una zona no global esparcida-raíz, GSKit debe instalarse primero en la zona global. En Solaris 11, los paquetes sólo se instalan en la zona en la que se ejecutan estos mandatos.

5. Utilice el mandato siguiente para instalar la API de IBM Spectrum Protect:

```
pkgadd -n -a ./tsmadmin -d ./TIVsmCapi.pkg TIVsmCapi
```

Nota: En Solaris 10, este mandato instala la API de IBM Spectrum Protect de 64 bits en la zona global y en todas las zonas no globales en ejecución. Si desea instalarla sólo en la zona global, utilice el parámetro `-G` del mandato `pkgadd`. En Solaris 11, la API sólo se instala en la zona en la que se ejecuta este mandato.


## Resultados

Importante: Para una zona no global de la raíz de archivos esparcidos de Solaris 10, el sistema de archivos `/usr` suele montarse como sistema de archivos de sólo lectura (LOFS) desde la zona global, y tienen aplicación las condiciones siguientes:

- Si no se ha instalado la API en la zona global, aparecerá un mensaje de aviso al final de la instalación. El mensaje solicitará al administrador global que cree los enlaces necesarios que se suministran como parte de los mensajes de aviso.
- Si ya se ha instalado la API en la zona global, no será necesario crear estos enlaces. Los enlaces ya están disponibles y hacen referencia a las bibliotecas y archivos ejecutables correctos.

### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Oracle Solaris

## Desinstalación de la API de Oracle Solaris SPARC

Puede desinstalar todos los paquetes que están relacionados con la API de Oracle Solaris SPARC de IBM Spectrum Protect.

## Acerca de esta tarea

---

Importante: Asegúrese de desinstalar los paquetes en el orden especificado.

Se utiliza el archivo de administración de instalación de IBM Spectrum Protect (`tmsadmin`) en lugar del archivo de administración predeterminado (`/var/sadm/install/admin`), para que no se le hagan preguntas sobre el permiso de superusuario, `setuid` o `setgid` durante la instalación. Si desea utilizar el archivo de administración predeterminado, elimine la opción `-a ./tmsadmin` de los mandatos siguientes y haga las preguntas sobre el permiso de superusuario, `setuid` o `setgid` durante la instalación con `y`.

## Procedimiento





---

1. Especifique el mandato siguiente para desinstalar la API de IBM Spectrum Protect:

```
pkgrm -n -a ./tmsadmin TIVsmCapi
```

2. Especifique los siguientes mandatos para desinstalar el GSKit:

```
pkgrm -n -a ./tmsadmin gsk8ssl64  
pkgrm -n -a ./tmsadmin gsk8cry64
```


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Actualizaciones de software

---

Las actualizaciones de software deben estar disponibles periódicamente mediante IBM® para su descarga.

Para obtener la información, las actualizaciones y los arreglos de mantenimiento más recientes, consulte el apartado IBM Support Portal for IBM Spectrum Protect.

 Sistemas operativos Windows

## Visión general de la instalación del cliente de copia de seguridad y archivado de Windows

---





Puede instalar el cliente de archivado y copia de seguridad IBM Spectrum Protect de Windows desde el soporte de instalación.

### Antes de empezar


---

Antes de empezar una instalación de cliente Windows, asegúrese de que el sistema en el que desea instalar el cliente cumple con los requisitos de cliente. A continuación, determine el tipo de instalación que necesita realizar y siga los pasos del procedimiento apropiado.


Para conocer los requisitos de hardware y software para el cliente, de Windows, consulte la nota técnica 1197133.

-  Sistemas operativos Windows Es posible que la instalación de cliente Windows necesite un rearranque. Como parte del proceso de instalación de cliente Windows, se instalan uno o varios paquetes redistribuibles de Microsoft C++, si aún no se han instalado en la estación de trabajo de Windows. Estos paquetes también se pueden actualizar de forma automática mediante el servicio de actualización de Windows. Si se actualizan los paquetes, la actualización puede hacer que el sistema rearranque cuando se inicie el programa de instalación de cliente Windows.
-  Sistemas operativos Windows Procedimientos de instalación. El procedimiento que debe seguir para instalar el cliente de copia de seguridad/archivado de Windows de IBM Spectrum Protect depende del tipo de instalación que desee realizar.
-  Sistemas operativos Windows Resolución de problemas durante la instalación de (Windows). Si desea realizar una actualización desde una versión anterior del cliente de copia de seguridad y archivado y hay servicios del cliente en ejecución (por ejemplo, aceptación de clientes o planificador), es posible que se muestre un error durante la instalación.
-  Sistemas operativos Windows Actualizaciones de software. Las actualizaciones de software deben estar disponibles periódicamente mediante IBM® para su descarga.

#### Conceptos relacionados:

 Sistemas operativos Windows Despliegue automático del cliente de copia de seguridad y archivado

#### Tareas relacionadas:

 Sistemas operativos Windows Creación y modificación del archivo de opciones del cliente

## Es posible que la instalación de cliente Windows necesite un rearranque

Como parte del proceso de instalación de cliente Windows, se instalan uno o varios paquetes redistribuibles de Microsoft C++, si aún no se han instalado en la estación de trabajo de Windows. Estos paquetes también se pueden actualizar de forma automática mediante el servicio de actualización de Windows. Si se actualizan los paquetes, la actualización puede hacer que el sistema rearranque cuando se inicie el programa de instalación de cliente Windows.

El rearranque, que se desencadena si se actualizan los paquetes redistribuibles C++, se puede producir incluso bajo cualquiera de las condiciones siguientes:

- Un despliegue automático de cliente fuerza una actualización del cliente en un nodo, y el cliente o planificador define la opción AUTODEPLOY=NOREBOOT.
- Se inicia una instalación o actualización manual del cliente.
- Se inicia una instalación silenciosa de cliente, incluso si se han establecido las opciones para suprimir solicitudes de rearranque y el propio rearranque de cliente.






De forma adicional, dado que el paquete redistribuible de Microsoft Visual Studio C++ es un componente Windows compartido, otras aplicaciones con dependencias en el paquete podrían ser detenidas o reiniciadas por Windows como parte de la instalación o actualización del paquete redistribuible de C++. Planifique las instalaciones y actualizaciones del cliente durante un periodo de mantenimiento en el que otras aplicaciones no se puedan ver afectadas si son detenidas o reiniciadas al instalar el paquete redistribuible C++. Supervise el resto de aplicaciones cuando se instale el cliente para comprobar si alguna aplicación se ha detenido o reiniciado.

## Procedimientos de instalación

El procedimiento que debe seguir para instalar el cliente de copia de seguridad/archivado de Windows de IBM Spectrum Protect depende del tipo de instalación que desee realizar.

Se proporcionan procedimientos para cada uno de los tipos de instalación siguientes:

Tipo de instalación	Descripción de instalación
Instalación del cliente Windows por primera vez	Describe cómo instalar el cliente de archivado y copia de seguridad de Windows por primera vez. Este procedimiento supone que el sistema Windows en el que está instalando el cliente no ha tenido nunca instalada una versión anterior del cliente.
Actualización del cliente Windows	Describe cómo actualizar una versión anterior del cliente de archivado y copia de seguridad de Windows a esta versión más reciente.
Reinstalación del cliente Windows	Describe cómo reinstalar el cliente de archivado y copia de seguridad de Windows si lo ha desinstalado.
Instalación silenciosa	Describe cómo instalar el cliente de archivado y copia de seguridad de Windows por primera vez sin interacción del usuario durante la instalación.
Reparación, modificación o desinstalación del cliente Windows	Describe cómo añadir o eliminar características de un cliente de archivado y copia de seguridad instalado (modificar), sustituir archivos dañados o claves de registro que faltan (reparar) o desinstalar el cliente de archivado y copia de seguridad Windows.

-  Sistemas operativos Windows Instalación del cliente Windows por primera vez  
Complete este procedimiento para instalar el cliente de archivado y copia de seguridad Windows por primera vez.
-  Sistemas operativos Windows Actualización del cliente Windows  
Puede actualizar una versión anterior del cliente de archivado y copia de seguridad IBM Spectrum Protect de Windows a la versión 8.1.2. Los valores de configuración anteriores se conservan, cuando es posible hacerlo. Sin embargo, las mejoras de la última versión del cliente pueden prohibir el uso o dejar obsoletas las opciones que estaban disponibles en versiones anteriores del cliente.
-  Sistemas operativos Windows Reinstalación del cliente Windows  
Si desinstala el cliente Windows de la versión 8.1.2, puede reinstalarlo si es necesario.
-  Sistemas operativos Windows Instalación silenciosa  
El programa de instalación del cliente de archivado y copia de seguridad admite instalaciones desatendidas y silenciosas.
-  Sistemas operativos Windows Modificación, reparación o desinstalación del cliente Windows  
Puede modificar, reparar o desinstalar un cliente Windows existente.

## Instalación del cliente Windows por primera vez

Complete este procedimiento para instalar el cliente de archivado y copia de seguridad Windows por primera vez.

### Antes de empezar

Si tiene una versión anterior del cliente de archivado y copia de seguridad de Windows ya instalada en un nodo y desea actualizarla a la versión 8.1.2, consulte Actualización del cliente Windows.

Importante: Debe conocer el nombre de host o la dirección IP del servidor de IBM Spectrum Protect, el número de puerto en el que el servidor escucha las comunicaciones de cliente y el método de comunicaciones a utilizar cuando el cliente se comunica con el servidor. Obtenga esta información del administrador del servidor de IBM Spectrum Protect antes de iniciar este procedimiento.

### Procedimiento

1. Descargue el archivo de paquete correspondiente de uno de los sitios web siguientes.
  - Descargue el paquete de cliente de Passport Advantage o de Fix Central.
  - Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.
2. Instale el producto utilizando el archivo de instalación comprimido descargado de Passport Advantage.
  - a. Copie el paquete de instalación comprimido descargado en un disco local o en una unidad compartida accesible por red. Asegúrese de extraer los archivos de instalación en un directorio vacío.
  - b. Para extraer los archivos de instalación en el mismo directorio, efectúe una doble pulsación en el paquete de instalación comprimido.
  - c. De forma predeterminada, los archivos no comprimidos se almacenan en la unidad de disco actual, en el directorio *directorio\_descarga*\TSMClient. Si el programa de instalación detecta archivos de otro intento de instalación de cliente en este directorio, se le solicitará que confirme si quiere sobrescribir los archivos anteriores. Si recibe esta solicitud, especifique **A** para sobrescribir los archivos existentes; esta selección garantiza que sólo se utilicen los archivos de la instalación actual.
  - d. Efectúe una doble pulsación en el archivo spinstall.exe para iniciar el programa de instalación de cliente.
3. Seleccione un idioma a utilizar para esta instalación y pulse Aceptar.
4. Si el asistente de instalación indica que se deben instalar uno o varios archivos redistribuibles de Microsoft C++, pulse Instalar. Estos archivos se necesitan para ejecutar el cliente Windows.
5. En la pantalla de bienvenida del cliente de IBM Spectrum Protect, pulse Siguiente para empezar a instalar el software de cliente.
6. Acepte el directorio de instalación predeterminado pulsando Siguiente o especifique un directorio de instalación diferente. El directorio de instalación predeterminado es C:\Archivos de programa\Tivoli\TSM.
7. Seleccione el tipo de instalación: Típica o Personalizada.

Opción	Descripción
<b>Típica</b>	Una instalación típica instala los siguientes componentes: <ul style="list-style-type: none"><li>○ Los archivos de la GUI del cliente de archivado y copia de seguridad (necesarios para utilizar la GUI de Java™)</li><li>○ El cliente de archivado y copia de seguridad de los archivos de la web del cliente (necesarios para utilizar el cliente web)</li><li>○ Los archivos de la API del cliente (que necesita el cliente y el sistema operativo)</li></ul>
<b>Personalizado</b>	Una instalación personalizada instala los mismos archivos que una instalación típica. Sin embargo, puede elegir instalar los componentes opcionales siguientes: <ul style="list-style-type: none"><li>○ Los archivos SDK de API (sólo necesarios si está desarrollando aplicaciones que funcionan con el cliente de archivado y copia de seguridad).</li><li>○ Los archivos de línea de mandatos de cliente administrativo (necesarios para ejecutar de forma remota las funciones de administrador en el servidor de IBM Spectrum Protect)</li></ul>

8. Pulse Siguiente y, a continuación, pulse Instalar.
9. Cuando el instalador complete la instalación, pulse Finalizar.
10. Verifique la instalación. Pulse Inicio > Todos los programas > IBM Spectrum Protect. Los componentes de cliente que ha instalado se muestran en la lista de programas iniciables de IBM Spectrum Protect. El cliente de línea de mandatos administrativo, el cliente de línea de mandatos de copia de seguridad y archivado y la GUI de copia de seguridad y archivado son los únicos componentes que se muestran en la lista. El cliente de línea de mandatos administrativo sólo aparece si realiza una instalación personalizada e incluye el cliente de línea de mandatos administrativo. Si ha instalado otros componentes, como el tiempo de ejecución de la API y SDK, no aparecerán en esta lista.
11. Pulse GUI de copia de seguridad y archivado para iniciar la GUI de cliente. Se inicia el Asistente de configuración de archivo de opciones de cliente. Pulse en Siguiente para iniciar el asistente.
12. En la pantalla Tarea de archivo de opciones, seleccione Crear un nuevo archivo de opciones y pulse Siguiente.

13. En la pantalla Nombre de nodo de cliente, especifique un nombre de nodo. Un nombre de nodo identifica de manera exclusiva el nodo en el servidor de IBM Spectrum Protect. El nombre de nodo predeterminado es el nombre de host abreviado del sistema Windows en el que está instalando el cliente. Acepte el nombre de nodo predeterminado o especifique un nombre de nodo nuevo. Pulse Siguiente.
14. En la pantalla IBM Spectrum Protect Client/Server Communications, especifique el método de comunicaciones que se utilizará cuando el cliente se comunique con el servidor y pulse Siguiente. Esta información se la debe proporcionar el administrador del servidor de IBM Spectrum Protect. Si no está seguro de qué debe seleccionar, acepte el valor predeterminado (TCP/IP). Si el valor predeterminado no funciona cuando el cliente intenta conectarse al servidor, póngase en contacto con el administrador de servidor para determinar qué método de comunicaciones se debe especificar.
15. En la pantalla Opciones de TCP/IP, especifique la información de puerto y dirección de servidor que le ha proporcionado el administrador de IBM Spectrum Protect. En el campo Dirección de servidor, especifique la dirección IP o el nombre de dominio completo del servidor de IBM Spectrum Protect. En el campo Número de puerto, especifique el número de puerto en el que el servidor escucha las comunicaciones de cliente. El número de puerto predeterminado es 1500. Pulse Siguiente.
16. La pantalla Lista de inclusión/exclusión recomendada contiene una lista de archivos y directorios de sistema que normalmente se incluyen o se excluyen de las operaciones de cliente. Normalmente los archivos excluidos no son necesarios para restaurar el sistema. Puede seleccionar o borrar todas las selecciones predeterminadas. Alternativamente, puede utilizar las teclas Mayús y Control para incluir objetos selectivamente. Para facilitar el proceso de instalación, pulse Seleccionar todo; puede añadir o eliminar archivos de la lista posteriormente, si necesita hacerlo. Pulse Siguiente.
17. La pantalla Selección de exclusión de archivo común proporciona una lista predeterminada de extensiones de archivo que puede excluir de las operaciones de cliente. Las extensiones de archivo que se proporcionan en esta lista son normalmente extensiones de archivos grandes, como gráficos o multimedia. Estos archivos consumen espacio en disco de servidor, pero no es posible que no sean necesarios para restaurar datos críticos. Pulse Seleccionar todo para excluir todas las extensiones de archivo predeterminadas. Alternativamente, puede utilizar las teclas Mayús y Control para elegir selectivamente qué extensiones se deben excluir de las operaciones de cliente. Pulse Borrar todo para borrar las extensiones que seleccionó. Puede modificar estas extensiones más tarde si lo desea. Pulse Siguiente.
18. La pantalla Dominios para copia de seguridad especifica los sistemas de archivos y objetos predeterminados que se deben incluir en las operaciones de cliente para las copias de seguridad incrementales y de imagen.
  - a. Para configurar los sistemas de archivos predeterminados para copias de seguridad incrementales, en el campo Tipo de copia de seguridad, seleccione Incremental. De forma predeterminada, está seleccionado Copia de seguridad de todos los sistemas de archivos locales. Si no desea hacer copia de seguridad de todos los sistemas de archivos locales como la acción predeterminada durante las copias de seguridad incrementales, borre esta opción y seleccione individualmente los sistemas de archivos que deben incluirse. Puede alterar temporalmente la selección predeterminada cuando inicie una operación de copia de seguridad incremental.
  - b. Para configurar los sistemas de archivos predeterminados para copias de seguridad de imagen, en el campo Tipo de copia de seguridad, seleccione Imagen. De forma predeterminada, está seleccionado Copia de seguridad de todos los sistemas de archivos locales. Si no desea hacer copia de seguridad de todos los sistemas de archivos locales como la acción predeterminada durante las copias de seguridad de imagen, borre esta opción y seleccione individualmente los sistemas de archivos que deben incluirse. Puede alterar temporalmente la selección predeterminada cuando inicie una operación de copia de seguridad de imagen.
  - c. Pulse Siguiente.
19. En la pantalla Confirmar y aplicar la configuración, pulse Aplicar. Es posible que se le solicite que introduzca un ID de usuario y una contraseña para iniciar la sesión en el servidor de IBM Spectrum Protect. El ID de usuario toma de forma predeterminada el nombre de nodo que ha especificado en el paso 13.
20. Puede aceptar el ID de usuario predeterminado o especificar un ID de usuario diferente. Especifique la contraseña que utilizará cuando inicie la sesión en el servidor. Pulse Iniciar sesión. Lo que sucede a continuación depende de si el servidor de IBM Spectrum Protect está configurado para el registro abierto o cerrado.


Opción	Descripción
<b>El servidor está configurado para inscripción abierta (servidor de IBM Spectrum Protect V8.1.1, V8.1.0, V7.1.7 o anterior)</b>	<p>La pantalla Registrar nodo nuevo le solicita información de contacto y le solicita de nuevo la contraseña.</p> <p>Se sugiere añadir texto en el campo Información de contacto, pero es opcional; especifique su nombre.</p> <p>Vuelva a entrar la contraseña, dos veces, en los dos campos Contraseña. Si la contraseña que especifica y confirma en estos campos Contraseña no coincide con la que ha especificado anteriormente en la pantalla Iniciar sesión en un servidor IBM Spectrum Protect, la contraseña que especifique y confirme aquí se convertirá en la necesaria para iniciar sesión en el servidor.</p> <p>Pulse Registrar para registrar este nodo en el servidor.</p> <p>Pulse Finalizar. La interfaz gráfica de usuario se abre y está lista para utilizarse. También puede iniciar cualquiera de los demás componentes de cliente instalado del menú Inicio.</p>



Opción	Descripción
<b>El servidor utiliza un registro cerrado</b>	<p>Pulse Finalizar. Proporcione la información que ha especificado en el asistente de configuración de cliente al administrador de servidor de IBM Spectrum Protect. Proporcione al administrador la información siguiente:</p> <ul style="list-style-type: none"> <li>○ El nombre de nodo que ha especificado.</li> <li>○ El ID de usuario y la contraseña que ha entrado.</li> <li>○ La información de contacto, por ejemplo el nombre, la dirección de correo electrónico y el número de teléfono, para que el administrador pueda ponerse en contacto cuando la información de nodo y usuario se haya registrado en el servidor.</li> </ul> <p>Una vez que el administrador haya registrado el nodo, podrá iniciar cualquiera de los componentes de cliente instalados desde el menú Inicio.</p>

**Conceptos relacionados:**

Resolución de problemas durante la instalación de (Windows)

 Sistemas operativos Windows

## Actualización del cliente Windows

Puede actualizar una versión anterior del cliente de archivado y copia de seguridad IBM Spectrum Protect de Windows a la versión 8.1.2. Los valores de configuración anteriores se conservan, cuando es posible hacerlo. Sin embargo, las mejoras de la última versión del cliente pueden prohibir el uso o dejar obsoletas las opciones que estaban disponibles en versiones anteriores del cliente.

### Antes de empezar

Espere a que se completen las tareas de cliente de archivado y copia de seguridad en curso (copia de seguridad, restauración, archivado, recuperación) antes de actualizar un nodo de cliente.

### Acerca de esta tarea

Para actualizar a la versión 8.1.2 del cliente Windows, instale la versión 8.1.2 del cliente Windows; no necesita desinstalar primero el software de cliente instalado anteriormente. El programa de instalación de cliente de la versión 8.1.2 conserva las opciones y valores de cliente actuales (en dsm.opt) y no sobrescribe o suprime los archivos dsmerror.log, dsmsched.log y dsmwebcl.log, si instala el nuevo cliente en el mismo directorio utilizado por la instalación anterior.

El componente de Logical Volume Snapshot Agent (LVSA) se ha sustituido en IBM Spectrum Protect versión 6.4. Si anteriormente tenía LVSA configurado como proveedor de instantáneas, instale el cliente de la versión 8.1.2 y, a continuación, configúrelo para utilizar Microsoft Volume Shadow Copy Service (VSS) como proveedor de instantáneas en la nueva instalación. Si se había instalado LVSA, el cliente rearrancará después de que se haya completado la instalación de actualización, para permitir la eliminación de entradas LVSA del registro.

El programa de instalación detiene los servicios de cliente que se ejecutan antes de actualizar el software de cliente. Si lo prefiere, puede detener manualmente los servicios utilizando el panel de control o la línea de mandatos. La Tabla 1 muestra los servicios que se pueden detener y los nombres que se deben buscar en la lista de Panel de control > Herramientas administrativas > Servicios, para poder detenerlos con el Panel de control. La tabla también proporciona los mandatos para detenerlos desde un indicador de mandatos o un script.

Nota: Los nombres de servicio que se muestran en la tabla son los nombres predeterminados establecidos por el programa de instalación. Puede cambiar algunos de estos nombres de servicio cuando configure los servicios utilizando uno de los asistentes de configuración de los menús Programas de utilidad > Asistente de configuración. Si cambia el nombre de servicio, anote el nombre que especifique y utilice el nombre para detener los servicios.

Tabla 1. Servicios detenibles

Nombre de visualización del panel de control	Procedimiento de línea de mandatos
Servicio de registro por diario de TSM	<code>net stop "tsm journal service"</code>
Aceptación de clientes de TSM	<code>net stop "tsm client acceptor"</code>
Planificador cliente de TSM	<code>net stop "tsm client scheduler"</code>
Agente de cliente remoto	<code>net stop "tsm remote client agent"</code>

Complete los pasos siguientes para actualizar una versión anterior del cliente de archivado y copia de seguridad de Windows a la versión 8.1.2:

### Procedimiento

1. Descargue el archivo de paquete correspondiente de uno de los sitios web siguientes.
  - Descargue el paquete de cliente de Passport Advantage o de Fix Central.
  - Para obtener la información más reciente, actualizaciones y arreglos de mantenimiento, vaya a IBM Support Portal.
2. Instale el producto utilizando el archivo de instalación comprimido descargado de Passport Advantage.
  - a. Copie el paquete de instalación comprimido descargado en un disco local o en una unidad compartida accesible por red. Asegúrese de extraer los archivos de instalación en un directorio vacío.
  - b. Para extraer los archivos de instalación en el mismo directorio, efectúe una doble pulsación en el paquete de instalación comprimido.
  - c. De forma predeterminada, los archivos no comprimidos se almacenan en la unidad de disco actual, en el directorio *directorio\_descarga*\TSMClient. Si el programa de instalación detecta archivos de otro intento de instalación de cliente en este directorio, se le solicitará que confirme si quiere sobrescribir los archivos anteriores. Si recibe esta solicitud, especifique **A** para sobrescribir los archivos existentes; esta selección garantiza que sólo se utilicen los archivos de la instalación actual.
  - d. Efectúe una doble pulsación en el archivo spinstall.exe para iniciar el programa de instalación de cliente.
3. Seleccione un idioma a utilizar para esta instalación y pulse Aceptar.
4. Si se le solicita que instale uno o más archivos redistribuibles de Microsoft C++, la solicitud indica que el nodo no tiene los archivos de C++ que son necesarios para el cliente de archivado y copia de seguridad de Windows. Pulse Instalar para instalar los archivos y continuar con la instalación de cliente o pulse Cancelar para finalizar el proceso de instalación.
5. Se inicia el programa de instalación del cliente de copia de seguridad y archivado. En la pantalla de bienvenida, pulse Siguiente para empezar a instalar el nuevo software de cliente.
6. Acepte o cambie el directorio de instalación predeterminado.
7. Seleccione el tipo de instalación: Típica o Personalizada.

Opción	Descripción
<b>Típica</b>	Una instalación típica instala los siguientes componentes: <ul style="list-style-type: none"> <li>○ Los archivos de la GUI del cliente de archivado y copia de seguridad (necesarios para utilizar la GUI de Java™)</li> <li>○ El cliente de archivado y copia de seguridad de los archivos de la web del cliente (necesarios para utilizar el cliente web)</li> <li>○ Los archivos de la API del cliente (que necesita el cliente y el sistema operativo)</li> </ul>
<b>Personalizado</b>	Una instalación personalizada instala los mismos archivos que una instalación típica. Sin embargo, puede elegir instalar los componentes opcionales siguientes: <ul style="list-style-type: none"> <li>○ Los archivos del SDK de la API. Estos archivos solo son necesarios si desarrolla aplicaciones que funcionan con el cliente de archivado y copia de seguridad.</li> <li>○ Los archivos de línea de mandatos del cliente administrativo. Estos archivos se necesitan si desea ejecutar las funciones de administrador en el servidor de IBM Spectrum Protect.</li> </ul>

8. Pulse Siguiente y, a continuación, pulse Instalar.
9. Cuando el instalador complete la instalación, pulse Finalizar.
10. Verifique la instalación. Pulse Inicio > Todos los programas > IBM Spectrum Protect. Los componentes de cliente que ha instalado se muestran en la lista de programas iniciables de IBM Spectrum Protect. Esta lista sólo incluye el cliente de línea de mandatos administrativo, el cliente de línea de mandatos de archivado y copia de seguridad o la GUI de archivado y copia de seguridad. Los restantes componentes instalables (los archivos de tiempo de ejecución de la API y SDK) no aparecen en esta lista.
11. Pulse la entrada GUI de archivado y copia de seguridad en la lista de programas que se pueden iniciar.
  - a. Cuando se le solicite, escriba el ID de usuario y la contraseña y pulse Iniciar sesión.
  - b. Cuando la GUI se haya iniciado, pulse Ayuda > Acerca de IBM Spectrum Protect. Verifique que la versión mostrada es la versión 8.1.2.

## Qué hacer a continuación


Los valores de configuración anteriores se conservan en el archivo dsm.opt. Si ha utilizado anteriormente LVSA como proveedor de instantáneas, se visualizan mensajes de aviso cuando se inicia el cliente de línea de mandatos. Los mensajes proporcionan instrucciones para editar el archivo dsm.opt y eliminar las opciones LVSA. No es necesario eliminar las opciones no utilizadas, pero la eliminación de opciones que no tienen ningún efecto o no se utilizan puede facilitar la resolución de problemas. Si está utilizando la GUI, los mensajes no se visualizan pero se registran en el archivo dsmerror.log, que está en el directorio de instalación de cliente, en el directorio baclient. Se emiten mensajes cuando se incluye cualquiera de las opciones siguientes en dsm.opt. Algunas de estas opciones son válidas para VSS y, si lo son, los mensajes sólo se visualizan y se registran si contienen parámetros específicos de LVSA.

- snapshotcachelocation
- snapshotfsidretries
- snapshotproviderimage
- snapshotproviderfs
- snapshotcachesize

Puede establecer opciones VSS en el separador Instantánea del Editor de preferencias. También pueden establecerse ejecutando los asistentes de configuración de soporte de imagen en línea y de soporte de archivo abierto. Para utilizar los asistentes, inicie la GUI y pulse Programas de utilidad > Asistente de configuración. Seleccione los asistentes que desea ejecutar, pulse Siguiente y siga las solicitudes para realizar las selecciones.

**Conceptos relacionados:**

Resolución de problemas durante la instalación de (Windows)

 Sistemas operativos Windows

## Reinstalación del cliente Windows

---

Si desinstala el cliente Windows de la versión 8.1.2, puede reinstalarlo si es necesario.

### Acerca de esta tarea

---

Si reinstala el cliente Windows en el mismo directorio donde está instalado anteriormente, el programa de instalación detecta la información de configuración anterior. Puesto que se detecta la información de configuración anterior, el proceso de instalación es igual que una instalación de actualización; siga los pasos de Actualización del cliente Windows para volver a instalar el cliente Windows.

Si no desea conservar la información de configuración anterior, puede eliminarla. Para obtener información sobre la eliminación exhaustiva de archivos y valores del cliente, consulte el artículo de IBM® developerWorks, [.How to completely remove the Backup-Archive client from Microsoft Windows](#)

Si elimina por completo todos los valores de configuración y posteriormente decide volver a instalar el cliente Windows, siga los pasos de Instalación del cliente Windows por primera vez. Éste es el procedimiento de instalación apropiado que debe seguir si reinstala el software en un directorio diferente o si reinstala el software en un sistema que no contiene información de configuración anterior.

 Sistemas operativos Windows

## Instalación silenciosa

---

El programa de instalación del cliente de archivado y copia de seguridad admite instalaciones desatendidas y silenciosas.

Nota: Los paquetes de redistribución de Microsoft Visual C++ 2010 y 2012 son necesarios para utilizar el cliente de archivado y copia de seguridad. El programa de instalación gráfico instala estos paquetes automáticamente. Si está realizando una instalación silenciosa del cliente utilizando MSIEXEC, debe instalar de forma separada los paquetes redistribuibles de Microsoft Visual C++ 2010 y 2012. Estos paquetes pueden instalarse antes o después de realizar la instalación silenciosa del cliente, pero deben estar instalados antes de utilizar el cliente de archivado y copia de seguridad.

Utilice los siguientes archivos ejecutables para instalar los paquetes redistribuibles de C++ 2010 y 2012. En las vías de acceso que se muestran, la serie de texto *dir* representa la unidad y el directorio donde ha guardado los archivos al extraerlos del paquete de instalación.

Archivos ejecutables de Windows para instalar paquetes de distribución de C++

*dir*\ISSetupPrerequisites\{270b0954-35ca-4324-bbc6-ba5db9072dad} (contiene MS 2010 x86 C++ Runtime - vcredist\_x86.exe)

*dir*\ISSetupPrerequisites\{BF2F04CD-3D1F-444e-8960-D08EBD285C3F} (contiene MS 2012 x86 C++ Runtime - vcredist\_x86.exe)

*dir*\ISSetupPrerequisites\{7f66a156-bc3b-479d-9703-65db354235cc} (contiene MS 2010 x64 C++ Runtime - vcredist\_x64.exe)

*dir*\ISSetupPrerequisites\{3A3AF437-A9CD-472f-9BC9-8EEDD7505A02} (contiene MS 2012 x64 C++ Runtime - vcredist\_x64.exe)

Para instalar un archivo *dsm.opt* predefinido (personalizado), utilice las siguientes instrucciones antes de comenzar la instalación silenciosa.

- Coloque la copia personalizada del archivo *dsm.opt* en el directorio ...\*CONFIG* que se encuentra en la imagen de instalación, por ejemplo:
  - C:\tsm\_images\TSMClient\Program Files 64\Tivoli\TSM\configEl archivo se debe llamar *dsm.opt*.
- El programa de instalación copia el archivo *dsm.opt* predefinido en el directorio ..\*BACLIENT* cuando se cumplen estas dos condiciones:
  - que NO exista el archivo *dsm.opt* en el directorio ..\*BACLIENT*. El programa de instalación no copia sobre un archivo *dsm.opt* existente.
  - *dsm.opt* existe en el directorio ..\*CONFIG* de la imagen de instalación, como se describió anteriormente.

Para instalar de forma silenciosa los paquetes redistribuibles C++ o el cliente de archivado y copia de seguridad, debe apagar el Control de cuentas de usuario (UAC).

Para desactivar el UAC, utilice el Panel de control de Windows o el programa de utilidad MSCONFIG.

- Para desactivar el UAC mediante el Panel de control, vaya al Panel de control y busque Valores de control de cuentas de usuario; defina el nivel de notificación en No notificar nunca.
- Para desactivar el UAC mediante el programa de utilidad MSCONFIG, abra una ventana de indicador de mandatos y escriba msconfig. Seleccione la herramienta de configuración del Control de cuenta de usuario y defina el nivel de notificación en No notificar nunca.

Tras instalar los redistribuibles C++ y el cliente Windows, recuerde activar el UAC.

La instalación de los redistribuibles C++ requieren privilegios elevados. Abra una ventana de indicador de mandatos del modo siguiente:

1. Pulse el menú Inicio > Todos los programas > Accesorios > Símbolo del sistema.
2. Pulse con el botón derecho del ratón sobre el icono Símbolo del sistema para ver las propiedades.
3. Seleccione Ejecutar como administrador.
4. Pulse Continuar en la ventana de permisos.
5. Comience la instalación del producto utilizando la ventana de indicador de mandatos.

Instalación silenciosa de los paquetes redistribuibles C++

Ejecute el siguiente mandato dos veces. Primero ejecútelo desde el directorio donde está almacenado el archivo vcredist\_x86.exe de C++ 2010. Después, vuelva a ejecutarlo desde el directorio donde está almacenado el archivo vcredist\_x86.exe de C++ 2012.

```
vcredist_x86.exe /install /quiet /norestart /log logfilename
```

Para obtener más información sobre el mandato vcredist\_x86.exe, ejecute el mandato siguiente:

```
vcredist_x86.exe /?
```

Ejecute el siguiente mandato dos veces. Primero ejecútelo desde el directorio donde está almacenado el archivo vcredist\_x64.exe de C++ 2010. Después, vuelva a ejecutarlo desde el directorio donde está almacenado el archivo vcredist\_x64.exe de C++ 2012.

```
vcredist_x64.exe /install /quiet /norestart /log logfilename
```

Para obtener más información sobre el mandato vcredist\_x86.exe, ejecute el mandato siguiente:

```
vcredist_x64.exe /?
```

Instale el cliente de archivado y copia de seguridad de Windows. UAC debe seguir desactivado. Si este no está desactivado, desactívelo ahora. Abra una ventana de indicador de mandatos con privilegios elevados.

1. Pulse el menú Inicio > Todos los programas > Accesorios > Símbolo del sistema.
2. Pulse con el botón derecho del ratón sobre el icono Símbolo del sistema para ver las propiedades.
3. Seleccione Ejecutar como administrador.
4. Pulse Continuar en la ventana de Permisos.
5. Comience la instalación silenciosa del cliente de archivado y copia de seguridad de Windows utilizando la ventana del indicador de mandatos. Utilice las siguientes instrucciones para realizar una instalación silenciosa del cliente y la API de Windows.

Instalación silenciosa del cliente Windows

Si incluye una versión personalizada del mandato msiexec (que llama al instalador de software de Microsoft) en un script o un archivo por lotes, podrá realizar instalaciones en varios sistemas que ejecuten Windows. A continuación se muestra un mandato de ejemplo para instalar el cliente de línea de mandatos de copia de seguridad y archivado, la GUI del cliente, el cliente web, la API y el cliente de línea de mandatos de administración. Puede que sea necesario personalizar este ejemplo para que el mandato se ejecute correctamente en el sistema que utiliza. Aunque el mandato ocupa físicamente varias líneas de esta página, se debe escribir en una sola línea de mandatos.

```
msiexec /i "Z:\tsm_images\TSMClient\IBM Tivoli Storage Manager Client.msi" RebootYesNo="No"
REBOOT="Suppress" ALLUSERS=1 INSTALLDIR="C:\Program Files\Tivoli\Tsm"
ADDLOCAL="BackupArchiveGUI,BackupArchiveWeb,Api64Runtime, AdministrativeCmd" TRANSFORMS=1033.mst
/qn /l*v "C:\log.txt"
```

Las descripciones de los parámetros de instalación silenciosa son los siguientes:

msiexec

Inicia el programa Microsoft Software Installer (MSI).

/i

Instala el paquete de origen especificado (sustituir por /x para desinstalar el paquete).

"Z:\tsm\_imagenes\TSMClient\IBM Tivoli Storage Manager Client.msi"

Especifica la vía de acceso completa al paquete de origen. En este ejemplo se muestra la unidad Z. Especifique la letra de unidad de la unidad de disco de su configuración que contiene la imagen de instalación.

RebootYesNo="No" REBOOT="Suppress"

En determinadas condiciones, puede ser necesario reiniciar el sistema para que la instalación se complete correctamente. Esta opción hace que el programa de instalación no reinicie el sistema si por otro lado existen factores que causarían el reinicio. Aunque esta opción resulta práctica, utilícela con precaución, pues la supresión del reinicio puede provocar que el programa se comporte de forma imprevisible. El caso más habitual en que es necesario un reinicio es el de una actualización de un cliente de copia de seguridad y archivado existente cuya instalación se realizó al tiempo que se ejecutaban los programas del cliente. Por lo tanto, cierre todos los programas y servicios del cliente de copia de seguridad y archivado antes de iniciar la instalación.

ALLUSERS=1

Especifica que el paquete es para todos los usuarios. Esta opción es obligatoria.

INSTALLDIR="C:\Program Files\Tivoli\TSM"

Especifica la vía de acceso de destino. Si ya se ha instalado este producto o una versión anterior del mismo en la estación de trabajo, utilice el directorio de instalación actual como vía de acceso de destino para este paquete.

ADDLOCAL="BackupArchiveGUI,BackupArchiveWeb,Api64Runtime"

Especifica las características que se van a instalar. Especifique todos los componentes en una sola línea entre comillas, separados por comas, sin espacios ni antes ni después de las comas. En la tabla siguiente se muestran las características instalables del cliente.

Funciones del cliente Windows	Descripción de la característica
BackupArchiveGUI	Interfaz gráfica de usuario
BackupArchiveWeb	Cliente web de archivado y copia de seguridad
Api64Runtime	Tiempo de ejecución de API
ApiSdk	SDK de la API
AdministrativeCmd	Línea de mandatos de administración

TRANSFORMS=1033.mst

Especifica la transformación de idioma que se debe utilizar. Existen las siguientes transformaciones de idioma:

Transformación	Idioma
1028.mst	CHT Chino tradicional
1029.mst	CSY Checo
1031.mst	DEU Alemán
1033.mst	ENG Inglés
1034.mst	ESP Español
1036.mst	FRA Francés
1038.mst	HUN Húngaro
1040.mst	ITA Italiano
1041.mst	JPN Japonés
1042.mst	KOR Coreano
1045.mst	PLK Polaco
1046.mst	PTB Portugués
1049.mst	RUS Ruso
2052.mst	CHS Chino simplificado

/qn

Especifica que la instalación se realizará de manera silenciosa.

/l\*v "C:\log.txt"

Especifica que las anotaciones serán detalladas así como el nombre y la ubicación del archivo de anotaciones.

El proceso de instalación crea la carpeta de IBM Spectrum Protect en la carpeta de programas del menú Inicio de Windows. Puede iniciar el cliente de copia de seguridad y archivado pulsando uno de los iconos de esta carpeta.

#### Conceptos relacionados:

Resolución de problemas durante la instalación de (Windows)

## Modificación, reparación o desinstalación del cliente Windows

Puede modificar, reparar o desinstalar un cliente Windows existente.

### Acerca de esta tarea

Utilice el panel de control de Windows para modificar, reparar o desinstalar el cliente Windows.

### Procedimiento

1. Pulse Inicio > Panel de control > Desinstalar un programa.
2. Seleccione IBM Spectrum Protect Client en la lista de programas instalados.
3. Seleccione la función que desee realizar: Reparar, Cambiar o Desinstalar.

Opción	Descripción
Reparar	<p>Espere a que se completen las tareas de cliente de archivado y copia de seguridad en curso antes de reparar el cliente Windows.</p> <p>Esta opción repara una instalación de cliente Windows existente. Si selecciona Reparar, se examinan los archivos instalados por el programa de instalación para determinar si se han corrompido de algún modo. Si se determina que un archivo está corrupto, la opción de reparación intenta sustituirlo desde la imagen de instalación guardada. La opción de reparación también repara iconos y atajos de programa dañados, archivos que faltan y claves de registro.</p>
Cambiar	<p>Espere a que se completen las tareas de cliente de archivado y copia de seguridad en curso antes de modificar el cliente Windows.</p> <p>Esta opción modifica una instalación existente. Si selecciona Cambiar, la siguiente pantalla que se visualiza muestra Modificar como la opción para cambiar programas instalados. Si ya ha instalado el cliente y necesita añadir o eliminar componentes, pulse Cambiar y seleccione Modificar. Elija el icono junto a la característica que desea instalar o eliminar y seleccione la acción apropiada en la lista desplegable. Por ejemplo, si ha seleccionado una instalación típica al instalar el cliente, los archivos de interfaz de línea de mandatos de cliente administrativo no se instalan. Si decide que un nodo necesita esta interfaz, seleccione el icono junto a Archivos de línea de mandatos de cliente administrativo y pulse la opción Esta característica se instalará en el disco duro local.</p> <p>Nota: Esta opción logra el mismo efecto que la actualización del cliente. La diferencia es que se eluden los pasos iniciales y el proceso de instalación empieza con el último tipo de instalación que ha seleccionado. Si desea cambiar el tipo de instalación, puede pulsar Atrás y seleccionar el nuevo tipo de instalación; a continuación complete la información a medida que se le solicite. Utilice la información proporcionada en 7 (empiece en el paso Actualización del cliente Windows) si tiene dudas acerca de una solicitud.</p>

<b>O p c i ó n</b>	<p><b>Descripción</b></p> <p><b>D</b> Espere a que se completen las tareas de cliente de archivado y copia de seguridad en curso antes de desinstalar el cliente Windows.</p> <p><b>e</b> Esta opción desinstala el programa de cliente Windows. No elimina ningún servicio de cliente. Tampoco suprime archivos de registro u otros elementos que se crearon al configurar o utilizar el cliente. La mayoría de estos artefactos permanecen en el directorio de instalación (directorio Archivos de programa\Tivoli\TSM), pero pueden existir en cualquier lugar del disco, según lo que haya elegido para el directorio de instalación y otras opciones. Esta opción tampoco elimina los archivos que se han copiado en el disco local si ha extraído los archivos de instalación de un archivo de distribución comprimido.</p> <p><b>s</b> Dejar estos artefactos en disco no es un problema si desea reinstalar el cliente en el futuro. Sin embargo, si quiere eliminar más a fondo los valores y archivos relacionados y de cliente, consulte el artículo de la wiki How to completely remove the Backup-Archive client from Microsoft Windows.</p> <p><b>i</b> El programa de instalación detiene los servicios de cliente que se están ejecutando antes de desinstalar el software. Si desea detener manualmente los servicios, escriba los siguientes mandatos en una ventana de indicador de mandatos:</p> <ul style="list-style-type: none"> <li>o net stop "tsm journal service"</li> <li>o net stop "tsm client acceptor"</li> <li>o net stop "tsm client scheduler"</li> <li>o net stop "tsm remote client agent"</li> </ul> <p><b>n</b> También puede utilizar el Panel de control para detener estos servicios. Los nombres de visualización de éstos coinciden con el nombre utilizado en la línea de mandatos.</p> <p>Nota: Los nombres de servicio mostrados aquí son los nombres predeterminados establecidos por el programa de instalación. Puede cambiar algunos de estos nombres de servicio cuando configure los servicios utilizando uno de los asistentes de configuración en los menús Programas de utilidad &gt; Asistente de configuración. Si cambia el nombre de servicio, anote el nombre que especifique y utilice el nombre para detener los servicios.</p> <p>Si desea eliminar alguno de estos servicios sin desinstalar el cliente, realice los pasos siguientes:</p> <ol style="list-style-type: none"> <li>a. Pulse Iniciar &gt; Todos los programas &gt; IBM Spectrum Protect &gt; GUI de archivado y copia de seguridad.</li> <li>b. Pulse Programas de utilidad &gt; Asistente de configuración.</li> <li>c. Seleccione y ejecute el asistente para cada servicio que desee eliminar. Las opciones de asistente de configuración también pueden eliminar la información de configuración para el soporte de imagen en línea y el soporte de archivo abierto.</li> </ol>
--	--

 Sistemas operativos Windows

## Resolución de problemas durante la instalación de (Windows)

Si desea realizar una actualización desde una versión anterior del cliente de copia de seguridad y archivado y hay servicios del cliente en ejecución (por ejemplo, aceptación de clientes o planificador), es posible que se muestre un error durante la instalación.

Si hay otros servicios de cliente de IBM Spectrum Protect en ejecución en cualquier cuenta, (por ejemplo Aceptador de cliente o Planificador), es posible que vea una solicitud para rearrancar el sistema durante la instalación. Debe detener todas las instancias del cliente de IBM Spectrum Protect en todas las cuentas antes de empezar la instalación.

Es posible que vea el siguiente error durante la instalación:

```
Error 1303. El programa de instalación no dispone de privilegios
suficientes para acceder a este directorio:
(Unidad de instalación):\Archivos de programa\Tivoli\TSM\baclient\plugins. La instalación
no puede continuar. Inicie la sesión como administrador o
póngase en contacto con el administrador del sistema.
```

Si este error se produce, debe detener la instalación. Después de detener el proceso de instalación, la versión anterior ya no estará instalada. Detenga los servicios del cliente y vuelva a intentar el proceso de instalación.

 Sistemas operativos Windows

## Actualizaciones de software

Las actualizaciones de software deben estar disponibles periódicamente mediante IBM® para su descarga.

Para obtener la información, las actualizaciones y los arreglos de mantenimiento más recientes, consulte el apartado IBM Support Portal for IBM Spectrum Protect.

 Sistemas operativos Linux  Sistemas operativos Windows

## Instalación del servicio de gestión de cliente para recopilar información de diagnóstico

---

Puede instalar los servicios de gestión de clientes de IBM Spectrum Protect para recopilar información de diagnóstico sobre el cliente de archivado y copia de seguridad. El servicio de gestión de cliente hace que la información esté disponible para IBM Spectrum Protect Operations Center, para poder realizar una supervisión básica.

### Acerca de esta tarea

---

Tras instalar el cliente de archivado y copia de seguridad, instale el servicio de gestión de cliente en el mismo equipo, para que el administrador de Servidor de IBM Spectrum Protect puede ver la información de diagnóstico desde el Centro de operaciones.

Para ver instrucciones de instalación y más información sobre el servicio de gestión de cliente, consulte el apartado Recopilación de información de diagnóstico con los servicios de gestión de clientes de IBM Spectrum Protect.

## Configuración de clientes de copia de seguridad/archivado

---

Puede configurar el cliente de archivado y copia de seguridad para utilizar muchas de las características de cliente disponibles. Se proporciona información para configurar los clientes de copia de seguridad/archivado.

- Configurar el cliente de IBM Spectrum Protect  
Tras instalar el cliente de copia de seguridad y archivado, debe configurarlo antes de empezar a llevar a cabo operaciones.
- Cómo empezar  
Antes de poder utilizar el cliente de archivado y copia de seguridad de IBM Spectrum Protect, debe aprender a iniciar una sesión en la GUI o en la línea de mandatos, y a iniciar el planificador de cliente automáticamente. También puede aprender otras tareas frecuentes.

#### Conceptos relacionados:

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

#### Tareas relacionadas:

Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad

Archivar y recuperar datos con clientes de archivado y copia de seguridad

Planificar operaciones para clientes de archivado y copia de seguridad





#### Referencia relacionada:


Opciones y mandatos del cliente de copia de seguridad/archivado

## Configurar el cliente de IBM Spectrum Protect






---

Tras instalar el cliente de copia de seguridad y archivado, debe configurarlo antes de empezar a llevar a cabo operaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si está actualizando el cliente de copia de seguridad y archivado, no es necesario volver a configurar el planificador, el cliente web u otros valores de configuración. Si los archivos dsm.opt y dsm.sys utilizados por la instalación del cliente anterior se encuentran en el directorio de instalación predeterminado, o en el directorio o archivo al que hacen referencia las variables de entorno DSM\_CONFIG y DSM\_DIR, el cliente accede a estos archivos para obtener información de configuración.



 Sistemas operativos Windows Si está actualizando el cliente de copia de seguridad y archivado, no es necesario volver a configurar el planificador, el cliente web u otros valores de configuración. Si el archivo dsm.opt utilizado por la instalación del cliente anterior se encuentran en el directorio de instalación predeterminado, o en el directorio o archivo al que hacen referencia las variables de entorno DSM\_CONFIG y DSM\_DIR, el cliente accede a este archivo para obtener información de configuración.

Algunas tareas de configuración son obligatorias mientras que otras son opcionales. Las siguientes tareas de configuración son obligatorias:














-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Creación y modificación del archivo opciones del sistema del cliente
-  Sistemas operativos Windows Creación y modificación del archivo de opciones del cliente
- Registrar la estación de trabajo en un servidor



Las siguientes tareas de configuración son opcionales:

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Creación de un archivo de opciones predeterminado de usuario-cliente
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Creación de un archivo de opciones del usuario cliente personalizado
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Variables de entorno
-  Sistemas operativos Windows Crear un archivo de opciones de directorio compartido
-  Sistemas operativos Windows Creación de varios archivos de opciones de cliente
-  Sistemas operativos Windows Variables de entorno
-  Sistemas operativos Windows Configuración del idioma para visualizar la GUI de Java
-  Sistemas operativos Windows Configuración del cliente web en sistemas Windows
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris
- Configuración del planificador
-  Sistemas operativos Windows Configuración del servicio de motor con registro por diario
-  Sistemas operativos Windows Configuración del soporte de copias de seguridad de imagen en línea
-  Sistemas operativos Windows Configuración del soporte de archivos abiertos
- Creación de una lista de inclusión/exclusión
-  Sistemas operativos Linux  Sistemas operativos Windows Configuración de copias de seguridad paralelas de máquinas virtuales VMware. Consulte Copias de seguridad paralelas de máquinas virtuales
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tareas de usuario root y autorizado del cliente de UNIX y Linux  
Un usuario autorizado es cualquier usuario no root con acceso de lectura y escritura a la contraseña almacenada (archivo TSM.sth) o cualquiera que conozca la contraseña y la indique de forma interactiva. Los usuarios autorizados utilizan la opción passworddir para definir el directorio en el que desean guardar su copia del archivo de contraseña.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Permitir que los usuarios no root gestionen sus propios datos  
Para permitir que usuarios no root utilicen el cliente de archivado y copia de seguridad para gestionar sus propios datos, el administrador del sistema debe realizar pasos adicionales a los pasos normales de configuración para configurar los usuarios autorizados por primera vez para usuarios no root.
- Descripción general del archivo de opciones de cliente  
Las opciones y valores del cliente se establecen (especifican) en un archivo de opciones de cliente. También puede definir opciones del cliente en un *conjunto de opciones de cliente* del servidor. Las opciones del cliente establecidas en un conjunto de opciones de cliente del servidor sustituyen a las opciones del cliente definidas en el archivo de opciones de cliente.
-  Sistemas operativos Windows Variables de entorno  
Normalmente, la definición de las variables de entorno es una tarea opcional. Si realiza esta definición, se recomienda que utilice la línea de mandatos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Variables de entorno  
Normalmente, la definición de las variables de entorno es una tarea opcional. Si define las variables, se recomienda que utilice la línea de mandatos.
-  Sistemas operativos Windows Configuración del idioma para visualizar la GUI de Java  
Puede seleccionar el idioma que desea utilizar para visualizar la GUI de Java del cliente de copia de seguridad y archivado.
- Descripción general de la configuración del cliente web  
El cliente web de IBM Spectrum Protect proporciona gestión remota de un nodo de cliente desde un navegador web. Los procedimientos para configurar el cliente web varían según el sistema operativo del nodo de cliente.
- Configuración del planificador  
El administrador de IBM Spectrum Protect puede planificar el cliente para que realice tareas automáticamente. Para sucesos planificados que deben producirse en el cliente, debe configurar el planificador del cliente para comunicarse con el servidor de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Iniciar el planificador cliente  
Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando la GUI y el cliente de la línea de mandato.
-  Sistemas operativos Windows Inicio del planificador cliente.  
Para iniciar el planificador del cliente, utilice el panel de control de servicios o el mandato **net start**.
- Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect a través de un cortafuegos  
En la mayoría de los casos, el servidor y los clientes de IBM Spectrum Protect pueden operar a través de un cortafuegos.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer  
Secure Sockets Layer (SSL) permite comunicaciones seguras estándar en el mercado basadas en SSL entre el cliente y el servidor de IBM Spectrum Protect.
-  Sistemas operativos AIX  Sistemas operativos Windows  Sistemas operativos Linux Configuración del sistema para copia de seguridad con registro por diario

Debe instalar y configurar el daemon de registro por diario (Linux) o el servicio de motor con registro por diario (Windows) antes de poder realizar copias de seguridad con registro por diario.

- Deduplicación de datos del lado del cliente  
La *eliminación de duplicados de datos* es un método de reducción de las necesidades de almacenamiento eliminando los datos redundantes.
- Configuración y uso de la migración tras error automática del cliente  
El cliente de archivado y copia de seguridad puede realizar la migración tras error automáticamente en un servidor secundario para recuperar los datos cuando el servidor de IBM Spectrum Protect no está disponible. Puede configurar el cliente para la migración tras error automática o evitar que el cliente migre tras el error. También puede determinar el estado de la réplica de sus datos en servidor secundario antes de restaurar o recuperar los datos replicados.
-  Sistemas operativos Linux  Sistemas operativos Windows Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack  
Antes de realizar una copia de seguridad o archivado de los datos del cliente de Tivoli Storage Manager FastBack, deberá completar las tareas de configuración.
-  Sistemas operativos Windows Configuración del cliente de copia de seguridad y archivado para proteger datos del cliente FastBack  
Puede configurar el cliente de copia de seguridad y archivado para proteger los datos del cliente FastBack mediante el asistente de configuración del cliente.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Configuración y utilización del entorno en clúster  
El término *clúster* tiene distintos significados en los distintos entornos. Puede significar alta disponibilidad, alto rendimiento, equilibrio de cargas, un entramado de sistemas informáticos o alguna combinación de estos términos.
-  Sistemas operativos Windows Configuración del cliente de copia de seguridad/archivado en un entorno de servidor en clúster  
Puede instalar localmente el software del cliente de copia de seguridad/archivado en cada nodo de un entorno de clúster de Microsoft Cluster Server (MSCS) o Veritas Cluster Server (VCS).
-  Sistemas operativos Windows Configuración del soporte de copias de seguridad de imagen en línea  
Si está configurada la característica de imagen en línea, el cliente de copia de seguridad y archivado realiza una copia de seguridad de imagen basada en instantánea durante la cual el volumen real queda disponible para las otras aplicaciones del sistema.
-  Sistemas operativos Windows Configuración del soporte de archivos abiertos  
Configure el Soporte de archivos abiertos (OFS) tras instalar el cliente de Windows.
-  Sistemas operativos AIX Consideraciones para la configuración de AIX antes de realizar copias de seguridad y archivado basadas en instantáneas  
Si está configurando el cliente de IBM Spectrum Protect de AIX para que realice copias de seguridad y archivado basadas en instantáneas, debe tener en cuenta algunos elementos.
-  Sistemas operativos Linux  Sistemas operativos Windows Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea  
Debe configurar información de la conexión del servidor de archivos de NetApp para ejecutar el mandato de copia de seguridad incremental de diferencia de instantánea en el cliente de copia de seguridad y archivado. Debe utilizar el mandato set password para especificar el nombre de host del sistema de archivos y el nombre de usuario que se utiliza para acceder al servidor de archivos.
- Registrar la estación de trabajo en un servidor  
Para poder utilizar IBM Spectrum Protect, es necesario configurar un nombre de nodo y una contraseña y el nodo debe registrarse con el servidor.
- Creación de una lista de inclusión/exclusión  
Si no crea una lista de inclusión/exclusión, el cliente de copia de seguridad y archivado tiene en cuenta todos los archivos para los servicios de copia de seguridad y utiliza la clase de gestión predeterminada para los servicios de copia de seguridad/archivado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Tareas de usuario root y autorizado del cliente de UNIX y Linux

Un usuario autorizado es cualquier usuario no root con acceso de lectura y escritura a la contraseña almacenada (archivo TSM.sth) o cualquiera que conozca la contraseña y la indique de forma interactiva. Los usuarios autorizados utilizan la opción passworddir para definir el directorio en el que desean guardar su copia del archivo de contraseña.

Tabla 1 muestra las tareas que puede y que no puede realizar el usuario root, los usuarios autorizados y los usuarios no autorizados.


Tabla 1. Tareas de usuarios root y usuarios autorizados


Tarea	Usuario root	Usuario autorizado
-------	--------------	--------------------

Tarea	Usuario root	Usuario autorizado
Iniciar sesión en un servidor de IBM Spectrum Protect utilizando un servidor LDAP para autenticar las credenciales .	Sí	Sí
Registrar nuevos nodos con el servidor IBM Spectrum Protect (si se ha definido el registro para que se abra en el servidor).	Sí	Sí
Definir o recrear la contraseña de IBM Spectrum Protect para estaciones de trabajo cliente	Sí	Sí
Copia seguridad	Sí Nota: El administrador de IBM Spectrum Protect puede especificar una opción en los mandatos Register Node o Update Node para especificar quién tiene permiso para realizar copia de seguridad de datos para un nodo. Definir BACKUPINITiation como root restringe las copias de seguridad de forma que solo los usuarios root o autorizados pueden realizar copias de seguridad de archivos en un nodo. El establecimiento de BACKUPINITiation en all permite a cualquier usuario realizar una copia de seguridad de datos en un nodo. Para obtener información sobre estos mandatos y opciones, consulte la documentación del servidor de IBM Spectrum Protect.	Sí, si dispone de permiso de lectura, independientemente de a quién pertenezca
Restore	Sí, cuando se restaura en la misma ubicación o en una nueva, se conservan los permisos y la propiedad de los archivos	Sí, pero el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. Cuando se restaura en la misma ubicación, se conservan los permisos y la propiedad de los archivos. Cuando se restaura en una ubicación distinta, se conservan los permisos de los archivos restaurados, pero cambia la propiedad a la del usuario actual.
Archive	Sí	Sí, si dispone de permiso de lectura, independientemente de a quién pertenezca

Tarea	Usuario root	Usuario autorizado
Realizar una recuperación	Sí. Cuando se recupera en una nueva ubicación o en la misma ubicación, se conservan los permisos y la propiedad de archivos.	Sí. Sin embargo, el sistema operativo impide que se grabe en la misma ubicación si el archivo solo tiene permiso de lectura. La propiedad de todos los objetos recuperados pasa al usuario actual.
Planificador cliente	Sí	Sí, si no utiliza el daemon de aceptador de cliente.  Tiene que ser usuario root para gestionar el daemon de aceptador de cliente. Los usuarios autorizados no root pueden utilizar el planificador (dsmc sched).
Conceder acceso a los archivos del servidor de IBM Spectrum Protect	Sí	Sí
Suprimir espacios de archivos del servidor de IBM Spectrum Protect	Sí, si el nodo dispone de autorización para suprimir copias de seguridad o archivadas otorgada por el administrador del servidor de IBM Spectrum Protect	Sí, si el nodo dispone de autorización para suprimir copias de seguridad o archivadas otorgada por el administrador del servidor de IBM Spectrum Protect

En sistemas Mac OS X, un administrador de sistema es cualquier usuario que tiene permiso para administrar el sistema. Puede comprobar el tipo de su cuenta mediante la herramienta Preferencias del sistema > Cuentas. Los administradores del sistema tienen un tipo de cuenta de Administrador.

 sistemas operativos Mac OS X El administrador del sistema es el encargado de configurar el cliente de copia de seguridad y archivado para que los que no son administradores puedan gestionar sus propios datos. Los usuarios que no son administradores (o usuarios no autorizados) cumplen los siguientes criterios:

 sistemas operativos Mac OS X

- No tienen un ID de usuario 0. No son el usuario root.
- Tienen una cuenta de usuario que no se ha configurado como administrador del sistema.






 sistemas operativos Mac OS X Cuando para completar una tarea se requiere una autorización adicional, debe utilizar la aplicación de autorizaciones para iniciar el cliente de archivado y copia de seguridad. Esto permite que el cliente se ejecute con los privilegios del sistema suficientes para completar la tarea. La tabla a continuación indica las herramientas de autorización que debe utilizar.

Tabla 2. Herramientas de autorización de Mac OS X y aplicaciones de IBM Spectrum Protect asociadas

Herramienta de autorización de Mac OS X	Aplicación de IBM Spectrum Protect asociada
IBM Spectrum Protect para administradores	IBM Spectrum Protect StartCad.sh StopCad.sh
sudo	dsmc

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

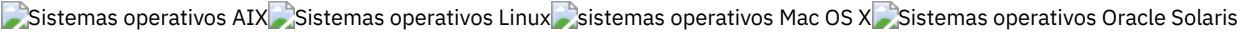
## Permitir que los usuarios no root gestionen sus propios datos

Para permitir que usuarios no root utilicen el cliente de archivado y copia de seguridad para gestionar sus propios datos, el administrador del sistema debe realizar pasos adicionales a los pasos normales de configuración para configurar los usuarios autorizados por primera vez para usuarios no root.

Además de los pasos normales de configuración, el administrador del sistema debe realizar los pasos siguientes para configurar los usuarios autorizados para usuarios no root:

1. Añada un stanza en el archivo de opciones del sistema, `dsm.sys`, para el usuario no root.
2. En esta stanza, utilice la opción `passwdidir` para que apunte a un directorio propiedad del usuario no root. A continuación, el usuario no root puede crear un archivo en este directorio `passwdidir`.
3. Asigne el usuario no root con un nombre de nodo exclusivo de TSM.
4. Asegúrese de que no exista en el directorio `passwdidir` un archivo `TSM.PWD` que no sea propiedad del usuario no root. Si existe dicho archivo, cambie la propiedad de este archivo al usuario no root o elimine el archivo.
5. Asegúrese de que los archivos `TSM.KDB`, `TSM.IDX` o `TSM.sth` que no sean propiedad del usuario no root no existan en el directorio `passwdidir`. Si dichos archivos existen, elimínelos.

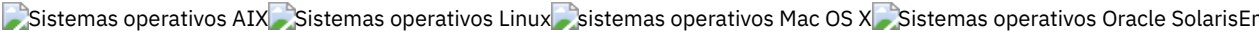
Cuando el administrador del sistema complete los pasos, el usuario no root deberá completar los pasos siguientes:

1. Cree un archivo de opciones del sistema del cliente, `dsm.opt`, y utilice la opción `servername` para especificar el nombre de stanza.
  2. Asegúrese de que el archivo `dsm.opt` lo pueda leer de forma predeterminada la variable del sistema `DSM_CONFIG`. Emita el mandato `export DSM_CONFIG=<dsm.opt>` desde una ventana de mandatos de shell para comprobarlo.
  3. Ejecute el mandato `dsmc q f` para utilizar los archivos de contraseñas a los que apunta la opción `passwdidir`. Si no existe ningún archivo de contraseña, se le solicitará al usuario.
-  **Habilitar el cifrado para usuarios cliente de copia de seguridad y archivado**  
Si configura el cliente de archivado y copia de seguridad para que cifre los datos durante las operaciones de archivado y copia de seguridad, y si especifica la opción de que se almacene la contraseña de la clave de cifrado (`encryptkey save`), de forma predeterminada sólo el usuario root y los usuarios autorizados de IBM Spectrum Protect pueden utilizar la contraseña almacenada para cifrar o descifrar archivos. Los usuarios autorizados incluyen usuarios no root que tienen acceso de lectura y escritura a la contraseña almacenada (archivo `TSM.sth`) o usuarios que conocen la contraseña y la especifican de forma interactiva.

## Descripción general del archivo de opciones de cliente

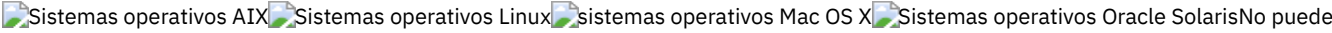
Las opciones y valores del cliente se establecen (especifican) en un archivo de opciones de cliente. También puede definir opciones del cliente en un *conjunto de opciones de cliente* del servidor. Las opciones del cliente establecidas en un conjunto de opciones de cliente del servidor sustituyen a las opciones del cliente definidas en el archivo de opciones de cliente.

 **En sistemas Windows, el archivo de opciones de cliente predeterminado se llama `dsm.opt`.**


 **En sistemas AIX, Linux, Mac y Solaris, el archivo de opciones de cliente predeterminado se denomina `dsm.opt`. Para estos sistemas operativos, dos archivos tienen opciones del cliente de archivado y copia de seguridad:**

- El archivo *opciones del usuario-cliente*. El nombre predeterminado para este archivo es `dsm.opt`. Por abreviar, este archivo se suele llamar *archivo de opciones de cliente*.
- El archivo *opciones sistema-cliente*. El nombre predeterminado para este archivo es `dsm.sys`. El archivo de opciones del sistema cliente es un archivo modificable donde se define el servidor y el método de comunicación, y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación. Por abreviar, este archivo se suele llamar *archivo de opciones del sistema*.

Puede crear varios archivos de opciones de cliente. Si su archivo de opciones de cliente no se llama `dsm.opt` o si `dsm.opt` no está en el directorio predeterminado, utilice la opción de cliente `OPTFILE` para indicar al cliente de archivado y copia de seguridad el archivo del que leer las opciones y parámetros, cuando se inicie el cliente de archivado y copia de seguridad.

 **No puede cambiar el nombre del archivo de opciones del sistema cliente. Se debe llamar `dsm.sys`.**

Puede utilizar una aplicación de edición de texto para editar directamente el archivo de opciones de cliente. También puede establecer opciones utilizando la GUI del cliente de archivado y copia de seguridad. En la GUI, seleccione `Editar > Preferencias` y utilice el editor de preferencias para establecer las opciones de cliente. Las opciones que establezca en el editor de preferencias se almacenan en el archivo de opciones de cliente. No todas las opciones del cliente se pueden establecer utilizando el Editor de preferencias.

 **Restricción:** Para Mac OS X, los archivos de opciones usuario-cliente y sistema-cliente deben ser archivos de texto sin formato, con codificación Unicode (UTF-8). De forma predeterminada, TextEdit no guarda los archivos como texto sin formato. Seleccione `Formato > Convertir en texto sin formato` para guardar los archivos como archivos de texto sin formato. Seleccione Unicode (UTF-8) en la lista desplegable `Codificación de texto sin formato`. No añada la extensión `.txt` cuando guarde el archivo.

Puede utilizar el mandato `query options` para visualizar todas o parte de las opciones y sus valores actuales. Este mandato acepta un argumento para poder especificar un subconjunto de opciones. El valor predeterminado consiste en visualizar todas las opciones.



Algunas opciones constan únicamente del nombre de la opción, como por ejemplo `verbose` y `quiet`. Puede especificar el nombre de opción completo o su abreviatura. Por ejemplo, puede especificar la opción `verbose` de alguna de las formas siguientes:


```
verbose
ve
```

Siga estas reglas cuando añada opciones a sus archivos de opciones:







- Puede anotar valores de opción añadiendo comentarios al archivo de opciones. Empiece cada comentario con un asterisco (\*) como primer carácter de la línea.
- No especifique opciones en una línea que contenga un comentario.
- Podría dar formato a las opciones con espacios o tabulaciones para que sea más sencillo ver las opciones y valores que especifique en el archivo.
- Especifique cada opción en una línea aparte y especifique todos los parámetros para una opción en la misma línea, según se muestra en los ejemplos siguientes:

```

 Sistemas operativos Linux  Sistemas operativos Oracle Solaris
domain /home /mfg /planning /mrkting /mgmt
domain / /Volumes/fs2 /Volumes/fs2 /Volumes/fs3 /Volumes/fs4


domain="c: d:"
domain="ALL-LOCAL -c: -systemstate"
```

- Para establecer una opción en este archivo, especifique el nombre de la opción y uno o varios espacios en blanco, seguidos del valor de la opción.
- Deje uno o más espacios en blanco entre los parámetros.
- La longitud de los nombres de vía de acceso y de archivo en los archivos de opciones de cliente no puede sobrepasar los límites siguientes:

-     En AIX, Mac OS y Solaris, la longitud máxima de un nombre de archivo es de 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.
-  En Linux, la longitud máxima para un nombre de archivo es de 255 bytes. La longitud máxima combinada de la vía de acceso y el nombre es de 4096 bytes. Este valor coincide con el de `PATH_MAX` soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación es el número de bytes de los componentes de vía de acceso y archivo, que puede corresponder o no a un número de caracteres igual.
-  En Windows, un nombre de archivo no puede tener más de 255 bytes. Los nombres de directorio, incluyendo el delimitador de directorio, también está limitado a 255 bytes. La longitud máxima combinada para un nombre de archivo y vía de acceso es de 5192 bytes. La representación Unicode de un carácter puede ocupar varios bytes, por ello puede que varíe el número máximo de caracteres que un archivo puede contener.


Los límites de vía de acceso de archivo y nombre de archivo se muestran en Tabla 1.

- Para operaciones de archivado o recuperación, la longitud máxima que puede especificar para un nombre de vía de acceso y archivo, es de 1024 bytes.

 Sistemas operativos Windows

Tabla 1. Límites de nombres y vía de accesos de archivos

Codificación MBCS	Límites de longitud de nombre de vía de acceso	Límites de longitud de nombre de archivo
1	5192 bytes	255 bytes
2	4092 bytes	127 bytes
3	2728 bytes	85 bytes

 En la tabla, la codificación MBCS tiene estos significados:

Latín básico


Los caracteres del idioma inglés de EE.UU. estándar, los números, símbolos y caracteres de control que se representan tradicionalmente en ASCII de 7 bits tienen una relación entre bytes y caracteres del 1:1.





Extensiones del latín
















Por ejemplo, los caracteres de latín con acentos graves o agudos, etc., al igual que los caracteres del griego, copto, cirílico, armenio, hebreo y árabe, generalmente tienen una relación entre bytes y caracteres del 2:1.

Chino, japonés, coreano, vietnamita

Estos caracteres y otros caracteres del idioma de Asia oriental generalmente tienen una relación entre bytes y caracteres del 3:1.

 Sistemas operativos Windows Si actualiza el archivo de opciones del cliente mientras hay activa una sesión, debe reiniciar la sesión para incorporar los cambios. Si utiliza el Asistente de configuración de GUI del cliente para realizar los cambios, éstos entrarán en vigor inmediatamente. Si no va a utilizar la Aceptación de clientes para gestionar el planificador, también deberá reiniciar el planificador.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si actualiza el archivo de opciones de usuario cliente mientras hay activa una sesión, debe reiniciar la sesión para incorporar los cambios.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Creación y modificación del archivo opciones del sistema del cliente  
El archivo opciones del sistema del cliente es un archivo modificable donde se define el servidor y el método de comunicación, y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación.
-  Sistemas operativos Windows Creación y modificación del archivo de opciones del cliente  
El archivo de opciones de cliente es un archivo de texto editable que contiene información sobre configuración del cliente de archivado y copia de seguridad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Creación de un archivo de opciones predeterminado de usuario-cliente  
Un archivo de opciones usuario-cliente almacena las opciones de procesamiento del cliente de archivado y copia de seguridad. Cuando instala el cliente de archivado y copia de seguridad, el programa de instalación del archivo de copia de seguridad coloca un archivo de opciones de usuario-cliente de ejemplo en el disco. Un usuario root o administrador del sistema puede editar este archivo para crear un archivo de opciones de cliente predeterminado, y hace que el archivo esté accesible a los usuarios de la estación de trabajo que utilicen el cliente de archivado y copia de seguridad. Los usuarios individuales pueden crear y utilizar su propio archivo de opciones de cliente.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Creación de un archivo de opciones del usuario cliente personalizado  
Si desea utilizar opciones diferentes de las especificadas en el archivo predeterminado de opciones del usuario cliente (dsm.opt), puede crear su propio archivo de opciones del usuario cliente.
-  Sistemas operativos Windows Crear un archivo de opciones de directorio compartido  
El administrador del servidor de IBM Spectrum Protect puede generar archivos de opciones de cliente en un directorio compartido.
-  Sistemas operativos Windows Creación de varios archivos de opciones de cliente  
Puede crear varios archivos de opciones de cliente si tiene que trabajar con distintos servidores o si ve que necesita varios conjuntos de parámetros para realizar tareas de copia de seguridad o archivado.

#### Referencia relacionada:

Optfile

Query Options

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Creación y modificación del archivo opciones del sistema del cliente


El archivo opciones del sistema del cliente es un archivo modificable donde se define el servidor y el método de comunicación, y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación.

### Acerca de esta tarea

La creación y modificación del archivo de opciones del sistema cliente (dsm.sys) es una tarea obligatoria.

La GUI del cliente de archivado y copia de seguridad ofrece un asistente de configuración que se puede utilizar para crear archivos de configuración básica y probar la conexión con el servidor de IBM Spectrum Protect. El asistente de configuración se inicia automáticamente si los archivos de configuración no se encuentran cuando se inicia la GUI. Si desea modificar los archivos de configuración una vez creados, pulse Asistente para la configuración en el menú Herramientas de la interfaz gráfica de usuario.


Si no utiliza el asistente para la configuración, podrá crear y modificar el archivo de opciones del cliente de forma manual.




 sistemas operativos Mac OS X En Mac OS X, copie el archivo dsm.sys.smp en dsm.sys de una de las siguientes ubicaciones. Las ubicaciones predeterminadas están enumeradas en el orden en el que se buscaron.

1. Una ubicación identificada por la variable de entorno DSM\_DIR
2. /Library/Application Support/tivoli/tsm/client/ba/bin/

### 3. /Library/Preferences/Tivoli Storage Manager/

El cliente utiliza el primer archivo de opciones que se encontró. Debe utilizar el nombre `dsm.sys` para este archivo. El archivo `dsm.sys` está controlado por el administrador del sistema.

 Sistemas operativos Oracle Solaris Para sistemas Oracle Solaris, no es necesario copiar `dsm.sys.smp` en `dsm.sys`. Los archivos de opciones del cliente (`dsm.opt` y `dsm.sys`) se crean automáticamente en `/usr/bin`, si aún no existen, y se enlazan al directorio de instalación del cliente cuando instala el cliente. Tenga en cuenta que los archivos no se eliminan si desinstala el cliente, por lo que debe reutilizar los valores si actualiza o reinstala el cliente.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux Para el resto de las plataformas, como el usuario `root`, copie el archivo `dsm.sys.smp` en `dsm.sys` y edite dicho archivo para configurar sus valores. El cliente buscará `dsm.sys` en el directorio especificado por la variable de entorno `DSM_DIR` (si está definida y exportada), y en el directorio de instalación.

Importante: Si va a realizar de nuevo la instalación y desea guardar el archivo `dsm.sys` tal cual está, no copie el archivo `dsm.sys.smp` en `dsm.sys`.




Utilice el archivo `dsm.sys` para especificar uno o más servidores con los que desea contactar para obtener servicios y las opciones de comunicación para cada servidor. Este archivo puede incluir opciones de autorización, opciones de proceso de copia de seguridad y archivado y de planificación.

Modifique el archivo `dsm.sys` para que incluya el servidor o los servidores con los que desea establecer contacto. A continuación, se muestra un ejemplo de una stanza de un archivo de opciones del sistema cliente que contiene las opciones necesarias para un servidor con el que desea que se pongan en contacto los usuarios. Puede especificar opciones para más de un servidor:

```
Servername          server_a
COMMMethod          TCPip
TCPPort             1500
TCPServeraddress    node.domain.company.com
```

Importante: Si desea utilizar el cliente web, debe especificar además la opción `passwordaccess=generate` e iniciar sesión con el cliente para guardar la contraseña.

Como valor predeterminado, el nodo cliente contacta con el primer servidor identificado en el archivo `dsm.sys`. Puede especificar un servidor diferente con el que contactar especificando la opción `servername` en el archivo de opciones del usuario cliente (`dsm.opt`) propio o especificando dicha opción con un mandato.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Además puede especificar en el archivo `dsm.sys` un servidor predeterminado y un servidor de migración (si ha instalado el cliente HSM en la estación de trabajo).

El archivo `dsm.sys` puede contener también las siguientes categorías de opciones:

- Opciones de comunicación
- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web

Puede modificar el archivo `dsm.sys` con uno de los siguientes métodos:

- En la ventana principal de la GUI de Java™ del cliente, seleccione `Edit > Client Preferences`.
- Utilice el editor de texto que prefiera.

 sistemas operativos Mac OS X Importante: En Mac OS X, el archivo de opciones del sistema debe ser un archivo de texto sin formato, codificado como Unicode (UTF-8). De forma predeterminada, TextEdit no guarda archivos como texto sin formato. Seleccione `Formato > Texto sin formato` para guardar el archivo de opciones del usuario como archivo de texto sin formato. Defina el Codificación del texto sin formato: en `Unicode (UTF-8)`. No añada la extensión `.txt`.

Si actualiza el archivo `dsm.sys` mientras el cliente esté en ejecución, deberá reiniciar la sesión para que los cambios entren en vigor.

#### Conceptos relacionados:

Descripción general del archivo de opciones de cliente

Opciones de proceso

#### Referencia relacionada:

Defaultserver

Passwordaccess



## Creación y modificación del archivo de opciones del cliente

El archivo de opciones de cliente es un archivo de texto editable que contiene información sobre configuración del cliente de archivado y copia de seguridad.

### Acerca de esta tarea

La primera vez que inicia la GUI del cliente de archivado y copia de seguridad de Windows, el programa de instalación busca un archivo de opciones de cliente existente, llamado `dsm.opt`. Si no se detecta este archivo, se inicia un asistente de configuración del archivo de opciones de cliente y se le solicita que especifique los valores de configuración del cliente iniciales. Una vez completado el asistente, se guarda la información especificada en el archivo `dsm.opt`. De forma predeterminada, el archivo `dsm.opt` se guarda en `C:\Archivos de programa\Tivoli\TSM\baclient`.

El archivo de opciones debe contener la siguiente información para comunicarse con el servidor:

- El nombre de host o dirección IP del servidor de IBM Spectrum Protect.
- El número de puerto que escucha el servidor para las comunicaciones con el cliente. El asistente de configuración del archivo de opciones de cliente configura un número de puerto predeterminado. A menos que su servidor esté configurado para escuchar un puerto diferente, no necesitará cambiar este número de puerto predeterminado.
- Su nombre de nodo de cliente. El nombre de nodo es un nombre que únicamente identifica a su nodo de cliente. El nombre de nodo predeterminado es el nombre de host abreviado del sistema en el que está instalado el cliente.

Puede especificar opciones de cliente adicionales según sea necesario.

Nota: También puede definir opciones del cliente en un *conjunto de opciones de cliente* del servidor. Las opciones del cliente definidas en un conjunto de opciones de cliente del servidor sustituyen a las opciones del cliente definidas en el archivo de opciones de cliente.

Al instalar el cliente de archivado y copia de seguridad, se copia un archivo de opciones de ejemplo en su disco. El archivo se denomina `dsm.smp`. De forma predeterminada, el archivo `dsm.smp` se copia en `C:\Archivos de programa\Tivoli\TSM\config`. Puede consultar el contenido de este archivo para ver ejemplos de diferentes opciones y saber cómo se especifican. El archivo también contiene comentarios que explican las convenciones de sintaxis para incluir listas, excluir listas y utilizar comodines. También puede utilizar este archivo como plantilla para su archivo de opciones de cliente editándolo y guardándolo como `dsm.opt` en el directorio `C:\Archivos de programa\Tivoli\TSM\baclient`.

Tras la creación inicial del archivo de opciones de cliente, puede modificar el mismo añadiendo o cambiando las opciones según sea necesario. Puede modificar el archivo `dsm.opt` de cualquiera de las formas siguientes:

- Ejecutando el asistente de configuración del archivo de opciones de cliente
- Utilizando el editor de preferencias del cliente
- Editando el archivo `dsm.opt` con un programa editor de texto, por ejemplo Notepad

Para modificar las opciones del cliente, siga los pasos indicados a continuación:

### Procedimiento

1. Seleccione un método para modificar el archivo.

Opción	Descripción
<b>Asistente para la instalación</b>	<ol style="list-style-type: none"><li>a. Pulse Iniciar &gt; Todos los programas &gt; IBM Spectrum Protect &gt; GUI de archivado y copia de seguridad.</li><li>b. Seleccione Programas de utilidad &gt; Asistente de configuración &gt; Ayuda para configurar el archivo de opciones del cliente. Cuando navega a través de los paneles del asistente se facilita texto en pantalla y ayuda en línea como orientación. Este asistente de configuración del archivo de opciones de cliente ofrece elecciones limitadas y configura solo las opciones más básicas.</li></ol>
<b>Editor de preferencias</b>	<ol style="list-style-type: none"><li>a. Pulse Iniciar &gt; Todos los programas &gt; IBM Spectrum Protect &gt; GUI de archivado y copia de seguridad.</li><li>b. Seleccione Editar &gt; Preferencias del cliente. Seleccione las pestañas del Editor de preferencias para definir las opciones del cliente. Especifique las opciones en los cuadros de diálogo, listas desplegadas y otros controles. Se facilita ayuda en línea. Pulse el icono de interrogación (?) para mostrar los temas de ayuda de la ayuda en línea de la pestaña que está editando. Puede definir más opciones en el Editor de preferencias que el asistente de configuración.</li></ol>

Opción	Descripción
<b>Editar el archivo dsm.opt</b>	<p>a. Edite el archivo dsm.opt utilizando un editor de texto sin formato. Todas las opciones se describen en detalle en la documentación de Consulta de opciones del cliente. Este método es el modo más versátil de definir las opciones del cliente, ya que con el asistente de configuración del archivo de opciones de cliente o el Editor de preferencias no se pueden definir todas las opciones.</p> <p>b. Para comentar un valor, inserte un asterisco (*) como primer carácter de la línea que desea comentar. Elimine el asterisco para que la opción comentada pase a estar activa.</p>

2. Guarde los cambios.

- a. Los cambios realizados en el asistente de configuración del archivo de opciones de cliente y el Editor de preferencias se guardan y son reconocidos por el cliente cuando se completa el asistente o sale de dicho editor.
- b. Si edita el archivo de opciones de cliente con un editor de texto mientras el cliente está en ejecución, debe guardar el archivo y reiniciar el cliente para que se detecten los cambios.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Creación de un archivo de opciones predeterminado de usuario-cliente

Un archivo de opciones usuario-cliente almacena las opciones de procesamiento del cliente de archivado y copia de seguridad. Cuando instala el cliente de archivado y copia de seguridad, el programa de instalación del archivo de copia de seguridad coloca un archivo de opciones de usuario-cliente de ejemplo en el disco. Un usuario root o administrador del sistema puede editar este archivo para crear un archivo de opciones de cliente predeterminado, y hace que el archivo esté accesible a los usuarios de la estación de trabajo que utilicen el cliente de archivado y copia de seguridad. Los usuarios individuales pueden crear y utilizar su propio archivo de opciones de cliente.

### Antes de empezar

Para completar este procedimiento, hay que ser root o administrador del sistema.

### Acerca de esta tarea

La creación de un archivo de opciones predeterminado de usuario-cliente es una tarea opcional.

De forma predeterminada, el archivo de opciones usuario-cliente se llama dsm.opt, y el archivo contiene los tipos de opción de cliente siguientes:

- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
- Opciones de formato
- Opciones de proceso de mandatos
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web

Para clientes Mac, el programa de instalación de cliente coloca un archivo de opciones de ejemplo de usuario-cliente llamado dsm.opt.smp en /Libraries/Preferences/Tivoli Storage Manager/. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opciones sistema-cliente de ejemplo (dsm.sys.smp).

Para clientes AIX y Linux, el programa de instalación de cliente coloca un archivo de muestra de opciones de usuario-cliente denominado dsm.opt.smp en el directorio de instalación de cliente predeterminado. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opciones sistema-cliente de ejemplo (dsm.sys.smp).

Para clientes Solaris de Oracle, el programa de instalación coloca el archivo de opciones usuario-cliente inicial llamado dsm.opt en el directorio /usr/bin. Este directorio es el mismo directorio en el que el programa de instalación coloca un archivo de opción sistema-cliente de muestra (dsm.sys).

Para todos los sistemas operativos de clientes, el procedimiento siguiente le indica cómo editar el archivo de opciones usuario-cliente de ejemplo y guardarlo con el nombre predeterminado, dsm.opt. Puede guardar el archivo con un nombre o vía de acceso distinto, si así lo prefiere, pero si cambia el nombre de archivo o si lo desplaza del directorio de instalación predeterminado, debe utilizar uno de los métodos siguientes para especificar la vía de acceso y el nombre del archivo de opciones usuario-cliente:

- Establezca la variable de entorno DSM\_CONFIG para indicar la vía de acceso y nombre de archivo del archivo de opciones usuario-cliente (dsm.opt). Establezca la variable de entorno DSM\_DIR para indicar la vía de acceso y nombre de archivo del

archivo de opciones sistema-cliente (dsm.sys). Para obtener más información sobre las variables de entorno, consulte Definir variables de entorno de proceso.

- Especifique la opción optfile del cliente de archivado y copia de seguridad para especificar la vía de acceso y nombre de archivo del archivo de opciones usuario-cliente.

Nota: Todos los usuarios del nodo deben tener acceso de lectura a la ubicación del disco en la que almacena el archivo de opciones usuario-cliente.

## Procedimiento

---

1. Acceda al directorio que contiene el archivo de opciones usuario-cliente de ejemplo.
2. Copie en archivo a dsm.opt.
3. Añada opciones para su nodo al archivo dsm.opt. Utilice uno de los métodos siguientes para establecer las opciones usuario-cliente:
  - Edite dsm.opt con un editor de texto para añadir las opciones necesarias en el nodo.  
Nota: En Mac OS X, el archivo dsm.opt se debe guardar como archivo de texto sin formato y utilizar Unicode (UTF-8) como esquema de codificación. De forma predeterminada, TextEdit no guarda los archivos como texto sin formato. Para guardar dsm.opt, en TextEdit, seleccione Formato > Crear texto sin formato. En la lista desplegable Codificación de texto sin formato, seleccione Unicode (UTF-8). No añada la extensión .txt al nombre de archivo.
  - Establezca las opciones de cliente utilizando el editor de preferencias. En la GUI del cliente de archivado y copia de seguridad, seleccione Editar > Preferencias del cliente y seleccione las opciones que quiera configurar. El editor de preferencias actualiza los archivos de configuración de cliente, dsm.opt y dsm.sys si añade, cambia o elimina opciones. Si actualiza el archivo dsm.opt mientras se ejecuta el cliente de archivado y copia de seguridad, debe reiniciar el cliente de archivado y copia de seguridad para que se reconozcan las actualizaciones.

El editor de preferencia utiliza la variable de entorno DSM\_DIR para localizar el archivo de opciones (dsm.sys) y la variable de entorno DSM\_CONFIG para localizar el archivo de opciones de usuario de cliente (dsm.opt). Si quiere que dsm.opt esté en una ubicación que no sea la predeterminada, establezca DSM\_CONFIG antes de iniciar el cliente de archivado y copia de seguridad y luego utilice el editor de preferencia para establecer las opciones. El editor de preferencias consulta al servidor cuáles son las opciones en el servidor pero no cambia el archivo de opciones del servidor.

### Conceptos relacionados:

Opciones de proceso

Definir variables de entorno de proceso

### Tareas relacionadas:

Creación y modificación del archivo opciones del sistema del cliente

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Creación de un archivo de opciones del usuario cliente personalizado

---

Si desea utilizar opciones diferentes de las especificadas en el archivo predeterminado de opciones del usuario cliente (dsm.opt), puede crear su propio archivo de opciones del usuario cliente.

### Acerca de esta tarea

---

Puede establecer todas las opciones que pueden definirse en el archivo predeterminado de opciones del usuario. La creación de un archivo de opciones del usuario cliente personalizado (dsm.opt) es una tarea opcional. Para crear o modificar un archivo de opciones del usuario cliente, utilice el siguiente método:

## Procedimiento

---

1. Póngase en contacto con el administrador de IBM Spectrum Protect de la estación de trabajo para determinar la ubicación del archivo de opciones del usuario cliente, dsm.opt.smp y para obtener la dirección TCP/IP del servidor de copia de seguridad al que se conectará y el puerto que está a la escucha.
2. Copie dsm.opt.smp en el directorio de inicio como dsm.opt o con un nombre de archivo nuevo de su elección. Almacene el archivo de opciones del usuario cliente en cualquier directorio para el que tenga acceso de grabación.
3. Establezca la variable de entorno DSM\_CONFIG para que apunte al nuevo archivo de opciones del usuario cliente.
4. Edite el archivo dsm.opt según proceda para su sistema o utilice el Editor de preferencias seleccionando Editar > Preferencias del cliente en la GUI del cliente de copia de seguridad y archivado.


## Resultados

---

Después de haber creado un archivo de opciones, puede realizar los siguientes pasos para editar el archivo de opciones desde la GUI.

1. Abra el menú Editar y seleccione Preferencias del cliente.

2. Realice los cambios necesarios y pulse en Aceptar para guardar estos cambios.

 sistemas operativos Mac OS X Importante: En Mac OS X, el archivo de opciones del sistema debe ser un archivo de texto sin formato, codificado como Unicode (UTF-8). De forma predeterminada, TextEdit no guarda archivos como texto sin formato. Seleccione Formato > Texto sin formato para guardar el archivo de opciones del usuario como archivo de texto sin formato. Defina la selección de la lista desplegable Codificación del texto sin formato en Unicode (UTF-8). No añada la extensión .txt.

#### Conceptos relacionados:

Variables de entorno

Descripción general del archivo de opciones de cliente

 Sistemas operativos Windows


## Crear un archivo de opciones de directorio compartido

---

El administrador del servidor de IBM Spectrum Protect puede generar archivos de opciones de cliente en un directorio compartido.

Los clientes de Windows pueden acceder al directorio compartido y utilizar los archivos que éste contiene para crear sus propios archivos de opciones de cliente.

La creación de un archivo de opciones de directorio compartido es una tarea opcional del usuario root o del usuario autorizado.

 Sistemas operativos Windows

## Creación de varios archivos de opciones de cliente

---

Puede crear varios archivos de opciones de cliente si tiene que trabajar con distintos servidores o si ve que necesita varios conjuntos de parámetros para realizar tareas de copia de seguridad o archivado.

### Acerca de esta tarea

---

Suponga que desea realizar copias de seguridad de sus archivos en un servidor (*server a*) y archivarlos en otro servidor (*server b*). En lugar de editar el archivo *dsm.opt* cada vez que desee conectarse a un servidor diferente, cree dos archivos de opciones. Por ejemplo, cree el archivo de opciones *a.opt* para *server a*, y *b.opt* para *server b*.

### Procedimiento

---

Puede utilizar uno de los siguientes métodos para especificar o utilizar un archivo de opciones de cliente distinto:

- Sustituya el archivo *dsm.opt* por el archivo de opciones adecuado antes de iniciar el cliente de archivado y copia de seguridad. Por ejemplo, emita los mandatos siguientes para copiar el archivo *a.opt* a *dsm.opt* y después inicie la GUI del cliente de archivado y copia de seguridad.

```
copy a.opt dsm.opt
dsm
```

- Inicie el cliente de archivado y copia de seguridad desde la línea de mandatos y utilice la opción *optfile* para especificar el archivo de opciones que desea utilizar. Por ejemplo:

```
dsm -optfile=b.opt
```

- Defina la variable de entorno *DSM\_CONFIG* para especificar el archivo de opciones que se debe utilizar antes de iniciar una sesión en el cliente de archivado y copia de seguridad. Por ejemplo:

```
SET DSM_CONFIG=C:\Archivos de programa\Tivoli\TSM\baclient\b.opt
```

### Qué hacer a continuación

---

Si se ejecuta el cliente de archivado y copia de seguridad desde la línea de mandatos, puede que también se tengan que configurar las variables de entorno *DSM\_DIR* y *DSM\_LOG*, tal como se indica a continuación:

- Defina la variable de entorno *DSM\_DIR* para que apunte al directorio en el que residen todos los demás archivos ejecutables:

```
SET DSM_DIR=C:\Archivos de programa\Tivoli\TSM\baclient
```

- Defina la variable de entorno *DSM\_LOG* para que apunte al directorio en el que reside *dsmerror.log*:

```
SET DSM_LOG=C:\Archivos de programa\Tivoli\TSM\baclient
```

Nota: La vía de acceso del directorio en el que se encuentran los archivos ejecutables del cliente debe incluirse en la variable de entorno PATH, o bien debe especificarse una vía de acceso completa.

 Sistemas operativos Windows

## Variables de entorno

---

Normalmente, la definición de las variables de entorno es una tarea opcional. Si realiza esta definición, se recomienda que utilice la línea de mandatos.

### Acerca de esta tarea

---

Debe definir las variables de entorno si la ejecución debe efectuarse en uno de los entornos siguientes:

- Desea invocar el cliente de copia de seguridad y archivado desde un directorio distinto del directorio de instalación del mismo.
- Desea especificar un archivo de opciones diferente para el cliente de copia de seguridad/archivado, el cliente de administración o ambos.

Nota: También puede especificar un archivo de opciones del cliente alternativo para el cliente de línea de mandatos (no el cliente de administración) mediante la opción **optfile**.

Debe definir cuatro variables de entorno:

PATH

Es la vía de acceso de búsqueda predeterminada que utiliza el sistema operativo para localizar archivos ejecutables. Defínala de manera que incluya las vías de acceso completas de los directorios de instalación del cliente.

DSM\_CONFIG

Establezca esta variable de entorno en la vía de acceso calificada al completo y el nombre del archivo de opciones de cliente.

DSM\_DIR

Defina esta variable de entorno en el directorio en el que se encuentra el archivo de mensajes de cliente dsc\*.txt.

DSM\_LOG

Establezca esta variable de entorno en el directorio en el que deberían residir los archivos de anotaciones.

Asegúrese de que las variables de entorno siguen estas pautas:

- Incluya el directorio en el que residen los archivos ejecutables (por ejemplo, dsm.exe) en la variable de entorno PATH actual. Si ha aceptado el directorio de instalación predeterminado mediante la unidad C:, puede establecer esto desde un indicador de mandatos de la manera siguiente:

```
SET PATH=C:\Archivos de programa\Tivoli\TSM\baclient
```

- Especifique el nombre de vía de acceso completa del archivo de opciones del cliente (dsm.opt) mediante la variable de entorno DSM\_CONFIG:





```
SET DSM_CONFIG=C:\Archivos de programa\Tivoli\TSM\baclient\dsm.opt
```

- Defina la variable de entorno DSM\_DIR de forma que haga referencia al directorio en el que se encuentra el archivo de mensajes de cliente dsc\*.txt:

```
SET DSM_DIR=C:\Archivos de programa\Tivoli\TSM\baclient
```

#### Referencia relacionada:









Optfile

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris













## Variables de entorno




---

Normalmente, la definición de las variables de entorno es una tarea opcional. Si define las variables, se recomienda que utilice la línea de mandatos.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Definir variables de entorno de idioma  
El cliente de copia de seguridad y archivado detecta automáticamente el idioma del entorno regional del sistema y muestra todo el programa en ese idioma.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Definir variables de entorno de proceso  
En determinadas circunstancias deberá establecer variables de entorno para garantizar que las aplicaciones de IBM Spectrum

Protect puedan localizar los archivos necesarios para realizar las operaciones del cliente y que las aplicaciones puedan crear archivos de registro que registren los sucesos y errores que se produzcan durante operaciones del cliente.

-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Definir variables de shell Bourne y Korn  
Especifique las variables de entorno del archivo `.profile` (shell Korn) o del archivo `.bash_profile` (shell Bourne) en el directorio `$HOME`.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Definir variables de shell C  
En el shell C, agregue las variables `DSM_CONFIG`, `DSM_LOG` y `DSM_DIR` al archivo `.cshrc` del directorio `$HOME`.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Definir variables de entorno de la API  
Si ha instalado la API de IBM Spectrum Protect, defina las siguientes variables de entorno.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Definir variables de entorno de idioma

---

El cliente de copia de seguridad y archivado detecta automáticamente el idioma del entorno regional del sistema y muestra todo el programa en ese idioma.

Por ejemplo, de forma predeterminada un sistema operativo francés mostrará el cliente de copia de seguridad y archivado en francés. Si el cliente de copia de seguridad y archivado no puede cargar el catálogo de mensajes en francés, toma como valor predeterminado el idioma inglés (Estados Unidos). Por ejemplo, si el cliente se ejecuta en una combinación de entorno regional e idioma no admitida, como por ejemplo Francés/Canadá o Español/México, el cliente tomará como valor predeterminado Inglés (Estados Unidos).

Puede utilizar la variable de entorno `LANG` para especificar el idioma para los clientes UNIX y Linux.

Nota: El entorno regional del sistema operativo, el juego de caracteres del terminal y la codificación del juego de caracteres de nombre de archivo deben coincidir para que puedan visualizarse o escribirse correctamente los nombres de archivo.

Para establecer la variable de entorno `LANG` en francés, escriba la sentencia siguiente:

```
export LANG=fr_FR
```

Nota:

- Esta tarea no se aplica a Mac OS X.
- Para visualizar los menús del navegador de ayuda de IBM Spectrum Protect en el entorno regional actual de idioma, asegúrese de que la variable de entorno `NLS_PATH` del archivo `/etc/profile` contiene la vía de acceso siguiente:

```
NLS_PATH=/usr/dt/lib/nls/msg/%L/%N.cat:$NLS_PATH
export NLS_PATH
```

Si el entorno local del cliente de copia de seguridad y archivado coincide con la codificación de caracteres de los nombres de archivo, la restauración o la copia de seguridad de todos esos archivos se realiza correctamente. Si utiliza un juego de caracteres de un solo byte (SBCS), todos los nombres de archivo serán válidos y el cliente de copia de seguridad/archivado los restaurará o realizará una copia de seguridad de los mismos.

Si utiliza un entorno local DBCS o UTF-8, los nombres de archivo compuestos por caracteres que no sean válidos en estos entornos, no podrán especificarse en la línea de mandatos del cliente de copia de seguridad y archivado. Estos archivos podrán pasarse por alto cuando se ejecute una copia de seguridad en la que se utilice la especificación de comodín (`"*"`). A continuación, se muestra un ejemplo del mensaje de error que se emite cuando se pasan por alto los archivos:

```
ANS4042E Object name '/testData/en_US_files/file3?'
contains one or more unrecognized characters and is not valid.
```

Si no todos los directorios y archivos se han creado con el mismo entorno regional, ejecute las copias de seguridad programadas en un entorno local de juego de caracteres de un solo byte. Esta acción asegura que no se omitan archivos porque el nombre de archivo contenga caracteres que no estén definidos en el entorno local actual. Al restaurar los archivos, hágalo en el entorno local que coincida con la codificación de entorno regional del nombre de archivo.

Por ejemplo, los nombres de archivo que consten de caracteres japoneses pueden contener caracteres de varios bytes no válidos si se visualizan en un entorno local chino. No se hará una copia de seguridad de estos archivos y tampoco se mostrarán en la interfaz gráfica de usuario. Si se encuentran estos archivos durante la copia de seguridad, el archivo `dsmerror.log` enumerará los archivos omitidos.

Consejo: Si utiliza la modalidad de planificación de cliente de copia de seguridad/archivado para realizar una copia de seguridad de todo un sistema, establezca la variable de entorno `LANG` en `en_US` (o en otro idioma SBCS) para evitar que no se omita ningún archivo.

 Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Definir variables de entorno de proceso

En determinadas circunstancias deberá establecer variables de entorno para garantizar que las aplicaciones de IBM Spectrum Protect puedan localizar los archivos necesarios para realizar las operaciones del cliente y que las aplicaciones puedan crear archivos de registro que registren los sucesos y errores que se produzcan durante operaciones del cliente.

Debe establecer las variables de entorno si se da cualquiera de las circunstancias siguientes:

- Desea invocar el cliente de copia de seguridad y archivado desde un directorio distinto del directorio de instalación del mismo.
- Desea especificar un archivo de opciones diferente para el cliente de copia de seguridad/archivado, el cliente de administración o ambos.
- Si no desea registrar los archivos que se van a grabar en el directorio de instalación predeterminado.

Consejo: También puede especificar un archivo de opciones del cliente alternativo para el cliente de línea de mandatos (no el cliente de administración) mediante la opción `optfile`.

Hay cuatro variables de entorno que puede ajustar que afectan al proceso del cliente de copia de seguridad y archivado:

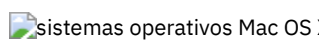
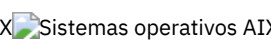
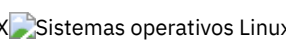
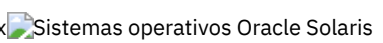
### PATH

Incluye el directorio en el que reside el archivo ejecutable para los ejecutables del cliente (`dsmc`, `dsmadmc`, `dsmj`).

### DSM\_DIR

Especifica el directorio en el que residen el archivo ejecutable para los ejecutables del cliente (`dsmc`, `dsmadmc`, `dsmj`) los archivos de recursos y el archivo `dsm.sys`. No puede especificar el directorio raíz (`/`) para `DSM_DIR`.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Cuando solicita una copia de seguridad de imagen, una copia de seguridad de archivos basada en instantáneas, una copia de seguridad NAS o una restauración NAS, el cliente utiliza la variable de entorno `DSM_DIR` para localizar la biblioteca de complementos correspondiente. Si no se establece `DSM_DIR`, el cliente busca la biblioteca de complementos en los siguientes directorios:

### AIX

`/usr/tivoli/tsm/client/ba/bin/plugins`

Oracle Solaris y todos los clientes Linux

`/opt/tivoli/tsm/client/ba/bin/plugins`

### DSM\_CONFIG

Especifica la vía de acceso calificada al completo y el nombre del archivo de opciones de usuario cliente para los usuarios que crean sus propios archivos de opciones personalizados. Si `DSM_CONFIG` no se ha establecido, o no se utiliza la opción `-optfile` del cliente, se espera que el archivo de opciones del usuario cliente cumpla estos requisitos:

1. El archivo de opciones debe denominarse `dsm.opt`.
2. Para clientes UNIX distintos de Mac OS X, si *no* se ha establecido `DSM_DIR`, el archivo debe residir en el directorio de instalación predeterminado. Si *sí* se ha establecido `DSM_DIR`, el directorio deberá residir en el directorio que especifica `DSM_DIR`.
3.  sistemas operativos Mac OS X Para Mac OS X, el archivo puede residir en cualquiera de las siguientes ubicaciones. Estos directorios se buscan en orden y se utiliza el primer archivo de opciones. `~/Library Preferences/Tivoli Storage Manager`, `/Library Preferences/Tivoli Storage Manager`, o `/Library/Application Support/tivoli/tsm/client/ba/bin`.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

### DSM\_LOG

Apunta al directorio en el que desea que residan los archivos de registro de IBM Spectrum Protect. No puede especificar el directorio raíz (`/`) para `DSM_LOG`. Los archivos de registro contienen información sobre los errores y sucesos que se producen durante el proceso. El cliente crea los registros para ayudar al equipo de soporte técnico a diagnosticar errores graves.

Consulte la sección de instalación relativa a su sistema operativo para obtener la información referente al directorio predeterminado de instalación.

Importante: Establezca la variable de entorno `DSM_LOG` para asignar el nombre de un directorio donde los permisos de lectura/grabación permitan el acceso de grabación necesario para que el usuario cree y grave información en el archivo de registro. Así se evitan anomalías en la grabación de anotaciones y terminaciones de procesos. Utilice los mandatos `chmod` o `setacl` para conceder permisos a los archivos de forma que todos los ID de usuario cliente puedan leer y grabar en ellos. Si los

nombres de las anotaciones son los nombres predeterminados, bastará con establecer la variable de entorno DSM\_LOG para que haga referencia al directorio en el que residen. Cuando el cliente no puede grabar en el archivo de anotaciones, se graba un mensaje de error en stderr y en el daemon syslog. El daemon syslog se debe estar ejecutando y debe estar configurado para procesar mensajes con una prioridad de LOG\_ERR para que el mensaje de error aparezca en las anotaciones del sistema. El inicio y la configuración del daemon syslog es propio de cada sistema. Utilice el mandato man syslogd para obtener información sobre cómo iniciar el daemon syslog. Utilice man syslog.conf para obtener información sobre cómo configurar el daemon syslog.

Nota:

1. Las opciones errorlogname y schedlogname alteran temporalmente la variable de entorno DSM\_LOG. Si especifica la opción del cliente errorlogname, el archivo se guarda en el directorio especificado por la opción errorlogname y no en la ubicación especificada por DSM\_LOG. Si especifica la opción de cliente schedlogname, se graba en el directorio especificado por la opción schedlogname y no en la ubicación especificada por DSM\_LOG.
2. Los archivos de anotaciones no pueden ser vínculos simbólicos. El cliente detecta los enlaces de este tipo, los suprime y, a continuación, sale de la operación. Esta acción evita que el cliente sobrescriba datos protegidos. Las anotaciones afectadas se crean en forma de archivos en una operación posterior.

Para utilizar programa de la GUI Java™ del cliente de archivado y copia de seguridad, tiene que exportar el directorio en el que haya instalado el archivo binario de Java. Por ejemplo, escriba el siguiente mandato:

```
export PATH=$PATH:java_bin_dir
```

donde: *java\_bin\_dir* es la vía de acceso del archivo binario de Java ejecutable en su sistema de archivos.

#### Referencia relacionada:

Optfile

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Definir variables de shell Bourne y Korn

---

Especifique las variables de entorno del archivo `.profile` (shell Korn) o del archivo `.bash_profile` (shell Bourne) en el directorio `$HOME`.

Lo siguiente es un ejemplo, en el que `/home/davehil/dsm.opt` es la vía de acceso y el nombre del archivo de opciones del usuario cliente y el directorio `/home/davehil` es la ubicación en la que desea almacenar el archivo `dsmerror.log`, el archivo ejecutable, los archivos de recursos y el archivo `dsm.sys`.

```
DSM_DIR=/home/davehil
DSM_CONFIG=/home/davehil/dsm.opt
DSM_LOG=/home/davehil
export DSM_DIR DSM_CONFIG DSM_LOG
```

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Definir variables de shell C

---

En el shell C, agregue las variables DSM\_CONFIG, DSM\_LOG y DSM\_DIR al archivo `.cshrc` del directorio `$HOME`.

Lo siguiente es un ejemplo, en el que `/home/davehil/dsm.opt` es la vía de acceso y el nombre del archivo de opciones del usuario cliente y el directorio `/home/davehil` es la ubicación en la que desea almacenar el archivo `dsmerror.log`, el archivo ejecutable, los archivos de recursos y el archivo `dsm.sys`.

```
setenv DSM_DIR /home/davehil
setenv DSM_CONFIG /home/davehil/dsm.opt
setenv DSM_LOG /home/davehil
```

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Definir variables de entorno de la API

---

Si ha instalado la API de IBM Spectrum Protect, defina las siguientes variables de entorno.

DSMI\_DIR

Hace referencia al directorio de instalación. El archivo `dsm.sys` debe residir en el directorio al que apunta DSMI\_DIR. Esta variable de entorno tiene que estar presente.

DSMI\_CONFIG

Nombre completo de vía de acceso del archivo de opciones de usuario de cliente propio (`dsm.opt`).

DSMI\_LOG




Vía de acceso para dsierror.log (esta vía de acceso no puede ser un enlace simbólico).

Nota: Los usuarios finales de las aplicaciones desarrolladas con la API pueden consultar las instrucciones de instalación de dicha aplicación para conocer los nombres de vía de acceso especiales u obtener directrices para las opciones.

Para obtener más información sobre las variables de entorno, consulte Definir variables de entorno de proceso.

Para obtener más información sobre la API de IBM Spectrum Protect, consulte Desarrollo de soluciones con la interfaz de programación de aplicaciones.

 Sistemas operativos Windows

## Configuración del idioma para visualizar la GUI de Java

---

Puede seleccionar el idioma que desea utilizar para visualizar la GUI de Java™ del cliente de copia de seguridad y archivado.

### Acerca de esta tarea

---

El idioma en el que se visualiza la GUI de Java del cliente de copia de seguridad y archivado viene determinado por el entorno local de visualización de Windows, no por el entorno local del sistema Windows. Por ejemplo, si el sistema Windows y el entorno local de entrada es el francés, pero el entorno local de visualización es el ruso, la GUI de Java se visualizará en ruso de forma predeterminada, si no se utiliza la opción idioma.

Si desea visualizar la GUI de Java en inglés de Estados Unidos o en otro idioma, puede modificar el idioma de visualización predeterminado mediante la opción language.

Consejo: La opción language no afecta al cliente web. El cliente web muestra sus mensajes en el idioma asociado al entorno local del navegador. Si el navegador se ejecuta en un entorno local no admitido por el cliente, el cliente web se visualizará en inglés de Estados Unidos.

### Procedimiento

---

Utilice uno de los siguientes métodos para configurar el idioma en el que se visualizará la GUI de Java:

- Añada la opción `language idioma` al archivo de opciones del cliente (`dsm.opt`). Por ejemplo, para establecer el idioma de visualización en inglés de EE.UU., añada la siguiente sentencia:

```
language enu
```

- Siga los pasos de la GUI de Java del cliente de copia de seguridad y archivado:
  1. En la ventana principal de la GUI de Java, pulse Editar > Preferencias del cliente.
  2. Pulse el separador Configuración regional.
  3. Pulse la lista desplegable Idioma y seleccione un idioma.
  4. Pulse en Aceptar.

#### Referencia relacionada:

Idioma


## Descripción general de la configuración del cliente web





---

El cliente web de IBM Spectrum Protect proporciona gestión remota de un nodo de cliente desde un navegador web. Los procedimientos para configurar el cliente web varían según el sistema operativo del nodo de cliente.

A partir de IBM Spectrum Protect Versión 8.1.2, ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior. Sin embargo, aún puede utilizar el cliente web para conectarse a servidores de IBM Spectrum Protect V8.1.1, V8.1.0 o V7.1.7 y anteriores. Para obtener más información, consulte Utilización del cliente web en el nuevo entorno de seguridad.






Las opciones de cliente de archivado y copia de seguridad se utilizan para configurar los valores del cliente web. Estas opciones incluyen `httpport`, `managedservices`, `webports` y `revokeremoteaccess`.

 Sistemas operativos Windows En los nodos de cliente Windows, se proporciona un asistente de configuración del cliente web en la GUI del cliente de archivado y copia de seguridad. Puede utilizar el asistente de configuración para configurar el cliente web. Las opciones que seleccione en el asistente se copian al archivo de opciones de usuario del cliente (`dsm.opt`). También puede añadir las opciones directamente al archivo `dsm.opt` editándolo y añadiéndolo las opciones del cliente web.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris En nodos de cliente AIX, Linux, Mac y Solaris, las opciones de cliente web se añaden al archivo de opciones client-systems (dsm.sys).

Para utilizar el cliente web desde la interfaz de IBM Spectrum Protect Operations Center, especifique la dirección del cliente web en el parámetro de la URL de REGISTER NODE o el mandato UPDATE NODE. La dirección web debe incluir el nombre de DNS o la dirección de IP del nodo, y el número de puerto que utiliza el cliente web. Por ejemplo, `http://node.example.com:1581`. Sustituya este nombre de host de ejemplo por la dirección IP o nombre de host de su nodo de cliente. Cuando acceda al cliente web utilizando un navegador web, especifique la misma sintaxis de URL en la barra de direcciones del explorador.





Todos los mensajes del cliente web se graban en el archivo de registro web, que se llama `dsmwebcl.log`. De forma predeterminada, el archivo `dsmwebcl.log` y el archivo de registro de errores del cliente de archivado y copia de seguridad (`dsmerror.log`) se crean en el directorio de instalación de cliente. Puede utilizar la variable de entorno `DSM_LOG` para sobrescribir las ubicaciones predeterminadas para los registros de errores. Si establece la variable de entorno `DSM_LOG`, no especifique el directorio raíz como la ubicación para los registros de errores. También puede utilizar la opción `errorlogname` del cliente de archivado y copia de seguridad para cambiar la ubicación del archivo de registro de errores. Si se especifica esta opción, sobrescribe el valor de la variable de entorno `DSM_LOG`.


-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris  
Para configurar el cliente web, edite el archivo de opciones del sistema cliente (`dsm.sys`) para especificar las opciones necesarias y, a continuación, inicie el daemon de aceptador de cliente.
-  Sistemas operativos Windows  
Configuración del cliente web en sistemas Windows  
En sistemas Windows, puede configurar e iniciar el cliente web utilizando un asistente que está disponible en la GUI del cliente de archivado y copia de seguridad, o mediante los mandatos de IBM Spectrum Protect y Windows.





#### Conceptos relacionados:

Opciones de cliente Web

#### Tareas relacionadas:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris

 Sistemas operativos Windows  
Configuración del cliente web en sistemas Windows

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Configuración del cliente web en sistemas AIX, Linux, Mac y Solaris


---

Para configurar el cliente web, edite el archivo de opciones del sistema cliente (`dsm.sys`) para especificar las opciones necesarias y, a continuación, inicie el daemon de aceptador de cliente.


### Procedimiento

---

1. Establezca las opciones siguientes en el archivo `dsm.sys`: `managedservices webclient schedule` y `passwordaccess generate`.
2. Genere la contraseña IBM Spectrum Protect. Especifique `dsmc query session`. Cuando se le pidan las credenciales, especifique el nombre de usuario y contraseña de IBM Spectrum Protect.

 Sistemas operativos Mac OS X En sistemas Mac OS X, también puede generar la contraseña utilizando la aplicación Herramientas de IBM Spectrum Protect para administradores. En la aplicación seleccione IBM Spectrum Protect para iniciar el cliente.

3. Inicie el daemon de aceptación de clientes. Especifique `dsmcad`.

 Sistemas operativos Mac OS X En Mac OS X, también puede iniciar el daemon de aceptador de cliente con la aplicación Herramientas de IBM Spectrum Protect para administradores. En la aplicación, seleccione Iniciar el daemon de aceptador de cliente.

4. Para acceder al cliente web desde un navegador, especifique el nombre de host o dirección IP del nodo de cliente en la barra de direcciones del navegador, seguido del número de puerto del cliente web. El número de puerto predeterminado es 1581. Por ejemplo, para acceder al cliente web en el nodo `myserver.example.com`, especifique: `http://myserver.example.com:1581`

Si debe cambiar el número de puerto del cliente web predeterminado, utilice la opción `httpport` del cliente de archivado y copia de seguridad para asignar un número de puerto distinto.

### Qué hacer a continuación

---

Tras configurar el cliente web, puede utilizar el IBM Spectrum Protect Operations Center o un navegador para hacer copia de seguridad y restaurar, o archivar y recuperar, datos de un nodo.

#### Conceptos relacionados:

Opciones de planificación

**Tareas relacionadas:**

Inicio de una sesión de cliente web

**Referencia relacionada:**

Httpport

Passwordaccess

 Sistemas operativos Windows

## Configuración del cliente web en sistemas Windows

En sistemas Windows, puede configurar e iniciar el cliente web utilizando un asistente que está disponible en la GUI del cliente de archivado y copia de seguridad, o mediante los mandatos de IBM Spectrum Protect y Windows.

### Procedimiento

Elija uno de los métodos siguientes para configurar el cliente web de Windows:

Método de configuración	Procedimiento
<b>Asistente para la instalación</b>	<p>a. Inicie la GUI del cliente de archivado y copia de seguridad.</p> <p>b. Pulse Programas de utilidad &gt; Asistente de configuración.</p> <p>c. Seleccione la casilla de verificación Ayuda para configurar el cliente web.</p> <p>d. Pulse NEXT y siga las instrucciones del asistente para configurar las opciones del cliente web.</p>
<b>Indicador de mandatos</b>	<p>a. Establezca las opciones siguientes en el archivo dsm.opt: managedservices webclient schedule y passwordaccess generate.</p> <p>b. Instale el servicio aceptador de cliente especificando el mandato siguiente:</p> <pre>dsmcutil install cad /name:"TSM CAD" /node:nodename /password:password /autostart:yes</pre> <p>donde:</p> <p><i>TSM CAD</i> es un nombre para el servicio. El nombre predeterminado es TSM Client Acceptor.</p> <p><i>nodename</i> es el nombre del nodo cliente.</p> <p><i>contraseña</i> es la contraseña de IBM Spectrum Protect.</p> <p><i>/autostart:yes</i> indica que el servicio aceptador de cliente se inicia cuando se inicia el sistema operativo.</p> <p>Inicie el servicio utilizando el mandato net start de Windows.</p> <p>c. Instale el servicio agente-cliente-remoto de IBM Spectrum Protect especificando el mandato siguiente:</p> <pre>dsmcutil install remoteagent /name:"TSM AGENT" /node:nodename /password:password /partnername:"TSM CAD"</pre> <p>donde:</p> <ul style="list-style-type: none"> <li>o <i>TSM AGENT</i> es un nombre para el servicio del agente-cliente-remoto. El nombre predeterminado de servicio es TSM Remote Client Agent.</li> <li>o <i>nodename</i> es el nombre del nodo cliente.</li> <li>o <i>contraseña</i> es la contraseña de IBM Spectrum Protect.</li> <li>o <i>TSM CAD</i> es el nombre del socio-servicio. Este nombre debe coincidir con el nombre de servicio que ha especificado cuando instaló el servicio aceptador de cliente. El nombre predeterminado es TSM Client Acceptor.</li> </ul> <p>No inicie el servicio TSM Remote Client Agent desde la vista Panel de control &gt; Herramientas administrativas &gt; Servicios, ni utilizando el mandato net start. El servicio aceptador de cliente inicia el agente de cliente remoto cuando lo necesite.</p>

## Qué hacer a continuación

Tras configurar el cliente web, puede utilizar el IBM Spectrum Protect Operations Center o un navegador para hacer copia de seguridad y restaurar, o archivar y recuperar, datos de un nodo.

### Conceptos relacionados:

Opciones de planificación

Opciones de cliente Web

### Tareas relacionadas:

Inicio de una sesión de cliente web

### Referencia relacionada:

Httpport

Passwordaccess






## Configuración del planificador

El administrador de IBM Spectrum Protect puede planificar el cliente para que realice tareas automáticamente. Para sucesos planificados que deben producirse en el cliente, debe configurar el planificador del cliente para comunicarse con el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

Por ejemplo, puede hacer copia de seguridad automáticamente al final de cada día o archivar algunos archivos cada viernes. Este procedimiento, que se conoce como planificación central, es un esfuerzo cooperativo entre el servidor y el nodo del cliente. El administrador asocia clientes con una o varias planificaciones que forman parte del dominio de políticas mantenidas en la base de datos del servidor. Cuando el administrador de IBM Spectrum Protect ha definido la planificación central en el servidor, ya puede iniciar el planificador cliente en la estación de trabajo. Después de iniciar el planificador de cliente, ya no es necesario volver a intervenir.

Con el planificador cliente, puede realizar las tareas siguientes:

- Visualizar información sobre las planificaciones disponibles.
- Visualizar información acerca del trabajo que ha completado la planificación.
-  Sistemas operativos Windows Modifique las opciones de planificación en el archivo de opciones del cliente (dsm.opt).
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Modifique las opciones de planificación en el archivo dsm.sys.

La forma más efectiva de gestionar el planificador de cliente es utilizar el servicio de aceptación de clientes. Puede obtener más información acerca de una comparación entre el aceptador de cliente y los servicios del planificador tradicional para gestionar el planificador. También puede aprender a configurar el cliente para que utilice el aceptador de cliente para gestionar el planificador.

- Comparación entre servicios gestionados por el aceptador de cliente y servicios del planificador tradicional  
Puede utilizar el servicio del aceptador de cliente o el servicio del planificador tradicionales para gestionar el planificador de IBM Spectrum Protect. Se suministra una comparación de estos métodos.
- Configuración del cliente para que utilice el servicio del aceptador de cliente para gestionar el planificador  
Una de las formas más efectivas de gestionar el planificador de cliente es utilizar el aceptador de clientes. Debe configurar el cliente para que utilice el aceptador de clientes para gestionar el planificador.






## Comparación entre servicios gestionados por el aceptador de cliente y servicios del planificador tradicional

Puede utilizar el servicio del aceptador de cliente o el servicio del planificador tradicionales para gestionar el planificador de IBM Spectrum Protect. Se suministra una comparación de estos métodos.

La siguiente tabla muestra las diferencias entre métodos de los servicios gestionados por el aceptador de cliente y los servicios del planificador tradicional predeterminados.

Tabla 1. Servicios gestionados por el aceptador de cliente frente a servicios del planificador tradicional

Servicios gestionados por el aceptador de cliente	Servicios del planificador tradicional de IBM Spectrum Protect
---	--

Servicios gestionados por el aceptador de cliente	Servicios del planificador tradicional de IBM Spectrum Protect
<p>Se definen utilizando la opción <code>managedservices schedule</code> y se inician con servicios del aceptador de cliente.</p> <p> Sistemas operativos AIX  Sistemas operativos Linux   sistemas operativos Mac OS X  Sistemas operativos Oracle SolarisEl daemon de aceptador de cliente se inicia con el mandato <code>dsmcad</code></p> <p> Sistemas operativos WindowsEl servicio del aceptador de cliente se inicia como un servicio Windows</p>	<p>Se inician con el mandato <code>dsmc sched</code>.</p>
<p>El servicio del aceptador de cliente inicia y detiene el proceso del planificador según resulta necesario para cada acción planificada.</p>	<p>Permanecen activos, incluso después de finalizar la copia de seguridad planificada.</p>
<p>Requiere menos recursos del sistema cuando está desocupado.</p>	<p>Requieren un mayor uso de los recursos del sistema cuando está desocupado.</p>
<p>Las opciones de cliente y las opciones de sustitución del servidor de IBM Spectrum Protect se renuevan cada vez que los servicios del aceptador de cliente inician una copia de seguridad planificada.</p>	<p>Las opciones de cliente y las opciones de sustitución del servidor de IBM Spectrum Protect sólo se procesan después de iniciar <code>dsmc sched</code>.</p>
<p>No pueden utilizarse con copias de seguridad <code>SESSIONINITiation=SERVEROnly</code>.</p>	<p>Debe reiniciar el proceso del planificador para que las opciones de cliente surtan efecto.  <b>Importante:</b> Si ejecuta el planificador del cliente en la línea de mandatos, el planificador no ejecuta el servicio en segundo plano.  <b>Consejo:</b> Reinicie el planificador tradicional de forma periódica para liberar los recursos del sistema que han utilizado previamente las llamadas del sistema.</p>

## Configuración del cliente para que utilice el servicio del aceptador de cliente para gestionar el planificador

Una de las formas más efectivas de gestionar el planificador de cliente es utilizar el aceptador de clientes. Debe configurar el cliente para que utilice el aceptador de clientes para gestionar el planificador.

### Antes de empezar





- Si incluye archivos para cifrado, asegúrese de que la opción `encryptkey` esté establecida en `save` en el archivo de opciones. Esta opción se define seleccionando Guardar contraseña de clave de cifrado localmente en la pestaña Autorización del editor de preferencia. Si establece esta opción, se habilitarán los servicios planificados desatendidos. Si no se ha guardado previamente la clave de cifrado, debe ejecutar una copia de seguridad atendida de al menos un archivo de forma que pueda obtener la solicitud de cifrado para guardar la clave.
- No puede utilizar el aceptador de clientes para realizar la planificación cuando la opción `sessioninitiation` esté establecida en `serveronly`.

### Acerca de esta tarea

El aceptador de clientes sirve de temporizador externo para el planificador. Al iniciar el planificador, éste realiza una consulta al servidor para saber si hay otro suceso planificado. El suceso se ejecuta de forma inmediata o el planificador se cierra. El aceptador de clientes reinicia el planificador cuando es el momento de ejecutar el suceso planificado. Esta acción reduce el número de procesos en segundo plano en la estación de trabajo y resuelve los problemas de retención de memoria que pueden ocurrir cuando el planificador se ejecuta sin la gestión del aceptador de clientes.

El servicio del aceptador de cliente también se conoce como daemon de aceptador de cliente.


### Procedimiento

-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Siga los siguientes pasos para utilizar el aceptador de clientes para gestionar el planificador de cliente:
  1. En la GUI del cliente de copia de seguridad y archivado, seleccione Editar > Preferencias.
  2. Pulse en la ficha Cliente Web.

3. En el campo Opciones de servicios gestionados, pulse Planificar. Si también desea que el aceptador de clientes gestione el cliente web, pulse la opción Ambos.
4. Inicie el daemon de aceptador de cliente ejecutando el siguiente mandato en la línea de mandatos:

```
dsmcad
```

**Consejo:**

- También puede utilizar la opción managedservices en el archivo de opciones de sistema del cliente (dsm.sys) para especificar si el aceptador de clientes debe gestionar el planificador.
- Si necesita el aceptador de clientes para gestionar el planificador en modalidad de sondeo sin abrir ningún puerto de escucha, utilice la opción cadlistenonport en el archivo dsm.sys.
-  **Sistemas operativos Windows** Siga los siguientes pasos para utilizar el aceptador de clientes para gestionar el planificador en el cliente de Windows:
  1. En la GUI del cliente de archivado y copia de seguridad, pulse Programas de utilidad > Asistente de configuración > Ayuda para configurar el planificador de cliente y pulse Siguiente.
  2. Lea la información de la página Asistente para el planificador y pulse Siguiente.
  3. En la página Tarea de planificador, seleccione Instalar un planificador nuevo o uno adicional y pulse Siguiente.
  4. En la página Nombre y ubicación del planificador, especifique un nombre para el servicio del aceptador de cliente que desea que gestione el planificador. A continuación, seleccione Utilizar el aceptador de cliente para gestionar el planificador y pulse Siguiente.
  5. Si ya se ha instalado el aceptador de clientes para que lo utilice el cliente web, seleccione dicho nombre del aceptador de clientes en la lista desplegable de la página Nombre de servicio web. Si no, escriba el nombre que desea asignar a este aceptador de clientes. El nombre predeterminado es TSM Client Acceptor. Pulse Siguiente.
  6. Siga las instrucciones en las pantallas que quedan para completar la configuración.

Utilice la siguiente información como ayuda para completar las páginas del asistente:

- Si la opción sessioninitiation está establecida en serveronly en el archivo de opciones de cliente (dsm.opt), el asistente de configuración del cliente y el servicio del planificador es posible que no puedan lanzar la autenticación con el servidor de IBM Spectrum Protect. Para evitar este problema, asegúrese de que la casilla de verificación Contactar con el servidor de IBM Spectrum Protect para validar la contraseña de la página de autenticación de IBM Spectrum Protect no esté seleccionada.
  - Para el planificador gestionado por el aceptador de clientes, seleccione Manualmente cuando inicie el servicio explícitamente en la página Opciones de inicio de sesión del servicio.
7. Inicie el servicio del aceptador de clientes desde el Panel de control de servicios, pero no inicie el servicio del planificador. El servicio del aceptador de clientes inicia y detiene automáticamente el servicio del planificador según resulta necesario.

**Consejo:**

- También puede utilizar la opción managedservices en el archivo de opciones de cliente (dsm.opt) para especificar si el aceptador de clientes debe gestionar el planificador.
- Si necesita el aceptador de clientes para gestionar el planificador en modalidad de sondeo sin abrir ningún puerto de escucha, utilice la opción cadlistenonport en el archivo dsm.opt.
- Si no desea utilizar el aceptador de clientes para gestionar el planificador, seleccione Automáticamente al arrancar Windows en la ventana Opciones de inicio de sesión del servicio. Este valor inicia automáticamente el servicio al arrancar Windows de forma que las planificaciones se ejecutan automáticamente. De forma alternativa, puede utilizar el Panel de control de servicios o el mandato net start para iniciar el servicio del planificador.
- También puede utilizar el programa de utilidad Configuración del servicio del planificador (dsmcutil.exe) para configurar el planificador. La herramienta de Configuración del servicio planificador debe ejecutarse desde una cuenta que pertenezca al grupo Administradores/ Administradores del dominio. Puede iniciar varios servicios de planificador cliente en el sistema.

**Conceptos relacionados:**

Descripción general de la configuración del cliente web

Activar o desactivar mandatos planificados

Opciones de planificación

**Tareas relacionadas:**




Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

**Referencia relacionada:**

Cadlistenonport





Managedservices


Sessioninitiation

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Iniciar el planificador cliente

Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando la GUI y el cliente de la línea de mandato.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Planificación de sucesos mediante el cliente de línea de mandatos  
Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando el cliente de línea de mandatos.

 Sistemas operativos Windows

## Inicio del planificador cliente.

---


Para iniciar el planificador del cliente, utilice el panel de control de servicios o el mandato **net start**.

### Acerca de esta tarea

---

Para evitar problemas, no ejecute el planificador cliente en la línea de mandatos. La línea de mandatos no ejecuta el planificador como un servicio en segundo plano.

Cuando inicie el planificador cliente, éste se ejecuta continuamente hasta que cierre la ventana, el sistema o la sesión del sistema. Si está ejecutando el servicio del planificador, el planificador se ejecutará hasta que se cierre el sistema o se detenga explícitamente utilizando el panel de control de servicios.

-  Sistemas operativos Windows Planificación de sucesos mediante la GUI  
Esta tarea le guía a través de los pasos necesarios para planificar sucesos utilizando la GUI.

#### Conceptos relacionados:

Opciones de proceso

## Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect a través de un cortafuegos

---

En la mayoría de los casos, el servidor y los clientes de IBM Spectrum Protect pueden operar a través de un cortafuegos.

### Acerca de esta tarea

---

Cada cortafuegos es distinto; por eso, es posible que el administrador del cortafuegos deba consultar las instrucciones del software o del hardware del cortafuegos que se utilice.

Hay dos métodos para permitir realizar operaciones de cliente y de servidor a través de un cortafuegos:

#### Método 1:

Para permitir que los clientes se comuniquen con un servidor a través de un cortafuegos, el administrador de cortafuegos debe abrir los siguientes puertos en el cortafuegos:

##### Puerto TCP/IP

Para habilitar el cliente de copia de seguridad/archivado, el cliente de administración de línea de mandatos y el planificador de modo que se ejecuten fuera de un cortafuegos, el administrador de cortafuegos debe abrir el puerto especificado por la opción del servidor **tcpport** (el valor predeterminado es 1500). Este puerto se establece en el cliente y en el servidor utilizando la opción **tcpport**. El valor debe ser el mismo en el cliente y en el servidor. Esto permite las comunicaciones del planificador de IBM Spectrum Protect tanto en modalidad de *sondeo* como en modalidad de *petición*, los planificadores gestionados por el cliente y las operaciones habituales del cliente de archivado y copia de seguridad.

**Nota:** el cliente no puede utilizar el puerto que especifica la opción **tcpadminport** (en el servidor) para una sesión del cliente. Ese puerto sólo puede utilizarse para las sesiones de administración.

##### Puerto HTTP

Para permitir que un cliente web se comuniquen con las estaciones de trabajo remotas a través de un cortafuegos, el puerto HTTP de la estación de trabajo remota debe estar abierto. Para especificar este puerto, utilice la opción **httpport** en el archivo de opciones del cliente de la estación de trabajo remota. El puerto HTTP predeterminado es 1581.

##### Puertos TCP/IP para la estación de trabajo remota

Los dos puertos TCP/IP para el cliente de la estación de trabajo remota deben estar abiertos. Utilice la opción **webports** en el archivo de opciones del cliente de la estación de trabajo remota para especificar estos puertos. Si no especifica los valores de la opción **webports**, el valor predeterminado, que es el cero (0), provoca que TCP/IP asigne aleatoriamente dos números de puerto libres.

Puerto TCP/IP para sesiones de administración

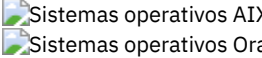


Especifica un número de puerto TCP/IP independiente en el que el servidor espera solicitudes de sesiones de cliente de administración, lo que permite sesiones de administración seguras dentro de una red privada.

## Método 2:

Para el planificador cliente en modalidad de solicitud, no es necesario abrir *ningún* puerto en el cortafuegos. Si establece la opción **sessioninitiation** en *serveronly*, el cliente no intentará establecer contacto con el servidor. *La planificación por solicitud de servidor inicia todas las sesiones* en el puerto que se ha definido en el cliente con la opción **tcpclientport**. La opción **sessioninitiation** sólo afecta al comportamiento del planificador cliente que se ejecuta en modalidad por solicitud.

El servidor de IBM Spectrum Protect debe establecer el parámetro SESSIONINITiation en los mandatos **register node** y **update node** para cada nodo. Si el servidor especifica SESSIONINITiation=*clientserver*, el valor predeterminado, el cliente puede decidir qué método utilizar. Si el servidor especifica SESSIONINITiation=*serveronly*, el servidor iniciará todas las sesiones.

Nota:

1. Si **sessioninitiation** se establece en *serveronly*, el valor de la opción de cliente **tcpclientaddress** debe ser igual al valor de la opción **HLAddress** del mandato de servidor **update node** o **register node**. El valor de la opción de cliente **tcpclientport** debe ser igual al valor de la opción **LLAddress** del mandato de servidor **update node** o **register node**.
2.  Si establece la opción **sessioninitiation** en *serveronly*, a excepción de los planificadores gestionados por el aceptador de cliente, el cliente de línea de mandatos, la GUI Java™ del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar las sesiones, pero se verán bloqueados por el servidor de IBM Spectrum Protect para nodos que tienen la opción **sessioninitiation** establecida en *serveronly*.
3.  Si establece la opción **sessioninitiation** en *serveronly*, a excepción de los planificadores gestionados por el aceptador de cliente, el cliente de línea de mandatos, la GUI del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar las sesiones, pero se verán bloqueados por el servidor de IBM Spectrum Protect para nodos que tienen la opción **sessioninitiation** establecida en *serveronly*.
4.  Si instala el planificador mediante el asistente para la configuración o **dsmcutil** y el servidor de IBM Spectrum Protect se encuentra detrás de un cortafuegos, la contraseña del nodo no se almacenan en la estación de trabajo del cliente. Como resultado de ello, es posible que el servicio del planificador no pueda autenticarse para el servidor cuando el servidor establece contacto con el cliente para ejecutar una planificación. En este caso, puede ejecutar el planificador desde la línea de mandatos (**dsmc schedule**), esperar a que se inicie una operación planificada y especificar la contraseña del nodo cuando se le solicite. Después de entrar la contraseña del nodo, reinicie el servicio del planificador. También puede utilizar el siguiente mandato **dsmcutil** para guardar la contraseña:

```
dsmcutil updatepw /node:nnn /password:ppp /validate:no
```

Si la opción **sessioninitiation** se establece en *serveronly* en el archivo de opciones de cliente (**dsm.opt**), el asistente para la instalación del cliente y el servicio del planificador no podrán iniciar la autenticación con el servidor de IBM Spectrum Protect. Para evitar este problema, cuando configure el planificador de cliente utilizando el asistente de configuración, asegúrese de que la casilla de verificación **Contactar con el servidor de IBM Spectrum Protect para validar la contraseña de la página de autenticación de IBM Spectrum Protect** no esté seleccionada.

Se puede producir un problema similar si se necesita una clave de cifrado para las operaciones de copia de seguridad. En este caso, puede ejecutar el planificador desde la línea de mandatos (**dsmc schedule**), esperar a que se inicie una copia de seguridad planificada y entrar la clave de cifrado cuando se le solicite. Después de actualizar la contraseña y la clave de cifrado, debe reiniciar el planificador.

5. Al configurar el planificador en una estación de trabajo cliente por primera vez, es posible que el servicio del planificador no pueda autenticarse para el servidor cuando el servidor establece contacto con el planificador cliente para ejecutar una planificación. Esto sucede cuando se establece **passwordaccess** para que se genere y el servidor de IBM Spectrum Protect está detrás de un cortafuegos y la contraseña cifrada no puede almacenarse localmente antes de iniciar el planificador. Para resolver este problema, es necesario ejecutar el planificador desde la línea de mandatos (**dsmc schedule**), esperar a que se inicie una operación planificada y entrar la contraseña del nodo cuando se le solicite.
6. el cliente no puede solicitar la contraseña de clave de cifrado en modalidad de planificador. Si utiliza el cifrado de datos de IBM Spectrum Protect, deberá ejecutar una copia de seguridad interactiva inicial una vez para establecer la clave de cifrado abriendo la conexión TCP/IP desde la estación de trabajo cliente hasta la estación de trabajo servidor. Consulte el **Método 1** para obtener más información acerca del establecimiento de esta comunicación. Después de haberse establecido la clave de cifrado, puede utilizar sesiones iniciadas por el servidor para realizar la copia de seguridad de los archivos utilizando el cifrado.

Si establece la opción **sessioninitiation** en *client*, el cliente inicia las sesiones con el servidor (**Método 1**) comunicándose en el puerto TCP/IP definido con la opción **tcpport** en *server*. Éste es el valor predeterminado. La planificación por solicitud de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.



Cuando se utilice IBM Spectrum Protect a través de un cortafuegos en la modalidad de *petición*, el servidor IBM Spectrum Protect debe contactar con el cliente. Para ello, puede que sea necesario instalar software en el servidor de IBM Spectrum Protect para direccionar la solicitud por medio del cortafuegos. Este software direcciona la solicitud del servidor a través de un puerto socks en el cortafuegos. Este método se suele denominar *activar la comunicación por socks* de un sistema. Los proxies no se admiten puesto que sólo direccionan algunos tipos de protocolos de comunicación (HTTP, FTP, GOPHER). Las comunicaciones de IBM Spectrum Protect no se direccionan mediante proxies. Es importante tener en cuenta que el cliente crea una nueva conexión con el servidor de IBM Spectrum Protect cuando se le solicita. Esto significa que debe emplearse la configuración del cortafuegos arriba mencionada.

**Tareas relacionadas:**

Configuración del planificador

**Referencia relacionada:**

Sessioninitiation

Tcpadminport

Tcpport

Webports

## Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer

---

Secure Sockets Layer (SSL) permite comunicaciones seguras estándar en el mercado basadas en SSL entre el cliente y el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

---

Los siguientes componentes del cliente admiten SSL:

- Cliente de la línea de mandatos
- Cliente de la línea de mandatos administrativo
- Interfaz gráfica de usuario de cliente
- API del cliente

Solo las conexiones de servidor/cliente de salida son compatibles con SSL. Un cliente V8.1.2 que se comunica con un servidor de nivel inferior soporta SSL. Un cliente V8.1.2 que se comunica con un servidor V8.1.2 debe utilizar SSL. Las conexiones de entrada (por ejemplo, aceptador de cliente, conexiones de planificación iniciadas por el servidor) no admiten SSL. Las comunicaciones cliente a cliente soportan SSL. Las interfaces gráficas de usuario web no soportan SSL. La interfaz gráfica de usuario web ya no se soporta en las comunicaciones con un servidor V8.1.2.

Cada servidor de IBM Spectrum Protect que esté habilitado para SSL debe tener un certificado exclusivo. El certificado puede ser de uno de los siguientes tipos:

- Un certificado autofirmado por IBM Spectrum Protect.
- Un certificado emitido por una entidad emisora de certificados (CA). La entidad emisora de certificados puede ser una empresa, como VeriSign o Thawte, o una entidad emisora de certificados interna, mantenida dentro de la empresa.

Siga los pasos que figuran a continuación para activar una comunicación SSL con un certificado autofirmado:

1. Obtener el certificado autofirmado del servidor de IBM Spectrum Protect (cert256.arm) Utilice el archivo del certificado cert.arm cuando el servidor no esté configurado para utilizar TLS (Transport Layer Security) 1.2; de lo contrario, utilice el archivo cert256.arm. El archivo del certificado del cliente debe ser el mismo que el archivo de certificado que utiliza el servidor.
2. Configure los clientes. Para poder utilizar SSL, cada cliente debe importar el certificado de servidor autofirmado.

Utilice el programa de utilidad dsmcert para importar el certificado.

3. En el caso de una recuperación tras desastre del servidor de IBM Spectrum Protect, si se ha perdido el certificado, el servidor generará de forma automática uno nuevo. Cada cliente deberá obtener e importar el nuevo certificado.

Para obtener detalles de la vía de acceso rápida entre un cliente V8.1.2 y un servidor V8.1.2, puede utilizar la opción SSLACCEPTCERTFROMSERV para aceptar automáticamente un certificado autofirmado. Consulte Valores de seguridad predeterminados para el cliente (vía de acceso rápida) para obtener más detalles.


Siga los pasos que figuran a continuación para activar una comunicación SSL con un certificado firmado por una entidad emisora de certificados:


1. Obtenga el certificado raíz de la entidad emisora de certificados.
2. Configure los clientes. Para poder utilizar SSL, cada cliente debe importar el certificado de servidor autofirmado.

Utilice el programa de utilidad dsmcert para importar el certificado.

Consejo: Después de completar este paso, si el servidor consigue un certificado nuevo firmado por el mismo CA, el cliente no necesita importar el certificado raíz de nuevo.

3. Si va a recuperar el cliente de copia de seguridad y archivado como parte de una recuperación tras desastre, deberá volver a instalar el certificado SSL en el servidor. Si se ha perdido el certificado, deberá obtener uno nuevo. No necesitará volver a configurar el cliente si el nuevo certificado ha sido firmado por una entidad emisora de certificados.

 Sistemas operativos Windows El programa de utilidad dsmcert lo proporciona el cliente de archivado y copia de seguridad y se instala automáticamente en C:\Archivos de programa\Tivoli\TSM\baclient.

 Sistemas operativos Windows Para poder configurar el certificado del servidor en el cliente, siga estos pasos:





1. Abra un indicador de mandatos y cambie el directorio por su directorio de cliente de copia de seguridad y archivado, por ejemplo:  
`cd "C:\Program Files\Tivoli\TSM\baclient"`
2. Añada la vía de acceso binaria del GSKit y la vía de acceso de acceso a biblioteca a la variable de entorno PATH; por ejemplo:


```
set PATH=C:\Archivos de programa\Common Files\Tivoli\TSM\api64\gsk8\bin\;  
C:\Archivos de programa\Common Files\Tivoli\TSM\api64\gsk8\lib64;%PATH%
```






Consulte Creación de un enlace simbólico para acceder a la última biblioteca GSKit y Códigos de retorno de IBM Global Security Kit para obtener detalles sobre las bibliotecas GSKit.

A continuación, debe importar el certificado de servidor o el certificado de la entidad emisora de certificados.

Si utiliza un certificado autofirmado

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Cada servidor de IBM Spectrum Protect genera su propio certificado. El certificado tiene el nombre de archivo fijo de cert.arm o cert256.arm. El archivo de certificado se almacena en la estación de trabajo del servidor en el directorio de instancias del servidor; por ejemplo, /opt/tivoli/tsm/server/bin/cert256.arm. Si el archivo de certificado no existe y especifica la opción de servidor SSLTCPPOINT o SSLTCPADMINPORT, el archivo de certificado se crea cuando inicia el servidor con este conjunto de opciones. Los servidores de IBM Spectrum Protect V6.3 (y versiones posteriores) generan archivos denominados cert256.arm y cert.arm. Los servidores anteriores a la V6.3 de IBM Spectrum Protect sólo generan archivos de certificado denominados cert.arm. Debe seleccionar el certificado que se define como el predeterminado en el servidor.

 Sistemas operativos Windows Cada servidor de IBM Spectrum Protect genera su propio certificado. El certificado tiene el nombre de archivo fijo de cert.arm o cert256.arm. El archivo de certificado se almacena en la estación de trabajo del servidor en el directorio de instancias del servidor; por ejemplo, C:\Archivos de programa\tivoli\tsm\server1\cert256.arm. Si el archivo de certificado no existe y especifica la opción de servidor SSLTCPPOINT o SSLTCPADMINPORT, el archivo de certificado se crea cuando inicia el servidor con este conjunto de opciones. Los servidores de IBM Spectrum Protect V6.3 (y versiones posteriores) generan archivos denominados cert256.arm y cert.arm. Los servidores anteriores a la V6.3 de IBM Spectrum Protect sólo generan archivos de certificado denominados cert.arm. Debe seleccionar el certificado que se define como el predeterminado en el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Realice estos pasos para configurar una conexión SSL en un servidor:

1. Obtenga el certificado del administrador de servidor.
2. Importe el certificado a la base de datos de claves de cliente utilizando el mandato siguiente:

```
dsmcert -add -server <servername> -file <path_to_cert256.arm>
```

Si utiliza un certificado de una entidad emisora de certificados

Si el certificado lo ha emitido una entidad emisora de certificados (CA), como VeriSign o Thawte, el cliente ya estará preparado para SSL y podrá omitir los pasos que figuran a continuación.

Para obtener una lista de los certificados de raíz instalados previamente desde las autoridades de certificados externos, consulte Certificados raíz de entidades emisoras de certificados.

Si el certificado no se ha emitido por una de las entidades emisoras de certificados más conocidas, siga estos pasos:









1. Obtenga el certificado raíz de la entidad emisora de certificados firmante.
2. Importe el certificado a la base de datos de claves de cliente utilizando el mandato siguiente:


```
dsmcert -add -server <servername> -file <path_to_cert256.arm>
```

Importante:

1. Se utiliza una contraseña pseudoaleatoria para cifrar la base de datos de claves. La contraseña se almacena automáticamente cifrada en el archivo stash (dsmcert.sth). El cliente de copia de seguridad y archivado utiliza el archivo stash para recuperar la contraseña de la base de datos de claves.
2. Se puede agregar más de un certificado de servidor al archivo de base de datos de claves del cliente para que el cliente se pueda conectar a distintos servidores. Además, se puede añadir más de un certificado raíz de entidad emisora de certificados a la base

de datos de claves del cliente.

3.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle SolarisSi no ejecuta los mandatos anteriores desde el directorio del cliente de copia de seguridad y archivado, tendrá que copiar `dsmcert.kdb` y `dsmcert.sth` en ese directorio.
4.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle SolarisDe forma predeterminada, los archivos de la base de datos de claves local tienen permisos y propiedades raíz y no los pueden leer otros usuarios. Si tiene previsto ejecutar el cliente como un usuario no root, tendrá que actualizar los permisos. Por ejemplo, para conceder acceso de lectura a todos los usuarios y grupos, ejecute el siguiente mandato:  

```
# chmod go+r dsmcert.*
```
5.  Sistemas operativos WindowsSi no ejecuta los mandatos anteriores desde el directorio del cliente de copia de seguridad y archivado, tendrá que copiar `dsmcert.kdb` y `dsmcert.sth` en ese directorio.
6. Por razones de rendimiento, utilice solo SSL para las sesiones en las que sea necesario. Un cliente V8.1.2 que se comunica con un servidor V8.1.2 debe utilizar SSL. SSL No (valor predeterminado) indica que el cifrado no se utiliza cuando se transfieren datos entre el cliente y el servidor en versiones anteriores a V8.1.2. Cuando el cliente se conecta a V8.1.2 o un servidor posterior, el valor predeterminado No indica que los datos de objeto no están cifrados. Toda la demás información se cifra, cuando el cliente se comunica con el servidor. Cuando el cliente se conecta a V8.1.2 o servidor posterior, el valor Yes indica que SSL se utiliza para cifrar toda la información, incluyendo los datos de objeto, cuando el cliente se comunica con el servidor. Plantéese la posibilidad de añadir recursos de procesador adicionales en el sistema servidor de IBM Spectrum Protect para gestionar la necesidad de más requisitos.
7. Para que un cliente se conecte a un servidor que está utilizando Transport Layer Security (TLS) versión 1.2, el algoritmo de la firma del certificado debe ser SHA-1 o más fuerte. Si utiliza un certificado autofirmado, debe utilizar el certificado `cert256.arm`. Es posible que el administrador de IBM Spectrum Protect necesite cambiar el certificado predeterminado en el servidor de IBM Spectrum Protect.

Detalles adicionales para un cliente V8.1.2 que se comunica con un servidor V8.1.1 y versiones V8 anteriores, y V7.1.7 y versiones anteriores.









Después de añadir el certificado de servidor a la base de datos de claves de cliente, añada la opción SSL Yes al archivo de opciones de cliente, y actualice el valor de la opción TCPSPORT. Es importante entender que el servidor normalmente se configura para conexiones SSL en un puerto distinto. En otras palabras, se abren dos puertos en el servidor:

1. Un puerto acepta conexiones de cliente no SSL regulares
2. El otro puerto acepta solamente conexiones SSL

No puede conectarse a un puerto no SSL con un cliente habilitado para SSL y a la inversa.

Si el valor de la opción `tcpport` es incorrecto, el cliente no se podrá conectar al servidor. Especifique el número de puerto correcto en la opción `tcpport`.

Para inhabilitar los protocolos de seguridad que son menos seguros que TLS 1.2, añada la opción `SSLDISABLELEGACYtls yes` al archivo de opciones de cliente o, en la GUI de Java™, seleccione el recuadro Requerir TLS 1.2 o superior en la pestaña Comunicación del Editor de preferencias. Requerir TLS 1,2 o superior ayuda a evitar ataques de programas maliciosos.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Creación de un enlace simbólico para acceder a la biblioteca de GSKit más reciente  
Puede crear un enlace simbólico que apunte el directorio donde está instalada la versión anterior de GSKit a la ubicación de las últimas bibliotecas GSKit del sistema.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Certificados raíz de entidades emisoras de certificados  
El cliente de archivado y copia de seguridad incluye una lista de certificados raíz para una cantidad determinada de autoridades de certificado.

#### Referencia relacionada:

Ssl  
Sslfipsmode

## Creación de un enlace simbólico para acceder a la biblioteca de GSKit más reciente

Puede crear un enlace simbólico que apunte el directorio donde está instalada la versión anterior de GSKit a la ubicación de las últimas bibliotecas GSKit del sistema.

### Acerca de esta tarea

Cuando instala DB2 para Linux, UNIX y Windows, en UNIX y Linux, también se instalan las bibliotecas GSKit locales. Estas bibliotecas se almacenan en <db2\_install\_path>/lib64/gskit\_db2 o <db2\_install\_path>/lib32/gskit\_db2. En Windows, la ubicación predeterminada es C:\Program Files\ibm\gsk8.

Durante la instalación de otros productos de IBM, como IBM Spectrum Protect, es posible que se instale otra copia de las bibliotecas GSKit. En función del producto, estas bibliotecas pueden ser bibliotecas GSKit locales o bibliotecas GSKit globales. Cuando en el mismo sistema se instala DB2 para Linux, UNIX y Windows y otro producto de IBM que incluya las bibliotecas GSKit, pueden surgir algunos problemas de interoperatividad. Estos problemas de interoperatividad pueden deberse a que GSKit solo permite bibliotecas de una única fuente de GSKit en cualquier proceso individual. Los problemas de interoperatividad pueden provocar comportamientos imprevisibles y errores de tiempo de ejecución.

Para asegurar que se utilice una única fuente de bibliotecas GSKit, se puede utilizar el método de enlace simbólico. Durante una instalación inicial de DB2 para Linux, UNIX, y Windows, el instalador crea un enlace simbólico <db2\_install\_path>/lib64/gskit o <db2\_install\_path>/lib32/gskit a <db2\_install\_path>/lib64/gskit\_db2 o <db2\_install\_path>/lib32/gskit\_db2. Estos enlaces simbólicos son las ubicaciones predeterminadas desde donde se cargan las bibliotecas GSKit. Los productos que incluyen DB2 para Linux, UNIX y Windows, y cambian el enlace simbólico del directorio predeterminado al directorio de biblioteca de otra copia de GSKit deben asegurarse de que el GSKit recién instalado esté al mismo nivel o posterior. Esta restricción se aplica a bibliotecas locales y globales. Durante una actualización de DB2 para Linux, UNIX y Windows, el enlace simbólico se mantiene. Si la copia recién instalada tiene un enlace simbólico a la ubicación predeterminada, se mantiene el enlace simbólico que está asociado a la copia de la instalación anterior. Si la copia recién creada no tiene un enlace simbólico a la ubicación predeterminada, se mantiene el enlace simbólico asociado a la copia de instalación más reciente.

Existen algunas limitaciones, ya que el enlace simbólico <db2\_install\_path>/lib64/gskit o <db2\_install\_path>/lib32/gskit es la vía de acceso de la copia de instalación de DB2 para Linux, UNIX y Windows. Por ejemplo, si se han creado dos o más instancias para cualquier copia de DB2, los cambios en el enlace simbólico afectan a todas las instancias.

También puede modificar un GSKit de servidor Domino de modo similar. Un servidor Domino no tiene una carpeta GSKit, pero tiene carpetas C y N, y una biblioteca libgsk8iccs\_64.so. Primero puede crear enlaces dinámicos para estas carpetas, y archivos que apunten a las carpetas correspondientes en el paquete de GSKit, donde está instalado el cliente de copia de seguridad/archivado IBM Spectrum Protect V8.1.2, del siguiente modo:

- In -s /usr/local/ibm/gsk8\_64/lib64/C /opt/ibm/lotus/notes/90010/zlinux
- In -s /usr/local/ibm/gsk8\_64/lib64/N /opt/ibm/lotus/notes/90010/zlinux
- In -s /usr/local/ibm/gsk8\_64/lib64/libgsk8iccs\_64.so /opt/ibm/lotus/notes/90010/zlinux

A continuación, cambie la contraseña del nodo DPD a domdsmc CHANGEADSMpwd tvt1054\_domnote2 tvt1054\_domnote2. Finalmente, ejecute domdsmc query adsm.

## Procedimiento

1. Cree un enlace simbólico en Windows, si tiene privilegios de administrador. Cambie el nombre de la copia de GSKit de DB2 del directorio lib64 que se encuentra en la ubicación predeterminada, C:\Program Files\ibm\gsk8. Inicie un shell DOS, vaya a la ubicación de GSKit de DB2 y cambie el nombre del directorio como se indica a continuación:





```
cd C:\Program Files\ibm\gsk8  
  
rename lib64 lib64-db2
```

2. Cree un enlace simbólico en la ubicación de la copia de GSKit de DB2 que apunte a la ubicación de la copia de GSKit de TSM ejecutando los siguientes mandatos en el shell DOS. Vaya a la ubicación de la copia de GSKit de DB2 y cree el enlace simbólico como se indica a continuación:

```
cd C:\Program Files\ibm\gsk8  
  
mklink /d lib64 "c:\Program Files\Common Files\Tivoli\TSM\api64\gsk8\lib64"
```

3. Reinicie DB2 para aplicar los cambios. Al volver a iniciar, DB2 cargará GSKit desde la nueva ubicación, que apunta a la copia IBM Spectrum Protect de GSKit. En el indicador de mandatos de DB2, escriba estos mandatos tal y como se indica a continuación:

```
db2stop  
  
db2start
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows




## Certificados raíz de entidades emisoras de certificados

El cliente de archivado y copia de seguridad incluye una lista de certificados raíz para una cantidad determinada de autoridades de certificado.

La siguiente es una lista de certificados raíz para varias autoridades de certificado que se entregan con el cliente:




- Entrust.net Global Secure Server Certification Authority
- Entrust.net Global Client Certification Authority
- Entrust.net Client Certification Authority
- Entrust.net Certification Authority (2048)
- Entrust.net Secure Server Certification Authority
- VeriSign Class 3 Public Primary Certification Authority
- VeriSign Class 2 Public Primary Certification Authority
- VeriSign Class 1 Public Primary Certification Authority
- VeriSign Class 4 Public Primary Certification Authority - G2
- VeriSign Class 3 Public Primary Certification Authority - G2
- VeriSign Class 2 Public Primary Certification Authority - G2
- VeriSign Class 1 Public Primary Certification Authority - G2
- VeriSign Class 4 Public Primary Certification Authority - G3
- VeriSign Class 3 Public Primary Certification Authority - G3
- VeriSign Class 2 Public Primary Certification Authority - G3
- VeriSign Class 1 Public Primary Certification Authority - G3
- Thawte Personal Premium CA
- Thawte Personal Freemail CA
- Thawte Personal Basic CA
- Thawte Premium Server CA
- Thawte Server CA
- RSA Secure Server Certification Authority

Para utilizar certificados emitidos por otras entidades emisoras de certificados, deberá instalar los certificados raíz de la entidad emisora de certificados en todos los clientes como parte de la configuración del cliente.

 Sistemas operativos AIX  Sistemas operativos Windows  Sistemas operativos Linux

## Configuración del sistema para copia de seguridad con registro por diario

Debe instalar y configurar el daemon de registro por diario (Linux) o el servicio de motor con registro por diario (Windows) antes de poder realizar copias de seguridad con registro por diario.

-  Sistemas operativos Windows Configuración del servicio de motor con registro por diario  
La copia de seguridad con registro por diario se puede utilizar para todos los clientes de Windows. Si instala el servicio de motor con registro por diario y está ejecutándose, de forma predeterminada el mandato incremental realiza automáticamente una copia de seguridad con registro diario en los sistemas de archivos seleccionados que el servicio de motor con registro por diario está supervisando.
-  Sistemas operativos AIX  Sistemas operativos Linux Configuración del daemon de registro por diario  
La copia de seguridad con registro por diario se habilita mediante la instalación y configuración del daemon de registro por diario de IBM Spectrum Protect.

 Sistemas operativos Windows

## Configuración del servicio de motor con registro por diario

La copia de seguridad con registro por diario se puede utilizar para todos los clientes de Windows. Si instala el servicio de motor con registro por diario y está ejecutándose, de forma predeterminada el mandato incremental realiza automáticamente una copia de seguridad con registro diario en los sistemas de archivos seleccionados que el servicio de motor con registro por diario está supervisando.

### Acerca de esta tarea

La copia de seguridad con registro por diario se habilita mediante la instalación y configuración del servicio de registro por diario de IBM Spectrum Protect. Puede instalar el servicio de diario con el asistente de configuración de la interfaz gráfica de usuario o con el mandato dsmcutil. La configuración básica del servicio de registro por diario puede realizarse con el asistente para la instalación de la GUI; si desea aplicar una configuración más avanzada, edite el archivo de configuración del servicio de registro por diario, tsmjbbd.ini. Consejo: La ubicación predeterminada para el archivo de configuración del servicio diario es C:\Program Files\Tivoli\TSM\baclient\tsmjbbd.ini. Si es la primera vez que configura el servicio de motor con registro y todavía no existe una copia

de tsmjbbd.ini, copie el archivo de ejemplo C:\Program Files\Tivoli\TSM\config\tsmjbbd.ini.smp a C:\Program Files\Tivoli\TSM\baclient\tsmjbbd.ini.

Para instalar y configurar este servicio mediante la utilización del asistente para la instalación de la GUI Java™ del cliente, realice los pasos siguientes:

## Procedimiento

---

1. En la ventana principal, abra el menú Herramientas y seleccione Asistente para la instalación.
2. Seleccione la casilla de verificación Ayuda para configurar el motor con registro por diario.
3. Seleccione la tarea que desea realizar. Puede instalar un nuevo motor con registro por diario, actualizar un motor con registro por diario anteriormente instalado o eliminar un motor con registro por diario anteriormente instalado del sistema.
4. Complete cada uno de los paneles del asistente y pulse el botón Siguiente para continuar. Para volver al panel anterior, pulse Atrás. Para visualizar información de ayuda sobre el panel, pulse el botón Ayuda.

## Resultados

---

Los valores de configuración del servicio de diario se almacenan en el archivo de configuración de diario tsmjbbd.ini. Este archivo se puede instalar y configurar con el asistente para la instalación de GUI o se puede editar manualmente.

Realice estos pasos para configurar varios servicios de registro por diario:

1. Cree y configure un archivo de configuración de registro por diario (tsmjbbd.ini) por separado para cada servicio de registro por diario que se desea instalar. Cada archivo de configuración deberá especificar un valor JournalPipe distinto y también deberá especificar unidades distintas para el registro por diario con el fin de que los dos servicios no interfieran entre sí. La existencia de varios servicios de registro por diario encargados de realizar el registro por diario de la misma unidad genera problemas. Los distintos servicios intentan grabar en la misma base de datos de diario, a menos que tal comportamiento se altere temporalmente y de forma específica mediante la especificación de distintos directorios de diario en los distintos archivos de configuración.
2. Instale los distintos servicios de registro por diario mediante la utilización de la herramienta dsmcutil.exe. Utilice nombres distintos para cada servicio y especifique la opción /JBBCONFIGFILE para identificar el archivo tsmjbbd.ini que ha de utilizarse para esa instancia de registro por diario en particular. Por ejemplo:

```
dsmcutil install journal /name:"TSM Journal Service 1"  
/JBBCONFIGFILE:c:\journalconfig\tsmjbbd1.ini  
  
dsmcutil install journal /name:"TSM Journal Service 2"  
/JBBCONFIGFILE:d:\journalconfig\tsmjbbd2.ini
```

Nota: En formato Uniform Naming Convention (UNC), la vía de acceso jbbconfigfile debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$: \\computer7\D\$\journalconfig\tsmjbbd1.ini

3. Ahora se pueden conectar clientes de copia de seguridad diferentes (en función del archivo dsm.opt distinto utilizado) al servicio de registro por diario deseado especificando la opción JournalPipe apropiada en el dsm.opt apropiado, que corresponde al valor de servicio de registro por diario JournalPipe.

Nota:

1. Cada instancia del servicio de registro por diario sólo se asocia a un único nombre de nodo cliente de copia de seguridad y archivado. Para cambiar la asociación será necesario volver a iniciar el servicio de registro por diario para que pueda reconocerse la nueva asociación.
2. No se pueden utilizar sistemas de archivos de red y extraíbles.

Los valores de configuración que se aplican al iniciar el servicio de diario y los cambios realizados mientras se está ejecutando el servicio de diario se aplican sin necesidad de reiniciar el servicio. También se aplica a la lista de exclusión de diario. Sin embargo, algunos valores para los sistemas de archivos con registro por diario no entran en vigor hasta que el sistema de archivos se desactive y vuelva a activar.

Se pueden activar (agregar) o desactivar (suprimir) sistemas de archivos sin detener y reiniciar el servicio de diario. Puede desactivar un sistema de archivos eliminándolo de la lista de sistemas de archivos con registro por diario del archivo de configuración de diario tsmjbbd.ini o concluyendo el servicio de diario. Puede volver a activar un sistema de archivos añadiéndolo a la lista de sistemas de archivos con registro por diario del archivo de configuración de diario tsmjbbd.ini o iniciando (reiniciando) el servicio de diario.

Atención: Si desactiva un sistema de archivos sin haber establecido el valor PreserveDbOnExit en 1, la base de datos de diario del sistema de archivos de diario se suprimirá. PreserveDbOnExit=1 especifica que la base de datos de diario del sistema de archivos con registro por diario no se suprime cuando se desactiva el sistema de archivos con registro por diario. La base de datos también es válida cuando se vuelve a activar el sistema de archivos con registro por diario.

A continuación se muestra la sintaxis de la stanza y de los valores de una stanza:





Sintaxis de stanzas:

[NombreStanza]

Sintaxis de los valores de una stanza:

configuraciónStanza=valor

Nota:

1. Puede incluir comentarios en el archivo; para ello, comience la línea con un signo de punto y coma.
  2. Los nombres de valor y de stanza no son sensibles a mayúsculas y minúsculas.
  3. Pueden especificarse valores numéricos en formato hexadecimal, especificando 0x delante del valor pues, de lo contrario, se interpretará que son valores decimales.
  4. No existe ninguna correlación entre estos valores y los del archivo de opciones del cliente de copia de seguridad/archivado. El servicio de diario es un proceso completamente independiente y no procesa opciones del cliente de copia de seguridad/archivado.
-  Sistemas operativos WindowsStanza JournalSettings (Windows)  
Los valores de esta sección son globales y se aplican a todo el servicio de diario.
  -  Sistemas operativos WindowsSección JournalExcludeList  
Esta lista de sentencias de exclusión filtra los cambios que podrían registrarse en la base de datos de diario. Los cambios realizados en objetos que coinciden con las sentencias de esta sección se pasan por alto y no se registran en la base de datos de diario.
  -  Sistemas operativos WindowsSección JournaledFileSystemSettings  
Los valores de esta stanza se aplican a cada uno de los sistemas de archivos de diario especificados, a menos que se alteren temporalmente para sistemas de archivos individuales en una stanza de alteración temporal.
  -  Sistemas operativos WindowsModificación de stanzas  
Cualquier valor de la stanza **JournaledFileSystemSettings**, a excepción de los tamaños de almacenamiento intermedio, puede alterarse temporalmente para un sistema de archivos de diario en particular creando una stanza de alteración temporal.

#### Conceptos relacionados:

Copia de seguridad con registro por diario

 Sistemas operativos Windows

## Stanza JournalSettings (Windows)

---

Los valores de esta sección son globales y se aplican a todo el servicio de diario.

A continuación se muestra la sintaxis para la stanza `JournalSettings`:

Sintaxis de la stanza `JournalSettings`:

[JournalSettings]

Sintaxis de los valores de una stanza:

configuraciónRegistropor diario=valor

Puede especificar los siguientes valores de `JournalSettings`:

`conductoRegistropor diario=nombreconducto`

Especifica, cuando se establece una sesión de copia de seguridad con registro por diario, el valor de pipe name del gestor de sesiones del servicio de registro por diario con el que se conectan inicialmente los clientes de copia de seguridad. Este valor se utiliza junto con la opción del cliente de copia de seguridad del mismo nombre. El nombre de conducto predeterminado es `\\.\pipe\jnlSessionMgr1`. Por ejemplo, en `dsm.opt`:

```
JournalPipe \\.\pipe\jnlSessionMgr1
```

En la sección `tsmjbbd.ini` [JournalSettings]:

```
JournalPipe=\\.\pipe\jnlSessionMgr1
```

Nota: El cliente debe especificar el mismo pipe name mediante la opción `JournalPipe`.

`NlsRepos`

Especifica el repositorio NLS (Soporte de idioma nacional) que utiliza el servicio de diario para generar mensajes. Puesto que el servicio de registro por diario no es interactivo, esto sólo se aplica a los mensajes que se graban en las anotaciones de errores de diario. El valor predeterminado es `dscameng.txt`. Por ejemplo:

```
NlsRepos=dscenu.txt
```

`ErrorLog`

Especifica el archivo de anotaciones donde se graban los mensajes de error detallados generados por el servicio de diario. Observe que los mensajes informativos y de error menos detallados también se graban en las anotaciones de sucesos de

aplicaciones de Windows. El valor predeterminado es `jbberror.log`. Por ejemplo:

```
ErrorLog=jbberror.log
```

En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$: `\\computer7\D$\temp\jbberror.log`.

#### JournalDir

Especifica el directorio donde se graban y almacenan los archivos de la base de datos de diario. El directorio predeterminado es el directorio de instalación del servicio de diario. Puede especificar ubicaciones de diario distintas para cada sistema de archivos que se registre por diario. Esto resulta útil cuando se ejecuta en un entorno en clúster, pues la ubicación del diario debe ser accesible para todas las estaciones de trabajo del clúster que ejecuten el servicio de diario. Normalmente, el diario para los recursos locales que se registren por diario reside en la misma ubicación y el diario para los recursos de clúster compartidos (que se pueden traspasar entre estaciones de trabajo) se ubica en el recurso compartido para garantizar que sea accesible para ambas máquinas.

Esta configuración se aplica de forma predeterminada a todos los sistemas de archivos con registro por diario, pero se puede alterar mediante una sección de alteración temporal para cada sistema de archivos con registro por diario. Si el valor predeterminado es una vía de acceso completa (por ejemplo, `c:\tsmjournal`), todos los archivos de base de datos de diario se graban en el directorio especificado. Si el valor predeterminado no especifica una letra de unidad, (por ejemplo, `\tsmjournal`) los archivos de base de datos de diario de cada sistema de archivos con registro por diario se graban en el directorio especificado en cada sistema de archivos con registro por diario.

En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$: `\\computer7\D$\temp\tsmjournal`.

A continuación se muestra una sección de configuración de ejemplo:

```
[JournalSettings]
;
; Store all resources in one location unless overridden
; by an override stanza
;
JournalDir=c:\tsmjournal
;
;
[JournaledFileSystemSettings.D:\]
;
; Journal for d: only is in location specified below
;
JournalDir=d:\tsmjournal
```

Nota: Los cambios realizados en este valor no entrarán en vigor hasta que los sistemas de archivos con registro por diario se activen.



Sistemas operativos Windows

## Sección JournalExcludeList

Esta lista de sentencias de exclusión filtra los cambios que podrían registrarse en la base de datos de diario. Los cambios realizados en objetos que coinciden con las sentencias de esta sección se pasan por alto y no se registran en la base de datos de diario.

Nota:

1. La exclusión de archivos del diario no tiene ninguna relación con que el cliente de copia de seguridad excluya esos archivos, sino que sirve para evitar que se envíen al cliente de copia de seguridad para que los procese durante la copia de seguridad con registro por diario. Un archivo que no se ha excluido del registro por diario debería excluirlo el cliente de copia de seguridad/archivado si hubiera una sentencia de exclusión coincidente en el archivo de opciones del cliente.
2. El servicio de registro por diario sólo proporciona un subconjunto de las posibilidades de la función INCLUDE/EXCLUDE que proporciona el cliente de copia de seguridad/archivado. El servicio de registro por diario no admite sentencias INCLUDE y no admite la opción `exclude.dir`.

No existe correlación entre la lista de exclusión de diario y la lista de exclusión del cliente de copia de seguridad/archivado.

A continuación encontrará ejemplos de las sentencias de exclusión de registro por diario equivalentes:

```
dsm.opt: tsmjbbd.ini
```

```
EXCLUDE c:\testdir\...\* c:\testdir\*
EXCLUDE.DIR c:\testdir\test* c:\testdir\test\*
```




Se admiten los siguientes metacaracteres de coincidencia con un patrón:

%  
Representa exactamente un carácter.  
\*  
representa cero o más caracteres.  
%EnvVar%  
Expande la variable de entorno.

A continuación se muestra un ejemplo de sintaxis de sentencia de exclusión:

```
[JournalExcludeList]
%SystemRoot%\System32\Config\*
C:\Program Files\Tivoli\TSM\baclient\adsm.sys\*
%TEMP%\*
%TMP%\*
c:\excluedir\*
c:\dir1\excludefile
*.*.tmp
```

Nota: La sentencia `c:\excluedir\*` compara todo el árbol, incluidos los subdirectorios y los archivos.

 Sistemas operativos Windows

## Sección `JournaledFileSystemSettings`

---

Los valores de esta stanza se aplican a cada uno de los sistemas de archivos de diario especificados, a menos que se alteren temporalmente para sistemas de archivos individuales en una stanza de alteración temporal.

A continuación, se muestra la sintaxis de la stanza `JournaledFileSystemSettings`:

Sintaxis de la stanza **`JournaledFileSystemSettings`** :

**`[JournaledFileSystemSettings]`**

Sintaxis de los valores de una stanza:

**`JournaledFileSystemSetting=valor`**

Puede especificar los siguientes valores de **`JournaledFileSystemSettings`**:

### *DirNotifyBufferSize*

Especifica el tamaño de la memoria intermedia para registrar notificaciones de cambio para un determinado sistema de archivos de registro por diario. Puede que deba incrementar este valor para los sistemas de archivos de diario que generan un volumen muy alto de actividad relacionada con los cambios. El tamaño del almacenamiento intermedio está limitado por la memoria. El valor predeterminado es 16 KB.

### *JournaledFileSystems*

Especifica una lista de espacio delimitado de los sistemas de archivo para registrar por diario. Se admiten las especificaciones para todo el sistema de archivos y los puntos de unión de Windows. No existe un valor predeterminado. Es preciso especificar al menos un sistema de archivos registrado por diario para que el servicio de diario funcione. Pueden agregarse o eliminarse sistemas de archivos de diario mientras éstos están activados, sin tener que reiniciar el servicio. Por ejemplo:

```
JournaledFileSystems=c: d:
```

### *JournalDbSize*

Especifica el tamaño máximo que puede alcanzar la base de datos de diario. El tamaño de la base de datos de diario se expresa en bytes. Un valor cero (0) indica que el tamaño de la base de datos sólo está limitado por la capacidad del sistema de archivos en el que se encuentra la base de datos de diario. El valor predeterminado es 0 (ilimitado). Por ejemplo:

```
JournalDBSize=0x10000000
```

### *NotifyBufferSize*

Especifica el tamaño de la memoria intermedia de la memoria para recibir notificaciones de cambio del sistema de archivos para un determinado sistema de archivos de registro por diario. Puede que deba incrementar este valor para los sistemas de archivos de diario que generan un volumen muy alto de actividad relacionada con los cambios. El tamaño del almacenamiento intermedio está limitado por la memoria. El valor predeterminado es 32 KB. Por ejemplo:

```
NotifyBufferSize=0x00008000
```

### *NotifyFilter*

Especifica qué acciones de cambio del sistema de archivos generan notificaciones al servicio de diario. **`NotifyFilter`** se aplica a los cambios realizados en los archivos y a las modificaciones realizadas en los directorios. Los cambios realizados en los nombres de los directorios, como las supresiones y las creaciones, siempre se rastrean, con independencia del valor del filtro. Pueden

supervisarse varias acciones combinando (agregando) valores. El valor predeterminado es 0x11F (cambios de nombre de archivo y directorio, atributo, atributo, última modificación y seguridad). También puede utilizar el Asistente del motor con registro por diario de IBM Spectrum Protect para especificar que se supervise cualquiera de estas acciones o todas ellas. Los valores admitidos son:

Tipo de valor	Decimal	Hexadecimal
Nombre de archivo	1	0x001
Nombre de directorio	2	0x002
Atributo	4	0x004
Tamaño de archivo*	8	0x008
Última modificación*	16	0x010
Último acceso	32	0x020
Fecha de creación	64	0x040
Seguridad (ACL)	256	0x100

El asterisco (\*) indica que la notificación podría haberse diferido hasta que se vacíe la caché de grabación del disco. Los cambios de nombre son creaciones de objetos, supresiones o cambios de denominación.

Ejemplo:

```
NotifyFilter=0x107
```

#### **Valor PreserveDbOnExit**

Este valor permite que un diario siga siendo válido cuando se desactiva y se vuelve a activar un sistema de archivos con registro por diario. Esto resulta útil para proteger el diario durante reinicios del sistema, sustituciones por anomalía de clústeres y traspaso de recursos.

Los sistemas de archivos se desactivan cuando el servicio de diario se detiene o el sistema de archivos se elimina del archivo de configuración. Los sistemas de archivos se vuelven a activar cuando el servicio de diario se inicia o el sistema de archivos se agrega al archivo de configuración.

Este valor permite que una copia de seguridad con registro por diario pueda seguir procesándose cuando se reinicia el servicio (o cuando el sistema de archivos vuelve a activarse) sin que se realice una copia de seguridad incremental completa.

Nota: No se registrará en el diario ninguna actividad de cambio que ocurra mientras no se esté ejecutando el servicio de diario (o el sistema de archivos esté desactivado).

En un entorno en clúster, los recursos compartidos se pueden traspasar a distintas estaciones de trabajo del clúster. El servicio de diario que se ejecuta en cada estación de trabajo del clúster debe incluir estos recursos compartidos en la lista de sistemas de archivos con registro por diario. El servicio de diario que se ejecuta en la estación de trabajo que es la propietaria actual del recurso registra por diario de forma activa el recurso compartido, mientras que los demás servicios de diario de las máquinas del clúster que no son propietarias del recurso deben diferir el registro por diario hasta que el recurso quede disponible (o se traspase a esa estación de trabajo). Los valores de configuración *deferFSMonStart*, *deferRetryInterval* y *logFSErrors* permiten el retraso para un sistema de archivos hasta que esté disponible y accesible.

El valor 1 especifica que la base de datos de diario del sistema de archivos con registro por diario no se suprime cuando se desactiva el sistema de archivos con registro por diario. La base de datos también es válida cuando se vuelve a activar el sistema de archivos con registro por diario. Este valor debe utilizarse con precaución, pues en la base de datos de diario no se refleja ninguna actividad de cambio del sistema de archivos que ocurra mientras el sistema de archivos con registro por diario esté desactivado. El valor predeterminado 0 suprime la base de datos de diario del sistema de archivos de diario.

Nota: El diario sólo se conserva cuando un sistema de archivos con registro por diario se desactiva normalmente o se desactiva cuando el recurso ya no está disponible y se especifica el valor *deferFSMonStart*. Si un sistema de archivos se desactiva debido a un error, como por ejemplo un desbordamiento de la memoria intermedia de notificaciones, el diario no se conservará.

Un ejemplo para no suprimir la base de datos de diario al salir es:

```
[JournaledFileSystemSettings.D:\]
;
; Do not delete the journal when D:\ goes offline
;
PreserveDbOnExit=1
```

#### **Valor deferFSMonStart**

Este valor difiere un intento de iniciar la supervisión de un sistema de archivos en los casos siguientes:

- Cuando el sistema de archivos con registro por diario especificado no sea válido o no esté disponible
- Cuando no se pueda crear el directorio de diario para el sistema de archivos con registro por diario especificado o no se pueda acceder al mismo

Se comprueban los recursos en los intervalos que especifique mediante el valor *deferRetryInterval*.

El valor *deferFSMonStart* se utiliza más comúnmente en un entorno en clúster, donde los recursos compartidos podrían traspasarse a las distintas estaciones de trabajo del clúster.

1 indica que este valor está activado y 0 que está desactivado. El valor predeterminado es desactivado (0).

#### **Valor *deferRetryInterval***

Este valor especifica el valor en segundos durante los que se comprueba la disponibilidad de los sistemas de archivos aplazados con el valor *deferRetryInterval* activado y se activan. El valor predeterminado es de 1 segundo.

#### **Valor *logFSErrors***

Este valor especifica si los errores detectados al acceder a un sistema de archivos o un directorio con diario se registran en las anotaciones *jbberor.log* y en las anotaciones de sucesos.

Utilice el valor *logFSErrors* con el valor *deferFSMonStart* para impedir que se anote un exceso de mensajes del tipo *sistema de archivos no disponible* cuando se aplaza la activación de un sistema de archivos con registro por diario. Se anota el primer error que causa el aplazamiento del sistema de archivos. Los errores siguientes no se registran. 1 indica que este valor está activado y 0 que está desactivado.

Un ejemplo para retrasar el registro hasta que los directorios de diario del sistema de archivos sean válidos es:

```
[JournalSettings]
;
; Place journal files in directory on each journaled file system
;
journalDir=\tsmjournal

[JournaledeFileSystemSettings]
;
;journal c:, d:, and f:
;
JournaledeFileSystems=c: d: d:\mountpoint f:
;
; Override stanza to defer starting journaling for f:\
; until it is a valid file system

[JournalFileSystemSettings.f:\]
;
; Keep database valid if file system goes offline
;
PreserveDBOnExit=1
;
; Defer journaling until file system and journal directory
; are valid
;
deferFSMonStart=1
;
; Attempt to start journaling every 120 seconds when deferred
;
deferRetryInterval=120
;
;Do not log excessive resource unavailable messages
;
logFsErrors=0
```

#### **Conceptos relacionados:**

Modificación de stanzas

 Sistemas operativos Windows

## Modificación de stanzas

Cualquier valor de la stanza ***JournaledeFileSystemSettings***, a excepción de los tamaños de almacenamiento intermedio, puede alterarse temporalmente para un sistema de archivos de diario en particular creando una stanza de alteración temporal.

A continuación, se muestra la sintaxis de la stanza ***JournaledeFileSystemSettings***:

Sintaxis de la sección *JournaledeFileSystemSettings*:

**[*JournaledeFileSystemSettings.fs*]**

Sintaxis de los valores de una stanza:

**JournaledFileSystemSetting**=alteración temporal

Ejemplo:

```
[JournalFileSystemSettings.C:\]  
NotifyBuffer=0x0020000  
NotifyFilter=0x107
```


 Sistemas operativos AIX  Sistemas operativos Linux


## Configuración del daemon de registro por diario

La copia de seguridad con registro por diario se habilita mediante la instalación y configuración del daemon de registro por diario de IBM Spectrum Protect.


Configure el de registro por diario editando el archivo de ejemplo de configuración del daemon de registro por diario, `tsmjbbd.ini.smp`, y guardando éste como `tsmjbbd.ini`. Ambos archivos deben encontrarse en el directorio de instalación predeterminado.

Una vez que haya configurado el archivo `tsmjbbd.ini`, inicie el daemon de registro por diario iniciando el archivo ejecutable `tsmjbbd`.

 Sistemas operativos AIX Para iniciar el daemon de registro por diario después de reiniciar el sistema en AIX, ejecute el archivo de script `jbbinittab` para añadir una entrada al archivo `/etc/inittab`. El archivo ejecutable `tsmjbbd` y el archivo de script `jbbinittab` deben estar en el directorio de instalación predeterminado.

 Sistemas operativos AIX Para detener el daemon de registro por diario en AIX, emita el mandato `kill nnnn`, donde `nnnn` es el ID de proceso de `tsmjbbd`. Antes de que concluya el proceso del daemon de registro por diario (`tsmjbbd`), este notifica la extensión de kernel filepath para dejar de guardar en el almacenamiento intermedio los cambios de archivos.

Importante: No utilice el mandato `kill -9 nnnn`, ya que el mandato `kill -9` finaliza inmediatamente el proceso sin notificar filepath para dejar de guardar en el almacenamiento intermedio los cambios de archivos.

 Sistemas operativos Linux En Linux, el instalador creará el servicio `tsmjbbd` en `/etc/init.d`. Para controlar el servicio, ejecute el mandato siguiente como raíz para que se detenga, inicie o reinicie el servicio, o para comprobar su estado:

```
>>-service tsmjbbd--+-start---+-----<<  
+-stop-----+  
+-restart--+  
'-status--'
```

Si el sistema operativo Linux ejecuta el servicio de inicialización `systemd`, siga estos pasos para iniciar el daemon de registro por diario y ejecutarlo durante el inicio del sistema:

1. Copie el archivo de unidad de `systemd /opt/tivoli/tsm/client/ba/bin/tsmjbbd.service` que se proporciona en el directorio `/etc/systemd/system/`.
2. Ejecute el siguiente mandato para renovar la lista de unidades `systemd`:

```
systemctl daemon-reload
```

3. Ejecute el mandato siguiente para iniciar el daemon de registro por diario al arrancar el sistema:

```
systemctl enable tsmjbbd.service
```

4. Ejecute el mandato siguiente para iniciar el daemon de registro por diario:

```
systemctl start tsmjbbd.service
```

Nota:

1. No se admiten sistemas de archivos de red ni extraíbles.
2. Las copias de seguridad incrementales completas periódicas deben realizarse para complementar las copias de seguridad diarias con registro por diario. La ejecución de las copias de seguridad incrementales progresivas puede llevar más tiempo que una copia de seguridad con registro por diario. Téngalo en cuenta al planificarlas, quizá planificando las copias de seguridad incrementales durante horas de baja actividad. Equilibre estas dos técnicas de copia de seguridad según sus necesidades empresariales. Por ejemplo, puede que decida planificar las copias de seguridad con registro por diario nocturnas y también planificar una copia de seguridad incremental progresiva completa semanal.
3. La copia de seguridad con registro por diario utiliza la extensión del kernel de vía de acceso para supervisar los cambios en el sistema de archivos. Para mejorar el rendimiento de las copias de seguridad con registro por diario, los directorios que no contienen archivos de usuarios no se supervisan en busca de cambios y no se incluyen en copias de seguridad con registro por diario. A continuación se listan los directorios que no se incluyen en copias de seguridad con registro por diario en sistemas AIX y

Linux. Los cambios en estos directorios se procesan si se realizan copias de seguridad incrementales completas periódicas mediante el mandato incremental con la opción -nojournal.

AIX	Linux
/bin	/bin
/dev	/boot
/etc	/dev
/lib	/etc
/usr/bin	/lib
/usr/lib	/proc
/usr/share	/sbin
	/sys
	/usr/bin
	/usr/lib
	/usr/share
	/var

Periódicamente se comprueba el archivo de configuración del daemon de registro por diario para determinar si existen actualizaciones en la lista de sistemas de archivos de diario. Puede añadir o eliminar sistemas de archivos de la lista de sistemas de archivos supervisados sin necesidad de detener el daemon de registro por diario.

Atención: Si desactiva un sistema de archivos que se está supervisando mediante el daemon de registro por diario, se suprimirá la base de datos diaria para dicho sistema de archivos. Para conservar la base de datos, establezca `PreserveDbOnExit=1` en la stanza de los valores de los sistemas de los archivos de diario. Este valor conserva la base de datos diaria cuando se desactiva y asegura que la base de datos diaria sea válida cuando el sistema de archivos vuelva a estar activado. Para obtener más información, consulte el apartado Sección `JournaledFileSystemSettings`.

La sintaxis de las stanzas y los valores de las mismas son los siguientes:

Sintaxis de stanzas:









`[NombreStanza]`

Sintaxis de los valores de una stanza:

`ConfiguraciónStanza=valor`

Nota:

1. Puede incluir comentarios en el archivo; para ello, comience la línea con un signo de punto y coma.
2. Los nombres de valor y de stanza no son sensibles a mayúsculas y minúsculas.
3. Pueden especificarse valores numéricos en formato hexadecimal, especificando `0x` delante del valor; de lo contrario, se interpretará que son valores decimales.
4. Estos valores del sistema de archivos de registro por diario no se correlacionan con ningún valor del archivo de opciones del cliente. El daemon de registro por diario es un proceso independiente; no procesa opciones del archivo del cliente.

-   [Sección JournalSettings](#)  
Los valores de esta sección son globales y se aplican a todo el daemon de registro por diario.
-   [Sección JournalExcludeList](#)  
Esta lista de sentencias de exclusión filtra los cambios que podrían registrarse en la base de datos de diario.
-   [Sección JournaledFileSystemSettings](#)  
Los valores de esta stanza se aplican a cada uno de los sistemas de archivos de diario especificados, a menos que se alteren temporalmente para sistemas de archivos individuales en una stanza de alteración temporal.
-   [Modificación de stanzas](#)  
Cualquier valor de la stanza `JournaledFileSystemSettings`, a excepción de los tamaños de almacenamiento intermedio, puede alterarse temporalmente para un sistema de archivos de diario en particular creando una stanza de alteración temporal.

## Sección `JournalSettings`

---

Los valores de esta sección son globales y se aplican a todo el daemon de registro por diario.

A continuación se muestra la sintaxis para la stanza `JournalSettings`:

Sintaxis de la stanza `JournalSettings`:

`[JournalSettings]`

Sintaxis de los valores de una stanza:

`configuraciónRegistropordiarior=valor`

Puede especificar los siguientes valores de `JournalSettings`:

`ErrorLog`

Especifica el archivo de anotaciones en el que se graban los mensajes de error detallados que genera el daemon de registro por diario. El valor predeterminado es `jbberror.log` y se encuentra en el directorio del ejecutable del daemon. Por ejemplo:

```
ErrorLog=/logs/jbberror.log
```

#### JournalDir

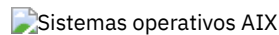
Directorio en el que se almacenan y graban los archivos de base de datos de diario.

Si la vía de acceso especificada es un nombre de vía de acceso absoluto (por ejemplo, empieza por un delimitador `dir`), se utiliza este directorio. Si la vía de acceso especificada es un nombre de directorio relativo, esta vía de acceso se agrega a cada uno de los nombres de los sistemas de archivos y se utiliza el nombre de vía de acceso resultante.

El valor predeterminado es un directorio denominado `.tSm_JoUrNaL` (se utiliza en cada uno de los sistemas de archivos que se registran por diario).

La ventaja de tener la base de datos de diario en el sistema de archivos que se registra por diario es que la base de datos está con el sistema de archivos. La desventaja es que las actualizaciones para la base de datos deben procesarse y descartarse. Importante: Dirigir la base de datos a un sistema de archivos sin registro por diario, a menos que el sistema de archivos se comparta en un entorno en clúster.

Este valor se aplica a todos los sistemas de archivos de diario, pero puede alterarse temporalmente con una sección de alteración temporal para cada sistema de archivos de diario.



## Sección JournalExcludeList

---

Esta lista de sentencias de exclusión filtra los cambios que podrían registrarse en la base de datos de diario.

Los cambios realizados en objetos que coinciden con las sentencias de esta sección se pasan por alto y no se registran en la base de datos de diario.

Nota:

1. La exclusión de archivos del diario no tiene ninguna relación con la exclusión de esos archivos que realiza el cliente de copia de seguridad, aparte de impedir que los nombres de archivos se envíen al cliente de copia de seguridad para que se procesen durante la realización de la copia de seguridad con registro por diario. Un archivo que no se ha excluido del registro por diario debería excluirlo el cliente de copia de seguridad/archivado si hubiera una sentencia de exclusión coincidente en el archivo de opciones del cliente.
2. El daemon de registro por diario sólo proporciona un subconjunto de las posibilidades de la función INCLUDE/EXCLUDE que proporciona el cliente de copia de seguridad/archivado. El daemon de registro por diario no admite sentencias INCLUDE y no admite la opción `exclude.dir`.

No existe correlación entre la lista de exclusión de diario y la lista de exclusión del cliente de copia de seguridad/archivado.

Se admiten los siguientes metacaracteres de coincidencia con un patrón:

%

Representa exactamente un carácter.

\*

representa cero o más caracteres.

%EnvVar%

Expande la variable de entorno.

A continuación se muestra un ejemplo de sintaxis de sentencia de exclusión:

```
[JournalExcludeList]
*.jbb.jbbdb
*.jbbInc.jbbdb
```



## Sección JournalFileSystemSettings

---

Los valores de esta stanza se aplican a cada uno de los sistemas de archivos de diario especificados, a menos que se alteren temporalmente para sistemas de archivos individuales en una stanza de alteración temporal.

Los sistemas de archivos que especifique en la stanza `JournalFileSystems.Extended` sobrescriben cualquier sistema de archivos especificado en la lista de sistemas de archivos de diario que pueda haber especificado anteriormente en la stanza `JournalFileSystemSettings`. Cualquier otra opción que haya especificado en la stanza `JournalFileSystemSettings` se preservará.

La sintaxis para la stanza `JournalFileSystemSettings` es como sigue:

Sintaxis de la stanza **`JournalFileSystemSettings`** :

**`[JournalFileSystemSettings]`**

Sintaxis de los valores de una stanza:

**`JournalFileSystemSetting=valor`**

Puede especificar los siguientes valores de **`JournalFileSystemSettings`**:

#### *JournalFileSystems*

Especifica una lista de espacio delimitado de los sistemas de archivo para registrar por diario. Se soportan las especificaciones de sistema de archivos completo y los cruces Windows. No existe un valor predeterminado. Debe especificar, como mínimo, un sistema de archivos de diario para que pueda ejecutarse el daemon de registro por diario. Pueden agregarse o eliminarse sistemas de archivos de diario mientras éstos están activados, sin tener que reiniciar el daemon. Por ejemplo:

```
JournalFileSystems=/home /other
```

Importante: El registro por diario selecciona los nombres de los objetos basándose estrictamente en una coincidencia de serie de caracteres. La implicación del usuario consiste en el cuidado que debe observarse al seleccionar los sistemas de archivos que han de registrarse por diario. Por ejemplo, imaginemos que existe un sistema de archivos denominado `/jbb` y otro sistema de archivos denominado `/jbb/mnt1`. Si solicita al registro por diario que supervise sólo `/jbb`, todos los cambios para `/jbb/mnt1` también coincidirán con esta serie de caracteres y se incluirán en la base de datos. Sin embargo, cuando realiza una copia de seguridad en el cliente, éste analiza el nombre basándose en los sistemas de archivos, detecta que el registro por diario no está supervisando este sistema de archivos y, a continuación, indica al registro por diario que elimine los archivos de `/jbb/mnt1` de la base de datos. La solución es supervisar ambos o bien utilizar `JournalExcludeList`. Lo mismo se aplica a las opciones de punto de montaje virtual. Debe ser coherente con esta lista. Por ejemplo, si especifica `/home/student1` como punto de montaje virtual en el archivo de opciones `dsm.sys` y desea registrar por diario `/home`, deberá especificar `JournalFileSystems=/home /home/student1`. En este caso, se crean dos bases de datos por separado.

#### *JournalDbSize*

Especifica el tamaño máximo que puede alcanzar la base de datos de diario. El tamaño de la base de datos de diario se expresa en bytes. Un valor cero (0) indica que el tamaño de la base de datos sólo está limitado por la capacidad del sistema de archivos en el que se encuentra la base de datos de diario. El valor predeterminado es 0 (ilimitado). Por ejemplo:

```
JournalDBSize=0x10000000
```

#### *NotifyBufferSize, DirNotifyBufferSize*

Especifican tamaños de memoria intermedia de notificación de cambios para un sistema de archivos de diario. La existencia de gran cantidad de actividad relacionada con los cambios podría hacer necesario el incremento de este valor. El valor predeterminado es `0x00020000` (128 k) para los archivos y `0x00010000` (64 k) para los directorios.

```
NotifyBufferSize=0x00200000
```

#### **Valor PreserveDbOnExit**

Este valor permite que un diario siga siendo válido cuando se desactiva y se vuelve a activar un sistema de archivos con registro por diario. Esto es útil para conservar el registro por diario durante los reinicios del sistema y el traspaso de recursos.

Este valor permite que una copia de seguridad con registro por diario pueda seguir procesándose cuando se reinicia el daemon (o cuando el sistema de archivos vuelve a activarse) sin que se realice una copia de seguridad incremental completa.

Nota: No se registrará en el diario ninguna actividad de cambio que suceda mientras no se esté ejecutando el daemon de registro por diario (o el sistema de archivos esté desactivado).

El valor 1 especifica que la base de datos de diario del sistema de archivos con registro por diario no se suprime cuando se desactiva el sistema de archivos con registro por diario. La base de datos también es válida cuando se vuelve a activar el sistema de archivos con registro por diario. Este valor debe utilizarse con precaución, pues en la base de datos de diario no se refleja ninguna actividad de cambio del sistema de archivos que ocurra mientras el sistema de archivos con registro por diario esté desactivado. El valor predeterminado 0 suprime la base de datos de diario del sistema de archivos de diario.

Nota: El diario sólo se conserva cuando un sistema de archivos con registro por diario se desactiva normalmente o se desactiva cuando el recurso ya no está disponible y se especifica el valor `deferFsMonStart`. Si un sistema de archivos se desactiva debido a un error, como por ejemplo un desbordamiento de la memoria intermedia de notificaciones, el diario no se conservará.

Nota: Establezca `PreserveDBonExit` solamente cuando pueda asegurar que es una finalización controlada del servicio de registro por diario. El alcance de la "finalización controlada" incluye detener el servicio diario para poder volver a arrancar el sistema, sustituir un recurso de clúster o mover un recurso de clúster. La base de datos diaria puede resultar dañada si la finalización no

es controlada. Por lo tanto, realice los siguientes pasos si el servicio diario no se cerró de una forma controlada o si la base de datos diaria se desactivó o no de una forma no controlada.

1. Detener el servicio diario (si se está ejecutando)
2. Eliminar las bases de datos diarias dañadas
3. Reiniciar el servicio diario
4. Realizar una copia de seguridad incremental

Un ejemplo para no suprimir la base de datos de diario al salir es:

```
preserveDBOnExit=1
```

#### Valor *deferFSMonStart*

Este valor difiere un intento de iniciar la supervisión de un sistema de archivos en los casos siguientes:

- Cuando el sistema de archivos con registro por diario especificado no sea válido o no esté disponible
- Cuando no se pueda crear el directorio de diario para el sistema de archivos con registro por diario especificado o no se pueda acceder al mismo

Se comprueban los recursos en los intervalos que especifique mediante el valor *deferRetryInterval*.



1 indica que este valor está activado y 0 que está desactivado. El valor predeterminado es desactivado (0).

#### Valor *deferRetryInterval*

Este valor especifica el valor en segundos durante los que se comprueba la disponibilidad de los sistemas de archivos aplazados con el valor *deferRetryInterval* activado y se activan. El valor predeterminado son 5 segundos.

#### Valor *logFSErrors*

El valor 1 indica que deben anotarse todos los errores detectados al acceder a un sistema de archivos de diario o a un directorio de diario. El valor cero indica que se suprime la anotación de los errores detectados al comprobar los directorios de diario y los sistemas de archivos diferidos. Este valor suele utilizarse junto con el valor *deferFSMonStart* para que no se grabe un número excesivo de mensajes relacionados con la no disponibilidad del sistema de archivos en las anotaciones cuando se ha diferido la activación de un sistema de archivos de diario. El valor predeterminado es 1 (anotar todos los errores).

-  Sistemas operativos Linux  Sistemas operativos AIX Stanza `JournalFileSystems.Extended`  
La stanza `JournalFileSystems.Extended` sobrescribe cualquier sistema de archivos que se incluye en la stanza `JournalFileSystems`. También elimina la limitación de caracteres de 1023 impuesta por la stanza `JournalFileSystem`.

#### Conceptos relacionados:

Modificación de stanzas

Stanza `JournalFileSystems.Extended`

 Sistemas operativos AIX  Sistemas operativos Linux

## Modificación de stanzas

---

Cualquier valor de la stanza `JournalFileSystemSettings`, a excepción de los tamaños de almacenamiento intermedio, puede alterarse temporalmente para un sistema de archivos de diario en particular creando una stanza de alteración temporal.

#### HookFileName

Para que el registro por diario inicie la supervisión de un sistema de archivos, debe conocer el nombre de un archivo que exista en ese sistema de archivos. Este valor especifica un archivo existente. Por lo tanto, el acceso a este archivo se utiliza para comprobar si este sistema de archivos está activado o no. (La definición del término "montado" del sistema no puede utilizarse porque, en el cliente de copia de seguridad/archivado, está permitido el uso de puntos de montaje virtuales. Esto significa que el sistema del cliente de copia de seguridad y archivado puede gestionar un directorio como si se tratara de un sistema de archivos (virtual)).

Por lo tanto, si este sistema de archivos puede montarse y desmontarse, debe proporcionarse un valor `HookFileName`.

Si no se especifica un valor `HookFileName`, el daemon de registro por diario intentará crear un archivo temporal en el directorio del primer nivel, lo utilizará para iniciar la supervisión y, a continuación, lo suprimirá.

A continuación, se muestra la sintaxis de la stanza `JournalFileSystemSettings`:

Sintaxis de la sección `JournalFileSystemSettings`:

**`JournalFileSystemSettings`**.*sistema de archivos*

Sintaxis de los valores de una stanza:

**`JournalFileSystemSetting`**=*alteración temporal*

Por ejemplo, el nombre de la sección de alteración temporal para `/home` sería:



## Deduplicación de datos del lado del cliente

---

La *eliminación de duplicados de datos* es un método de reducción de las necesidades de almacenamiento eliminando los datos redundantes.

### Visión general

---

Existen dos tipos de eliminación de datos redundantes: *eliminación de duplicados de datos del lado del cliente* y *eliminación de duplicados de datos del lado del servidor*.

*Optimización de almacenamiento de datos del lado de cliente* es una técnica de optimización de almacenamiento de datos que se utiliza en el cliente de archivado y copia de seguridad para eliminar datos redundantes durante el proceso de copia de seguridad y archivado antes de que los datos se transfieran al servidor de IBM Spectrum Protect. El uso de la eliminación de duplicados de datos del lado del cliente puede reducir la cantidad de datos que se envían a través de la red de área local.

La *eliminación de duplicados de datos del lado del servidor* es una técnica de eliminación de duplicados de datos que pone en práctica el servidor. El administrador de IBM Spectrum Protect puede especificar la ubicación de la eliminación de datos duplicados (cliente o servidor) a utilizar con el parámetro DEDUP en el mandato del servidor REGISTER NODE o UPDATE NODE.

### Mejoras

---

Con una eliminación de duplicados de datos del lado del cliente, puede realizar las siguientes tareas:

- Excluir archivos específicos en un cliente de una eliminación de duplicados de datos.
- Habilitar una memoria caché de eliminación de duplicados de datos que reduzca el tráfico de la red entre el cliente y el servidor. La memoria caché contiene extensiones que se enviaron al servidor en operaciones de copia de seguridad incremental anteriores. En lugar de consultar al servidor sobre la existencia de una extensión, el cliente consulta su memoria caché.

Especificar un tamaño y una ubicación para la memoria caché de un cliente. Si se detecta una incoherencia entre el servidor y la memoria caché, la memoria caché local se elimina y se vuelve a repoblar.

Nota: Para las aplicaciones que utilizan la API de IBM Spectrum Protect, no se debe utilizar la caché de deduplicación de datos porque pueden producirse errores de copia de seguridad debido a que la caché no está sincronizada con el servidor de IBM Spectrum Protect. Si existen varias sesiones de cliente simultáneas del cliente de copia de seguridad y archivado, debe tener configurada una memoria caché independiente para cada sesión.

- Habilitar la eliminación de duplicados de datos y la compresión del lado del cliente para reducir la cantidad de datos almacenados por el servidor. Todas las extensiones se comprimen antes de ser enviadas al servidor. El equilibrio se establece entre el ahorro en el almacenamiento y la potencia de proceso necesaria para comprimir los datos del cliente. En general, si comprime y elimina duplicados de datos del sistema cliente, está utilizando aproximadamente el doble de potencia de proceso que si sólo realizara la eliminación de duplicados de datos.

El servidor puede trabajar con datos cuyos duplicados se han eliminado y que han sido comprimidos. Además, los clientes de archivado y copia de seguridad anteriores a la V6.2 pueden restaurar datos comprimidos y con duplicados de datos eliminados.

La eliminación de duplicados de datos del lado del cliente utiliza el siguiente proceso:

- El cliente crea extensiones. Las *extensiones* son fragmentos de archivo que se comparan con otras extensiones para identificar duplicados.
- El cliente y el servidor colaboran para identificar las extensiones duplicadas. El cliente envía extensiones no duplicadas al servidor.
- Las operaciones subsiguientes de eliminación de duplicados de datos del cliente crean nuevas extensiones. Algunas o todas las extensiones pueden coincidir con las extensiones que han sido creadas en operaciones de eliminación de duplicados de datos anteriores y enviadas al servidor. Las extensiones que coinciden no se vuelven a enviar al servidor.

### Ventajas

---

La eliminación de duplicados de datos del lado del cliente presenta las siguientes ventajas:

- Puede reducir la cantidad de datos enviados a la red de área local (LAN).
- La potencia de procesamiento necesaria para identificar datos duplicados se descarga desde el servidor a los nodos cliente. La eliminación de duplicados de datos en el lado del servidor siempre está habilitada para la agrupación de almacenamiento con la eliminación de duplicados de datos habilitada. Sin embargo, los archivos que se encuentran en la agrupación de almacenamiento

habilitada para eliminación de duplicados de datos y cuyos duplicados han sido eliminados por el cliente no requieren ningún proceso adicional.

- Se elimina el poder de procesamiento necesario para eliminar datos duplicados del servidor, lo que permite ahorrar inmediatamente espacio en el servidor.

La eliminación de duplicados de datos del lado del cliente tiene una desventaja posible. El servidor no tendrá copias completas de los archivos del cliente *hasta* que haga una copia de seguridad de las agrupaciones de almacenamiento primarias que contienen extensiones de cliente en una agrupación de almacenamiento de copia sin optimización de almacenamiento. (Las *extensiones* son partes de un archivo que se crean durante el proceso de optimización de almacenamiento de datos). Durante la copia de seguridad de la agrupación de almacenamiento en una agrupación de almacenamiento sin eliminación de datos duplicados, las extensiones del cliente se vuelven a ensamblar en archivos contiguos.

De manera predeterminada, debe realizarse una copia de seguridad de las agrupaciones de almacenamiento de acceso secuencial primarias que están configuradas para la eliminación de duplicados de datos en agrupaciones de almacenamiento de copia sin eliminación de duplicados para que puedan reclamarse y para que puedan eliminarse los datos duplicados. Esta opción predeterminada garantiza que el servidor tenga copias de archivos completos en todo momento, en una agrupación de almacenamiento primaria o en una agrupación de almacenamiento de copia.

Importante: Para obtener una reducción aún mayor de los datos, puede habilitar de forma conjunta la compresión y la eliminación de duplicados de datos del lado del cliente. Todas las extensiones se comprimen antes de ser enviadas al servidor. La compresión ahorra espacio, pero aumenta el tiempo de proceso en la estación de trabajo cliente.

En una agrupación de almacenamiento con eliminación de duplicados de datos habilitada (agrupación de archivos) solo se conserva una instancia de una extensión de datos. Otras instancias de la misma extensión de datos se sustituyen por un puntero a la instancia conservada.

Cuando está habilitada la eliminación de duplicados de datos, y el servidor se ha quedado sin almacenamiento en la agrupación de destino, pero hay una agrupación siguiente definida, el servidor detendrá la transacción. El cliente de copia de seguridad y archivado vuelve a intentar la transacción sin la eliminación de duplicados de datos del lado del cliente. En el caso de la recuperación, el administrador de IBM Spectrum Protect debe añadir más volúmenes reutilizables a la agrupación de archivos original o volver a intentar la operación con la eliminación de duplicados inhabilitada.

Para la deduplicación de datos del cliente, el servidor de IBM Spectrum Protect debe tener la Versión 6.2 o posterior.

## Requisitos previos

---

Cuando se configura la deduplicación de datos del lado del cliente, se deben cumplir los siguientes requisitos:

- El cliente y el servidor deben tener la versión 6.2.0 o posterior. Se debe utilizar siempre la versión de mantenimiento más reciente.
- Cuando un cliente realiza una copia de seguridad o archiva archivos, los datos se graban en la agrupación de almacenamiento primaria especificada por el grupo de copia de la clase de gestión vinculada a los datos. Para eliminar duplicados de datos de cliente, la agrupación de almacenamiento primaria debe ser una agrupación de almacenamiento de disco de acceso secuencial (FILE) en la que se haya habilitado la eliminación de duplicados de datos.
- Especifique YES como valor de la opción DEDUPLICATION para el cliente. También puede establecer la opción DEDUPLICATION en el archivo de opciones del cliente, en el editor de preferencias en la GUI del cliente de copia de seguridad y archivado o en el conjunto de opciones de cliente en el servidor IBM Spectrum Protect. Utilice el mandato DEFINE CLIENTOPT para definir la opción DEDUPLICATION en un conjunto de la opción del cliente. Para evitar que el cliente sustituya el valor en el conjunto de opciones de cliente, especifique FORCE=YES.
- La eliminación de duplicación de datos del lado del cliente debe estar habilitada en el servidor. Para habilitar la optimización de almacenamiento de datos del lado del cliente, utilice el parámetro DEDUPLICATION en el mandato de servidor REGISTER NODE o UPDATE NODE. Establezca el valor del parámetro a CLIENTORSERVER.
- Asegúrese de que los archivos en el cliente no se excluyan de la deduplicación de datos del lado del cliente. De manera predeterminada, se incluyen todos los archivos. Opcionalmente, puede excluir archivos específicos de la deduplicación de datos del lado del cliente con la opción de cliente exclude.dedup.
- No deben cifrarse los archivos del cliente. No pueden eliminarse los duplicados de datos de los archivos cifrados y los archivos de sistemas de archivos cifrados.
- Los archivos deben superar los 2 KB y las transacciones deben estar por debajo del valor especificado en la opción CLIENTDEDUPTXNLIMIT. En los archivos de 2 KB o menos no se eliminan los datos duplicados.

El servidor puede limitar el tamaño máximo de transacción para la eliminación de duplicados de datos estableciendo la opción CLIENTDEDUPTXNLIMIT en el servidor. Para obtener más información sobre esta opción, consulte la documentación del servidor de IBM Spectrum Protect.

Las siguientes operaciones tienen preferencia sobre la eliminación de duplicados de datos del lado del cliente:

- traspaso de datos sin LAN

- Operaciones de grabación simultánea
- Cifrado de datos

Importante: No planifique ni habilite ninguna de estas operaciones durante la eliminación de duplicados de datos del lado del cliente. Si se inicia alguno de estos procesos durante la eliminación de duplicados de datos del lado del cliente, ésta se detiene y se graba un mensaje en el registro de errores.

La configuración del servidor determina en última instancia si se habilita la eliminación de duplicados de datos del lado del cliente. Consulte el apartado Tabla 1.

Tabla 1. Configuración de eliminación de duplicados de datos: cliente y servidor

Valor de la opción DEDUPLICATION de cliente	Valor en el servidor	Ubicación de eliminación de duplicados de datos
Yes	En el servidor o en el cliente	Client
Yes	Solo en el servidor	Servidor
No	En el servidor o en el cliente	Servidor
No	Solo en el servidor	Servidor

## Archivos cifrados

El servidor y el cliente de archivado y copia de seguridad de IBM Spectrum Protect no pueden optimizar el almacenamiento de los archivos cifrados. Si se encuentra un archivo cifrado durante el proceso de eliminación de duplicados de datos, no se elimina el duplicado de datos del archivo y se registra un mensaje.

Consejo: No tiene que procesar los archivos cifrados y los archivos que sí son aptos para la eliminación de duplicados de datos del lado del cliente por separado. Ambos tipos de archivo pueden procesarse en la misma operación. Sin embargo, se envían al servidor en transacciones diferentes.

Como medida de seguridad, puede seguir uno o varios de los pasos que se indican a continuación:

- Habilite el cifrado del dispositivo de almacenamiento junto con la eliminación de duplicados de datos del lado del cliente.
- Utilice la eliminación de duplicados de datos del lado del cliente sólo para los nodos que crea que son seguros.
- Si no está seguro de la seguridad de la red, habilite la Capa de sockets seguros (SSL).
- Si no desea que la eliminación de duplicados de datos del lado del cliente procese ciertos objetos (por ejemplo, objetos de imagen), puede excluirlos del cliente. Si se excluye un objeto de la eliminación de duplicados de datos del lado del cliente y se envía a una agrupación de almacenamiento en la que se ha establecido la eliminación de duplicados de datos, la eliminación del duplicado de datos del objeto se lleva a cabo en el servidor.
- Utilice el mandato SET DEDUPVERIFICATIONLEVEL para detectar posibles ataques a la seguridad del servidor durante la eliminación de duplicados de datos del lado del cliente. Cuando utilice este mandato, puede especificar un porcentaje de extensiones de cliente para que las verifique el servidor. Si el servidor detecta un posible ataque a la seguridad, aparecerá un mensaje.
- Configuración del cliente para la eliminación de duplicados de datos  
Configure el cliente para que pueda utilizar la eliminación de duplicados de datos para realizar una copia de seguridad/archivado de los archivos.
- Excluir archivos de la eliminación de duplicados de datos  
Puede excluir archivos de la eliminación de duplicados de datos durante el proceso de copia de seguridad o archivado.

### Tareas relacionadas:

Configuración del cliente para la eliminación de duplicados de datos

### Referencia relacionada:

Eliminación de duplicados

Opciones exclude

Dedupcachepath

Dedupcachesize

Enablededupcache

Ieobjtype

## Configuración del cliente para la eliminación de duplicados de datos

Configure el cliente para que pueda utilizar la eliminación de duplicados de datos para realizar una copia de seguridad/archivado de los archivos.

### Antes de empezar

Antes de configurar el cliente para utilizar la eliminación de duplicados de datos, asegúrese de que se cumplen los requisitos enumerados en Deduplicación de datos del lado del cliente:






- El servidor debe habilitar el cliente para la eliminación de duplicados de datos del lado del cliente con el parámetro DEDUP=CLIENTORSERVER en el mandato REGISTER NODE o UPDATE NODE.
- El destino de la agrupación de almacenamiento para los datos debe ser una agrupación de almacenamiento habilitada para la eliminación de duplicados de datos.
- Asegúrese de que los archivos están enlazados a la clase de gestión correcta.
- Los archivos deben superar los 2 KB.

Se puede excluir un archivo del proceso de eliminación de duplicados de datos del lado del cliente. De manera predeterminada, se incluyen todos los archivos. Consulte la opción exclude.dedup para obtener más detalles.

El servidor puede limitar el tamaño máximo de transacción para la eliminación de duplicados de datos estableciendo la opción CLIENTEDEDUPTXNLIMIT en el servidor.

## Procedimiento











Utilice uno de los siguientes métodos para habilitar la eliminación de datos duplicados en el cliente:

Opción	Descripción
<b>Edite el archivo de opciones de cliente del cliente</b>	<ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Añada la opción <code>deduplication yes</code> al archivo <code>dsm.sys</code>.</li> <li>•  Sistemas operativos Windows Añada la opción <code>deduplication yes</code> al archivo <code>dsm.opt</code>.</li> </ul>
<b>Editor de preferencias</b>	<ol style="list-style-type: none"> <li>a. En la ventana IBM Spectrum Protect, pulse en Editar &gt; Preferencias de cliente.</li> <li>b. Pulse en Eliminación de duplicados.</li> <li>c. Seleccione la casilla de verificación Habilitar eliminación de duplicados.</li> <li>d. Pulse Aceptar para guardar las selecciones que haya realizado y cerrar el Editor de preferencias.</li> </ol>

## Resultados

Una vez configurado el cliente para eliminación de duplicados de datos, inicie una operación de copia de seguridad o de archivado. Cuando la operación finalice, el informe de copia de seguridad o archivado mostrará los datos duplicados de esta operación y el número de archivos que se han procesado mediante la eliminación de duplicados de datos del lado del cliente.

Si no dispone de suficiente espacio de disco para realizar la operación de copia de seguridad o de archivado, puede habilitar la eliminación de datos duplicados del lado del cliente sin memoria caché local de eliminación de datos duplicados en el cliente siguiendo estos pasos:

1. Añada la opción `deduplication yes` en el archivo de opciones de cliente del cliente.
  - o  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Añada la opción `deduplication yes` al archivo `dsm.sys`. También puede establecer esta opción en la interfaz gráfica de usuario.
  - o  Sistemas operativos Windows Añada la opción `deduplication yes` al archivo `dsm.opt`. También puede establecer esta opción en la interfaz gráfica de usuario.
2. Desactive la memoria caché local de eliminación de datos duplicados completando uno de los siguientes pasos.
  - o  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Añada la opción `ENABLEDEDUPCACHE NO` en el archivo `dsm.sys`.
  - o  Sistemas operativos Windows Añada la opción `ENABLEDEDUPCACHE NO` en el archivo `dsm.opt`.

También puede definir esta opción en el editor de preferencias del cliente de archivado y copia de seguridad deseleccionando el recuadro Habilitar memoria caché para eliminación de duplicados.

## Ejemplo

El siguiente ejemplo utiliza el mandato de sesión de consulta para mostrar el tipo de datos que se han procesado para la eliminación de duplicados de datos:

```
Protect> q sess
Información de conexión de IBM Spectrum Protect Server

Nombre de servidor.....: SERVER1
Tipo de servidor.....: Windows
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 2, Niv. 0.0
```

```
Last Access Date.....: 08/25/2009 13:38:18
Suprimir archivos copia seg....: "No"
Suprimir copias archivadas.....: "Sí"
Deduplication.....: "Client Or Server"
```

```
Node Name.....: AVI
Nombre de usuario.....:
```

El siguiente ejemplo utiliza el mandato de clase de gestión de consulta para mostrar el tipo de datos que se han procesado para la eliminación de duplicados de datos:

```
Protect> q mgmt -det
Domain Name : DEDUP
Activated Policy Set Name : DEDUP
Activation date/time : 08/24/2009 07:26:09
Default Mgmt Class Name : DEDUP
Grace Period Backup Retn. : 30 day(s)
Grace Period Archive Retn.: 365 day(s)
```

```
MgmtClass Name : DEDUP
Description : dedup - values like standard
Space Management Technique : None
Auto Migrate on Non-Usage : 0
Backup Required Before Migration: YES
Destination for Migrated Files : SPACEMGPOOL
Copy Group
Copy Group Name.....: STANDARD
Copy Type.....: Backup
Copy Frequency.....: 0 day(s)
Versions Data Exists...: 2 version(s)
Versions Data Deleted..: 1 version(s)
Retain Extra Versions..: 30 day(s)
Retain Only Version....: 60 day(s)
Copy Serialization.....: Shared Static
Copy Mode.....: Modified
Copy Destination.....: AVIFILEPOOL
Lan Free Destination...: NO
Deduplicate Data.....: YES
```

```
Copy Group Name.....: STANDARD
Copy Type.....: Archive
Copy Frequency.....: Cmd
Retain Version.....: 365 day(s)
Copy Serialization.....: Shared Static
Copy Mode.....: Absolute
Retain Initiation.....: Create
Retain Minimum.....: 65534 day(s)
Copy Destination.....: FILEPOOL
Lan Free Destination...: NO
Deduplicate Data.....: YES
```

El código de retorno de ANSI900I es 0.

#### **Conceptos relacionados:**

Deduplicación de datos del lado del cliente

#### **Referencia relacionada:**

Opción CLIENTDEDUPTXNLIMIT

Mandato REGISTER NODE

Mandato UPDATE NODE

Eliminación de duplicados

Enablededupcache

Opciones exclude





## Excluir archivos de la eliminación de duplicados de datos

---


Puede excluir archivos de la eliminación de duplicados de datos durante el proceso de copia de seguridad o archivado.

### Acerca de esta tarea

---



 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Solo podrá excluir archivos de la eliminación de datos de archivado. Podrá excluir archivos e imágenes (cuando proceda) de la eliminación de


duplicados de datos de copia de seguridad.

 Sistemas operativos Windows Solo podrá excluir archivos de la eliminación de datos de archivado. Podrá excluir archivos, imágenes, objetos de estado del sistema y ASR de la eliminación de duplicados de datos de copia de seguridad.

## Procedimiento





Si no desea que la eliminación de duplicados de datos del lado del cliente procese determinados archivos, utilice la GUI para excluirlos del proceso de eliminación de duplicados de datos:

1. Pulse Editar > Preferencias del cliente.
2. Pulse la pestaña Incluir/excluir.
3. Pulse Añadir para abrir la ventana Definir opciones de inclusión/exclusión.
4. Seleccione una categoría para el proceso.
  - Para excluir un archivo de la eliminación de duplicados de datos durante el proceso de archivado, seleccione Archivado en la lista Categoría.
  - Para excluir un archivo de la eliminación de duplicados de datos durante el proceso de copia de seguridad, seleccione Copia de seguridad en la lista Categoría.
5. Seleccione Excluye.Dedup en la lista Tipo.
6. Seleccione un elemento de la lista Tipo de objeto.
  - En el caso del proceso de archivado, solo está disponible el tipo de objeto Archivo.
  - Para el proceso de copia de seguridad, seleccione uno de los siguientes tipos de objeto:
    - Archivo
    - Imagen
    -  Sistemas operativos Windows Estado del sistema
    -  Sistemas operativos Windows ASR
7. Especifique un archivo o patrón en el campo Archivo o patrón. Puede utilizar caracteres comodín. Si no desea escribir un archivo o patrón, pulse Examinar para abrir una ventana de selección y seleccionar un archivo. En el caso de los espacios de archivos, puede seleccionar el punto de montaje desde la ventana de selección.


 Sistemas operativos Windows En el caso de ASR y del estado del sistema, este campo se rellena de forma automática. Cuando especifique el tipo de objeto de imagen, la letra de unidad debe ir seguida de :\*\\*. Por ejemplo, para excluir la unidad E:, especifique el siguiente patrón:

```
E: \*\*
```
8. Pulse Aceptar para cerrar la ventana Definir opciones de inclusión/exclusión. Las opciones de exclusión que haya definido aparecerán en una sentencia de exclusión en la parte inferior del recuadro de lista Sentencias en la pestaña Preferencias de inclusión/exclusión.
9. Pulse Aceptar para guardar las selecciones que haya realizado y cerrar el Editor de preferencias.

## Qué hacer a continuación

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris También puede excluir archivos del proceso de eliminación de duplicados de datos editando el archivo `dsm.sys`:

1. Añada la opción `deduplication yes`.
2. Excluya los archivos de un directorio de la eliminación de duplicados de datos. Por ejemplo, para excluir los archivos del directorio `/Users/Administrator/Documents/Taxes/`, añada la sentencia siguiente: `EXCLUDE.dedup /Users/Administrator/Documents/Taxes/.../*`
3. Excluya la eliminación de duplicados de datos del lado del cliente de la copia de seguridad de imágenes de un sistema de archivos. Por ejemplo, para excluir el sistema de archivos `/home`, añada la sentencia siguiente: `EXCLUDE.DEDUP /home/*/* IEOBJTYPE=Image`.

 Sistemas operativos Windows También podrá excluir los archivos del proceso de eliminación de duplicados de datos editando el archivo `dsm.opt`:

1. Añada la opción `deduplication yes`.
2. Excluya la eliminación de duplicados de datos del lado del cliente de la copia de seguridad de imágenes de la unidad. Por ejemplo, para excluir la unidad E:, añada la sentencia siguiente: `EXCLUDE.DEDUP E: \*\* IEOBJTYPE=Image to dsm.opt`.

Importante: Si se envía un objeto a una agrupación de eliminación de duplicados, la eliminación de duplicados de datos se producirá en el servidor aunque el objeto se excluya de la eliminación de duplicados de datos del lado del cliente.

### Conceptos relacionados:

Deduplicación de datos del lado del cliente

### Referencia relacionada:

Eliminación de duplicados

## Configuración y uso de la migración tras error automática del cliente

El cliente de archivado y copia de seguridad puede realizar la migración tras error automáticamente en un servidor secundario para recuperar los datos cuando el servidor de IBM Spectrum Protect no está disponible. Puede configurar el cliente para la migración tras error automática o evitar que el cliente migre tras el error. También puede determinar el estado de la réplica de sus datos en servidor secundario antes de restaurar o recuperar los datos replicados.

- **Visión general de migración tras error de cliente automatizado**  
Cuando hay un corte en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad puede migrarse de forma automática a servidor secundario para recuperar los datos.
- **Configuración del cliente de migración automática tras error**  
Puede configurar de forma manual el cliente para que se migre de forma automática al servidor secundario.
- **Determinación del estado los datos replicados del cliente**  
Puede verificar si la copia de seguridad más reciente del cliente se replicó en el servidor secundario antes de restaurar o recuperar los datos desde servidor secundario.
- **Prevención de la migración tras error automática del cliente**  
Puede configurar el cliente para evitar que se realice la migración tras error automática al servidor secundario.
- **Forzar al cliente a la migración tras error**  
El cliente puede realizar la migración tras error al cliente servidor secundario si el servidor primario es operacional. Por ejemplo, puede utilizar esta técnica para verificar que el cliente va a realizar la migración al servidor secundario esperado.

### Tareas relacionadas:

Restaurar o recuperar datos durante una migración tras error


## Visión general de migración tras error de cliente automatizado

Cuando hay un corte en el servidor de IBM Spectrum Protect, el cliente de archivado y copia de seguridad puede migrarse de forma automática a servidor secundario para recuperar los datos.

El servidor de IBM Spectrum Protect al que se conecta el cliente durante los procesos de producción normal se denomina *servidor primario*. Cuando los nodos del cliente de servidor primario y están configurados para la réplica del nodo, el servidor también se conoce como *source replication server*. Los datos del cliente del servidor de réplica de origen se pueden replicar en otro servidor de IBM Spectrum Protect, que es el *servidor de réplica de destino*. Este servidor también se denomina *servidor secundario*, y es el servidor sobre el que el cliente realiza la migración tras error automáticamente cuando el servidor primario falla.





Para que el cliente realice una migración tras error automáticamente en el servidor secundario, la información de conexión para el servidor secundario debe estar disponible en el cliente. Durante las operaciones normales, la información de conexión para el servidor secundario se enviará automáticamente al cliente desde el servidor primario durante el proceso de inicio de sesión. La información del servidor secundario se guardará automáticamente en el archivo de opciones del cliente. No se necesita intervención manual del cliente para añadir la información del servidor secundario.

Cada vez que el cliente inicia sesión en el servidor de IBM Spectrum Protect, el cliente intenta ponerse en contacto con el servidor primario. Si el servidor primario no está disponible, el cliente se migra automáticamente al servidor secundario, según la información de servidor secundario disponible en el archivo de opciones del cliente. En esta modalidad de migración tras error, puede restaurar o recuperar cualquier dato del cliente replicado. Cuando el servidor primario vuelva a estar en línea, el cliente volverá automáticamente al servidor primario la próxima vez que se inicie el cliente.

 **Sistemas operativos Windows** Por ejemplo, el siguiente texto de ejemplo presenta la información de conexión sobre el servidor secundario que se envía al cliente y se guarda en el archivo de opciones del cliente (dsm.opt):

```
*** Estas opciones no se deben cambiar manualmente
REPLSERVERNAME          TARGET
REPLTCPSERVERADDRESS    192.0.2.9
REPLTCPSPORT            1501
REPLSSLPORT             1502
REPLSERVERGUID          60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3
```

```
MYREPLICATIONServer TARGET
MYPRIMARYServer SERVER1
*** end of automatically updated options
```

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **sistemas operativos Mac OS X**  **Sistemas operativos Oracle Solaris** Por ejemplo, el siguiente texto de ejemplo muestra la información de conexión que servidor secundario envía al cliente y guarda en el archivo de opciones del sistema del cliente (dsm.sys):

```

*** Estas opciones no se deben cambiar manualmente
REPLSERVERNAME      TARGET
REPLTCPSERVERADDRESS 192.0.2.9
REPLTCPSPORT        1501
REPLSSLPORT         1502
REPLSERVERGUID      60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

```

```

MYREPLICATIONServer TARGET
*** end of automatically updated options

```

- Requisitos para la migración tras error automática del cliente  
Antes de configurar o utilizar la migración tras error automática del cliente el cliente de archivado y copia de seguridad y el servidor de IBM Spectrum Protect debe cumplir varios requisitos.
- Restricciones de la migración tras error automática de cliente  
Revise la siguiente información para tener un mejor conocimiento del proceso y de las restricciones que se aplican a la migración tras error automática del cliente.
- Funciones de migración tras error de los componentes de IBM Spectrum Protect  
Los componentes y productos de IBM Spectrum Protect se basan en el cliente de archivado y copia de seguridad o la API para realizar la copia de seguridad de los datos en el servidor primario de IBM Spectrum Protect. Cuando servidor primario deja de estar disponible, algunos de estos productos y componentes pueden migrarse tras error a servidor secundario, mientras que otros no son capaces de migrarse tras el error.

## Requisitos para la migración tras error automática del cliente

Antes de configurar o utilizar la migración tras error automática del cliente el cliente de archivado y copia de seguridad y el servidor de IBM Spectrum Protect debe cumplir varios requisitos.

Asegúrese de que el cliente cumpla los siguientes requisitos para la migración tras error automática del cliente:

- El servidor primario, el servidor secundario, y el cliente de archivado y copia de seguridad deben tener IBM Spectrum Protect Versión 7.1 o posterior.
- Los servidores primario y secundario deben estar configurados para la réplica del nodo.
- El nodo del cliente debe estar configurado para la réplica del nodo en el servidor de réplica de origen utilizando los mandatos del servidor `REGISTER NODE REPLSTATE=ENABLED` o `UPDATE NODE REPLSTATE=ENABLED`.
- De forma predeterminada, se habilita el cliente para la migración tras error del cliente automatizado. Sin embargo, si se especifica la opción `usereplicationfailover no` en el archivo de opciones del cliente, bien cambie el valor a `yes`, o elimine la opción.
- La información de conexión válida para el servidor secundario debe existir en el archivo de opciones del cliente. Durante las operaciones normales, esta información se enviará automáticamente al cliente desde el servidor primario.
- Para guardar la información de conexión de servidor secundario que se envía desde servidor primario, el cliente debe tener acceso de grabación al archivo `dsm.opt` en los clientes de Windows y el archivo `dsm.sys` en los clientes de AIX, Linux, Mac OS X y Oracle Solaris. Si el cliente no tiene acceso de grabación a estos archivos, la información de servidor secundario no se guarda en el archivo de opciones del cliente y se añade un error al registro de error.
- Los usuarios no raíz no pueden utilizar la ubicación predeterminada para la tabla de réplica del nodo. Debe especificar una ubicación diferente añadiendo la opción `nrtablepath` al archivo `dsm.sys`. Para obtener más información, consulte `Nrtablepath`.
- Los procesos siguientes se deben producir antes de la información de conexión para que se envíe el servidor secundario al archivo de opciones:
  - Se debe realizar una copia de seguridad del cliente en el servidor de réplica de origen al menos una vez.
  - Se debe volver a aplicar el nodo del cliente al servidor de réplica de destino al menos una vez.
- La migración tras error ocurre en los nodos de cliente que se copian con soporte de proxy del nodo del cliente cuando tanto los nodos de destino como de agente se configuran para la réplica en servidor de réplica de destino. Cuando el nodo de destino se replica de forma explícita, el nodo del agente también se replica de forma implícita en el servidor de réplica de destino, junto con la relación de proxy.  
Por ejemplo, `Node_B` tiene autoridad para llevar a cabo operaciones de cliente en nombre de `Node_A` con el siguiente mandato del servidor:

```
grant proxynode target=Node_A agent=Node_B
```

Si ambos nodos están configurados para la réplica con la opción `replstate=enabled` en la definición del nodo, cuando el `Node_A` se replica, el `Node_B` y la relación de proxy también se replican.

## Restricciones de la migración tras error automática de cliente

Revise la siguiente información para tener un mejor conocimiento del proceso y de las restricciones que se aplican a la migración tras error automática del cliente.



Las siguientes restricciones se aplican a la migración tras error automática del cliente:

- Cuando el cliente está en modo migración tras error, no puede utilizar ninguna función que requiera que los datos se almacenen en servidor secundario, como las operaciones de archivado y copia de seguridad. Puede utilizar solo las funciones de recuperación de los datos como la restauración, recuperación u operaciones de consulta. También puede editar las opciones del cliente y cambiar la contraseña del cliente de IBM Spectrum Protect.
- Las planificaciones no se replican en el servidor secundario. Por lo tanto, las planificaciones no se ejecutan mientras servidor de servidor primario no está disponible.
- Una vez que el cliente se conecta a servidor secundario en el modo de recuperación tras error, no intenta conectarse a servidor primario hasta el siguiente inicio de sesión inicial del servidor. El cliente intenta realizar la migración tras error en el servidor secundario solo cuando falla la conexión inicial al servidor primario. La conexión inicial es la primera conexión que el cliente realiza con el servidor.

Si el servidor primario deja de estar disponible durante una operación del cliente, el cliente no realiza la recuperación tras error en el servidor secundario, y la operación falla. Debe reiniciar el cliente para que pueda realizar la migración tras error en el servidor secundario, y después ejecutar la operación del cliente de nuevo.

Las operaciones de restauración que se interrumpen cuando el servidor primario se desconecta no se pueden restaurar después de que el cliente realice la migración tras error. Debe ejecutar la operación de restauración completa de nuevo después de que el cliente realice la migración tras error al servidor secundario.

- Si la contraseña de IBM Spectrum Protect se cambia antes de que se replique el nodo del cliente, la contraseña no se sincronizará entre los servidores primarios y secundarios. Si la migración tras error se produce durante este tiempo, debe reiniciar de forma manual la contraseña en el servidor secundario y en el cliente. Cuando la servidor primario vuelve a estar disponible, la contraseña debe reiniciarse para que el cliente se conecte a servidor primario.

Si la contraseña se restaura mientras que el cliente está conectado a servidor secundario, la contraseña debe reiniciarse en el servidor primario antes de que el cliente pueda iniciar sesión en el servidor primario. Esta restricción es verdadera si la opción `passwordaccess` se define en `generate` o si la contraseña se restaura de forma manual.

- Si has realizado la copia de seguridad o archivado los datos del cliente, pero servidor primario se queda inactivo antes de replicar el nodo del cliente, la copia de seguridad o los datos de archivado más reciente no se replican en el servidor secundario. El estado de réplica del espacio de archivos no es el actual. Si intenta restaurar o recuperar los datos en el modo de migración tras error y el estado de réplica no es el actual, se muestra un mensaje que indica que los datos que está a punto de recuperar están desfasados. Puede decidir si va a seguir con la recuperación o esperar hasta que servidor primario vuelva a estar online.
- Si existe un ID de usuario administrativo con una autoridad de cliente propietario en el servidor de réplica de origen, y el ID de usuario tiene el mismo nombre que el nodo del cliente, el ID de usuario administrativo se replica durante el proceso de réplica en el servidor. Su dicho ID de usuario no existe en el servidor de réplica de origen, el proceso de réplica no crea esta definición de administrador en el servidor de réplica de destino.

Si otro ID de usuario administrativo se asigna al nodo, el administrador de IBM Spectrum Protect debe configurar de forma manual el ID de usuario administrativo en el servidor de réplica de destino. De lo contrario, el usuario administrativo no puede conectarse al servidor de réplica de destino (servidor secundario) con el cliente web de IBM Spectrum Protect.

- Si restaura un archivo desde IBM Spectrum Protect, y el sistema de archivos está gestionado por IBM Spectrum Protect for Space Management, no debe restaurar el archivo como un archivo de resguardo. Debe restaurar el archivo completo. Utilice la opción `restoremigstate=no` para restaurar el archivo completo. Si restaura el archivo como un resguardo desde el servidor de destino, se pueden producir las siguientes consecuencias:
  - No puede recuperar el archivo del servidor de origen de IBM Spectrum Protect utilizando el cliente de IBM Spectrum Protect for Space Management.
  - El proceso de reconciliación de IBM Spectrum Protect for Space Management que se ejecuta contra el servidor de origen de IBM Spectrum Protect hace caducar el archivo. Si el archivo ha caducado por un proceso de reconciliación, puede restaurar el archivo completo con el cliente de copia de seguridad/archivado y la opción `restoremigstate=no`.

## Funciones de migración tras error de los componentes de IBM Spectrum Protect

---

Los componentes y productos de IBM Spectrum Protect se basan en el cliente de archivado y copia de seguridad o la API para realizar la copia de seguridad de los datos en el servidor primario de IBM Spectrum Protect. Cuando servidor primario deja de estar disponible, algunos de estos productos y componentes pueden migrarse tras error a servidor secundario, mientras que otros no son capaces de migrarse tras el error.

Para obtener más información sobre las funciones de migración tras error de los componentes y productos de IBM Spectrum Protect, consulte la nota técnica 1649484.

## Tareas relacionadas:

Determinación del estado los datos replicados del cliente

# Configuración del cliente de migración automática tras error

Puede configurar de forma manual el cliente para que se migre de forma automática al servidor secundario.

## Antes de empezar

Antes de iniciar la configuración:

- Asegúrese de que el nodo del cliente participa en la réplica en servidor primario.
- Asegúrese de que el cliente cumple con los requisitos de para la migración tras error automática del cliente.
- Utilice este procedimiento solo si la información de la conexión para servidor secundario no es actual o si no está en el archivo de opciones del cliente.

## Acerca de esta tarea





Es posible que deba configurar el cliente para la migración tras error automática en las siguientes situaciones:

- La configuración de servidor secundario ha cambiado y el servidor primario no está disponible antes de que el cliente se registra en el servidor. Cuando añade información de conexión de forma manual, el cliente se activa para la migración tras error al servidor secundario.
- Ha eliminado de forma accidental toda la información de conexión de servidor secundario del archivo de opciones del cliente. Consejo: En vez de configurar de forma manual el archivo de opciones del cliente, puede ejecutar el mandato `dsmc q session`, que le solicita iniciar sesión en servidor primario. La información de la conexión para servidor secundario se envía automáticamente al archivo de opciones del cliente.

## Procedimiento

Para configurar de forma manual el cliente para la migración tras error automática, siga estos pasos:

1. Asegúrese de que el cliente está activado para la migración tras error automática del cliente verificando que la opción `usereplicationfailover` no está en el archivo de opciones del cliente o que está ajustada en `yes`. De forma predeterminada, el cliente está activado para la migración tras error automática, así que `usereplicationfailover` no es necesario en el archivo de opciones del cliente.
2. Obtenga la información de conexión sobre servidor secundario desde el administrador del servidor de IBM Spectrum Protect y añada la información al comienzo del archivo de opciones del cliente. Agrupe las sentencias en una stanza en la sentencia `replservername`.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Por ejemplo, añada las siguientes sentencias al archivo `dsm.sys`:





```
REPLSERVERNAME          TARGET
REPLTCPSEVERADDRESS    192.0.2.9
REPLTCPPOINT           1501
REPLSSLPORT            1502
REPLSERVERGUID         60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3
```

```
SERvername      server_a
COMMethod       TCPip
TCPport         1500
TCPserveraddress server_hostname1.example.com
PASSWORDaccess  prompt
MYREPLICATIONServer TARGET
```

 Sistemas operativos Windows Por ejemplo, añada las siguientes sentencias al archivo `dsm.opt`:

```
REPLSERVERNAME          TARGET
REPLTCPSEVERADDRESS    192.0.2.9
REPLTCPPOINT           1501
REPLSSLPORT            1502
REPLSERVERGUID         60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3
```

```
MYREPLICATIONServer TARGET
MYPRIMARYSERVERNAME SERVER1
```

3.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Los usuarios no raíz deben especificar una ubicación para la tabla de réplica del nodo añadiendo la opción `nrtblepath` al archivo

dsm.sys. El cliente de copia de seguridad y archivado utiliza esta tabla para almacenar la información acerca de cada operación de copia de seguridad o archivado en el servidor de IBM Spectrum Protect.

Debe especificar una ubicación a la que tu ID de usuario tenga acceso. Por ejemplo:

```
nrtablepath /Volumes/nrtbl
```

Restricción: No especifique el directorio raíz (/) para la ubicación de la tabla de réplica del nodo.

4. Guarde y cierre el archivo de opciones del cliente.

5. Reinicie la GUI del cliente de archivado y copia de seguridad o inicie sesión en el servidor de IBM Spectrum Protect desde la interfaz de la línea de mandatos. El cliente está conectado a servidor secundario.

## Ejemplo

---

Después de configurar el cliente para la migración tras error automática, el cliente intenta iniciar sesión en el servidor y se muestra el siguiente ejemplo de salida de mandato:

```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de seguridad/archivado
  Versión de cliente 8, release 1, nivel 0.0
  Fecha/hora del cliente: 12/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Nombre de nodo: MY_NODE_NAME
ANS2106I Connection to primary IBM Spectrum Protect server 192.0.2.1 failed

ANS2107I Attempting to connect to secondary server TARGET at 192.0.2.9 : 1501

Nombre de nodo: MY_NODE_NAME
Session established with server TARGET: Windows
  Versión de servidor 8, release 1, nivel 0.0
  Fecha/hora del servidor: 12/16/2016 12:05:35  Último acceso: 12/15/2016 09:55:56

  Session established in failover mode to secondary server
ANS2108I Connected to secondary server TARGET.
```

## Qué hacer a continuación

---

Puede restaurar o recuperar cualquier dato de réplica en el modo de migración tras error.

### Conceptos relacionados:

Visión general de migración tras error de cliente automatizado

### Tareas relacionadas:

Restaurar o recuperar datos durante una migración tras error

### Referencia relacionada:

Forcefailover

 Sistemas operativos WindowsMyprimaryserver

Myreplicationserver

Nrtablepath

Replserverguid

Replservername

Replsslport

Repltcpport

Repltcpserveraddress

Userreplicationfailover

## Determinación del estado los datos replicados del cliente

---

Puede verificar si la copia de seguridad más reciente del cliente se replicó en el servidor secundario antes de restaurar o recuperar los datos desde servidor secundario.

## Acerca de esta tarea

---

Puede obtener el estado de los datos de cliente replicados para determinar si la copia de seguridad del cliente más reciente se replicó en el servidor secundario.

Si la indicación de fecha y hora de la operación de copia de seguridad más reciente coincide con la indicación de fecha y hora de la copia de seguridad de servidor secundario, el estado de la réplica es actual.

Si la indicación de fecha y hora de la operación de copia de seguridad más reciente es diferente de la indicación de fecha y hora de la copia de seguridad de servidor secundario, el estado de la réplica no es corriente. Esta situación puede ocurrir si ha realizado la copia de seguridad del cliente, pero antes de que se pueda replicar el nodo del cliente, el servidor primario pasa a estar no disponible.

## Procedimiento

Para determinar el estado de los datos del cliente replicado, emita el siguiente mandato en el indicador de mandatos:

```
dsmc query filesystem -detail
```

El siguiente ejemplo muestra la salida de la indicación de fecha y hora en el servidor y en la réplica del cliente, por tanto, el estado de la réplica es actual:

#	Fecha último Incr	Tipo	fsID	Unicode	Réplica	Espacio	archivos
1	00/00/0000 00:00:00	HFS		9	Yes	Current	/
	Fecha últ. alm.	Servidor			Local		
	-----	-----			-----		
	Backup Data :	04/22/2013 19:39:17			04/22/2013 19:39:17		
	Datos archivado:	Ninguna fecha disponible			Ninguna fecha disponible		

La siguiente salida de ejemplo muestra que la indicación de fecha hora del servidor y el cliente no coinciden, por tanto, el estado de réplica no es actual:

#	Fecha último Incr	Tipo	fsID	Unicode	Réplica	Espacio	archivos
1	00/00/0000 00:00:00	HFS		9	Yes	Not Current	/
	Fecha últ. alm.	Servidor			Local		
	-----	-----			-----		
	Backup Data :	04/22/2013 19:39:17			04/24/2013 19:35:41		
	Datos archivado:	Ninguna fecha disponible			Ninguna fecha disponible		

## Qué hacer a continuación

Si intenta restaurar los datos en el modo de migración tras error y el estado de réplica no es el actual, se muestra un mensaje que indica que los datos que está a punto de restaurar están desfasados. Puede decidir si va a seguir con la restaure el servidor primario esté online.

### Tareas relacionadas:

Restaurar o recuperar datos durante una migración tras error

### Referencia relacionada:

Nrtablepath

## Prevención de la migración tras error automática del cliente

Puede configurar el cliente para evitar que se realice la migración tras error automática al servidor secundario.

## Acerca de esta tarea

Es posible que le interese evitar la migración tras error automática, por ejemplo, si sabe que los datos del cliente no se replicaron al servidor secundario antes de que servidor primario se desconectara. En este caso, si no desea recuperar los datos replicados de es posible que el servidor secundario sea antiguo.

## Procedimiento

Para impedir que el nodo del cliente migre tras error al servidor secundario, añada la siguiente sentencia al archivo de opciones del cliente:

```
usereplicationfailover no
```

Este ajuste sustituye a la configuración que proporciona el servidor de IBM Spectrum Protect en el servidor primario.

## Resultados

El nodo del cliente no realiza la migración tras error de forma automática en el servidor secundario la próxima vez e intenta conectarse al servidor primario sin conexión.

**Tareas relacionadas:**

Determinación del estado los datos replicados del cliente

**Referencia relacionada:**

Use replication failover

## Forzar al cliente a la migración tras error






---

El cliente puede realizar la migración tras error al cliente servidor secundario si el servidor primario es operacional. Por ejemplo, puede utilizar esta técnica para verificar que el cliente va a realizar la migración al servidor secundario esperado.

### Procedimiento

---

Para forzar al cliente a que realice la migración tras error a servidor secundario, siga estos pasos:

-     Añada la opción `forcefailover yes` al archivo de opciones del sistema del cliente (`dsm.sys`).
-  Añada la opción `forcefailover yes` en el archivo de opciones del cliente (`dsm.opt`).
- Conéctese al servidor secundario reiniciando la GUI del cliente de archivado y copia de seguridad o iniciando una sesión de mandatos con el mandato `dsmc`.
- Opcional: En vez de actualizar el archivo de opciones, puede establecer una conexión con el servidor secundario si especifica la opción `-forcefailover=yes` con un mandato. Por ejemplo:

```
dsmc q sess -forcefailover=yes
```

### Qué hacer a continuación

---

Puede verificar que está conectado a servidor secundario mediante uno de los siguientes métodos:

- Compruebe el campo Secondary Server Information de la ventana Connection Information de la GUI del cliente de archivado y copia de seguridad.
- Compruebe la salida del mandato cuando inicie una sesión de mandatos. El estado del servidor secundario se muestra en la salida.

## Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack


---

Antes de realizar una copia de seguridad o archivado de los datos del cliente de Tivoli Storage Manager FastBack, deberá completar las tareas de configuración.

Asegúrese de que ha configurado el cliente de archivado y copia de seguridad y de que ha instalado el cliente de Tivoli Storage Manager FastBack.

Instale el cliente de FastBack utilizando la información de Tivoli Storage Manager FastBack.

 Después de instalar el cliente de FastBack, realice las siguientes tareas:

 Después de instalar el cliente de FastBack, complete las siguientes tareas. También puede utilizar el asistente para la configuración del cliente con Tivoli Storage Manager FastBack.

- Registre un nodo para cada cliente de FastBack en el que los datos se copian o archivan. El nombre de nodo tiene que ser el nombre de host abreviado del cliente de FastBack.

Esta es una configuración única que se realiza una vez para cada cliente de FastBack cuyos volúmenes necesitan una copia de seguridad o archivado.

Este paso de registro debe realizarse de forma manual solo cuando el cliente de archivado y copia de seguridad se utiliza como una aplicación autónoma.

El Centro de administración realiza el registro de este nodo de forma automática cuando el usuario crea planificaciones para el archivado o la copia de seguridad de datos de FastBack mediante el Centro de administración. A partir de la versión 7.1, el componente del Centro de administración ya no se distribuye con Tivoli Storage Manager o IBM Spectrum Protect. Los usuarios de FastBack que tienen un Centro de administración de una versión de servidor anterior pueden seguir utilizándolo para crear y modificar planificaciones de FastBack. Si no tiene instalado el Centro de administración, puede descargar la versión anterior de

<ftp://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/>. Si no tiene el Centro de administración instalado, tiene que crear y modificar planificaciones de FastBack en el servidor de IBM Spectrum Protect. Para obtener información sobre creación de planificaciones en el servidor, consulte la documentación del servidor de IBM Spectrum Protect

2. Utilice el mandato de servidor GRANT PROXY para otorgar autorización de proxy al nodo actual del cliente de archivado y copia de seguridad en cada nodo que represente al cliente de FastBack creado en el paso 1. El nodo de FastBack debe ser el destino y el nodo actual del cliente debe ser el proxy.

Se trata de una configuración única y la realiza el Centro de administración si es este el que inicia la copia de seguridad o archivado.

3. Ejecute el mandato set password para almacenar las credenciales de los repositorios de FastBack donde se conecta el cliente de archivado y copia de seguridad. Ejecute el mandato `set password -type=fastback` una vez para cada repositorio donde esté previsto que se conecte el cliente de copia de seguridad y archivado.


Las credenciales que se almacenan dependen de las siguientes configuraciones:


- o Cliente de archivado y copia de seguridad del servidor de FastBack
- o Cliente de archivado y copia de seguridad de FastBack Disaster Recovery Hub
- o Cliente de copia de seguridad y archivado en una estación de trabajo proxy dedicada

Para obtener información sobre cómo integrar IBM Spectrum Protect y Tivoli Storage Manager FastBack, consulte Integración de Tivoli Storage Manager FastBack y IBM Spectrum Protect.

#### Conceptos relacionados:

Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack

 Sistemas operativos WindowsAsistente para la configuración del cliente para Tivoli Storage Manager FastBack

 Sistemas operativos WindowsConfiguración del cliente de copia de seguridad y archivado para proteger datos del cliente FastBack

#### Referencia relacionada:

Establecer contraseña

 Sistemas operativos Windows

## Configuración del cliente de copia de seguridad y archivado para proteger datos del cliente FastBack

---

Puede configurar el cliente de copia de seguridad y archivado para proteger los datos del cliente FastBack mediante el asistente de configuración del cliente.

Para poder utilizar el asistente para la configuración del cliente de IBM Spectrum Protect para FastBack, deberá realizar las siguientes tareas:

- Asegúrese de que el servidor FastBack o FastBack Disaster Recovery Hub esté instalado y configurado para la retención de datos a corto plazo.
- Asegúrese también de que se ha tomado al menos una instantánea.
- Asegúrese de que el cliente de archivado y copia de seguridad esté correctamente configurado con el servidor de IBM Spectrum Protect. También asegúrese de que el servicio de aceptación de clientes (`dsmcad.exe`) se esté ejecutando. Puede utilizar el asistente de configuración de cliente de IBM Spectrum Protect de la GUI de cliente de copia de seguridad y archivado después de instalar el cliente de copia de seguridad y archivado.
- Lleve a cabo una configuración de post-instalación única con los siguientes fines:
  - o Para especificar el nombre de usuario y la contraseña de FastBack que utilizará el asistente, para consultar y montar volúmenes desde el repositorio de FastBack
  - o Para ejecutar scripts de planificador de IBM Spectrum Protect
- Configure el archivo de credenciales de FastBack. El ID de usuario que especifique debe tener autoridad administrativa de Tivoli Storage Manager FastBack.
  1. Configure el ID de usuario y la contraseña. Ejecute el siguiente mandato en la estación de trabajo en la que están instalados el cliente de copia de seguridad y archivado y el servidor FastBack o Disaster Recovery Hub:

```
cd <TSM_FastBack_install_location>\FastBack\shell
```

donde <TSM\_FastBack\_install\_location> es la ubicación del directorio donde se encuentra instalado el cliente de Tivoli Storage Manager FastBack.

2. Si no existe, cree una carpeta denominada FastbackTSMScripts en la unidad de sistema de la estación de trabajo utilizando el siguiente mandato:

```
mkdir <machine_system_drive>:\FastbackTSMScripts
```

### 3. Ejecute el mandato fastbackshell:

```
FastBackShell -c encrypt -u userName -d domain -p password -f  
<machine_system_drive>:\FastbackTSMScripts\credential.txt
```

En el ejemplo de mandato anterior se utilizan las siguientes opciones:

- -u especifica el nombre de usuario de administrador de Tivoli Storage Manager FastBack.
- -p especifica la contraseña del administrador de Tivoli Storage Manager FastBack.
- -d especifica el dominio de Tivoli Storage Manager FastBack para el nombre de usuario.
- -f especifica el archivo de salida donde se escriben las credenciales cifradas.

Importante: El archivo de credenciales debe generarse con el nombre "credential.txt". El archivo de credenciales debe también estar ubicado en el directorio FastbackTSMScripts de la unidad de sistema de la estación de trabajo para que el asistente funcione correctamente.

Puede utilizar el asistente para la configuración del cliente con la GUI Java™ del cliente de archivado y copia de seguridad o con el cliente web de archivado y copia de seguridad.

Siga estos pasos para utilizar el asistente para la configuración del cliente con la GUI de Java:

1. Asegúrese de que el cliente de archivado y copia de seguridad esté correctamente configurado con el servidor de IBM Spectrum Protect.
2. El asistente para la configuración se inicia de forma automática para crear el archivo de configuración.
3. Siga las instrucciones del panel para completar el asistente.
4. En la ventana principal de la GUI del cliente de archivado y copia de seguridad, seleccione Herramientas > Asistente para la configuración.
5. En la página de bienvenida, seleccione Ayuda para configurar el cliente para proteger los datos del cliente de FastBack y pulse Siguiente.
6. Utilice el asistente para completar el proceso de configuración.

Siga estos pasos para iniciar el asistente para la configuración del cliente en el cliente web:

1. Asegúrese de que el cliente web esté configurado correctamente con el servidor de IBM Spectrum Protect, y de que el servicio aceptador de cliente de IBM Spectrum Protect se esté ejecutando.

Para configurar el cliente web, siga estos pasos:





- a. En la ventana principal de la GUI del cliente de archivado y copia de seguridad de la GUI de Java, pulse en Herramientas > Asistente para la configuración.
  - b. En la página de bienvenida, seleccione Ayuda para configurar el cliente web y pulse Siguiente. Siga las instrucciones del panel para completar el asistente.
2. Inicie el cliente web. En el navegador web, especifique el nombre de nodo y el número de puerto de cliente donde se esté ejecutando el servicio aceptador de clientes.

Por ejemplo: `http://<nombre_máquina_o_dirección_ip>:1585`

3. En la ventana principal de la GUI del cliente de archivado y copia de seguridad, pulse Herramientas > Asistente para la configuración.
4. En la página de bienvenida, seleccione Ayuda para configurar el cliente para proteger los datos del cliente de FastBack y pulse Siguiente.
5. Utilice el asistente para completar el proceso de configuración.

#### Conceptos relacionados:

Asistente para la configuración del cliente para Tivoli Storage Manager FastBack

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X
















## Configuración y utilización del entorno en clúster





---

El término *clúster* tiene distintos significados en los distintos entornos. Puede significar alta disponibilidad, alto rendimiento, equilibrio de cargas, un entramado de sistemas informáticos o alguna combinación de estos términos.

Actualmente hay disponibles varios productos de clústeres para UNIX y Linux, y este apartado define los aspectos de un entorno en clúster que deben existir para que esta metodología de copia de seguridad funcione correctamente. Es necesario disponer de conocimientos básicos sobre las funciones de software del clúster. Las actividades relacionadas con el software de clúster, como por ejemplo el desarrollo de los scripts de inicio y detención de una aplicación, no se describen en este apartado.

Un entorno de clúster hace referencia a un entorno de UNIX o de Linux que presenta las características siguientes:













- Los discos se comparten entre estaciones de trabajo, ya sea de forma exclusiva (solamente un host accede al disco lógico cada vez) o de forma simultánea.
- Los discos parecen discos locales del host y no recursos de red.  
Importante: Monte los sistemas de archivos de forma local para el sistema, no a través de un protocolo de compartición de archivos basado en una LAN, como por ejemplo el sistema de archivos de red (NFS).
- Los puntos de montaje de los discos locales son idénticos en cada host físico en el entorno (si el sistema de archivos `/group1_disk1` falla del `NodoA` al `NodoB`, se montará en el `NodoB` como `/grupol_discol`).
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Visión general de entornos en clúster  
Los entornos en clúster se pueden configurar de muchas formas distintas. En este apartado se describen las configuraciones de clúster más conocidas.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster  
El cliente de copia de seguridad/archivado de ha sido diseñado para gestionar la copia de seguridad de las unidades de clúster colocando el cliente de copia de seguridad/archivado en el contexto de los grupos de recursos del clúster.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Habilitación del acceso al cliente web en un entorno de clúster  
Si se necesita acceso al cliente web de IBM Spectrum Protect durante una condición de migración tras error, tendrá que configurar el daemon de aceptación de clientes web asociado al clúster para poder llevar a cabo una migración tras error junto con el recurso de clúster.
-  Sistemas operativos AIX  Migración de configuraciones de AIX  IBM PowerHA SystemMirror antiguas  
Si actualmente utiliza el cliente de copia de seguridad y archivado en un entorno IBM® PowerHA SystemMirror mediante la opción `clusternode`, debe actualizar las configuraciones actuales. La opción `clusternode` ya no está admitida.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Visión general de entornos en clúster

---

Los entornos en clúster se pueden configurar de muchas formas distintas. En este apartado se describen las configuraciones de clúster más conocidas.





-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Activa/Activa: Agrupación de recursos de clúster  
En una configuración activa/activa, cada nodo gestiona de forma activa al menos un recurso y se configura como copia de seguridad para uno o más recursos del clúster. Activa/activa es la forma más común de un entorno de clúster.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Activa/Pasiva: Tolerante a errores  
En una configuración activa/pasiva, un nodo gestiona de forma activa el recurso.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Acceso simultáneo  
En una configuración simultánea, hay más de un nodo que gestiona un recurso. Cuando se produce un error, otros nodos continúan gestionando el recurso.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Activa/Activa: Agrupación de recursos de clúster

---

En una configuración activa/activa, cada nodo gestiona de forma activa al menos un recurso y se configura como copia de seguridad para uno o más recursos del clúster. Activa/activa es la forma más común de un entorno de clúster.



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Activa/Pasiva: Tolerante a errores

---

En una configuración activa/pasiva, un nodo gestiona de forma activa el recurso.

El otro nodo solamente se utiliza si el nodo principal detecta un error y el recurso tiene que llevar a cabo una sustitución por anomalía. Un clúster activo/pasivo es un subtipo de un clúster activo/activo.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Acceso simultáneo

---



En una configuración simultánea, hay más de un nodo que gestiona un recurso. Cuando se produce un error, otros nodos continúan gestionando el recurso.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster

El cliente de copia de seguridad/archivado de ha sido diseñado para gestionar la copia de seguridad de las unidades de clúster colocando el cliente de copia de seguridad/archivado en el contexto de los grupos de recursos del clúster.

### Acerca de esta tarea

De esta forma se puede sacar partido a la acción de copia de seguridad de datos de recursos locales (en vez de tener que acceder a los datos a través de la red) para maximizar el rendimiento de la operación de copia de seguridad y para gestionar los datos de copia de seguridad relacionados con el grupo de recursos. Por consiguiente, el cliente de copia de seguridad/archivado siempre puede realizar copias de seguridad de datos en recursos de clúster como si los datos fueran datos locales y maximizar el rendimiento de copia de seguridad. De esta forma se garantiza que se realiza una copia de seguridad de los datos importantes de errores del sistema.

Por ejemplo, un entorno de clúster activo/activo tiene tres hosts físicos en el clúster denominados `NodoA`, `NodoB` y `NodoC`.

Los nodos tienen las siguientes calidades:

- `NodoA` posee el recurso de clúster con un sistema de archivos `/A1` y `/A2`
- `NodoB` posee los recursos de cluster con sistemas de archivos `/B1` y `/B2`
- `NodoC` posee los recursos de clúster con los sistemas de archivos `/C1` y `/C2`

Nota: `NodoA` también puede tener dos volúmenes que no estén en clúster, `/fs1` y `/fs2`, de los que se debe realizar copia de seguridad.

Para obtener el mejor rendimiento posible de la copia de seguridad, tal vez desee que todos los nodos del clúster realicen las copias de seguridad de los sistemas de archivos compartidos que poseen. Cuando se produce una sustitución por anomalía, las tareas de copia de seguridad del nodo que ha fallado pasan al nodo en el que se ha producido la sustitución por anomalía. Por ejemplo, cuando se produce una sustitución por anomalía del `NodoA` al `NodoB`, la copia de seguridad de `/A1` y de `/A2` pasan al `NodoB`.

A continuación encontrará los requisitos previos antes de configurar el cliente de copia de seguridad/archivado para realizar una copia de seguridad de volúmenes en clúster y fuera del clúster:

- Se debe ejecutar un proceso del planificador del cliente de copia de seguridad/archivado para cada grupo de recursos que se vaya a proteger. En condiciones normales, cada nodo debería tener dos procesos del planificador: uno para los recursos del clúster y otro para los sistemas de archivo locales. Después de una anomalía, se inician procesos del planificador adicionales en un nodo para poder proteger los recursos que se han pasado a otro nodo.
- Los archivos de contraseñas del cliente de copia de seguridad/archivado se deben almacenar en discos del clúster para que después de la anomalía, la contraseña del cliente de copia de seguridad/archivado que se ha generado esté disponible para el nodo que toma el control.
- Los sistemas de archivos que se han de proteger como parte de un grupo de recursos se definen utilizando la opción del dominio del cliente de copia de seguridad/archivado. La opción del dominio se especifica en el archivo `dsm.sys`, que también debería estar almacenado en un disco del clúster para que el nodo que toma el control tenga acceso al mismo.

Lleve a cabo los pasos siguientes para configurar el cliente de copia de seguridad/archivado en un entorno de clúster.

### Procedimiento

1. Registre las definiciones de nodo del cliente de archivado y copia de seguridad en el servidor IBM Spectrum Protect. Todos los nodos del clúster deben estar definidos en el servidor de IBM Spectrum Protect. Si se definen varios recursos de clúster en un entorno de clúster para la sustitución por anomalía independiente, se deben definir nombres de nodo exclusivos para cada grupo de recursos. Para la configuración de ejemplo anterior de un clúster activo/activo de tres vías, defina tres nodos (uno para cada recurso), tal como se muestra a continuación: (1) `Protect: IBM>register node nodeA nodeApw domain=standard`, (2) `Protect: IBM>register node nodeB nodeBpw domain=standard`, (3) `Protect: IBM>register node nodeC nodeCpw domain=standard`.
2. Configure el archivo de opciones del sistema del cliente de archivado y copia de seguridad. Cada nodo del clúster debe tener secciones independientes del servidor para cada grupo de recursos del clúster con el fin de realizar una copia de seguridad en cada archivo `dsm.sys` respectivo. Debe asegurarse de que las secciones del servidor sean idénticas en los archivos de opciones del sistema de cada nodo. De forma alternativa, puede colocar el archivo `dsm.sys` en una ubicación del clúster compartida. Las secciones de servidor definidas para realizar copias de seguridad de volúmenes con clústeres deben tener las siguientes características especiales:

- o La opción nodename debe hacer referencia al nombre del nodo del cliente registrado en el servidor de IBM Spectrum Protect. Si no se ha definido el nombre del nodo del cliente, el nombre del nodo toma de forma predeterminada el nombre del host del nodo, que entra en conflicto con otros nombres de nodo que se utilizan en el mismo sistema cliente. Importante: Utilice la opción nodename para definir el nodo de cliente de forma explícita. node.
  - o La opción tcpclientaddress debe hacer referencia a la dirección IP de servicio del nodo del clúster.
  - o La opción passworddir debe hacer referencia a un directorio de los volúmenes compartidos que forman parte del grupo de recursos de clúster.
  - o Las opciones errorlogname y schedlogname deben hacer referencia a archivos de los volúmenes compartidos que forman parte del grupo de recursos de clúster para mantener un solo archivo de registro continuo.
  - o Todas las sentencias exclude deben hacer referencia a archivos de los volúmenes compartidos que forman parte del grupo de recursos de clúster.
  - o Si utiliza la opción inclexcl, debe hacer referencia a una vía de acceso de archivo en los volúmenes compartidos que forme parte del grupo del clúster.
  - o Los nombres de las secciones identificados con la opción servername deben ser idénticos en todos los sistemas.
3. Las demás opciones del cliente de copia de seguridad/archivado se pueden establecer como se desee. En el ejemplo siguiente, los tres nodos, `NodoA`, `NodoB` y `NodoC`, deben tener las siguientes tres secciones del servidor en sus archivos `dsm.sys`:

```
Servername      server1_nodeA
nodename       NodoA
commmethod     tcpip
tcpport        1500
tcpserveraddress server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess generate
passworddir    /A1/tsm/pwd
managementservices schedule
schedlogname   /A1/tsm/dsmsched.log
errorlogname   /A1/tsm/errorlog.log
```

```
Servername      server1_nodeB
nodename       NodoB
commmethod     tcpip
tcpport        1500
tcpserveraddress server1.example.com
tcpclientaddress nodeB.example.com
passwordaccess generate
passworddir    /B1/tsm/pwd
managementservices schedule
schedlogname   /B1/tsm/dsmsched.log
errorlogname   /B1/tsm/errorlog.log
```

```
Servername      server1_nodeC
nodename       NodoC
commmethod     tcpip
tcpport        1500
tcpserveraddress server1.example.com
tcpclientaddress nodeC.example.com
passwordaccess generate
passworddir    /C1/tsm/pwd
managementservices schedule
schedlogname   /C1/tsm/dsmsched.log
errorlogname   /C1/tsm/errorlog.log
```

4. Configure el archivo de opciones de usuario del cliente de archivado y copia de seguridad. El archivo de opciones (`dsm.opt`) debe residir en los volúmenes compartidos del grupo de recursos del clúster. Defina la variable de entorno `DSM_CONFIG` para que haga referencia a este archivo. Asegúrese de que el archivo `dsm.opt` tiene la siguiente configuración:
- o El valor de la opción `servername` debe ser la sección del servidor del archivo `dsm.sys` que define parámetros para realizar copias de seguridad de volúmenes con clústeres.
  - o Defina los sistemas de archivos de clústeres para que se realicen copias de seguridad de los mismos con la opción `domain`.
- Nota: Asegúrese de definir la opción de dominio en el archivo `dsm.opt` o especifique la opción en la planificación o en la línea de mandatos del cliente de copia de seguridad y archivado. Esto es para restringir las operaciones en clúster para recursos del clúster y las operaciones no en clúster para los recursos que no son del clúster.

En el ejemplo, los nodos `NodoA`, `NodoB` y `NodoC` tienen configurados sus respectivos archivos `dsm.opt` y la variable de entorno `DSM_CONFIG` tal como se indica a continuación:

**NodoA:**

```
1) Configure el archivo /A1/tsm/dsm.opt:

servername server1_nodeA
```

```
domain /A1 /A2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/A1/tsm/dsm.opt
```

**NodoB:**

1) Configure el archivo /B1/tsm/dsm.opt:

```
servername server1_nodeB  
domain /B1 /B2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/B1/tsm/dsm.opt
```

**NodoC:**

1) Configure el archivo /C1/tsm/dsm.opt:

```
servername server1_nodeC  
domain /C1 /C2
```

2) Emita el mandato siguiente o inclúyalo en el perfil de usuario:

```
export DSM_CONFIG=/C1/tsm/dsm.opt
```

5. Configure las definiciones de planificación para cada grupo de recursos del clúster. Tras llevar a cabo la configuración básica, defina las planificaciones automáticas para que las copias de seguridad de los recursos del clúster cumplan los requisitos de copia de seguridad. El procedimiento ilustra la configuración de planificación utilizando el planificador incorporado de IBM Spectrum Protect. Si utiliza un planificador adquirido a un proveedor, consulte la documentación que le suministra el proveedor del planificador.

- Defina una planificación en el dominio de política en el que están definidos los nodos del clúster. Asegúrese de que la ventana de inicio de la planificación es suficientemente grande para iniciar la planificación en el nodo de sustitución por anomalía si se produce un suceso de anomalía o de recuperación tras error. Esto significa que la duración de la planificación debe haberse establecido en un valor superior al tiempo que se tarda en llevar a cabo la copia de seguridad de los datos del clúster para ese nodo, en condiciones normales.

Si la reconexión se realiza en el intervalo de inicio de ese suceso, se reiniciará el mandato planificado. Esta copia de seguridad incremental planificada vuelve a examinar los archivos enviados al servidor antes de la sustitución. Entonces, la copia de seguridad "vuelve" al lugar en el que se detuvo antes de la situación de sustitución.

En el ejemplo siguiente, la planificación `clus_backup` se define en el dominio estándar para iniciar la copia de seguridad cada día a las 12:30 A.M. con una duración establecida en dos horas (el tiempo normal para una copia de seguridad de los datos de cada nodo).

```
Protect: IBM>define schedule standard clus_backup action=incr  
starttime=00:30 startdate=TODAY Duration=2
```

- Asocie la planificación con todos los nodos del cliente de copia de seguridad/archivado definidos para realizar una copia de seguridad de los recursos del clúster del siguiente modo: (1) `Protect: IBM>define association standard clus_backup nodeA`, (2) `Protect: IBM>define association standard clus_backup nodeB`, (3) `Protect: IBM>define association standard clus_backup nodeC`.

6. Configure el servicio de planificador para realizar la copia de seguridad. En cada nodo cliente, se debe configurar un servicio de planificador para cada recursos del cual sea ese nodo responsable de realizar la copia de seguridad, en condiciones normales. La variable de entorno `DSM_CONFIG` de cada servicio de planificador de recursos debe establecerse para que haga referencia al archivo `dsm.opt` correspondiente a ese recurso. Para el ejemplo de configuración, se deben crear los siguientes scripts de shell para poder iniciar los procesos `dsmcad`, según convenga, desde cualquier nodo del clúster.

```
NodoA: /A1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/A1/tsm/dsm.opt  
dsmcad  
NodoB: /B1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/B1/tsm/dsm.opt  
dsmcad  
NodoC: /C1/tsm/startsched  
#!/bin/ksh  
export DSM_CONFIG=/C1/tsm/dsm.opt  
dsmcad
```

7. Defina el cliente de archivado y copia de seguridad en la aplicación del clúster. Para continuar con la copia de seguridad del recurso que ha fallado después de una condición de sustitución por anomalía, el servicio de planificador de IBM Spectrum Protect (para cada nodo del cliente del clúster) debe estar definido como recurso en la aplicación del clúster para poder participar en el proceso de sustitución por anomalía. Es necesario que sea así para poder proseguir con la copia de seguridad de los recursos anómalos desde el nodo que toma control del recurso. Si se produjera un error, la copia de seguridad del recurso que ha fallado sería incompleta. Los scripts de ejemplo del paso 5 se pueden asociar a los recursos del clúster para garantizar que se inician en los nodos del clúster mientras que los recursos de discos que se protegen pasan de un nodo a otro. Los pasos reales necesarios para configurar el servicio de planificador como recursos del clúster son específicos para el software del clúster. Consulte la documentación de su aplicación del clúster si desea información adicional.

8. Asegúrese de que se genere la contraseña de cada nodo y que se guarde en la memoria caché en la ubicación correcta que se ha especificado mediante la opción `passworddir`. Esta validación se puede realizar siguiendo estos pasos:

a. Compruebe que cada nodo se pueda conectar al servidor de IBM Spectrum Protect sin la solicitud de contraseña. Puede hacerlo ejecutando la interfaz de línea de mandatos del cliente de archivado y copia de seguridad y emitiendo el mandato siguiente en cada nodo:

```
#dsmc query session
```

Si se le solicita que indique su contraseña, escríbala para que el mandato se ejecute correctamente y vuelva a ejecutar el mandato. La segunda vez, el mandato se debería ejecutar sin que se le solicite la contraseña. Si se le solicita la contraseña, compruebe la configuración.

b. Compruebe que todos los demás nodos del clúster pueden iniciar sesiones en el servidor de IBM Spectrum Protect para el nodo que ha realizado la sustitución por anomalía. Puede hacerlo ejecutando los mismos mandatos, según se ha descrito en el paso anterior, en los nodos de copia de seguridad. Por ejemplo, para validar si el `NodoB` y el `NodoC` pueden iniciar una sesión como `NodoA` en el suceso de sustitución por anomalía sin que se le solicite la contraseña, ejecute los mandatos siguientes en el `NodoB` y en el `NodoC`

```
#export DSM_CONFIG=/A1/tsm/dsm.opt  
#dsmc query session
```

La solicitud de la contraseña puede aparecer en esta ocasión, pero solo ahora. Si se le solicita la contraseña, es porque no estaba almacenada en la ubicación compartida correcta. Compruebe el valor de la opción `passworddir` que utiliza el `NodoA` y siga otra vez los pasos de configuración.

c. Asegúrese de que las planificaciones se ejecutan correctamente en cada nodo. Puede activar una planificación definiendo el tiempo de inicio de la planificación en `now`. Recuerde restablecer el tiempo de inicio tras finalizar la comprobación.

```
Protect: IBM>update sched standard clus_backup starttime=now
```

d. La sustitución por error y la recuperación tras error entre el `nodeA` y el `nodeB`, mientras el `nodeA` está en medio de la operación de copia de seguridad y la ventana de inicio de la planificación, siguen siendo válidas. Compruebe que la copia de seguridad incremental continúa ejecutándose y que finaliza correctamente tras una sustitución por anomalía y una recuperación por error.

e. Emita el mandato siguiente para que caduque la contraseña del nodo (`nodeA`). Asegúrese de que la copia de seguridad continúa normalmente en las operaciones normales del clúster, así como las operaciones de sustitución por anomalía y recuperación tras error:

```
Protect: IBM>update node nodeA forcepw=yes
```

9. Configure el cliente de copia de seguridad/archivado para realizar una copia de seguridad de los recursos locales.

a. Defina nodos de cliente en el servidor de IBM Spectrum Protect. De los recursos locales nunca se debería realizar copia de seguridad ni archivado utilizando los nombres de nodo definidos para los datos del clúster de copia de seguridad. Si se hacen copias de seguridad de los volúmenes locales no definidos como recursos de clúster, se deben usar nombres de nodo independientes (e instancias de cliente independientes) tanto para los volúmenes con clústeres como para los volúmenes sin clústeres.

En el ejemplo siguiente, vamos a suponer que solamente el `NodoA` tiene sistemas de archivos locales `/fs1` y `/fs2` de los que se deba realizar copia de seguridad. Para poder gestionar los recursos locales, registre un nodo `NodeA_local` en el servidor de IBM Spectrum Protect: `Protect: IBM>register node nodeA_local nodeA_localpw domain=standard.`

b. Añada una stanza independiente en cada archivo de opciones del sistema del nodo `dsm.sys` que tenga que hacer copia de seguridad de los recursos locales con las características especiales siguientes:

- El valor de la opción `tcpclientaddress` debe ser el nombre de host local o la dirección IP. Ésta es la dirección IP que se utiliza para el tráfico principal desde y hacia el nodo.
- Si el cliente realiza copias de seguridad y restaura volúmenes sin clústeres sin estar conectado al clúster, el valor de la opción `tcpclientaddress` debe ser la dirección IP de arranque. Se trata de la dirección IP que se utiliza para iniciar el sistema (nodo) antes de que se una al clúster:

Sección de ejemplo para `NodoA_local`:

```
Servername      server1_nodeA_local
nodename        nodeA_local
commmethod      tcpip
tcpport         1500
tcpserveraddress server1.example.com
tcpclientaddress nodeA_host.example.com
passwordaccess  generate
managementservices schedule
```

c. Defina el archivo de opciones del usuario `dsm.opt` en una vía de acceso que esté en un recurso fuera del clúster.

- El valor de la opción `servername` debe ser la sección del servidor del archivo `dsm.sys` que define parámetros para realizar copias de seguridad de volúmenes con clústeres.
- Utilice la opción de dominio para definir los sistemas de archivos fuera del clúster para que se realicen copias de seguridad de los mismos.

Nota: Asegúrese de definir la opción del dominio en el archivo `dsm.opt` o de especificar la opción en la planificación o en la línea de mandatos del cliente de copia de seguridad y archivado para restringir las operaciones de copia de seguridad/archivado a volúmenes fuera del clúster.

En el ejemplo siguiente, el `nodeA` utiliza el archivo `/home/admin/dsm.opt` siguiente y establece el entorno de `DSM_CONFIG` para que haga referencia a `/home/admin/A1.dsm.opt`.

Contenido de `/home/admin/A1.dsm.opt`

```
servername ibm_nodeA_local
domain      /fs1 /fs2
```

```
export DSM_CONFIG=/home/admin/A1.dsm.opt
```

d. Defina y configure una planificación para llevar a cabo la copia de seguridad incremental para sistemas de archivos fuera del clúster.

```
Protect: IBM>define schedule standard local_backup action=incr
starttime=00:30 startdate=TODAY Duration=2
```





Asocie la planificación con todos los nodos del cliente de copia de seguridad/archivado definidos para realizar copia de seguridad de los recursos de fuera del clúster.

```
Protect: IBM>define association standard nodeA_local
```

10. Restaure los datos del sistema de archivos del clúster. Se realiza copia de seguridad de todos los volúmenes de un recurso del clúster bajo el nodo de destino definido para ese recurso del clúster. Si tiene que restaurar los datos que residen en un volumen del clúster, puede hacerlo desde el nodo cliente que posee el recurso del clúster en el momento de la restauración. El cliente de copia de seguridad/archivado debe utilizar el mismo archivo de opciones de usuario (`dsm.opt`) que se utilizó durante la operación de copia de seguridad para restaurar los datos. No hay más requisitos de configuración necesarios para restaurar datos en volúmenes de clúster.
11. Restaure los datos del sistema de archivos locales. Se realiza copia de seguridad de los volúmenes fuera de clúster con un nombre de nodo independiente configurado para las operaciones fuera del clúster. Para restaurar los datos, el cliente de archivado y copia de seguridad debe utilizar el mismo archivo de opciones de usuario `dsm.opt` que se utilizó durante la copia de seguridad. En el ejemplo, establezca la variable de entorno `DSM_CONFIG` para que haga referencia a `/home/admin/A1.dsm.opt` antes de llevar a cabo una restauración del cliente para el nodo local `nodeA_local`.

#### Conceptos relacionados:

Restauración de los datos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Habilitación del acceso al cliente web en un entorno de clúster

Si se necesita acceso al cliente web de IBM Spectrum Protect durante una condición de migración tras error, tendrá que configurar el daemon de aceptación de clientes web asociado al clúster para poder llevar a cabo una migración tras error junto con el recurso de clúster.

### Antes de empezar

A partir de IBM Spectrum Protect Versión 8.1.2, ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior. Sin embargo, aún puede utilizar el cliente web para conectarse a servidores de IBM Spectrum Protect V8.1.1, V8.1.0 o V7.1.7 y anteriores. Para obtener más información, consulte Utilización del cliente web en el nuevo entorno de seguridad.

## Acerca de esta tarea

Tras completar los pasos de configuración que se describen en el apartado *Configuración del cliente de copia de seguridad/archivado en un entorno de clúster*, lleve a cabo los pasos adicionales que se describen a continuación para finalizar la configuración del acceso al cliente web:

## Procedimiento

1. Configure el daemon de aceptación de clientes para gestionar el cliente web y el planificador. El daemon de aceptación de clientes se debe configurar para que gestione planificadores así como el acceso al cliente web. Así se reduce la cantidad de daemons que se tienen que configurar como aplicaciones de clúster y, por tanto, se simplifica la configuración y la administración. Cuando se produce una migración tras error, se inicia el aceptador de clientes en el nodo que gestiona el cambio de control.
2. Actualice la opción `managedservices` en el archivo de opciones del sistema `dsm.sys` en cada nodo para cada sección del servidor, tal como se muestra a continuación para el `NodoA`:

```
Servername      server1_NodoA
nodename        NodoA
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
schedlog        /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
managedservices webclient schedule
```

3. Configure el daemon de aceptación de clientes para que utilice un puerto HTTP conocido. De forma predeterminada, el daemon de aceptación de clientes utiliza el puerto HTTP 1581, cuando está disponible, para acceder al cliente web. Si el puerto no está disponible, el aceptador de clientes busca el primer puerto disponible, comenzando por el 1581. En una condición de migración tras error de una configuración de clúster activa-activa, probablemente haya un sistema host de clúster para la migración tras error que ejecute varias instancias del aceptador de clientes. Si se utilizan valores predeterminados para el puerto HTTP, el nodo de migración tras error utiliza cualquier puerto disponible para el aceptador de clientes que se migra, puesto que probablemente el puerto predeterminado está siendo utilizado por procesos actuales del aceptador de clientes del host de migración tras error. Esto ocasiona problemas para el cliente web asociado al aceptador de clientes que se ha migrado, puesto que los usuarios del cliente web no conocen el nuevo puerto HTTP. `httpport` puede utilizar la opción de especificar los puertos concretos para el acceso al cliente web de este recurso. Así podrá utilizar el mismo puerto cuando se conecte desde un navegador web, independientemente del nodo que preste servicio al recurso del clúster. Añada la opción `httpport` en el archivo de opciones del sistema (`dsm.sys`) en cada nodo para cada sección del servidor tal como se indica a continuación, asegurándose de que cada sección utilice un valor exclusivo:

```
Servername      server1_NodoA
nodename        NodoA
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess  generate
passworddir     /A1/tsm/pwd
managedservices webclient schedule
schedlog        /A1/tsm/dsmsched.log
errorlogname    /A1/tsm/errorlog.log
httpport        1510
```


```
Servername      server1_NodoB
nodename        NodoB
commmethod      tcpip
tcpp            1500
tcps            server1.example.com
tcpclientaddress nodeB.example.com
passwordaccess  generate
passworddir     /B1/tsm/pwd
managedservices webclient schedule
schedlog        /B1/tsm/dsmsched.log
errorlogname    /B1/tsm/errorlog.log
httpport        1511
```

```
Servername      server1_NodoC
nodename        NodoC
```

```

commmethod      tcpip
tcpp            1500
tcps           server1.example.com
tcpclientaddress nodeC.example.com
passwordaccess generate
passworddir     /C1/tsm/pwd
managementservices webclient schedule
schedlogn      /C1/tsm/dsmsched.log
errorlogname   /C1/tsm/errorlog.log
httpport       1512

```

 Sistemas operativos AIX

## Migración de configuraciones de AIX IBM PowerHA SystemMirror antiguas

Si actualmente utiliza el cliente de copia de seguridad y archivado en un entorno IBM® PowerHA SystemMirror mediante la opción `clusternode`, debe actualizar las configuraciones actuales. La opción `clusternode` ya no está admitida.

### Acerca de esta tarea

Siga estos pasos para actualizar sus configuraciones actuales:

### Procedimiento

1. Actualice el archivo de opciones del sistema del cliente de archivado y copia de seguridad. Al igual que con la opción `clusternode`, cada nodo del clúster debe continuar teniendo secciones de servidor independientes para cada grupo de recursos del clúster con el fin de realizar una copia de seguridad en cada archivo `dsm.sys` respectivo. El archivo `dsm.sys` existente para `NodoA` puede parecerse al siguiente:

```

Servername      server1_nodeA
commmethod      tcpip
tcpp            1500
tcps           server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess generate
passworddir     /A1
clusternode     yes
managementservices schedule
schedlogn      /A1/dsmsched.log
errorlogname   /A1/errorlog.log

```

2. Observe que en este ejemplo se utiliza la opción `nodename`. Realice los cambios siguientes en el archivo `dsm.sys` existente para `NodoA`.
  - Elimine la opción `clusternode`.
  - Especifique una opción `nodename` si todavía no lo ha hecho.
3. En nuevo archivo `dsm.sys` para `NodoA` debería parecerse al siguiente:

```

Servername      server1_nodeA
commmethod      tcpip
nodename       myclus (myclus is the existing cluster name )
tcpp            1500
tcps           server1.example.com
tcpclientaddress nodeA.example.com
passwordaccess generate
passworddir     /A1
managementservices schedule
schedlogn      /A1/dsmsched.log
errorlogname   /A1/errorlog.log

```

4. Registre los nodos del cliente de archivado y copia de seguridad en el servidor IBM Spectrum Protect. Si en el primer paso se agregan nuevos nodos del cliente de copia de seguridad/archivado para sustituir el valor actual predeterminado del nombre del nodo de clúster, registre esos nodos en el servidor de IBM Spectrum Protect.
5. Actualice las definiciones de planificación. Si se añaden nuevos nodos del cliente de copia de seguridad/archivado en el paso anterior, asegúrese de que las definiciones de planificación de copia de seguridad que se han utilizado antes de realizar la copia de seguridad de estos datos de nodo estén asociadas a los nombres de los nuevos nodos del cliente.
6. Valide la configuración. Para obtener más información detallada, consulte Configuración de un cliente de copia de seguridad/archivado en un entorno de clúster.

 Sistemas operativos Windows

## Configuración del cliente de copia de seguridad/archivado en un entorno de servidor en clúster

---

Puede instalar localmente el software del cliente de copia de seguridad/archivado en cada nodo de un entorno de clúster de Microsoft Cluster Server (MSCS) o Veritas Cluster Server (VCS).

Puede utilizar el cliente de copia de seguridad y archivado en un entorno VCS en las plataformas de servidor Windows admitidas.

También puede instalar y configurar el servicio del planificador para cada nodo del clúster a fin de gestionar todos los discos locales y cada grupo de clúster que contenga recursos de disco físico.




Por ejemplo, el clúster MSCS mscs-cluster contiene dos nodos: nodo-1 y nodo-2 y dos grupos de clúster que contienen recursos de disco físico: grupo-a y grupo-b. En este caso, debe instalarse una instancia del servicio del planificador de copia de seguridad/archivado de IBM Spectrum Protect para el nodo-1, el nodo-2, el grupo-a y el grupo-b. De este modo se garantiza la disponibilidad de los recursos adecuados para el cliente de copia de seguridad/archivado cuando se traspasan (o se sustituyen) discos entre nodos de clúster.

La opción clusternode garantiza que el cliente gestiona lógicamente los datos de copia de seguridad, independientemente de qué nodo de clúster realiza copia de seguridad de un recurso de disco de clúster. Utilice esta opción para nodos de cliente que procesen recursos de disco de clúster, y no recursos locales.

Nota: Debe establecer la opción clusternode: en *yes* para todas las operaciones de clúster que IBM Spectrum Protect gestiona. El uso desigual de la opción clusternode para un nombre de nodo de clúster de IBM Spectrum Protect determinado puede dar lugar a que el cliente invalide la contraseña cifrada del nombre de nodo de clúster y solicite al usuario que introduzca de nuevo la contraseña durante la siguiente invocación del programa de cliente.

Utilice la opción optfile para llamar correctamente al archivo dsm.opt (clúster) adecuado para todos los programas de cliente para garantizar la funcionalidad correcta para las operaciones relacionadas con clústeres.

La instalación y configuración del cliente de archivado y copia de seguridad en un entorno de clúster depende de la tecnología del servidor de clúster utilizada (MSCS o VCS) y del sistema operativo que utilicen los nodos en el clúster.

-  Sistemas operativos Windows Protección de los datos en los clústeres de MSCS (clientes del servidor Windows)  
Se utiliza un asistente de configuración de clientes en nodos en un entorno en clúster de MSCS para automatizar y simplificar la configuración del cliente de archivado y copia de seguridad para proteger los grupos de discos de clúster. El asistente solo puede utilizarse en los nodos que ejecutan clientes del servidor de Windows compatibles en su sistema operativo.
-  Sistemas operativos Windows Configurar el cliente web en un entorno en clúster  
Para utilizar el cliente web en un entorno de clúster, debe configurar la GUI Java del cliente de copia de seguridad/archivado para que se ejecute en un entorno de clúster.
-  Sistemas operativos Windows Preguntas frecuentes  
Esta sección contiene algunas preguntas y respuestas frecuentes acerca de la utilización de los servicios en clúster.

### Referencia relacionada:


Optfile

 Sistemas operativos Windows

## Protección de los datos en los clústeres de MSCS (clientes del servidor Windows)

---

Se utiliza un asistente de configuración de clientes en nodos en un entorno en clúster de MSCS para automatizar y simplificar la configuración del cliente de archivado y copia de seguridad para proteger los grupos de discos de clúster. El asistente solo puede utilizarse en los nodos que ejecutan clientes del servidor de Windows compatibles en su sistema operativo.

-  Sistemas operativos Windows Configuración de la protección de clúster (clientes de Windows Server)  
Utilice el asistente de clústeres de IBM Spectrum Protect para configurar el cliente de archivado y copia de seguridad a fin de proteger los recursos de clúster. El asistente recopila la información necesaria para que el cliente de archivado y copia de seguridad pueda proteger los recursos del clúster, e inicie sesión en el servidor.

 Sistemas operativos Windows


## Configurar el cliente web en un entorno en clúster


---


Para utilizar el cliente web en un entorno de clúster, debe configurar la GUI Java del cliente de copia de seguridad/archivado para que se ejecute en un entorno de clúster.



A partir de IBM Spectrum Protect Versión 8.1.2, ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior. Sin embargo, aún puede utilizar el cliente web para conectarse a servidores de IBM Spectrum Protect V8.1.1, V8.1.0 o V7.1.7 y anteriores. Para obtener más información, consulte Utilización del cliente web en el nuevo entorno de seguridad.

Consulte  Sistemas operativos Windows Configuración de la protección de clúster (clientes de Windows Server) para obtener información detallada sobre la instalación y configuración del cliente de archivado y copia de seguridad en un entorno MSCS o VCS.

-  Sistemas operativos Windows Configurar el cliente web para procesar recursos de disco en clúster  
Tras instalar y configurar el cliente de copia de seguridad/archivado en un entorno MSCS o VCS, debe realizar unos pasos para procesar recursos de disco de clúster.

 Sistemas operativos Windows

## Preguntas frecuentes

---

Esta sección contiene algunas preguntas y respuestas frecuentes acerca de la utilización de los servicios en clúster.

### Acerca de esta tarea

---

P: ¿Cómo debo configurar un acceso directo para la GUI del cliente de archivado y copia de seguridad en un entorno de clúster?

R: Para configurar un icono de la GUI del cliente de archivado y copia de seguridad (por ejemplo, en el escritorio de Windows) que se podrá utilizar para gestionar operaciones para un grupo de recursos de clúster en un clúster de Windows, siga estos pasos:

### Procedimiento

---

1. Pulse el botón derecho del ratón y seleccione Nuevo > Acceso directo.
2. En la ventana que aparece, busque la vía de acceso del ejecutable dsm.exe (situado de forma predeterminada en el directorio `C:\archivos de programa\tivoli\tsm\baclient\`). Si escribe la vía de acceso en vez de utilizar el botón Examinar, la vía de acceso debe indicarse entre comillas. Por ejemplo: "`C:\Archivos de programa\tivoli\tsm\baclient\dsm.exe`"
3. Después de especificar la vía de acceso y el ejecutable en el campo de texto, añada la siguiente información después de las comillas de cierre (deje un espacio entre las comillas y lo siguiente): `-optfile="x:\path\to\cluster\dsm.opt"`. Esto identifica el archivo de opciones de clúster de IBM Spectrum Protect adecuado que desea utilizar. En este ejemplo se da por supuesto que el archivo de opciones del clúster está situado en la carpeta "`x:\path\to\cluster\`" y se denomina `dsm.opt`.
4. La línea completa del campo de texto debe parecerse a la siguiente: "`C:\Program Files\tivoli\tsm\baclient\dsm.exe -optfile="x:\path\to\cluster\ dsm.opt"`".
5. Pulse Siguiente y otorgue a este método abreviado un nombre que tenga sentido, como por ejemplo, GUI de copia de seguridad/archivado: grupo de clúster X.
6. Pulse Finalizar. Ahora debería aparecer un icono en el escritorio. Las propiedades de este icono muestran el siguiente destino correcto, tal como se ha indicado en el paso 4: "`C:\Archivos de programa\tivoli\tsm\baclient\dsm.exe" -optfile="x:\path\to\cluster\ dsm.opt"`".

### Resultados

---

P: ¿Cómo verificar que una instalación del servicio del planificador en un entorno de clúster funciona?

R: La instalación de un servicio del planificador para un grupo de recursos en clúster de Microsoft puede requerir mucho tiempo y puede alargarse debido a equivocaciones y errores en la sintaxis de los mandatos que se utilizan. Si los mandatos se entran con cuidado y se anota la información importante sobre la instalación del clúster se podrá minimizar el tiempo necesario. Para instalar satisfactoriamente un servicio del planificador para entornos en clúster de Microsoft:

1. Lea detenidamente la información de este apéndice para obtener la sintaxis correcta para instalar el servicio del planificador para un grupo de clúster.
2. Asegúrese de que se utilizan los archivos `dsm.opt` adecuados para el clúster. En una estación de trabajo normal, sólo se utiliza un archivo `dsm.opt`. En un entorno de clúster, son necesarios más archivos `dsm.opt`. Cada grupo de clúster incluido en la copia de seguridad debe tener su propio archivo `dsm.opt`. Un grupo de clúster es cualquier grupo indicado bajo la carpeta GRUPOS de la herramienta Administrador de clústeres de Microsoft o VCS Configuration Editor.
3. Comprenda el significado de las siguientes opciones `dsmcutil.exe` y cuándo utilizarlas. (1) `/clusternode:clusternode` - Especifica el nombre del clúster de Microsoft, donde `clusternode` es el nombre de nivel superior del árbol dentro de la herramienta Administrador de clústeres de Microsoft o VCS Configuration Editor. Utilice esta opción con `dsmcutil.exe` sólo al instalar un servicio de planificador para un grupo de clúster. No especifique un nombre de clúster que tenga más de 64 caracteres. Si especifica más de 256 caracteres y utiliza Veritas Storage Foundation con la función de alta disponibilidad o una configuración de Microsoft Cluster Server, es posible que no pueda instalar o iniciar el servicio del planificador de IBM Spectrum Protect. (2) `/clusternode:yes` - Especifica que desea activar el soporte para recursos de clúster. Utilice esta opción en el archivo `dsm.opt` para cada grupo de clúster y con `dsmcutil.exe` al instalar un servicio del planificador para un grupo de clúster.

4. Es frecuente que se cometan equivocaciones al escribir el mandato `dsmcutil.exe`. Una forma fácil de evitarlo es crear un archivo de texto temporal al que pueda acceder el grupo de clúster (por ejemplo, colóquelo en una unidad del clúster que pertenezca a dicho grupo de clúster) y escriba el mandato en este archivo. Cuando sea necesario, córtelo y péguelo en el indicador de DOS y pulse la tecla Intro. Con ello se garantiza la coherencia de la sintaxis del mandato independientemente del sistema en el que lo escriba.
5. Si el servicio del planificador no puede reiniciarse después de producirse una sustitución por anomalía del grupo de clúster (por ejemplo, mediante la opción `MOVE GROUP` en el Administrador de clústeres), podrían surgir problemas de sincronización de contraseñas entre las dos estaciones de trabajo del clúster. Una forma fácil de verificar si las contraseñas son iguales es acudir a la siguiente clave de registro de cada estación de trabajo y comparar el valor de contraseña cifrada: `HKEY_LOCAL_MACHINE\SOFTWARE\IBM\ADSM\CurrentVersion\Nodes\nodename\servername`.

Si las claves cifradas para este nodo no coinciden en las dos estaciones de trabajo del clúster, significa que hay una discrepancia de contraseñas en una o en las dos estaciones de trabajo finales. Para corregir este problema, utilice el programa `dsmc.exe` para actualizar manualmente la contraseña en las dos estaciones de trabajo.

Por ejemplo, suponga que la unidad Y: forme parte de un grupo de clúster que tiene problemas cuando se hace su copia de seguridad mediante un servicio del planificador. El directorio `Y:\tsm` contiene el archivo `dsm.opt` para este grupo de clúster en el directorio `Y:\tsm`. Para actualizar la contraseña manualmente, especifique el siguiente mandato en las dos estaciones de trabajo finales: `dsmc -optfile=Y:\tsm\dsm.opt -clusternode=yes`, y utilice el siguiente mandato para recibir la solicitud del nombre de nodo y contraseña: `dsmc q se -optfile=Y:\tsm\dsm.opt -clusternode=yes`.

Verifique que las contraseñas están sincronizadas y reinicie el servicio del planificador para verificar si la contraseña sigue siendo correcta. Si sigue sin existir coincidencia entre las contraseñas, ello podría deberse a un error de sintaxis en el mandato `dsmcutil.exe` original que se ha utilizado para instalar el servicio del planificador. En este caso, desinstale el servicio del planificador (con el mandato `dsmcutil remove /name:nombre_planificación`) y vuelva a instalar el servicio del planificador (utilizando la sintaxis del archivo de texto compartido, como se ha descrito anteriormente).

P: ¿Cómo agregar una unidad de clúster a un recurso del servicio del planificador del clúster existente para la copia de seguridad?

R: Para agregar un recurso de unidad de clúster adicional a un servicio del planificador del clúster del cliente de copia de seguridad y archivado existente, deben modificarse o actualizarse los siguientes componentes de modo que reflejen correctamente este cambio:

1. El recurso de la unidad de clúster y todos los recursos compartidos relacionados deben existir y residir dentro del grupo de clúster designado, como se ha definido en la herramienta Administrador de clústeres de Microsoft o en VCS Configuration Editor. El grupo de clúster designado debe contener el recurso del servicio del planificador del clúster para el que se añade esta nueva unidad.
2. Debe modificarse el archivo `dsm.opt` utilizado por el recurso del servicio del planificador de clúster designado de forma que incluya el recurso de unidad de clúster adicional en la sentencia de la opción `domain`. Por ejemplo, si desea añadir la unidad `R:\` y la sentencia `domain` identifica actualmente las unidades de clúster `Q:` y `S:`, actualice la sentencia `domain` del archivo `dsm.opt` como se indica a continuación: `domain Q: S: R:`
3. Debe modificar las propiedades del recurso del servicio del planificador del clúster de forma que incluya este archivo en la lista de los recursos dependientes que son necesarios para activar este recurso. Así se garantiza que el recurso de unidad de clúster que se añade se incluya en las nuevas copias de seguridad y para las copias de seguridad que se ejecutan después de producirse una sustitución por anomalía.

Después de efectuar los cambios indicados anteriormente, desactive el recurso del servicio del planificador de clúster y actívelo otra vez. La planificación ahora debe procesar este recurso adicional para las copias de seguridad.

P: Se ha eliminado el servicio de aceptación de clientes y ahora el recurso del servicio genérico para el grupo de clúster está fallando.

¿Cómo se puede corregir?

R: El aceptador de clientes puede utilizarse para controlar el planificador, el cliente web o ambos para un entorno de clúster. Si se elimina el aceptador de clientes sin actualizar el recurso de clúster genérico, el recurso falla. Para corregirlo, haga lo siguiente:

1. Verifique qué servicio del planificador estaba controlado por el aceptador de clientes.
2. Mediante la herramienta Administrador de clústeres de Microsoft o VCS Configuration Editor, vaya a la ventana de propiedades del recurso del servicio, seleccione la ficha `Parámetros` y escriba el nombre del servicio del planificador correcto que debe utilizarse.
3. Repita los pasos uno y dos para cada grupo de clúster gestionado por el aceptador de clientes específico.
4. Para probar el recurso del servicio actualizado, inicie una anomalía del recurso. Si el recurso vuelve a ponerse en línea sin anomalías, la actualización ha funcionado correctamente.

Nota: Para desactivar totalmente el servicio de aceptación de clientes, elimine la opción `managedservices` del archivo `dsm.opt` del grupo de clúster o conviértala en un comentario.



## Configuración del soporte de copias de seguridad de imagen en línea

---

Si está configurada la característica de imagen en línea, el cliente de copia de seguridad y archivado realiza una copia de seguridad de imagen basada en instantánea durante la cual el volumen real queda disponible para las otras aplicaciones del sistema.

### Acerca de esta tarea

---

Durante el proceso de copia de seguridad de imagen activada, se mantiene una imagen constante del volumen.

Para configurar la copia de seguridad de imágenes en línea, realice los pasos siguientes:

### Procedimiento

---

1. Seleccione Programas de utilidad > Asistente de configuración en la ventana principal de la GUI del cliente de copia de seguridad y archivado. Aparece el panel del asistente para la configuración de cliente.
2. Seleccione Ayuda para configurar el soporte de imágenes en línea y pulse Siguiente. Aparece el panel para el soporte de imágenes en línea.
3. Pulse Servicios de duplicación de volúmenes (VSS) y, a continuación, pulse Siguiente. Para desactivar la compatibilidad de imagen en línea, pulse Ninguno (Inhabilitar el soporte de imágenes en línea).
4. Pulse el botón Finalizar para completar la configuración.
5. Complete cada uno de los paneles del asistente y pulse Siguiente para continuar. Para volver al panel anterior, pulse Atrás. Para mostrar información de ayuda para un panel, pulse el icono de ayuda.

### Resultados

---

Para definir preferencias para el soporte de archivos abiertos, utilice la ficha Inclusión-Exclusión del editor de preferencias de IBM Spectrum Protect. Puede establecer estas opciones para todos los volúmenes o para volúmenes individuales con la opción `include.fs: snapshotproviderfs, presnapshotcmd` o `postsnapshotcmd`.

#### Conceptos relacionados:

Consulta de opciones del cliente

Copia de seguridad de imagen

 Sistemas operativos Windows

## Configuración del soporte de archivos abiertos

---

Configure el Soporte de archivos abiertos (OFS) tras instalar el cliente de Windows.

### Acerca de esta tarea

---

Si está configurada la característica Open File Support, el cliente de copia de seguridad y archivado realiza una operación a nivel de archivos basada en instantánea durante la cual el volumen real queda disponible para las otras aplicaciones del sistema. Se mantiene una imagen coherente del volumen durante la operación.

Para configurar OFS, efectúe los pasos siguientes:

### Procedimiento

---

1. Inicie la GUI Java del cliente Windows (ejecute `dsm.exe`).
2. Seleccione Programas de utilidad > Asistente de configuración.
3. Seleccione Ayuda para configurar el soporte de imágenes en línea y pulse Siguiente.
4. Pulse Siguiente de nuevo.
5. Seleccione el proveedor de instantáneas VSS para habilitar el Soporte de archivos abiertos o seleccione Ninguno para realizar copias de seguridad normales (no instantánea) de los archivos de su volumen; a continuación pulse Siguiente.
6. Pulse Aplicar y después Finalizar.

### Resultados

---

Para definir preferencias para el soporte de archivos abiertos, utilice la ficha Inclusión-Exclusión del editor de preferencias. Puede definir estas opciones para todos los volúmenes o para un volumen individual utilizando la opción `include.fs: snapshotproviderfs, presnapshotcmd, postsnapshotcmd`

#### Conceptos relacionados:

## Consideraciones para la configuración de AIX antes de realizar copias de seguridad y archivado basadas en instantáneas

---

Si está configurando el cliente de IBM Spectrum Protect de AIX para que realice copias de seguridad y archivado basadas en instantáneas, debe tener en cuenta algunos elementos.

- Asegúrese de que el grupo de volúmenes que contiene el sistema de archivos del que realizará la instantánea tiene espacio de disco suficiente para que se creen instantáneas externas JFS2 para el sistema de archivos.
- El cliente utiliza un tamaño predeterminado del 100 por cien del tamaño del sistema de archivos. Este valor ha demostrado ser el más adecuado para los sistemas de archivo, incluso si la actividad del sistema de archivos es moderada. Si necesita disminuir este valor según su experiencia con su propia actividad del sistema de archivos, puede utilizar la opción `snapshotcachesize` para ajustar con más precisión este valor.
- No active las instantáneas internas cuando cree nuevos sistemas de archivos JFS2 en AIX 6.1 o posterior para todos los sistemas de archivos gestionados por IBM Spectrum Protect. El cliente utiliza instantáneas externas y JFS2 no permite crear instantáneas externas e internas al mismo tiempo para el mismo sistema de archivos.

### Referencia relacionada:

`Snapshotcachesize`

 Sistemas operativos Linux  Sistemas operativos Windows

## Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea

---

Debe configurar información de la conexión del servidor de archivos de NetApp para ejecutar el mandato de copia de seguridad incremental de diferencia de instantánea en el cliente de copia de seguridad y archivado. Debe utilizar el mandato `set password` para especificar el nombre de host del sistema de archivos y el nombre de usuario que se utiliza para acceder al servidor de archivos.

### Procedimiento

---

1. Establezca una sesión de consola en el archivador NetApp y defina un nuevo usuario en el servidor de archivos siguiendo los pasos indicados a continuación:
  - a. Añada el ID de usuario a un grupo que permita a los usuarios iniciar sesión en el servidor de archivos con mandatos `http` y de ejecución de API.
  - b. Desde el servidor de archivos, especifique el siguiente mandato para listar el ID de usuario para verificar los valores y verificar que la salida es similar:

```
useradmin user list snapdiff_user
```





```
Nombre: snapdiff_user  
Info:  
Identificador de registro: 131077  
Grupos: snapdiff_group  
Nombre completo:
```

En los gestores de archivos 7-mode de NetApp:

```
Prestaciones permitidas: login-http-admin,api-*
```

Para los gestores de archivos ONTAP NetApp de datos en clúster, la única funcionalidad necesaria es `ontapapi` con el rol `admin`.

- c. Si la opción `security.passwd.firstlogin.enable` para el ID de usuario en el servidor de NetApp está definida en `on`, asegúrese de que todos los grupos tienen las prestaciones `login-telnet` y `cli-passwd*`.  
Consejo: Cuando se habilita la opción `security.passwd.firstlogin.enable`, el ID de usuario se establece como caducado cuando se crea. El usuario no puede ejecutar ningún mandato, incluido el de seguridad incremental mediante instantáneas, hasta que se cambie la contraseña. Los usuarios en los grupos que no tienen estas prestaciones no pueden iniciar sesión en el sistema de almacenamiento. Para obtener información sobre cómo definir un ID de usuario y una contraseña en el servidor de archivos de NetApp, consulte la documentación de NetApp.
2. Configure el servidor HTTP incorporado en NetApp Data ONTAP para permitir sesiones remotas de administración en el archivador NetApp.

- a. Si tiene previsto utilizar una conexión HTTP sencilla para las copias de seguridad diferenciales de instantáneas, active la opción `httpd.admin.enable` en el archivador NetApp.
  - b. Si tiene previsto utilizar una conexión HTTPS segura para las copias de seguridad diferenciales de instantáneas (especificando la opción `-snapdiffhttps`), active la opción `httpd.admin.ssl.enable` en el archivador NetApp.
  - c. Desde el nodo de cliente de IBM Spectrum Protect, compruebe la conexión entre el sistema cliente de IBM Spectrum Protect y el servidor NetApp ONTAP para asegurarse de que los cortafuegos u otras opciones de configuración de NetApp no le impiden conectarse al servidor NetApp.  
Consejo: Consulte la documentación sobre NetApp ONTAP para conocer instrucciones sobre cómo comprobar la conexión.
3.  **Sistemas operativos Windows** Exporte los volúmenes de NetApp y tenga en cuenta los siguientes ajustes:  
Consejo: Consulte la documentación acerca de NetApp para obtener más detalles sobre la exportación de volúmenes de NetApp para su uso con Windows.
    - o Correlacione los volúmenes de NetApp utilizando CIFS.
    - o Asegúrese de que los volúmenes de NetApp tienen el valor de seguridad NTFS.
  4.  **Sistemas operativos Linux** Exporte los volúmenes de NetApp y tenga en cuenta los siguientes ajustes:  
Consejo: Consulte la documentación de NetApp para obtener información sobre cómo exportar los volúmenes de NetApp para utilizarlos con hosts Linux.
    - o Correlacione los volúmenes de NetApp utilizando un montaje NFS.
    - o Asegúrese de que los volúmenes de NetApp tienen valores de seguridad UNIX
  5. Defina el ID de usuario y la contraseña en el cliente de copia de seguridad y archivado para el ID de usuario que creó en el paso 1 mediante los siguientes pasos:
    - a.  **Sistemas operativos Linux** Inicie sesión con ID de usuario root.
    - b.  **Sistemas operativos Windows** Inicie sesión como usuario con acceso de lectura/escritura a la compartición de CIFS.
    - c. Desde la línea de mandatos del cliente de copia de seguridad y archivado, especifique el siguiente mandato:

```
dsmc set password -type=filer my_file_server snapdiff_user newPassword
```

Sustituya los siguientes valores:

*my\_file\_server*





Este valor es el nombre de host completo del servidor de archivos NetApp.

*snapdiff\_user*

Este valor es el ID de usuario que creó en el paso 1.

*newPassword*

Este valor es la contraseña para el ID de usuario que creó en el paso 1.

-  **Sistemas operativos Linux**  **Sistemas operativos Windows** Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster  
Puede crear una copia de seguridad incremental diferencial de instantánea de un volumen que esté en un servidor de archivos NetApp que forme parte de una configuración ONTAP de datos en clúster (servidor de archivos de modalidad-c).
-  **Sistemas operativos Linux**  **Sistemas operativos Windows** Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)  
Puede utilizar el proceso de copia de seguridad SnapDiff de NetApp junto con la réplica SnapMirror de NetApp para realizar una copia de seguridad de volúmenes de archivos de destino u origen NetApp.

#### Tareas relacionadas:

Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster

#### Referencia relacionada:

Snapdiff

Snapdiffhttps

Createnewbase

 **Sistemas operativos Linux**  **Sistemas operativos Windows**

## Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster

Puede crear una copia de seguridad incremental diferencial de instantánea de un volumen que esté en un servidor de archivos NetApp que forme parte de una configuración ONTAP de datos en clúster (servidor de archivos de modalidad-c).

### Antes de empezar

- Lleve a cabo el procedimiento de Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea.
- Asegúrese de que el administrador de la máquina virtual de almacenamiento NetApp haya configurado correctamente entorno ONTAP de datos en clúster.

Restricción: El soporte de IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea de volúmenes ONTAP de datos en clúster se soporta solo en NetApp ONTAP 8.2.1 y versiones posteriores.

## Acerca de esta tarea

---

En un entorno ONTAP de datos en clúster, las máquinas virtuales de almacenamiento (también conocidas como vServers de datos) contienen volúmenes de datos que se pueden proteger mediante el cliente de copia de seguridad y archivado.

Una máquina virtual consta de un solo volumen infinito de uno o varios volúmenes flex. Se accede a los volúmenes de forma remota mediante el uso compartido de archivos (CIFS en sistemas operativos Windows, NFS en sistemas operativos Linux).

Las máquinas virtuales de almacenamiento se gestionan mediante el archivador de gestión de clústeres, que es el archivador físico (el archivador c-mode) en el que residen las máquinas virtuales de almacenamiento. El cliente de copia de seguridad está instalado en la máquina remota que accede a los volúmenes.

El cliente de archivado y copia de seguridad se tiene que configurar con credenciales para los gestores de archivos c-mode de NetApp a los que se accede para las operaciones de seguridad.

Requisitos:

- Se necesita la siguiente información para este procedimiento:
  - El nombre de host o la dirección IP del archivador de gestión de clústeres.
  - El nombre de host o la dirección IP de la máquina virtual de almacenamiento
  - El nombre de la máquina virtual de almacenamiento.
  - Las credenciales del archivador de gestión de clústeres (nombre de usuario y contraseña).
- Al usuario gestor de archivos de gestión de clústeres configurado por el cliente se le tiene que asignar la funcionalidad `ontapapi` con el rol `admin`.

La funcionalidad `ontapapi` no permite el acceso interactivo al gestor de archivos con métodos como `telnet`, `ssh` o `http/https`. No se necesita ninguna otra funcionalidad de usuario para ejecutar copias de seguridad incrementales de instantáneas.

## Procedimiento

---

Siga los pasos siguientes en la máquina remota en la que se ha instalado el cliente de copia de seguridad y archivado:

1. Configure el cliente de archivado y copia de seguridad con las credenciales del gestor de archivos de gestión de clústeres. Utilice el mandato `dsmc set password` para almacenar las credenciales del gestor de archivos de gestión asociado a la máquina virtual de almacenamiento. Por ejemplo, escriba el siguiente mandato:

```
dsmc set password -type=filer management_filer_hostname  
management_filer_username management_filer_password
```

Donde:

*management\_filer\_hostname*

El nombre de host o la dirección IP del archivador de gestión de clústeres.

*management\_filer\_username*

El nombre de usuario del archivador de gestión de clústeres.

*management\_filer\_password*

La contraseña del usuario del archivador de gestión de clústeres.

Consejo: La contraseña del gestor de archivos de gestión de clústeres se cifra cuando se almacena mediante el cliente de archivado y copia de seguridad.

2. Asocie cada máquina virtual de almacenamiento con el archivador de gestión mediante el mandato `dsmc set netappsvm`. Por ejemplo, escriba el siguiente mandato:

```
dsmc set netappsvm storage_virtual_machine_hostname  
management_filer_hostname storage_virtual_machine_name
```

Donde:

*storage\_virtual\_machine\_hostname*

El nombre de host o la dirección IP de la máquina virtual de almacenamiento que se utiliza para montar los volúmenes que se van a copiar.

*management\_filer\_hostname*


El nombre de host o la dirección IP del archivador de gestión de clústeres.

*storage\_virtual\_machine\_name*

El nombre de la máquina virtual de almacenamiento.

Nota: El nombre de host o la dirección IP de la máquina virtual de almacenamiento que se utiliza para montar los volúmenes debe ser coherente con lo que se ha especificado en los mandatos `dsmc set`. Por ejemplo, si los volúmenes están montados con una dirección IP de máquina virtual de almacenamiento, se debe utilizar la dirección IP (no el nombre de host) en los mandatos `dsmc set`. De lo contrario, la autenticación de cliente con el archivador de gestión de clústeres fallará.

Solo tiene que especificar el mandato `dsmc set netappsvm` una vez para cada máquina virtual de almacenamiento. Si la máquina virtual de almacenamiento se mueva a otro archivador de gestión de clústeres, debe utilizar el mandato para actualizar el nombre de host del archivador de gestión de clústeres actualizado.

3.  **Sistemas operativos Windows** Correlacione los volúmenes con letras de unidad. Por ejemplo, escriba el siguiente mandato para cada máquina virtual de almacenamiento:

```
net use y: \\storage_virtual_machine_hostname domain_name\CIFS_share_name
```

Donde:

y:


La unidad que se va a correlacionar con el volumen.

*storage\_virtual\_machine\_hostname*

El nombre de host o la dirección IP de la máquina virtual de almacenamiento

*domain\_name\CIFS\_share\_name*

La unidad compartida CIFS definida en el archivador en el volumen que se va a copiar.

4.  **Sistemas operativos Linux** Monte la máquina virtual de almacenamiento en un sistema de archivos local. Por ejemplo, escriba el siguiente mandato para cada máquina virtual de almacenamiento:

```
mount storage_virtual_machine_hostname/tmp/fs1
```

Donde:

*storage\_virtual\_machine\_hostname*

El nombre de host o la dirección IP de la máquina virtual de almacenamiento

*/tmp/fs1*


Un ejemplo de un sistema de archivos en el que montar el volumen de la máquina virtual de almacenamiento.

5. Inicie una copia de seguridad incremental progresiva de un volumen flex o infinito.

De forma predeterminada, el acceso HTTP al servidor de archivos NetApp no está habilitado. Si no ha configurado el servidor de archivos para permitir acceso utilizando HTTP, use la opción `snappdiffhttps` del cliente de archivado y copia de seguridad para permitir el acceso al servidor de gestión de clústeres con el protocolo HTTPS.

 **Sistemas operativos Windows** Por ejemplo, en clientes Windows, especifique el siguiente mandato:


```
dsmc incr y: -snapdiff -snapdiffhttps
```

 **Sistemas operativos Linux** Por ejemplo, en clientes Linux, indique el mandato siguiente:


```
dsmc incr /tmp/fs1 -snapdiff -snapdiffhttps
```

Consejo: Solo tiene que ejecutar la copia de seguridad incremental progresiva completa una vez. Una vez realizada correctamente la copia de seguridad, se ejecutan copias de seguridad diferenciales en futuras operaciones de copia de seguridad.

6. Inicie una copia de seguridad diferencial de instantánea del volumen flex o infinito.

 **Sistemas operativos Windows** Por ejemplo, en clientes Windows, especifique el siguiente mandato:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

 **Sistemas operativos Linux** Por ejemplo, en clientes Linux, indique el mandato siguiente:

```
dsmc incr /tmp/fs1 -snapdiff -snapdiffhttps
```

## Ejemplo

Un usuario cliente de copia de seguridad y archivado desea completar una copia de seguridad incremental diferencial de instantánea de los volúmenes de un servidor de archivos c-mode. El usuario utiliza el cliente de copia de seguridad y archivado de Windows para realizar la copia de seguridad y los volúmenes están montados en unidades compartidas CIFS. La configuración del archivador c-mode es la siguiente:

Archivador de gestión ONTAP 8.31

```
Hostname: netapplmgmt.example.com
User: netapplmgmt_user
Password: pass4netapplmgmt
CIFS Domain Controller: WINDC
Domain User: domainuser
```

#### Máquina virtual de almacenamiento de volumen flex

```
Hostname: netappl-v1.example.com
Storage virtual machine name: netappl-client1
CIFS share: demovol
Volume name: demovol
```

#### Máquina virtual de almacenamiento de volumen infinito

```
Hostname: netappl-v4.example.com
Storage virtual machine name: netappl-infiniteVolume1
CIFS Share: InfiniteVol
```

El usuario lleva a cabo los pasos siguientes en el cliente de copia de seguridad y archivado:

1. Configure el cliente con las credenciales del gestor de archivos de gestión emitiendo el siguiente mandato:

```
dsmc set password -type=filer netapplmgmt.example.com netapplmgmt_user pass4netapplmgmt
```

2. Define asociaciones de máquinas virtuales de almacenamiento para cada máquina virtual de almacenamiento con los mandatos siguientes:

```
dsmc set netappsvm netappl-v1.example.com netapplmgmt.example.com netappl-client1
```

```
dsmc set netappsvm netappl-v4.example.com netapplmgmt.example.com netappl-infiniteVolume1
```

3. Correlaciona volúmenes remotos con letras de unidad para cada máquina virtual:

```
net use y: \\netappl-v1.example.com\demovol WINDC\domainuser
```

```
net use z: \\netappl-v4.example.com\InfiniteVol WINDC\domainuser
```

4. Ejecuta una copia de seguridad incremental progresiva completa del volumen flex y del volumen infinito:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

```
dsmc incr z: -snapdiff -snapdiffhttps
```

Solo tiene que ejecutar la copia de seguridad incremental progresiva completa una vez. Una vez realizada correctamente la copia de seguridad, se ejecutan copias de seguridad diferenciales en futuras operaciones de copia de seguridad.

5. Ejecuta una copia de seguridad diferencial de instantánea del volumen flex y del volumen infinito:

```
dsmc incr y: -snapdiff -snapdiffhttps
```

```
dsmc incr z: -snapdiff -snapdiffhttps
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)


---

Puede utilizar el proceso de copia de seguridad SnapDiff de NetApp junto con la réplica SnapMirror de NetApp para realizar una copia de seguridad de volúmenes de archivos de destino u origen NetApp.

En un entorno NetApp SnapMirror, los datos que están en volúmenes asociados al centro de datos primario se copian en volúmenes asociados a un servidor remoto ubicado en un sitio de recuperación ante desastres. El archivador NetApp del centro de datos primario se denomina archivador de origen; el archivador NetApp del sitio de recuperación ante desastres se denomina archivador de destino. Puede utilizar el cliente de archivado y copia de seguridad para crear copias de seguridad diferenciales de instantánea de los volúmenes del archivador de origen o destino.


### Escenario: Copia de seguridad de datos en un volumen de archivador de origen


---


 Sistemas operativos Linux Puede configurar el cliente de archivado y copia de seguridad para realizar copias de seguridad de los datos de volúmenes del archivador de origen. Este escenario requiere la configuración de un nodo cliente de archivado y copia de



seguridad que tenga acceso a los volúmenes de archivador de origen NetApp utilizando NFS exportadas para montar los volúmenes del archivador.

 Sistemas operativos Windows Puede configurar el cliente de archivado y copia de seguridad para realizar copias de seguridad de los datos de volúmenes del archivador de origen. Este escenario requiere la configuración de un nodo cliente de archivado y copia de seguridad que tenga acceso a los volúmenes de archivador de origen NetApp utilizando unidades compartidas CIFS para montar los volúmenes del archivador.

 Sistemas operativos Linux Por ejemplo, suponga que tiene una configuración en la que el archivador de origen se llama ProdFiler. Suponga que existe un volumen llamado UserDataVol en el archivador ProdFiler y que el volumen es accesible utilizando NFS desde un nodo cliente de archivado y copia de seguridad. Suponga que la acción se monta como UserDataVol\_Share.

 Sistemas operativos Windows Por ejemplo, suponga que tiene una configuración en la que el archivador de origen se llama ProdFiler. Suponga que existe un volumen llamado UserDataVol en el archivador ProdFiler y que el volumen es accesible utilizando CIFS desde un nodo cliente de archivado y copia de seguridad. Suponga que la acción se monta como UserDataVol\_Share.

Cuando inicia una copia de seguridad diferencial de instantánea, el archivador NetApp crea una nueva instantánea diferencial en el volumen que se está copiando. La instantánea diferencial se compara con la instantánea base (anterior). El nombre de la instantánea base se registró en el servidor IBM Spectrum Protect cuando se completó la copia de seguridad anterior. El contenido de la instantánea base se compara con la instantánea diferencial creada en el volumen del archivador de origen. Las diferencias entre las dos instantáneas se copian en el servidor.

Para iniciar la copia de seguridad diferencial de la instantánea se utiliza el mandato indicado a continuación. El mandato se especifica en la consola de un nodo cliente configurado para acceder y proteger los volúmenes del archivador de origen. Dado que este mandato se emite para realizar copias de seguridad de volúmenes de un archivador de origen, se crea una nueva instantánea (la instantánea diferencial) y la instantánea registrada en el servidor de IBM Spectrum Protect se utiliza como instantánea base. La creación de ambas instantáneas, diferencial y base, es el comportamiento predeterminado; la opción `-diffsnapshot=create` es un valor predeterminado y no es necesario que se especifique de manera explícita en este mandato.



```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=create
```


## Datos de copia de seguridad en un archivador de destino

---

Una configuración más típica consiste en descargar las copias de seguridad del archivador de origen creando copias de seguridad de los volúmenes de origen mediante el uso de instantáneas de volumen replicadas almacenadas en el archivador de destino. Por lo general, realizar una copia de seguridad de un archivador de destino presenta un problema, ya que la creación de una copia de seguridad de instantánea diferencial requiere que se cree una nueva instantánea en el volumen del que está realizando la copia de seguridad. Los volúmenes del archivador de destino que duplican el contenido de los volúmenes de origen son volúmenes de solo lectura, por lo que no se pueden crear instantáneas en los mismos.

Para solucionar esta restricción de solo lectura, se proporcionan opciones de configuración del cliente que le permiten utilizar las instantáneas diferencial y base existentes en el volumen de destino de solo lectura para copiar los cambios en el servidor de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux Al igual que en el escenario del archivador de origen, a los volúmenes del archivador de destino se accede utilizando acciones exportadas NFS.

 Sistemas operativos Windows Al igual que en el escenario del archivador de origen, a los volúmenes del archivador de destino se accede utilizando acciones CIFS.

## Resumen de opciones diferenciales de instantánea

---

La opción `useexistingbase` hace que la instantánea más reciente del volumen se utilice como instantánea base cuando se deba establecer una instantánea base. Cuando una de las condiciones indicadas a continuación sea verdadera, se establecerá una instantánea base:

- Cuando esta copia de seguridad es la copia de seguridad inicial.
- Cuando se especifica `createnewbase=yes`.
- Cuando la instantánea base registrada por una instantánea diferencial anterior ya no existe, y no existe una instantánea más antigua que la instantánea que falta.

Si no se especifica esta opción, se crea una nueva instantánea en el volumen del que se está realizando una copia de seguridad. Dado que los volúmenes del archivador de destino son de solo lectura, se debe especificar `useexistingbase` al crear copias de seguridad diferenciales de instantánea de dichos volúmenes. Si no se especifica `useexistingbase`, las copias de seguridad diferenciales de instantánea de un volumen de archivador de destino fallan porque no se puede crear la instantánea nueva en el volumen de solo lectura.

Cuando realice una copia de seguridad de volúmenes de archivador de destino, utilice las opciones `useexistingbase` y `diffsnapshot=latest` para asegurarse de que se usan las instantáneas diferencial y base más recientes.

Utilice la opción `basesnapshotname` para especificar qué instantánea del volumen de archivador de destino desea utilizar como instantánea base. Si no especifica esta opción, se utilizará la instantánea más reciente del volumen del archivador de destino como instantánea base. Puede utilizar caracteres comodín para especificar el nombre de la instantánea base.

Utilice la opción `diffsnapshotname` para especificar qué instantánea diferencial del volumen de archivador de destino desea utilizar durante la copia de seguridad diferencial. Esta opción sólo se especifica si también se especifica `diffsnapshot=latest`. Puede utilizar caracteres comodín para especificar el nombre de la instantánea diferencial.

La opción `diffsnapshot=latest` especifica que desea utilizar la última instantánea encontrada en el servidor de archivos como instantánea de origen.

En los temas de Consulta de opciones del cliente, se facilita información adicional sobre cada una de estas opciones.

## Ejemplos de mandato de copia de seguridad diferencial de instantánea

---

En los ejemplos indicados a continuación, se considera que se replican los volúmenes de un archivador de origen utilizando la tecnología SnapMirror de NetApp en un archivador de recuperación tras desastre (su nombre de host es DRFiler). Dado que los volúmenes de DRFiler son de solo lectura, utilice las opciones para especificar qué instantáneas replicadas desea utilizar como instantánea base y cuál como instantánea diferencial. Especificando las instantáneas que desea utilizar al crear una copia de seguridad diferencial de un archivador de destino, no se intenta crear una instantánea en volúmenes de solo lectura.

Para iniciar copias de seguridad diferenciales de instantánea se utilizan los siguientes mandatos. La mayoría de los mandatos crean copias de seguridad diferenciales utilizando instantáneas almacenadas en volúmenes del archivador de destino. Al realizar una copia de seguridad de un volumen de archivador de destino, asegúrese de incluir la opción `-useexistingbase`, ya que esta evita el intento de creación de una nueva instantánea en los volúmenes del archivador de destino de solo lectura.

**Ejemplo 1:** Copia de seguridad de un archivador de destino utilizando copias de seguridad nocturnas predeterminadas creadas por el planificador de instantáneas de NetApp

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
-diffsnapshot=latest -basesnapshotname="nightly.?"
```

Puede utilizar una interrogación (?) para que coincida con un carácter individual. En este ejemplo, `-basesnapshotname=nightly.?` se utiliza la última instantánea base, llamada "nightly.", seguida de un carácter individual (por ejemplo: `nightly.0`, `nightly.1`, etc.).

**Ejemplo 2:** Copia de seguridad de un archivador de destino utilizando copias de seguridad creadas manualmente (no creadas por el planificador de instantáneas de NetApp)

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
-diffsnapshot=latest -basesnapshotname="share_vol_base?"
-diffsnapshotname="share_vol_diff?"
```

Este ejemplo también utiliza interrogaciones (?) como comodín para ilustrar la sintaxis si los nombres de la instantánea base y diferencial tienen números diferentes como parte de este.

**Ejemplo 3:** Copia de seguridad de un volumen de archivador de destino especificando que instantáneas utilizar como instantánea base y diferencial

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
-diffsnapshot=latest -basesnapshotname="share_vol_base"
-diffsnapshotname="share_vol_diff_snap"
```

**Ejemplo 4:** Copia de seguridad de instantáneas generadas por script que utilizan la convención de nomenclatura

En este ejemplo, un script que se ejecuta en el archivador NetApp añade una indicación de fecha y hora a los nombres de las instantáneas. Por ejemplo, una instantánea creada el 3 de noviembre de 2012 a las 11:36:33 PM se llamará `UserDataVol_20121103233633_snapshot`. Puede utilizar comodines con las opciones para seleccionar las instantáneas diferencial y base más recientes. Por ejemplo:

```
dsmc incr \\DRFiler\UserDataVol_Share -snapdiff -useexistingbase
-basesnapshotname="UserDataVol_Share_*_snapshot" -diffsnapshot=latest
-diffsnapshotname="UserDataVol_Share_*_snapshot"
```

`-useexistingbase` selecciona la instantánea base más reciente. Si añade un asterisco (\*) a `-basesnapshotname` seleccionará la instantánea base más reciente que sigue la convención de nomenclatura de scripts. La opción `-diffsnapshot=latest` suprime la creación de una nueva instantánea diferencial y `-diffsnapshotname=` selecciona la instantánea diferencial más reciente que sigue la convención de nomenclatura de scripts. (El comodín asterisco coincide con cualquier serie).

**Ejemplo 5:** Realiza una copia de seguridad diferencial utilizando una instantánea diferencial existente en el archivador de origen

Para utilizar una instantánea diferencial existente en el archivador de origen, utilice `-diffsnapshot=latest` para evitar la creación de una instantánea diferencial nueva. Utilice también la opción `-diffsnapshotname` para especificar la instantánea diferencial

existente que desea utilizar. La instantánea que especifique se compara con la instantánea base, registrada en la base de datos de servidor de IBM Spectrum Protect durante la creación de la última copia de seguridad. Por ejemplo:

```
dsmc incr \\ProdFiler\UserDataVol_Share -snapdiff -diffsnapshot=latest  
-diffsnapshotname="share_vol_diff_snap"
```

## Registrar la estación de trabajo en un servidor





---

Para poder utilizar IBM Spectrum Protect, es necesario configurar un nombre de nodo y una contraseña y el nodo debe registrarse con el servidor.

El proceso de configuración de un nombre de nodo y una contraseña se conoce como *inscripción*. Hay dos tipos de registro disponibles, *abiertos* y *cerrados*.

El administrador del servidor de IBM Spectrum Protect elige el tipo de registro del sitio.

Restricción: A partir del servidor de IBM Spectrum Protect Versión 8.1.2, la inscripción abierta ya no está disponible. Debe utilizar la inscripción cerrada. La inscripción abierta sólo está disponible para el servidor de IBM Spectrum Protect V8.1.1, V8.1.0, V7.1.7 o anterior.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Debe ser un usuario root o usuario autorizado para poder realizar esta tarea.

Si quiere utilizar el cliente web, necesita un ID de usuario de administración con privilegio de sistema, privilegio de política, autorización de acceso a cliente o autorización de propietario de cliente. Si se registra un nuevo nodo, el administrador del servidor tiene que crear un ID de usuario de administración que coincida con el nombre del nodo. De forma predeterminada, este nodo tiene autorización de propietario de cliente.

El administrador del servidor de IBM Spectrum Protect tiene que especificar el parámetro `userid` con el mandato de servidor REGISTER NODE:

```
REGISTER NODE nombre_nodo contraseña userid=ID_usuario
```

donde el nombre de nodo y el ID de usuario de administración tienen que ser iguales. Por ejemplo:

```
REGISTER NODE node_a mypassw0rd userid=node_a
```

- **Inscripción cerrada**  
Con la inscripción cerrada, el administrador de IBM Spectrum Protect debe inscribir su estación de trabajo como nodo cliente en el servidor. Si la empresa utiliza una inscripción cerrada, deberá proporcionar la información siguiente al administrador de IBM Spectrum Protect.
- **Inscripción abierta**  
Con la inscripción abierta, un administrador del sistema puede inscribir la estación de trabajo como un nodo cliente con el servidor de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.

## Inscripción cerrada

---

Con la inscripción cerrada, el administrador de IBM Spectrum Protect debe inscribir su estación de trabajo como nodo cliente en el servidor. Si la empresa utiliza una inscripción cerrada, deberá proporcionar la información siguiente al administrador de IBM Spectrum Protect.

### Acerca de esta tarea

---

Debe proporcionar los siguientes elementos a su administrador de IBM Spectrum Protect:

- El nombre de nodo (el valor que devuelve el mandato **hostname**, el nombre de la estación de trabajo o el nombre de nodo que especifica con la opción **nodename**). Si no especifica un nombre de nodo con la opción **nodename**, el ID de inicio de sesión predeterminado es el mismo que el que devuelve el mandato **hostname**.
- La contraseña inicial que desea utilizar, si es necesario.
- Información de contacto, como nombre, identificador de usuario y número de teléfono.

El administrador de IBM Spectrum Protect define lo siguiente:

- El dominio de políticas al que pertenece el nodo cliente. Un dominio de políticas contiene juegos de políticas y clases de gestión que controlan cómo gestiona IBM Spectrum Protect los archivos de los que hace copia de seguridad y copias archivadas.
- Si se pueden comprimir los archivos antes de enviarlos al servidor.
- Si puede eliminar datos archivados y de copia de seguridad del almacenamiento del servidor.

## Inscripción abierta

---

Con la inscripción abierta, un administrador del sistema puede inscribir la estación de trabajo como un nodo cliente con el servidor de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.

### Acerca de esta tarea

---

La primera vez que se inicia una sesión, se le solicitará la información necesaria para inscribir su estación de trabajo en el servidor de IBM Spectrum Protect identificado en el archivo de opciones del cliente. Debe proporcionar el nombre de nodo, una contraseña e información de contacto.

Al utilizar la inscripción abierta:

- El nodo cliente se asigna a un dominio de políticas denominado **standard**.
- Puede suprimir copias archivadas de archivos del almacenamiento del servidor, pero no versiones de copia de seguridad de archivos.

Si es necesario, el administrador de IBM Spectrum Protect puede modificar estos valores predeterminados posteriormente.

## Creación de una lista de inclusión/exclusión

---


Si no crea una lista de inclusión/exclusión, el cliente de copia de seguridad y archivado tiene en cuenta todos los archivos para los servicios de copia de seguridad y utiliza la clase de gestión predeterminada para los servicios de copia de seguridad/archivado.


### Acerca de esta tarea





---


Esta es una tarea opcional, pero importante.





Puede crear una lista de inclusión/exclusión para excluir un archivo o grupo de archivos específico de los servicios de copia de seguridad, y para asignar clases de gestión específicas a los archivos. El cliente realiza una copia de seguridad de todos los archivos que no estén excluidos. Debe excluir de los servicios de copia de seguridad los directorios del cliente de IBM Spectrum Protect. Puede utilizar el mandato query inclexcl para visualizar una lista de sentencias de inclusión y exclusión en el orden en el que se examinan cuando determine si se debe incluir un objeto.

 **Sistemas operativos Windows** Especifique la lista de inclusión/exclusión en el archivo de opciones de cliente (dsm.opt). La lista de inclusión/exclusión también puede encontrarse en otro archivo, al que hace referencia la opción inclexcl. Las sentencias de inclusión/exclusión no son sensibles a las mayúsculas y minúsculas.

 **Sistemas operativos Windows** El archivo de opciones de cliente, dsm.opt, debe tener un formato que no sea Unicode. Sin embargo, si utiliza un archivo de inclusión/exclusión distinto, puede tener formato Unicode o no de Unicode.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Especifique la lista de inclusión/exclusión en el archivo dsm.sys. Si tiene más de un servidor definido en el archivo dsm.sys, cada servidor debe tener su propia lista de inclusión/exclusión. Esta lista también puede contener sentencias de inclusión/exclusión obtenidas de los archivos de inclusión/exclusión especificados mediante la opción inclexcl.

 **Sistemas operativos Windows** Cuando el cliente procesa sentencias de inclusión/exclusión, las del archivo de inclusión/exclusión se colocan en la posición de lista ocupada por la opción inclexcl en dsm.opt, en el mismo orden, y se procesan en consecuencia.











 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Cuando el cliente procesa sentencias de inclusión/exclusión, las del archivo de inclusión/exclusión se colocan en la posición de lista ocupada por la opción inclexcl en dsm.sys, en el mismo orden, y se procesan en consecuencia.

## Procedimiento

---

Puede utilizar los siguientes métodos para crear una lista de inclusión/exclusión o para especificar un archivo de inclusión/exclusión:


- Puede añadir sentencias de inclusión/exclusión en el árbol de directorios del cliente de copia de seguridad y archivado. La ayuda en línea proporciona instrucciones detalladas.
  1. Abra el menú Editar y seleccione Preferencias del cliente. En el diálogo Preferencias, seleccione el separador Inclusión/exclusión. Puede especificar un archivo INCLEXCL mediante el editor de preferencias. Sin embargo, no puede crear el archivo INCLEXCL mediante dicho editor.
  2. Cree la lista de inclusión-exclusión de forma manual siguiendo los pasos enumerados.
- Puede crear una lista de inclusión/exclusión manualmente, realizando los pasos siguientes:
  1. Determine las necesidades de inclusión y exclusión.

2.  Sistemas operativos Windows Localice el archivo de opciones de cliente
3.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  
 Sistemas operativos Oracle Solaris Localice la stanza de servidor en el archivo dsm.sys. Cada stanza de servidor debe tener su propia lista de inclusión/exclusión.
4.  Sistemas operativos Windows **Importante:** agrupe las opciones de inclusión/exclusión conjuntamente en el archivo de opciones de cliente.
5.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  
 Sistemas operativos Oracle Solaris Especifique las sentencias include y exclude. El cliente evalúa *en primer lugar* todas las sentencias de exclude.fs y exclude.dir (con independencia de la posición que ocupen en la lista de inclusión/exclusión) y elimina los espacios de archivos, los directorios y los archivos excluidos de la lista de objetos que están disponibles para procesarse. Todas las demás sentencias de inclusión/exclusión se procesan de abajo a arriba, empezando por el final de la lista. Por lo tanto, es importante especificar las sentencias de inclusión/exclusión en el orden correcto. Por ejemplo, en la lista de inclusión/exclusión siguiente *no* se hace una copia de seguridad del archivo includefile.cpp:

```
include /Users/user01/Documents/includefile.cpp
exclude /Users/user01/Documents/.../*
```

Sin embargo, en la lista de inclusión/exclusión siguiente se hace una copia de seguridad del archivo includefile.cpp:

```
exclude /Users/user01/Documents/.../*
include /Users/user01/Documents/includefile.cpp
```


6.  Sistemas operativos Windows Especifique las sentencias include y exclude. El cliente evalúa *en primer lugar* todas las sentencias exclude.dir (con independencia de la posición que ocupen en la lista de inclusión/exclusión), y elimina los directorios y los archivos excluidos de la lista de objetos que están disponibles para procesarse. Todas las demás sentencias de inclusión/exclusión se procesan de abajo a arriba, empezando por el final de la lista. Por lo tanto, es importante especificar las sentencias de inclusión/exclusión en el orden correcto. Por ejemplo, en la lista de inclusión/exclusión siguiente *no* se hace una copia de seguridad del archivo includefile.txt:






```
include c:\test\includefile.txt
exclude c:\test\...*
```






Sin embargo, en la lista de inclusión/exclusión siguiente *sí* que se hace una copia de seguridad del archivo includefile.txt:

```
exclude c:\test\...*
include c:\test\includefile.txt
```





7. Guarde el archivo y ciérrelo.

 sistemas operativos Mac OS X En Mac OS X, no olvide guardar el archivo como un texto sin formato codificado como Unicode (UTF-8 o UTF-16). No añada la extensión .txt.

8.  Sistemas operativos Windows Reinicie el cliente y los servicios del planificador y de aceptación de clientes para activar la lista de inclusión/exclusión.
9.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  
 Sistemas operativos Oracle Solaris Reinicie el cliente para habilitar la lista de inclusión/exclusión.

- Opciones de inclusión/exclusión  
Este tema proporciona descripciones breves de las opciones incluir y excluir que puede especificar en el archivo de opciones del cliente, una lista mínima inclusión-exclusión que excluye a los archivos del sistema, una lista de caracteres comodín admitidos, y ejemplos de cómo se deben utilizar los caracteres comodín con patrones incluir y excluir.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Proceso de enlaces simbólicos y alias  
El cliente de copia de seguridad y archivado evalúa todas las sentencias exclude.fs y exclude.dir y elimina los espacios de archivos y los directorios excluidos.
- Determinar el proceso de compresión y cifrado  
El cliente de copia de seguridad y archivado evalúa exclude.dir y todas las demás opciones de inclusión/exclusión que controlan el proceso de copia de seguridad y archivado para determinar qué archivos se someten al proceso de compresión y cifrado compresión y cifrado.
- Vista previa de los archivos de la lista de inclusión-exclusión  
Puede realizar una previsualización de la lista de objetos de los que se va a realizar una copia de seguridad o archivado según la lista de inclusión/exclusión, antes de enviar los datos al servidor.
- Inclusión y exclusión de proceso de opciones  
El servidor de IBM Spectrum Protect puede definir opciones de inclusión/exclusión mediante el parámetro inclexcl en un archivo de opciones del cliente.
-  Sistemas operativos Windows Reglas de proceso y utilización de nombres UNC  
Cuando se procesan archivos con nombres UNC, hay unas reglas que se deben seguir.

**Conceptos relacionados:**

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Consideraciones sobre los clientes habilitados para Unicode

Archivos del sistema a excluir





Políticas de gestión de almacenamiento

**Referencia relacionada:**

Inclxcl

## Opciones de inclusión/exclusión

Este tema proporciona descripciones breves de las opciones incluir y excluir que puede especificar en el archivo de opciones del cliente, una lista mínima inclusión-exclusión que excluye a los archivos del sistema, una lista de caracteres comodín admitidos, y ejemplos de cómo se deben utilizar los caracteres comodín con patrones incluir y excluir.

- Exclusión de espacios de archivos y directorios  
Utilice las sentencias `exclude.dir` para excluir del proceso todos los archivos y subdirectorios del directorio especificado.
-  Sistemas operativos Windows Sentencias de inclusión/exclusión para sistemas de archivos en red  
Las sentencias de inclusión/exclusión que implican a sistemas de archivos en red (unidades remotas) deben escribirse en formato UNC.
-  Sistemas operativos AIX  Sistemas operativos Windows Excluir archivos y directorios de la copia de seguridad con registro por diario  
Hay dos métodos para excluir archivos y directorios de una copia de seguridad con registro por diario.
- Controlar proceso de sentencias de exclusión  
Después de que el cliente ha evaluado todas las sentencias `exclude` se evalúan las opciones siguientes con la lista restante de objetos disponibles para el proceso.
- Archivos del sistema a excluir  
Hay algunos archivos del sistema que deben ubicarse en el archivo de opciones de cliente para que se puedan excluir.
-  Sistemas operativos Windows Excluir archivos con nombres UNC  
Para excluir los archivos a los que se accede de forma remota, puede especificar sus nombres UNC (Universal naming convention) en la sentencia de exclusión.
- Incluir y excluir archivos con caracteres comodín  
Debe utilizar caracteres especiales cuando incluya o excluya archivos y directorios que contengan caracteres comodín.
- Inclusión y exclusión de grupos de archivos con caracteres comodín  
Puede utilizar caracteres comodín para incluir o excluir grupos de archivos.
- Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión  
El cliente de copia de seguridad y archivado cliente acepta la opción `exclude.dir`, que se puede utilizar para excluir entradas de directorio. No obstante, las opciones `include` y `exclude.dir` no pueden utilizarse al mismo tiempo.









## Exclusión de espacios de archivos y directorios









Utilice las sentencias `exclude.dir` para excluir del proceso todos los archivos y subdirectorios del directorio especificado.



El cliente de copia de seguridad y archivado evalúa *en primer lugar* todas las sentencias `exclude.dir` (con independencia de la posición que ocupen en la lista de inclusión/exclusión), y elimina los directorios y los archivos excluidos de la lista de objetos que están disponibles para procesarse. Las sentencias `exclude.dir` modifican todas las sentencias de inclusión que coinciden con el patrón.


Tabla 1 enumera las opciones que puede utilizar para excluir los espacios de archivos y directorios del proceso.

Tabla 1. Opciones para excluir espacios de archivos y directorios

Opción	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X <code>exclude.fs</code> Opciones <code>exclude</code>	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluye los espacios de archivos que coinciden con el patrón. El cliente no ha tenido en cuenta el espacio de archivos especificado para el proceso, por lo que no se ha realizado el proceso normal de caducidad de archivos eliminados. Si se excluye un espacio de archivos que se había incluido previamente, las versiones de copia de seguridad existentes permanecen en el servidor sujetas a las reglas de retención especificadas en la definición de clase de gestión que se haya asociado.

Opción	Descripción
<p>  sistemas operativos Mac OS X   Sistemas operativos AIX   Sistemas operativos Linux   Sistemas operativos Oracle Solaris            exclude.dir Opciones exclude         </p>	<p>  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux   Sistemas operativos Oracle Solaris Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia <code>exclude.dir /test/dan/data1</code> excluye el directorio <code>/test/dan/data1</code>, sus archivos y todos sus subdirectorios y sus archivos. Para excluir directorios grandes con una gran cantidad de archivos de los que no desea hacer la copia de seguridad, es mejor utilizar la opción <code>exclude.dir</code> que la opción <code>exclude</code>. No puede utilizar las opciones <code>include</code> para alterar temporalmente la opción <code>exclude.dir</code>. Utilice <code>exclude.dir</code> sólo cuando se excluye toda una rama del directorio.         </p> <ul style="list-style-type: none"> <li>           Utilice las siguientes sentencias para excluir los volúmenes <code>/Volumes/disk2</code> en su conjunto del proceso de copia de seguridad. Recuerde que todavía será posible realizar la copia de seguridad del volumen (<code>/Volumes/disk2</code>), pero quedarán excluidos todos los demás directorios que se encuentren en <code>/Volumes/disk2</code>.           <pre>exclude /Volumes/disk2/* exclude.dir /Volumes/disk2/*</pre> </li> <li>           Un método alternativo para excluir un volumen completo de la realización de la copia de seguridad incremental del dominio consiste en utilizar una sentencia de dominio para excluir el volumen. Por ejemplo:           <pre>domain "-/Volumes/disk2"</pre> <p>Esta alternativa sigue permitiendo el proceso de la copia de seguridad selectiva de los archivos que se encuentran en <code>/Volumes/disk2</code>.</p> </li> </ul>

Opción	Descripción
 Sistemas operativos Windows exclude.dir Opciones exclude	 Sistemas operativos Windows Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia <code>exclude.dir c:\test\dan\data1</code> excluye el directorio <code>c:\test\dan\data1</code> , sus archivos y todos sus subdirectorios y sus archivos. Para excluir directorios grandes con una gran cantidad de archivos de los que no desea hacer la copia de seguridad, es mejor utilizar la opción <code>exclude.dir</code> que la opción <code>exclude</code> . No puede utilizar las opciones <code>include</code> para alterar temporalmente la opción <code>exclude.dir</code> . Utilice <code>exclude.dir</code> sólo cuando se excluye toda una rama del directorio.  Si define una sentencia de exclusión sin utilizar una letra de unidad como, por ejemplo, <code>exclude.dir nombredir</code> , se excluirán del proceso todos los directorios de la unidad con el nombre <code>nombredir</code> de todas las unidades.  <ul style="list-style-type: none"> <li>En los siguientes ejemplos se muestran sentencias <code>exclude.dir</code> válidas:                Excluir el directorio <code>C:\MyPrograms\Traverse</code> y sus archivos y subdirectorios:   <pre>exclude.dir c:\MyPrograms\Traverse</pre>               Excluir todos los directorios que <code>c:\MyPrograms\Traverse</code> contiene. Recuerde que sigue siendo posible realizar una copia de seguridad del directorio <code>C:\MyPrograms\Traverse</code> y de los archivos que se encuentran inmediatamente a continuación de <code>C:\MyPrograms\Traverse</code>.   <pre>exclude.dir c:\MyPrograms\Traverse\*</pre>               Excluir todos los directorios cuyos nombres empiezan por <code>temp</code> y que se encuentran en el directorio <code>x:\documents and settings</code> y en sus subdirectorios, donde <code>x:</code> puede ser cualquier unidad.   <pre>exclude.dir "x:\documents and settings\...\temp"</pre>               Excluir todos los directorios cuyos nombres empiezan por <code>temp</code>, con independencia de la unidad o directorio en el que residan:   <pre>exclude.dir temp*</pre>               El ejemplo que se muestra a continuación no es válido, pues finaliza por un delimitador de directorio:   <pre>exclude.dir c:\MyPrograms\Traverse\</pre> </li> <li>Utilice las siguientes sentencias para excluir la unidad <code>x:</code> en su conjunto del proceso de copia de seguridad. Observe que se realiza una copia de seguridad de la raíz de la unidad (<code>x:\</code>), pero se excluyen todos los demás archivos y directorios que se encuentran en <code>x:</code>.   <pre>exclude x:\* exclude.dir x:\*</pre> </li> <li>Un método alternativo para excluir una unidad completa de la realización de la copia de seguridad incremental del dominio consiste en utilizar una sentencia de dominio para excluir la unidad. Por ejemplo:   <pre>domain -x:</pre>               Esta alternativa sigue permitiendo el proceso de la copia de seguridad incremental selectiva y explícita de los archivos que se encuentran en <code>x:</code>. Por ejemplo:   <pre>dsmc s x:\ -subdir=yes dsmc i x: dsmc i x:\MyPrograms\ -subdir=yes</pre> </li> </ul>

 Sistemas operativos Windows

## Sentencias de inclusión/exclusión para sistemas de archivos en red

Las sentencias de inclusión/exclusión que implican a sistemas de archivos en red (unidades remotas) deben escribirse en formato UNC.

En el ejemplo siguiente `z:` es una unidad que se ha correlacionado con un sistema de archivos remoto en `vista.example.com`.






El formato anterior consistía en excluir a \dir\dir2 en el sistema de archivos remoto, como en este ejemplo:

```
EXCLUDE.DIR "Z:\dir1\dir2"
```

Éste es un ejemplo del nuevo formato, que utiliza UNC:

```
EXCLUDE.DIR "\\vista.example.com\d$\dir1\dir2"
```

El cliente no reconocerá las sentencias de inclusión y exclusión escritas en el formato anterior.


 Sistemas operativos AIX  Sistemas operativos Windows  Sistemas operativos Linux


## Excluir archivos y directorios de la copia de seguridad con registro por diario

Hay dos métodos para excluir archivos y directorios de una copia de seguridad con registro por diario.

 Sistemas operativos AIX  Sistemas operativos Linux

- En AIX y Linux, uno de los métodos consiste en añadir sentencias de exclusión al archivo de opciones de cliente para impedir que se realice la copia de seguridad de los archivos o directorios durante el proceso de copia de seguridad.
- En AIX y Linux, el otro método consiste en añadir sentencias de exclusión en el archivo de configuración `tsmjbbd.ini`, para evitar añadir entradas con registro por diario de los archivos o directorios, y de esta forma no procesarlos durante la copia de seguridad con registro por diario.

 Sistemas operativos AIX Si está ejecutando AIX Versión 6.1 o posterior, añada una sentencia `exclude .snapshot` al archivo `tsmjbbd.ini` para evitar que se supervisen directorios de instantáneas internas de JFS2 mediante el daemon de copia de seguridad con registro por diario.

 Sistemas operativos Windows

- Uno de los métodos consiste en agregar sentencias de exclusión al archivo de opciones de cliente para impedir que se realice la copia de seguridad de los archivos o directorios durante el proceso de copia de seguridad.
- El otro método también consiste en agregar sentencias de exclusión en el archivo de configuración `tsmjbbd.ini`, para evitar agregar entradas con registro por diario de los archivos o directorios, y de esta forma no procesarlos durante la copia de seguridad con registro por diario.

Nota: No existe correlación entre las dos sentencias de exclusión. El lugar preferido para las sentencias de exclusión en `tsmjbbd.ini` para evitar que entren en la base de datos de diario y que sean procesados durante una copia de seguridad con registro por diario.


































## Controlar proceso de sentencias de exclusión

























Después de que el cliente ha evaluado todas las sentencias `exclude` se evalúan las opciones siguientes con la lista restante de objetos disponibles para el proceso.

Tabla 1 enumera las opciones que puede utilizar para controlar el proceso con las sentencias de inclusión y exclusión.

Tabla 1. Opciones para controlar el proceso utilizando sentencias de inclusión y exclusión

Opción	Descripción	Página
<b>Proceso de copia de seguridad</b>		
<code>exclude</code> <code>exclude.backup</code> <code>exclude.file</code> <code>exclude.file.backup</code>	<i>Estas opciones son equivalentes.</i> Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción <code>exclude.backup</code> sólo excluye archivos de la copia de seguridad normal, no de HSM.	Opciones <code>exclude</code>
<code>include</code> <code>include.backup</code> <code>include.file</code>	Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad.	Opciones <code>include</code>

Opción	Descripción	Página
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X include.fs	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Controla la forma en que el cliente procesa el espacio de archivos para las copias de seguridad incrementales.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Opciones include
 Sistemas operativos Windows include.fs	 Sistemas operativos Windows Utilice esta opción para configurar opciones según cada espacio de archivos.	 Sistemas operativos Windows Opciones include
<b>Proceso de archivado</b>		
exclude.archive	Excluye un archivo o grupo de archivos de los servicios de archivado.	Opciones exclude
include include.archive	<i>Estas opciones son equivalentes.</i> Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias archivadas.	Opciones include
<b>Proceso de copia de seguridad de imagen</b>		
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris exclude.fs.nas	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado se aplica a todos los servidores de archivos NAS. El mandato backup nas pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias exclude.fs y exclude.dir. Esta opción <i>sólo</i> es válida para clientes AIX y Solaris.	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Opciones exclude
 Sistemas operativos Windows exclude.fs.nas	 Sistemas operativos Windows Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado se aplica a todos los servidores de archivos NAS. El mandato backup nas pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias exclude.dir. Esta opción es válida para todos los clientes Windows.	 Sistemas operativos Windows Opciones exclude
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris exclude.image	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. exclude.image no afectará a las operaciones de copia de seguridad de imágenes incremental. Esta opción es válida para AIX, Solaris y todos los clientes Linux.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Opciones exclude


Opción	Descripción	Página
 Sistemas operativos Windows exclude.image	 Sistemas operativos Windows Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. exclude.image no afectará a las operaciones de copia de seguridad de imágenes incremental. Esta opción es válida para todos los clientes Windows.	 Sistemas operativos Windows Opciones exclude
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris include.fs.nas	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). Para especificar si el cliente debe guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, utilice la opción toc con la opción include.fs.nas en el archivo dsm.sys. Para obtener más información, consulte el apartado Toc. Esta opción solo es válida para los clientes AIX y Solaris.	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Opciones include
 Sistemas operativos Windows include.fs.nas	 Sistemas operativos Windows Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). Para especificar si el cliente debe guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, utilice la opción toc con la opción include.fs.nas en el archivo de opciones del cliente (dsm.opt). Para obtener más información, consulte el apartado Toc. Esta opción es válida para todos los clientes Windows.	 Sistemas operativos Windows Opciones include
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris include.image	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión, o permite asignar una de las diferentes opciones de copia de seguridad de imagen en un volumen lógico cuando se utiliza con el mandato backup image. El mandato backup image ignora todas las demás opciones de inclusión. Esta opción es válida para AIX, Solaris, Linux x86_64 y Linux on POWER únicamente.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Opciones include
 Sistemas operativos Windows include.image	 Sistemas operativos Windows Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión, o permite asignar una de las diferentes opciones de copia de seguridad de imagen en un volumen lógico cuando se utiliza con el mandato backup image. El mandato backup image ignora todas las demás opciones de inclusión. Esta opción es válida para todos los clientes Windows.	 Sistemas operativos Windows Opciones include
 Sistemas operativos Windows <b>Proceso de estado del sistema</b>		
 Sistemas operativos Windows include.systemstate	 Sistemas operativos Windows Asigna clases de gestión para la copia de seguridad del estado del sistema Windows. El valor predeterminado consiste en vincular el objeto de estado del sistema con la clase de gestión predeterminada.	 Sistemas operativos Windows Opciones include
 sistemas operativos Mac OS X  Sistemas operativos Windows		

## Archivos del sistema a excluir


Hay algunos archivos del sistema que deben ubicarse en el archivo de opciones de cliente para que se puedan excluir.


Atención: Estos archivos, o los bloquea el sistema operativo, o pueden causar problemas durante la restauración. Estos son archivos del sistema que no se pueden recuperar sin correr el riesgo de dañar el sistema operativo o los archivos temporales con datos que pueden volver a crearse fácilmente.

Las sentencias que se generan implícitamente pueden verse en las líneas de la salida del mandato query inclexcl con el "sistema operativo" de origen.

 Sistemas operativos Windows Utilice la lista de inclusión-exclusión de ejemplo del archivo dsm.smp como punto de partida para la lista de inclusión-exclusión. Esta es la lista de inclusión-exclusión mínima que debe tener. El archivo dsm.smp está ubicado en la

carpeta config del directorio de instalación. Si ha aceptado los valores predeterminados, la vía de acceso de este archivo será C:\Archivos de programa\Tivoli\TSM\config\dsm.smp.


 Sistemas operativos Windows Hay sentencias de exclusión generadas desde una lista definida por el sistema operativo de Windows en el registro de Windows. Estas sentencias generadas de modo implícito se pueden ver en las líneas de salida del mandato query inlexcl con el origen "operating system".

 sistemas operativos Mac OS X El cliente de copia de seguridad y archivado añade las siguientes sentencias de exclusión a la lista de inclusión-exclusión del archivo dsm.sys. No incluya ninguna de estas sentencias del archivo dsm.sys o se producirán entradas duplicadas.

```
EXCLUDE.ARCHIVE "/.../Desktop DB"
EXCLUDE.BACKUP "/.../Desktop DB"
EXCLUDE.ARCHIVE "/.../Desktop DF"
EXCLUDE.BACKUP "/.../Desktop DF"
EXCLUDE.ARCHIVE /.vol
EXCLUDE.BACKUP /.vol
EXCLUDE.ARCHIVE /automount
EXCLUDE.BACKUP /automount
EXCLUDE.ARCHIVE /Network
EXCLUDE.BACKUP /Network
EXCLUDE.ARCHIVE /dev
EXCLUDE.BACKUP /dev
EXCLUDE.BACKUP /.vol/.../*
EXCLUDE.ARCHIVE /.vol/.../*
EXCLUDE.BACKUP /automount/.../*
EXCLUDE.ARCHIVE /automount/.../*
EXCLUDE.BACKUP /Network/.../*
EXCLUDE.ARCHIVE /Network/.../*
EXCLUDE.BACKUP /dev/.../*
EXCLUDE.ARCHIVE /dev/.../*
EXCLUDE.DIR /.vol
EXCLUDE.DIR /automount
EXCLUDE.DIR /Network
EXCLUDE.DIR /dev
```

 sistemas operativos Mac OS X Nota:

1. No incluya puntos cuando especifique el nombre de los volúmenes (...). El cliente de copia de seguridad y archivado utiliza la secuencia de puntos como parte del proceso de inclusión/exclusión. El cliente informará de la existencia de una sentencia de inclusión/exclusión no válida si un nombre de volumen contiene puntos. *Debe* cambiarse el nombre del volumen.
2. Los objetos que tienen el tipo rhaps y el creador lcmt quedarán excluidos del proceso. Por lo general, son objetos del sistema de archivos especiales aunque también pueden crearse con el mandato mknod, o son puntos de montaje de UNIX. Cuando se realiza una restauración completa del sistema, es necesario volver a crear manualmente los objetos o los puntos de montaje.

 sistemas operativos Mac OS X Debería disponer de una lista de inclusión/exclusión mínima en el archivo de opciones de inclusión/exclusión:

```
EXCLUDE /.../dsmsched.log
EXCLUDE /.../dsmprune.log
EXCLUDE /.../dsmj.log
EXCLUDE /.../dsmerror.log
EXCLUDE /.../.hotfiles.bTree

EXCLUDE.DIR /private/tmp
EXCLUDE.DIR /private/var/vm
EXCLUDE.DIR /private/var/tmp
EXCLUDE.DIR /private/var/db/netinfo/local.nidb

EXCLUDE.DIR /.../.Trashes
EXCLUDE.DIR /.../.Spotlight-*
EXCLUDE.DIR /.../Library/Caches
EXCLUDE.DIR /.../.fsevents
```

 Sistemas operativos Windows

## Excluir archivos con nombres UNC

Para excluir los archivos a los que se accede de forma remota, puede especificar sus nombres UNC (Universal naming convention) en la sentencia de exclusión.

En el siguiente ejemplo se supone que la letra de la unidad local g está correlacionada con el punto compartido remoto

```
\\remote\books
```

En este caso, sería recomendable excluir de las copias de seguridad todos los archivos situados en la raíz de este punto compartido con extensión .txt. Para hacerlo, debe utilizar los mandatos siguientes:

```
exclude g:\*.txt
exclude \\remote\books\*.txt
```

No es posible especificar nombres UNC para unidades extraíbles, como unidades DVD, ZIP o disquetes. Por ejemplo, el mandato siguiente *no es válido*:





```
exclude \\ocean\as\winnt\system32\...\*
```

## Incluir y excluir archivos con caracteres comodín


Debe utilizar caracteres especiales cuando incluya o excluya archivos y directorios que contengan caracteres comodín.

El cliente de copia de seguridad y archivado trata los caracteres comodín de distinta manera en diferentes plataformas.


Los nombres de los directorios y de los archivos pueden incluir diferentes símbolos. Los tipos de símbolos permitidos dependen del sistema operativo.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Por ejemplo, en AIX, los nombres de los directorios o de los archivos pueden incluir:

```
* ? : [ ]
```

 Sistemas operativos Windows Por ejemplo, en Windows, los nombres de los directorios y de los archivos no pueden incluir los siguientes símbolos:





```
? * < > " / \ : |
```

 Sistemas operativos Windows Sin embargo, sí pueden incluir estos símbolos:





```
[ ]
```

Para especificar archivos y directorios en las sentencias de inclusión y exclusión, utilice el carácter de escape "\" para especificar los caracteres comodín. Sin embargo, el carácter de escape solo se puede utilizar dentro de las clases de carácter "[ ]".





En el siguiente ejemplo, se muestra cómo especificar archivos y directorios que contienen caracteres comodín utilizando el carácter de escape y las clases de caracteres en las sentencias de inclusión o de exclusión.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Para excluir el directorio único /usr1/[dir2] del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.sys o el archivo de inclusión-exclusión:

```
exclude.dir "/usr1/[\\[]dir2[\\]"
```


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Para excluir el archivo único /usr1/fi\*le1 del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.sys o el archivo de inclusión-exclusión:

```
exclude "/usr1/fi[\\*]le1"
```


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Consejo: Si utiliza el Editor de preferencias para incluir o excluir un archivo o un directorio único que contenga caracteres comodín, deberá editar de forma manual la sentencia de inclusión o de exclusión para evitar los caracteres comodín. El Editor de preferencias no evita de forma automática los caracteres comodín. Siga los ejemplos anteriores para editar las sentencias de inclusión o de exclusión en el archivo dsm.sys o el archivo de inclusión-exclusión.

 Sistemas operativos Windows Para excluir el directorio único C:\[dir2] del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.opt:

```
exclude.dir "C:[\\[]dir2[\\]"
```

 Sistemas operativos Windows Para excluir el archivo único C:\file[.txt] del proceso de copia de seguridad, especifique lo siguiente en el archivo dsm.opt:

```
exclude.dir "C:\file[\\.].txt"
```

 Sistemas operativos Windows Consejo: Si utiliza el Editor de preferencias para incluir o excluir un archivo o un directorio único que contenga caracteres comodín, deberá editar de forma manual la sentencia de inclusión o de exclusión para evitar los caracteres

comodín. El Editor de preferencias no evita de forma automática los caracteres comodín. Siga los ejemplos anteriores para editar las sentencias de inclusión o de exclusión en el archivo dsm.opt o el archivo de inclusión-exclusión.

**Conceptos relacionados:**

Caracteres comodín












## Inclusión y exclusión de grupos de archivos con caracteres comodín













Puede utilizar caracteres comodín para incluir o excluir grupos de archivos.


Para especificar los grupos de archivos que deben incluirse o excluirse, utilice los caracteres comodín que se indican en la siguiente tabla. Esta tabla *sólo* se aplica a las sentencias include y exclude.

una lista de inclusión/exclusión muy larga puede afectar negativamente al rendimiento de la copia de seguridad. Utilice caracteres comodín y elimine sentencias de inclusión innecesarias para que la lista sea lo más corta posible.

Tabla 1. Caracteres comodín y otros caracteres especiales

Carácter	Función
?	<p>La coincidencia de un único carácter puede utilizarse para buscar la coincidencia con cualquier carácter individual, <i>excepto</i> el separador de directorio; no se aplica a la búsqueda de la coincidencia en el final de la serie de caracteres. Por ejemplo:</p> <ul style="list-style-type: none"> <li>El <b>patrón</b> ab? <b>coincide con</b> abc, pero <b>no coincide con</b> ab, abab ni abzzz.</li> <li>El <b>patrón</b> ab?rs <b>coincide con</b> abfrs, pero <b>no coincide con</b> abrs ni abllrs.</li> <li>El <b>patrón</b> ab?ef?rs <b>coincide con</b> abdefjrs, pero <b>no coincide con</b> abefrs, abdefrs ni abefjrs.</li> <li>El <b>patrón</b> ab??rs <b>coincide con</b> abcdrs, abzzrs, pero <b>no coincide con</b> abrs, abjrs ni abkkrs.</li> </ul>
*	<p>Este carácter puede coincidir con varios caracteres. Por ejemplo:</p> <ul style="list-style-type: none"> <li>El <b>patrón</b> ab* <b>coincide con</b> ab, abb, abxxx, pero <b>no coincide con</b> a, b, aa, bb.</li> <li>El <b>patrón</b> ab*rs <b>coincide con</b> abrs, abtrs, abrsrs, pero <b>no coincide con</b> ar, aabrs ni abrrs.</li> <li>El <b>patrón</b> ab*ef*rs <b>coincide con</b> abefrs, abefghrs, pero <b>no coincide con</b> abefr, abers.</li> <li>El <b>patrón</b> abcd.* <b>coincide con</b> abcd.c, abcd.txt, pero <b>no coincide con</b> abcd, abcdc ni abcdtxt.</li> </ul>
 Sistemas operativos Windows Windows \...	<p> Sistemas operativos Windows            Carácter de coincidencia con n caracteres que coincide con cero o más directorios.            El siguiente patrón especifica todos los archivos del directorio raíz de la unidad C:</p> <pre>c:\*</pre> <p>El siguiente patrón especifica todos los archivos y todos los directorios de la unidad C:</p> <pre>c:\...\*</pre>
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X /...	<p> Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X            Carácter de coincidencia con n caracteres que coincide con cero o más directorios.</p>
[	<p>El carácter de apertura de clase de caracteres inicia la enumeración de una clase de caracteres. Por ejemplo:</p> <pre>xxx[abc]</pre> <p>produce las coincidencias xxxa, xxxb o xxxc.</p>
-	<p>El rango de clase de caracteres incluye caracteres desde el primer carácter al último carácter especificado. Por ejemplo:</p> <pre>xxx[a-z]</pre> <p>produce las coincidencias xxxa, xxxb, xxxc... hasta xxxz.</p> <p> Sistemas operativos Windows            Este formato no debe utilizarse para especificar unidades remotas en una sentencia <b>exclude</b>.</p>

Carácter	Función
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows \	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Es el carácter de escape literal. Cuando se utiliza en una clase de caracteres, trata el siguiente carácter literalmente. Cuando se utiliza fuera de una clase de caracteres, éste no se trata de esta forma. Por ejemplo, si desea incluir ']' en una clase de caracteres, especifique [...]\...]. El carácter de escape no aplica el significado normal de ']' como carácter de clase de caracteres de cierre.
]	El carácter de cierre de clase de caracteres finaliza la enumeración de una clase de caracteres.
 Sistemas operativos Windows :	 Sistemas operativos Windows El carácter separador de unidad separa una especificación de archivo. El carácter que aparece <i>antes</i> de los dos puntos identifica una letra de unidad. Los caracteres que aparecen <i>después</i> de los dos puntos identifican la especificación de archivo o patrón. Por ejemplo: d:\direct\file.nam

 Sistemas operativos Windows Nota: Nota: Dado que una especificación de unidad sólo consta de una letra, para designar una especificación de unidad no debe utilizar más de un carácter comodín o de una combinación de caracteres comodín con una letra. Los siguientes patrones no están permitidos y, si se especifican en el archivo de opciones del cliente (dsm.opt), el programa cliente se detiene inmediatamente después de iniciarse:

 Sistemas operativos Windows

- ?\*:\test.txt
- ?\*:\..\pagefile.sys
- H\*:\test.\*
- \*H:\test.txt
- myvolume\*:\
- myvolume?\*:\


 Sistemas operativos Windows Si utiliza nombres UNC, en la Tabla 2 se muestra cómo especificar correctamente las unidades compartidas.

Tabla 2. Especificar una especificación de unidad con caracteres comodín






Incorrecto	Correcto
\\remote\*:\..\**	\\remote\*\$\..\**
\\remote\?:\..\**	\\remote\?\$\..\**
\\remote\*:\..\pagefile.sys	\\remote\*\$\..\pagefile.sys

**Conceptos relacionados:**

Caracteres comodín

## Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión

El cliente de copia de seguridad y archivado cliente acepta la opción exclude.dir, que se puede utilizar para excluir entradas de directorio. No obstante, las opciones include y exclude.dir no pueden utilizarse al mismo tiempo.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X Nota: En el archivo dsm.sys, las opciones include y exclude no funcionan con vínculos simbólicos a directorios. Por ejemplo, no utilice /u en las sentencias de inclusión o exclusión porque /u es un vínculo simbólico con el directorio /home. En lugar de escribir:

```
include /u/tmp/save.fil
```

escriba:

```
include /home/tmp/save.fil
```

Sin embargo, la opción `exclude` sí funciona con enlaces simbólicos a directorios cuando se especifica el mandato de copia de seguridad con la vía de acceso absoluta que contiene el enlace simbólico.

Tabla 1 muestra cómo utilizar los caracteres comodín para los archivos de inclusión o exclusión.

Tabla 1. Utilización de caracteres comodín con patrones de inclusión y exclusión

Tarea	Patrón
Excluir todos los archivos que acaben por <code>.doc</code> , excepto los que se encuentren en el directorio de inicio de <code>aleko</code> , directorio <code>Documents</code> .	<pre>EXCLUDE /.../*.doc INCLUDE "/home/aleko/Documents/ *.doc"</pre>
Excluir todos los archivos durante la operación de copia de seguridad que tengan la extensión <code>bak</code> , excepto los detectados en el sistema de archivos <code>/usr</code> en el directorio <code>dev</code> .	<pre>exclude /.../*.bak include /usr/dev/*.bak</pre>
Excluir todos los archivos durante la operación de copia de seguridad que tengan la extensión <code>bak</code> , excepto los detectados en la unidad <code>d:</code> en el directorio <code>dev</code> .	<pre>exclude ?:\*.bak include d:\dev\*.bak</pre>
Excluir todos los archivos y directorios que pudieran existir en cualquier directorio <code>Documents</code> , <i>excepto</i> el archivo <code>Current</code> del usuario <code>aleko</code> .	<pre>EXCLUDE /.../Documents/.../* INCLUDE "/home/aleko/Documents/ Current"</pre>
Excluir todos los archivos en cualquier directorio llamado "tmp" y sus subdirectorios, <i>excepto</i> el archivo <code>/home/tmp/save.fil</code> .	<pre>exclude /.../tmp/.../* include /home/tmp/save.fil</pre>
Excluir todos los archivos en cualquier directorio llamado "tmp" y sus subdirectorios, <i>excepto</i> el archivo <code>d:\tmp\save.fil</code> .	<pre>exclude ?:\...tmp\...*\ include d:\tmp\save.fil</pre>
Excluir todos los archivos <code>.cpp</code> de cualquier directorio de los volúmenes <code>Vol1</code> , <code>Vol2</code> , <code>Vol3</code> y <code>Vol4</code> .	<pre>EXCLUDE /Volumes/Vol[1-4]/.../*.cpp</pre>
Excluir todos los archivos <code>.cpp</code> de cualquier directorio de los volúmenes <code>Vol1</code> , <code>Vol2</code> , <code>Vol3</code> y <code>Vol4</code> .	<pre>EXCLUDE /Volumes/Vol[1-4]/.../*.cpp</pre>
Excluir cualquier archivo <code>.cpp</code> de cualquier directorio de los sistemas de archivos <code>/fs1</code> , <code>/fs2</code> , <code>/fs3</code> y <code>/fs4</code> .	<pre>EXCLUDE /fs[1-4]/.../*.cpp</pre>
Excluir los archivos <code>.cpp</code> que se encuentran en el directorio <code>/fs2/source</code> .	<pre>EXCLUDE /fs2/source/*.cpp</pre>



Tarea	Patrón
Sistemas operativos Windows Excluir cualquier objeto .obj para la operación de copia de seguridad de cualquier directorio de las unidades c: e: f: y g:.	Sistemas operativos Windows exclude [ce-g]:\...\*.obj  Las unidades c: e: f: y g: son locales o extraíbles.
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir cualquier archivo .o de cualquier directorio de los sistemas de archivos /usr1, /usr2 y /usr3.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude /usr[1-3]/.../*.o
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir <i>sólo</i> los archivos .o detectados en el directorio raíz del sistema de archivos usr2.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude /usr2/*.o
Sistemas operativos Windows Excluir <i>sólo</i> los archivos .obj detectados en el directorio raíz de la unidad d:.	Sistemas operativos Windows exclude d:\*.obj
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir cualquier archivo que resida en el directorio tmp situado en cualquier sistema de archivos.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude /.../tmp/.../*
Sistemas operativos Windows Excluir cualquier archivo que resida en el directorio tmp situado en cualquier unidad.	Sistemas operativos Windows exclude ?:\tmp\...\*
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir toda la estructura de directorios /var/spool de todo el proceso.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude.dir /var/spool
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir un único sistema de archivos del proceso de copia de seguridad.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude.fs /fs1 exclude.fs home:
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir del proceso de copia de seguridad todos los sistemas de archivos que se han montado en cualquier ubicación del árbol de directorios /test/myfs/fs01 y /test/myfs/fs02.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude.fs /test/myfs/fs01/.../* exclude.fs /test/myfs/fs02/*
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir el directorio /home/mydir/test1 y cualquier archivo y subdirectorio que contenga.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude.dir /home/mydir/test1
Sistemas operativos Windows Excluir el directorio c:\mydir\test1 y cualquier archivo y subdirectorio que contenga.	Sistemas operativos Windows exclude.dir c:\mydir\test1
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluir todos los directorios del directorio /home/mydir cuyo nombre empiece por test.	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X exclude.dir /home/mydir/test*
Sistemas operativos Windows Excluir todos los directorios del directorio \mydir cuyo nombre empiece por test.	Sistemas operativos Windows exclude.dir c:\mydir\test*

Tarea	Patrón
Sistemas operativos Linux sistemas operativos Mac OS X Excluir todos los directorios inmediatamente a continuación del directorio /mydir cuyo nombre empiece por test, en cualquier sistema de archivos.	Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  exclude.dir /.../mydir/test*
Excluir todos los directorios inmediatamente a continuación del directorio \mydir cuyo nombre empiece por test, en cualquier unidad.	Sistemas operativos Windows  exclude.dir ?:\mydir\test*
Sistemas operativos Linux Excluir el volumen lógico RAW de la copia de seguridad de la imagen.	Sistemas operativos Linux Sistemas operativos Oracle Solaris  exclude.image /dev/hd0
Excluir el volumen lógico RAW de la copia de seguridad de la imagen.	Sistemas operativos Windows  exclude.image c:\*
Sistemas operativos Linux sistemas operativos Mac OS X Excluir todos los enlaces simbólicos o alias (los alias se aplican a Mac OS X) del proceso de copia de seguridad, excepto el directorio Docs de user1.	Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X sistemas operativos Mac OS X  EXCLUDE.ATTRIBUTE.SYMLINK /.../* INCLUDE.ATTRIBUTE.SYMLINK /Users/ user1/Docs/*
Excluir todos los directorios y archivos de las unidades locales, con la excepción de la unidad c:.	Sistemas operativos Windows  exclude [abd-z]:\...\* exclude.dir [abd-z]:\...\*

**Conceptos relacionados:**

Ejemplos de utilización de caracteres comodín en patrones de inclusión y exclusión

**Referencia relacionada:**

Opciones exclude

sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris

## Proceso de enlaces simbólicos y alias

El cliente de copia de seguridad y archivado evalúa todas las sentencias exclude.fs y exclude.dir y elimina los espacios de archivos y los directorios excluidos.

Después de esta evaluación inicial, el cliente evalúa todas las sentencias de inclusión/exclusión para controlar el proceso de vínculos simbólicos y alias (exclude.attribute.symlink e include.attribute.symlink) con la lista restante de objetos disponibles para su proceso.

El proceso de alias se aplica a Mac OS X.

En Tabla 1 se definen opciones para controlar el proceso de vínculos simbólicos y alias.

Tabla 1. Opciones para controlar el proceso de vínculos simbólicos y alias

Opción	Descripción	Página
exclude.attribute.symlink	Excluye un archivo o un grupo de archivos que son vínculos simbólicos o alias sólo del proceso de copia de seguridad.	Opciones exclude
include.attribute.symlink	Incluye un archivo o un grupo de archivos que son vínculos simbólicos o alias dentro de un amplio grupo de archivos excluidos sólo para el proceso de copia de seguridad.	Opciones include

## Determinar el proceso de compresión y cifrado

El cliente de copia de seguridad y archivado evalúa exclude.dir y todas las demás opciones de inclusión/exclusión que controlan el proceso de copia de seguridad y archivado para determinar qué archivos se someten al proceso de compresión y cifrado compresión y

cifrado.

Las siguientes opciones determinan cuáles son los archivos que se someterán al proceso de cifrado y compresión.


 Sistemas operativos Windows

Tabla 1. Opciones para controlar el proceso de compresión y cifrado

Opción	Descripción	Página
<b>Proceso de compresión</b>		
exclude.compression	Excluye archivos del proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	Opciones exclude
include.compression	Incluye archivos en el proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	Opciones include
<b>Proceso de cifrado</b>		
exclude.encrypt	Excluye archivos del proceso de cifrado.	Opciones exclude
include.encrypt	Incluye archivos para el proceso de cifrado.  Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.  <b>Importante:</b> el cifrado sólo puede habilitarse en el cliente de archivado y copia de seguridad mediante la opción <code>include.encrypt</code> . Si no se utiliza ninguna sentencia <code>include.encrypt</code> , no se realizará el cifrado.	Opciones include




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

Tabla 2. Opciones para controlar la compresión y el cifrado

Opción	Descripción	Página
<b>Proceso de compresión</b>		
exclude.compression	Excluye archivos del proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	Opciones exclude
include.compression	Incluye archivos en el proceso de compresión si se especifica <code>compression=yes</code> . Esta opción se aplica a copias de seguridad y copias archivadas.	Opciones include
<b>Proceso de cifrado</b>		
exclude.encrypt	Excluye archivos del proceso de cifrado.	Opciones exclude
include.encrypt	Incluye archivos para el proceso de cifrado.  Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.  <b>Importante:</b> el cifrado sólo puede habilitarse en el cliente de archivado y copia de seguridad mediante la opción <code>include.encrypt</code> . Si no se utiliza ninguna sentencia <code>include.encrypt</code> , no se realizará el cifrado.	Opciones include

## Vista previa de los archivos de la lista de inclusión-exclusión

Puede realizar una previsualización de la lista de objetos de los que se va a realizar una copia de seguridad o archivado según la lista de inclusión/exclusión, antes de enviar los datos al servidor.

El árbol de directorios de la GUI web del cliente de copia de seguridad y archivado muestra información detallada sobre los objetos incluidos y excluidos. Las ventanas del árbol de directorios de la GUI web del cliente de copia de seguridad y archivado permiten seleccionar los archivos y directorios que se deben incluir o excluir. Debe utilizar el mandato `preview` para asegurarse de incluir o excluir los archivos correctos. A continuación, encontrará un ejemplo de cómo utilizar la función de previsualización de inclusión/exclusión.

Por ejemplo, siga estos pasos para realizar una copia de seguridad de los archivos del espacio de archivos `/Users/home`:

1. Inicie la GUI del cliente de copia de seguridad y archivado y abra el árbol de copias de seguridad. Puede ver todos los directorios y archivos que se han excluido mediante el archivo de opciones y mediante otras formas.

2. Avance por el árbol y observe que se realiza la copia de seguridad de todos los archivos \* .o de /Volumes/home/mary/myobjdir.
3. Puesto que no desea hacer una copia de seguridad de todos los archivos \* .o, pulse el botón derecho del ratón en un archivo .o y elija "Ver detalles de archivo" en el menú emergente.
4. El diálogo muestra que estos archivos están incluidos; por lo tanto, pulse el botón "Avanzado" y cree una regla para excluir todos los archivos .o del espacio de archivos DATA:\home.
5. Se habrá creado una regla en la parte final del archivo de opciones. El directorio actual se renueva en el árbol Copia de seguridad y los archivos .o aparecen con una 'X' de color rojo, que significa que se han excluido.
6. Cuando busque en otros directorios, mostrarán las nuevas exclusiones que se hayan agregado. Pulse en "Copia de seguridad" y realice la copia de seguridad de los archivos del espacio de archivos /home.

#### Referencia relacionada:


Preview Archive





Previsualizar copia de seguridad

## Inclusión y exclusión de proceso de opciones


El servidor de IBM Spectrum Protect puede definir opciones de inclusión/exclusión mediante el parámetro `inlexcl` en un archivo de opciones del cliente.





Las sentencias de inclusión/exclusión que especifica el servidor se evalúan junto con las del archivo de opciones del cliente. Las sentencias de inclusión/exclusión del servidor siempre se aplican y se colocan al final de la lista de inclusión/exclusión, evaluándose antes que las sentencias de inclusión/exclusión del cliente.


 **Sistemas operativos Windows** Si la lista de inclusión/exclusión del archivo de opciones del cliente contiene una o más opciones `inlexcl` que especifican archivos de inclusión/exclusión, las sentencias de inclusión/exclusión de tales archivos se colocan en la posición de la lista que ocupa la opción `inlexcl` y se procesan como corresponde.





 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Mac OS X** Si la lista de inclusión/exclusión del archivo `dsm.sys` contiene una o más opciones `inlexcl` que especifican archivos de inclusión/exclusión, las sentencias de inclusión/exclusión de tales archivos se colocan en la posición de la lista que ocupa la opción `inlexcl` y se procesan como corresponde.

una lista de inclusión/exclusión muy larga puede afectar negativamente al rendimiento de la copia de seguridad. Utilice caracteres comodín y elimine sentencias de inclusión innecesarias para que la lista sea lo más corta posible.

 **Sistemas operativos Windows** Cuando se realiza una copia de seguridad incremental, el cliente evalúa primero todas las sentencias `exclude.dir` y elimina los directorios y archivos excluidos de la lista de objetos disponibles para procesarse.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Mac OS X** Cuando se realiza una copia de seguridad incremental, el cliente evalúa primero todas las sentencias `exclude.fs` y `exclude.dir` y elimina los espacios de archivos, directorios y archivos excluidos de la lista de objetos disponibles para procesarse.

 **Sistemas operativos Windows** Después de haber evaluado todas las sentencias `exclude.dir`, el cliente evalúa la lista de inclusión/exclusión empezando por el final y se detiene si encuentra una sentencia de inclusión o exclusión que coincide con el archivo que está procesando. Por consiguiente, el orden en que se especifican las opciones de inclusión y exclusión afecta a los archivos que se incluyen y excluyen.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Mac OS X** Después de haber evaluado todas las sentencias `exclude.fs` y `exclude.dir`, el cliente evalúa las sentencias de inclusión/exclusión para controlar el proceso de los enlaces simbólicos o alias (`exclude.attribute.symlink` e `include.attribute.symlink`), empezando por el final y se detiene si encuentra una sentencia de inclusión o exclusión que coincide con el archivo que está procesando. Después de procesar las sentencias de inclusión/exclusión para controlar el proceso de enlaces simbólicos o alias, el cliente evalúa la lista de inclusión/inclusión restante empezando por el final y se detiene cuando encuentra una sentencia de inclusión o exclusión que coincide con el archivo que se está procesando. Por consiguiente, el orden en que se especifican las opciones de inclusión y exclusión afecta a los archivos que se incluyen y excluyen.

Para visualizar una lista de todas las sentencias de inclusión/exclusión en vigor en la estación de trabajo cliente en el orden en el que se procesan, utilice el mandato `query inlexcl`.

El programa cliente procesa la lista de sentencias de inclusión/exclusión de acuerdo con las siguientes reglas:

1. Se comprueban los archivos; los directorios sólo se comprueban si se ha especificado la opción `exclude.dir`.
2. Los nombres de archivo se comparan con los patrones en la lista `include-exclude` de abajo a arriba. Cuando se detecta una coincidencia, el proceso se detiene y comprueba si la opción es `include` o `exclude`. Si la opción es `include`, se realiza una copia de seguridad del archivo. Si la opción es `exclude`, no se realiza ninguna copia de seguridad del archivo.

Nota: Si no se encuentra ninguna coincidencia, los archivos se incluyen de forma implícita y se realiza la copia de seguridad.

3. Cuando se realiza la copia de seguridad de un archivo, se vincula con la clase de gestión predeterminada a menos que coincida con la sentencia include que especificaba un nombre de clase de gestión diferente, y en este caso se vincula con dicha clase de gestión.

En los ejemplos siguientes se muestra el proceso ascendente.  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

#### Ejemplo 1

Imaginemos que La Pomme no es el disco de arranque.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

El archivo que está procesándose es: `/Volumes/La Pomme/Foo/Dev/test.cpp`. El proceso sigue estos pasos:

1. En primer lugar se comprueba la regla 3 (la última sentencia include o exclude definida), porque se trata de un proceso ascendente. El patrón `/Volumes/La Pomme/Foo/Junk/*.cpp` no coincide con el nombre del archivo que está procesándose.
2. El proceso sigue con la regla 2 y realiza la comprobación pertinente. Ahora, el patrón `/Volumes/La Pomme/Foo/.../*.cpp` coincide con el nombre del archivo que está procesándose. El proceso se detiene, se comprueba la opción y se incluye el archivo.
3. Se realiza la copia de seguridad del archivo `/Volumes/La Pomme/Foo/Dev/test.cpp`.

#### Ejemplo 2

Imaginemos que La Pomme no es el disco de arranque.

```
EXCLUDE /.../*.cpp
INCLUDE "/Volumes/La Pomme/Foo/.../*.cpp"
EXCLUDE "/Volumes/La Pomme/Foo/Junk/*.cpp"
```

El archivo que está procesándose es: `/Volumes/La Pomme/Widget/Sample File`. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y no se encuentra ninguna coincidencia.
4. Puesto que no se ha encontrado ninguna coincidencia, `Volumes/La Pomme/Widget/Sample File` se incluye implícitamente y se realiza la copia de seguridad de éste.

#### Ejemplo 3

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude *.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose es: `/home/foo/dev/test.o`. El proceso sigue estos pasos:

1. En primer lugar se comprueba la regla 3 (la última sentencia definida) porque se trata de un proceso ascendente. El patrón `/home/foo/junk/*.o` no coincide con el nombre del archivo que está procesándose.
2. El proceso sigue con la regla 2 y realiza la comprobación pertinente. Ahora, el patrón `/home/foo/.../*.o` coincide con el nombre del archivo que está procesándose. El proceso se detiene, se comprueba la opción y se advierte que se trata de include.
3. Se realiza la copia de seguridad del archivo `/home/foo/dev/test.o`.

#### Ejemplo 4

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude
*.obj
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose es: `/home/widg/copyit.txt`. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y no se encuentra ninguna coincidencia.
4. Puesto que no se ha encontrado una coincidencia, el archivo `/home/widg/copyit.txt` se incluye implícitamente y se realiza la copia de seguridad de éste.

### Ejemplo 5

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude /.../*.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que se está procesando actualmente es: /home/lib/objs/printf.o. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y se encuentra una coincidencia.
4. El proceso se detiene, se comprueba la opción y se excluye.
5. No se realiza la copia de seguridad del archivo /home/lib/objs/printf.o.

### Ejemplo 6

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude.attribute.symlink /.../*
exclude /.../*.o
include /home/foo/.../*.o
exclude /home/foo/junk/*.o
```

El archivo que está procesándose actualmente es: /home/lib/objs/printf.o. El proceso sigue estos pasos:

1. En primer lugar se comprueba la sentencia exclude.attribute.symlink. Si el archivo printf.o es un vínculo simbólico, se excluye. Si no lo es, vaya al paso siguiente. Tenga en cuenta que las sentencias exclude.attribute.symlink siempre se procesan antes que las otras sentencias de inclusión/exclusión, independientemente de su posición en la lista de inclusión/exclusión.
2. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
4. Se comprueba la regla 1 y se encuentra una coincidencia.
5. El proceso se detiene, se comprueba la opción y se excluye.
6. No se realiza la copia de seguridad del archivo /home/lib/objs/printf.o.

## Sistemas operativos Windows

### Ejemplo 1

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude ?:\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```

El archivo que está procesándose es: c:\foo\dev\test.obj. El proceso sigue estos pasos:

1. En primer lugar se comprueba la regla 3 (la última sentencia definida) porque se trata de un proceso ascendente. El patrón c:\foo\junk\\*.obj no coincide con el nombre del archivo que está procesándose.
2. El proceso sigue con la regla 2 y realiza la comprobación pertinente. Ahora, el patrón c:\foo\...\\*.obj coincide con el nombre del archivo que está procesándose. El proceso se detiene, se comprueba la opción y se incluye el archivo.
3. Se realiza la copia de seguridad del archivo c:\foo\dev\test.obj.

### Ejemplo 2

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude ?:\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```

El archivo que está procesándose es: c:\widg\copyit.bat. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y no se encuentra ninguna coincidencia.
4. Puesto que no se ha encontrado una coincidencia, el archivo c:\widg\copyit.bat se incluye implícitamente y se realiza la copia de seguridad de éste.

### Ejemplo 3

Supongamos que define las sentencias siguientes para las opciones include y exclude:

```
exclude ?:\...\*.obj
include c:\foo\...\*.obj
exclude c:\foo\junk\*.obj
```


El archivo que está procesándose actualmente es: c:\lib\objs\printf.obj. El proceso sigue estos pasos:

1. Se comprueba la regla 3 y no se encuentra ninguna coincidencia.
2. Se comprueba la regla 2 y no se encuentra ninguna coincidencia.
3. Se comprueba la regla 1 y se encuentra una coincidencia.
4. El proceso se detiene, se comprueba la opción y se excluye.
5. No se realiza ninguna copia de seguridad del archivo c:\lib\objs\printf.obj.

**Conceptos relacionados:**

Exclusión de espacios de archivos y directorios  
Opciones de proceso




**Referencia relacionada:**


Opciones exclude  
Query Inclxcl  
 Sistemas operativos Windows

## Reglas de proceso y utilización de nombres UNC

Cuando se procesan archivos con nombres UNC, hay unas reglas que se deben seguir.

El cliente de copia de seguridad y archivado utiliza las reglas que se describen en el apartado Inclusión y exclusión de proceso de opciones. También se aplican las reglas de Uso explícito de nombres UNC para unidades remotas.

-  Sistemas operativos Windows Uso explícito de nombres UNC para unidades remotas  
El cliente de copia de seguridad y archivado reconoce el uso explícito de nombres UNC para las unidades remotas.
-  Sistemas operativos Windows Conversión de nombres de vía de accesos de DOS para unidades fijas y remotas  
El cliente de copia de seguridad y archivado convierte los nombres de vía de acceso de DOS que están correlacionados con puntos compartidos remotos.
-  Sistemas operativos Windows Ejemplos de coincidencia de clases de caracteres  
En este tema se muestran ejemplos de coincidencias válidas utilizando clases de caracteres.

 Sistemas operativos Windows

## Uso explícito de nombres UNC para unidades remotas


El cliente de copia de seguridad y archivado reconoce el uso explícito de nombres UNC para las unidades remotas.

Por ejemplo, como se muestra en Tabla 1, el patrón de nombre UNC puede sustituirse por el patrón de DOS.

Supongamos que la letra de la unidad local r: se correlaciona con un punto compartido remoto \\remote\c\$, s: se correlaciona con \\remote\share4 y t: se correlaciona con \\remote\share2.

Tabla 1. Patrones de nombres UNC y patrones de DOS

Patrón de nombres UNC	Patrón de DOS
\\remote\c\$\include\archivo.out	r:\include\archivo.out
\\remote\c\$\...\archivo.out	r:\...\archivo.out
\\remote\share4\exclude\*	s:\exclude\*
\\remote\share2\...\?.out	t:\...\?.out


 Sistemas operativos Windows

## Conversión de nombres de vía de accesos de DOS para unidades fijas y remotas

El cliente de copia de seguridad y archivado convierte los nombres de vía de acceso de DOS que están correlacionados con puntos compartidos remotos.

Por ejemplo, se convierte un punto compartido remoto que se correlaciona de r:\test\...\exclude.out a \\remote\share\test\...\exclude.out Los puntos compartidos remotos que no están correlacionados no se convierten. Los

archivos de los medios extraíbles no se convierten.

 Sistemas operativos Windows

## Ejemplos de coincidencia de clases de caracteres

---

En este tema se muestran ejemplos de coincidencias válidas utilizando clases de caracteres.

```
\\remote[a-z]\share\file.txt  
coincide con    \\remotea\share\file.txt  
\\remote\share[a-z]\file.txt  
coincide con    \\remote\sharex\file.txt  
\\remote\share\file[a-z].txt  
coincide con    \\remote\share\fileg.txt
```

## Cómo empezar





---

Antes de poder utilizar el cliente de archivado y copia de seguridad de IBM Spectrum Protect, debe aprender a iniciar una sesión en la GUI o en la línea de mandatos, y a iniciar el planificador de cliente automáticamente. También puede aprender otras tareas frecuentes.










Antes de utilizar el cliente de archivado y copia de seguridad, complete las siguientes tareas:

- Inicio de una sesión en la GUI Java
- Inicio de una sesión de línea de mandatos
- Inicio de una sesión de cliente web
- Iniciar automáticamente el planificador cliente
- Cambio de la contraseña

También puede completar las siguientes tareas:

- Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado
- Visualización de ayuda en línea
- Finalización de una sesión
- Configuración de los valores de seguridad del cliente para la conexión al servidor de IBM Spectrum Protect versión 8.1.2 y posterior  
Existen varias opciones de configuración que pertenecen a los valores de seguridad del cliente de IBM Spectrum Protect al conectarse al servidor de IBM Spectrum Protect versión 8.1.2 y posterior. Aceptar los valores predeterminados para estas opciones configura de forma transparente el cliente para mejorar la seguridad, y se recomienda en la mayoría de los casos de uso.
- Almacenamiento seguro de contraseñas  
A partir de IBM Spectrum Protect Versión 8.1.2, la ubicación de la contraseña de IBM Spectrum Protect ha cambiado.
-  Sistemas operativos Windows Derechos de seguridad y operaciones del cliente de archivado y copia de seguridad  
En este apartado se explican los tipos de operaciones del cliente de copia de seguridad/archivado de IBM Spectrum Protect que pueden realizarse y los derechos de seguridad que se necesitan.
-  Sistemas operativos Windows Permisos necesarios para restaurar archivos que utilizan la copia de seguridad adaptable de subarchivos  
La copia de seguridad de subarchivos adaptativa está en desuso, pero aún puede restaurar los datos de seguridad de subarchivos creados con la versión 7.1 del cliente, o alguna anterior. Para restaurar archivos que se procesaron mediante la copia de seguridad adaptable de subarchivos, debe ser el propietario de los archivos o tener acceso de lectura.
-  Sistemas operativos Windows Permisos necesarios para copias de seguridad, archivado, restauración o recuperación de archivos en recursos de clúster  
Para realizar una copia de seguridad, archivar o recuperar datos que residan en el MSCS (Microsoft Cluster Server) o los recursos del clúster Veritas Cluster Server, su cuenta de Windows debe pertenecer al grupo de administradores de dominio o al grupo de operadores de copia de seguridad.
- Autenticación del cliente de IBM Spectrum Protect  
Si se utiliza la interfaz gráfica de usuario o la interfaz de línea de mandatos del cliente de IBM Spectrum Protect, se puede iniciar la sesión utilizando un nombre de nodo y una contraseña o un ID y una contraseña de usuario de administración.
-  Sistemas operativos Windows Control de cuentas de usuario  
El control de cuenta de usuario (UAC) es una característica de seguridad de Windows que ayuda a impedir que cualquier programa malicioso ponga en peligro el sistema operativo. El control de cuenta de usuario limita los programas a los privilegios de usuario estándar.
- Inicio de una sesión en la GUI Java  
Los pasos que se utilizan para iniciar el programa de la interfaz gráfica de usuario del cliente de archivado y copia de seguridad depende del sistema operativo.



- Inicio de una sesión de línea de mandatos  
Puede iniciar una sesión de línea de mandatos por medio del mandato `dsmc`.
- Especificación de cadenas de entrada que contengan espacios en blanco o comillas  
Debe seguir ciertas reglas cuando especifique una cadena de entrada que tenga espacios en blanco o comillas.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Inicio: consideraciones adicionales  
Puede incluir opciones en forma de argumentos para los mandatos **dsmj** y **dsmc**. Por ejemplo, puede utilizar opciones para modificar el formato que muestra fechas, horas y números o para incluir la contraseña para que el cliente de copia de seguridad y archivado no la solicite.
- Utilización del cliente web en el nuevo entorno de seguridad  
A partir de IBM Spectrum Protect Versión 8.1.2, ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Iniciar automáticamente el planificador cliente  
Puede iniciar el planificador cliente automáticamente al iniciar la estación de trabajo.
- Cambio de la contraseña  
El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.
- Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado  
Puede utilizar la interfaz gráfica de usuario del cliente de copia de seguridad y archivado para mostrar, ordenar o seleccionar archivos.
- Visualización de ayuda en línea  
Puede visualizar la ayuda en línea de cualquiera de los siguientes modos: en la GUI del cliente de copia de seguridad y archivado, desde el cliente web, o desde la línea de mandatos de `dsmc`.
- Finalización de una sesión  
Puede terminar una sesión de cliente desde la GUI del cliente de copia de seguridad y archivado o desde la línea de mandatos `dsmc`.
- Foros en línea  
Para participar en debates de usuarios de IBM Spectrum Protect puede inscribirse en el servidor de listas ADSM-L.

## Configuración de los valores de seguridad del cliente para la conexión al servidor de IBM Spectrum Protect versión 8.1.2 y posterior

Existen varias opciones de configuración que pertenecen a los valores de seguridad del cliente de IBM Spectrum Protect al conectarse al servidor de IBM Spectrum Protect versión 8.1.2 y posterior. Aceptar los valores predeterminados para estas opciones configura de forma transparente el cliente para mejorar la seguridad, y se recomienda en la mayoría de los casos de uso.

- Valores de seguridad predeterminados para el cliente (vía de acceso rápida)  
La vía de acceso rápida detalla las opciones de configuración que afectan a la seguridad de la conexión del cliente al servidor y el comportamiento para varios casos de uso cuando se aceptan los valores predeterminados. Este caso de ejemplo minimiza los pasos del proceso de configuración en los puntos finales. Obtiene certificados automáticamente desde el servidor cuando el cliente se conecta por primera vez, asumiendo que el parámetro 'SESSIONSECURITY' del servidor IBM Spectrum Protect está definido en 'TRANSITIONAL', que es el valor predeterminado y recomendado. Puede seguir este caso de ejemplo si actualiza por primera vez el servidor de IBM Spectrum Protect a la versión 8.1.2 y a continuación actualiza el cliente a la versión 8.1.2 o viceversa.
- Configuración del cliente sin distribución de certificados automática  
En este caso de ejemplo, se detallan las opciones de configuración que afectan a la seguridad del cliente cuando la distribución automática de certificados desde el servidor no es aceptable. La distribución automática de certificados desde el servidor no se acepta si el servidor está configurado para utilizar la autenticación LDAP o si es necesario que los certificados estén firmados por una entidad emisora de certificados.

## Valores de seguridad predeterminados para el cliente (vía de acceso rápida)

La vía de acceso rápida detalla las opciones de configuración que afectan a la seguridad de la conexión del cliente al servidor y el comportamiento para varios casos de uso cuando se aceptan los valores predeterminados. Este caso de ejemplo minimiza los pasos del proceso de configuración en los puntos finales. Obtiene certificados automáticamente desde el servidor cuando el cliente se conecta por primera vez, asumiendo que el parámetro 'SESSIONSECURITY' del servidor IBM Spectrum Protect está definido en 'TRANSITIONAL', que es el valor predeterminado y recomendado. Puede seguir este caso de ejemplo si actualiza por primera vez el servidor de IBM Spectrum Protect a la versión 8.1.2 y a continuación actualiza el cliente a la versión 8.1.2 o viceversa.

Atención: Este caso de ejemplo no se puede utilizar si el servidor de IBM Spectrum Protect está configurado para la autenticación LDAP. Si se utiliza LDAP, puede importar manualmente los certificados necesarios utilizando el programa de utilidad `dsmcert`. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.

## Opciones de cliente que afectan a la seguridad de sesión

1. **SSLREQUIRED.** El valor predeterminado Default habilita las conexiones existentes de seguridad de sesión en versiones anteriores a V8.1.2, y configura automáticamente el cliente para que se conecte de forma segura a V8.1.2 o una versión más reciente utilizando TLS para la autenticación.
2. **SSLACCEPTCERTFROMSERV.** El valor predeterminado Yes habilita que el cliente acepte automáticamente un certificado público autofirmado desde el servidor, y configura automáticamente el cliente para utilizar dicho certificado cuando el cliente se conecte a un servidor V8.1.2 o versión posterior.
3. **SSL.** El valor predeterminado No indica que el cifrado no se utiliza cuando se transfieren datos entre el cliente y el servidor en versiones anteriores a V8.1.2. Cuando el cliente se conecta a V8.1.2 o un servidor posterior, el valor predeterminado No indica que los datos de objeto no están cifrados. Toda la demás información se cifra, cuando el cliente se comunica con el servidor. Cuando el cliente se conecta a V8.1.2 o servidor posterior, el valor Yes indica que SSL se utiliza para cifrar toda la información, incluyendo los datos de objeto, cuando el cliente se comunica con el servidor.
4. **SSLFIPSMODE.** El valor predeterminado No indica que no se necesita una biblioteca SSL certificada FIPS (Federal Information Processing Standards).

Además, las siguientes opciones solo se aplican cuando el cliente utiliza las conexiones SSL a un servidor de versión anterior a V8.1.2. Se ignoran cuando el cliente se conecta a V8.1.2 o una versión posterior.

1. **SSLDISABLELEGACYTLS.** El valor predeterminado No indica que se permiten las conexiones en TLS 1.1 y protocolos SSL inferiores cuando el cliente se comunica con un servidor V8.1.1 y niveles V8 anteriores, y V7.1.7 y niveles anteriores.
2. **LANFREESL.** Especifica si el cliente utiliza la comunicación SSL con el agente de almacenamiento cuando se configura la transferencia de datos sin LAN.
3. **REPLSSLPORT.** Especifica la dirección del puerto TCP/IP habilitada para SSL cuando el cliente se comunica con el servidor de destino de réplica.

## Casos de uso para los valores de seguridad predeterminados para el cliente (vía de acceso rápida)

1. Primero, el servidor se actualiza a V8.1.2. A continuación, se actualiza el cliente. El cliente existente no utiliza comunicaciones SSL:
  - No es necesario realizar cambios en las opciones de seguridad de cliente.
  - La configuración de cliente se actualiza automáticamente para utilizar TLS cuando el cliente se autentica con el servidor.
2. Primero, el servidor se actualiza a V8.1.2. A continuación, se actualiza el cliente. El cliente existente está utilizando comunicaciones SSL:
  - No es necesario realizar cambios en las opciones de seguridad de cliente.
  - Sigue utilizándose la comunicación SSL con el certificado público del servidor.
  - La comunicación SSL se mejora automáticamente para utilizar el nivel de TLS que el servidor necesita.
3. Primero, el cliente se actualiza a V8.1.2. A continuación, se actualiza el servidor. El cliente existente no utiliza comunicaciones SSL:
  - No es necesario realizar cambios en las opciones de seguridad de cliente.
  - Sigue utilizándose el protocolo de autenticación existente para servidores en versiones anteriores a V8.1.2.
  - La configuración de cliente se actualiza automáticamente para utilizar TLS cuando el cliente se autentica con el servidor después de actualizar el servidor a la versión V8.1.2 o posterior.
4. Primero, el cliente se actualiza a V8.1.2. A continuación, se actualiza el servidor. El cliente existente está utilizando comunicaciones SSL:
  - No es necesario realizar cambios en las opciones de seguridad de cliente.
  - Sigue utilizándose la comunicación SSL con el certificado público del servidor existente con servidores en versiones anteriores a V8.1.2.
  - La comunicación SSL se mejora automáticamente para utilizar el nivel de TLS que el servidor necesita después de actualizarse a V8.1.2 o versión posterior.
5. Primero, el cliente se actualiza a V8.1.2. A continuación, el cliente se conecta a múltiples servidores. Los servidores se actualizan a V8.1.2 en distintos momentos:
  - No es necesario realizar cambios en las opciones de seguridad de cliente.
  - El cliente utiliza el protocolo de seguridad de sesión y la autenticación existentes para los servidores de versiones anteriores a V8.1.2, y se actualiza automáticamente para utilizar la autenticación TLS cuando se conecte inicialmente a un servidor de versión V8.1.2 o posterior. La seguridad de sesión se gestiona por servidor.
6. En una nueva instalación de cliente, el servidor está en versión V8.1.2 o posterior:
  - Configure el cliente de acuerdo con una nueva instalación de cliente.
  - Los valores predeterminados para las opciones de seguridad de cliente configuran automáticamente el cliente para la autenticación de sesión cifrada TLS.
  - Establezca el parámetro SSL en el valor Yes si se necesita el cifrado de todas las transferencias de datos entre el cliente y el servidor.
7. En una nueva instalación de cliente, el servidor está en una versión anterior a V8.1.2:
  - Configure el cliente de acuerdo con una nueva instalación de cliente.

- Acepte los valores predeterminados para los parámetros de seguridad de sesión del cliente si no se necesita el cifrado SSL de todas las transferencias de datos.
  - Se utiliza el protocolo de autenticación no SSL hasta que el servidor se actualiza a la versión V8.1.2 o posterior.
- Establezca el parámetro SSL en el valor Yes si se necesita el cifrado de todas las transferencias de datos entre el cliente y el servidor, y continúe con la configuración del cliente manual para SSL.
  - Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
  - La comunicación SSL se mejora automáticamente para utilizar el nivel de TLS que el servidor necesita después de actualizarse a V8.1.2 o versión posterior.

**Referencia relacionada:**

Sslrequired  
 Sslacceptcertfromserv  
 Ssl  
 Sslfipsmode  
 Ssldisablelegacytls  
 Lanfreesl  
 Replsslport

## Configuración del cliente sin distribución de certificados automática

En este caso de ejemplo, se detallan las opciones de configuración que afectan a la seguridad del cliente cuando la distribución automática de certificados desde el servidor no es aceptable. La distribución automática de certificados desde el servidor no se acepta si el servidor está configurado para utilizar la autenticación LDAP o si es necesario que los certificados estén firmados por una entidad emisora de certificados.

Nota: En este caso de ejemplo, puede aceptar los valores predeterminados para la mayoría de las opciones de seguridad de sesión, excepto para la opción SSLACCEPTCERTFROMSERV.

### Opciones de cliente que afectan a la seguridad de sesión

1. SSLREQUIRED. El valor predeterminado Default habilita las conexiones existentes de seguridad de sesión en versiones anteriores a V8.1.2, y configura automáticamente el cliente para que se conecte de forma segura a V8.1.2 o una versión más reciente utilizando TLS para la autenticación.
2. SSLACCEPTCERTFROMSERV. Establezca este valor en No para asegurarse de que el cliente no acepte automáticamente un certificado público autofirmado del servidor cuando el cliente se conecte por primera vez a un servidor V8.1.2 o versión posterior.
3. SSL. El valor predeterminado No indica que el cifrado no se utiliza cuando se transfieren datos entre el cliente y el servidor en versiones anteriores a V8.1.2. Cuando el cliente se conecta a V8.1.2 o un servidor posterior, el valor predeterminado No indica que los datos de objeto no están cifrados. Toda la demás información se cifra, cuando el cliente se comunica con el servidor. Cuando el cliente se conecta a V8.1.2 o servidor posterior, el valor Yes indica que SSL se utiliza para cifrar toda la información, incluyendo los datos de objeto, cuando el cliente se comunica con el servidor.
4. SSLFIPSMODE. El valor predeterminado No indica que no se necesita una biblioteca SSL certificada FIPS (Federal Information Processing Standards).

Además, las siguientes opciones solo se aplican cuando el cliente utiliza las conexiones SSL a un servidor de versión anterior a V8.1.2. Se ignoran cuando el cliente se conecta a V8.1.2 o una versión posterior.

1. SSLDISABLELEGACYTLS. El valor predeterminado No indica que se permiten las conexiones en TLS 1.1 y protocolos SSL inferiores cuando el cliente se comunica con un servidor V8.1.1 y niveles V8 anteriores, y V7.1.7 y niveles anteriores.
2. LANFREESL. Especifica si el cliente utiliza la comunicación SSL con el agente de almacenamiento cuando se configura la transferencia de datos sin LAN.
3. REPLSSLPORT. Especifica la dirección del puerto TCP/IP habilitada para SSL cuando el cliente se comunica con el servidor de destino de réplica.

### Casos de uso para configurar el cliente sin distribución de certificados automática

1. Primero, el servidor se actualiza a V8.1.2. A continuación, se actualiza el cliente. El cliente existente no utiliza comunicaciones SSL:
  - Utilice el asistente de configuración de cliente para establecer la opción SSLACCEPTCERTFROMSERV con el valor No.
  - Obtenga el certificado necesario desde un origen de confianza.
  - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
2. Primero, el servidor se actualiza a V8.1.2. A continuación, se actualiza el cliente. El cliente existente está utilizando comunicaciones SSL:

- No es necesario realizar cambios en las opciones de seguridad de cliente. Si el cliente ya tiene un certificado de servidor para la comunicación SSL, no se aplica la opción SSLACCEPTCERTFROMSERV.
  - Sigue utilizándose la comunicación SSL con el certificado público del servidor.
  - La comunicación SSL se mejora automáticamente para utilizar el nivel de TLS que el servidor necesita.
3. Primero, el cliente se actualiza a V8.1.2. A continuación, se actualiza el servidor. El cliente existente no utiliza comunicaciones SSL:
- Utilice el asistente de configuración de cliente para establecer la opción SSLACCEPTCERTFROMSERV con el valor No.
  - Sigue utilizándose el protocolo de autenticación existente para servidores en versiones anteriores a V8.1.2.
  - Antes el cliente se conecta a un servidor 8.1.2 o versión posterior:
    - Obtenga el certificado necesario desde un origen de confianza.
    - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
4. Primero, el cliente se actualiza a V8.1.2. A continuación, se actualiza el servidor. El cliente existente está utilizando comunicaciones SSL:
- No es necesario realizar cambios en las opciones de seguridad de cliente. Si el cliente ya tiene un certificado de servidor para la comunicación SSL, no se aplica la opción SSLACCEPTCERTFROMSERV.
  - Sigue utilizándose la comunicación SSL con el certificado público del servidor existente con servidores en versiones anteriores a V8.1.2.
  - La comunicación SSL se mejora automáticamente para utilizar el nivel de TLS que el servidor necesita después de actualizarse a V8.1.2 o versión posterior.
5. Primero, el cliente se actualiza a V8.1.2. A continuación, el cliente se conecta a múltiples servidores. Los servidores se actualizan a V8.1.2 en distintos momentos:
- Utilice el asistente de configuración de cliente para establecer la opción SSLACCEPTCERTFROMSERV con el valor No.
  - Sigue utilizándose el protocolo de autenticación existente para servidores en versiones anteriores a V8.1.2.
  - Antes de que el cliente se conecte a un servidor 8.1.2 o posterior, o cuando se necesita la comunicación SSL en cualquier nivel de servidor:
    - Obtenga el certificado necesario para un servidor de destino desde un origen de confianza.
    - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
  - El cliente utiliza el protocolo de seguridad de sesión y la autenticación existentes para los servidores de versiones anteriores a V8.1.2, y se actualiza automáticamente para utilizar la autenticación TLS cuando se conecte inicialmente a un servidor de versión V8.1.2 o posterior. La seguridad de sesión se gestiona por servidor.
6. En una nueva instalación de cliente, el servidor está en versión V8.1.2 o posterior:
- Configure el cliente de acuerdo con una nueva instalación de cliente.
  - Utilice el asistente de configuración de cliente para establecer la opción SSLACCEPTCERTFROMSERV con el valor No.
  - Obtenga el certificado necesario desde un origen de confianza.
  - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
  - Establezca el parámetro SSL en el valor Yes si se necesita el cifrado de todas las transferencias de datos entre el cliente y el servidor.
7. En una nueva instalación de cliente, el servidor está en una versión anterior a V8.1.2, se necesitan sesiones cifradas por SSL:
- Configure el cliente de acuerdo con una nueva instalación de cliente.
  - Establezca el parámetro SSL en el valor Yes.
  - Obtenga el certificado necesario desde un origen de confianza.
  - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.
8. En la nueva instalación de cliente, el servidor está en una versión anterior V8.1.2, no se necesitan las sesiones cifradas por SSL:
- Configure el cliente de acuerdo con una nueva instalación de cliente.
  - Utilice el asistente de configuración de cliente para establecer la opción SSLACCEPTCERTFROMSERV con el valor No.
    - Se utiliza el protocolo de autenticación no SSL hasta que el servidor se actualiza a la versión V8.1.2 o posterior.
  - Antes el cliente se conecta a un servidor 8.1.2 o versión posterior:
    - Obtenga el certificado necesario desde un origen de confianza.
    - Utilice el programa de utilidad dsmcert para importar el certificado para que el cliente lo utilice. Consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer para obtener más detalles.

**Referencia relacionada:**

Sslrequired  
 Sslacceptcertfromserv  
 Ssl  
 Sslfipsmode  
 Ssldisablelegacytls  
 Lanfreessl

## Almacenamiento seguro de contraseñas

A partir de IBM Spectrum Protect Versión 8.1.2, la ubicación de la contraseña de IBM Spectrum Protect ha cambiado.

En los clientes de V8.1.0, V7.1.6 y anteriores, la contraseña de IBM Spectrum Protect se almacena en el registro de Windows para clientes de Windows y se almacena en el archivo TSM.PWD en los clientes de UNIX y Linux.

A partir de V8.1.2, se utilizan los almacenes de claves de IBM® Global Security Kit (GSKit) para almacenar todas las contraseñas de IBM Spectrum Protect. El proceso de la importación de certificados de servidor se ha simplificado. Para obtener información sobre la importación de certificados de servidor, consulte Configuración de las comunicaciones cliente/servidor de IBM Spectrum Protect con Secure Sockets Layer.

Al actualizar al cliente de archivado y copia de seguridad de IBM Spectrum Protect V8.1.2, las contraseñas existentes se migran a los archivos siguientes en el nuevo almacén de contraseñas:

### TSM.KDB

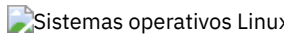
El archivo que almacena las contraseñas cifradas.

### TSM.sth

Archivo que almacena la clave de cifrado aleatoria utilizada para cifrar contraseñas en el archivo TSM.KDB. Este archivo está protegido por el sistema de archivos. Este archivo es necesario para las operaciones automatizadas.

### TSM.IDX

Archivo de índices utilizado para realizar el seguimiento de las contraseñas en el archivo TSM.KDB.

 Para clientes de Data Protection for VMware, la contraseña de administración del servidor de GUI de Data Protection for VMware se migra a un almacén de claves.

 Sistemas operativos Windows

## Ubicaciones de contraseña en clientes Windows

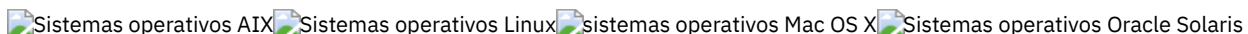
En clientes Windows, las contraseñas de la clave de registro SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient\Nodes y la clave de registro SOFTWARE\IBM\ADSM\CurrentVersion\Nodes se migran al nuevo almacén de contraseñas.

Las entradas de contraseña de estas claves de registro se suprimen tras la migración.

El servidor migrado y las contraseñas de cifrado se almacenan en los almacenes de contraseñas en subdirectorios distintos del directorio C:\ProgramData\Tivoli\TSM\baclient (un directorio oculto). Si se separan las contraseñas del servidor de esta forma se permite que un administrador otorgue un acceso de usuario no administrativo a contraseñas individuales sin proporcionar acceso de usuario a todas las demás contraseñas. Los directorios siguientes son ejemplos de ubicaciones de archivos de contraseñas:

- C:\ProgramData\Tivoli\TSM\BAclient\NodeName\ServerName
- C:\ProgramData\Tivoli\TSM\BAclient\VCB\ServerName
- C:\ProgramData\Tivoli\TSM\BAclient\DOMAIN\ServerName
- C:\ProgramData\Tivoli\TSM\BAclient\FILER\ServerName

El acceso a los archivos stash de contraseñas (TSM.sth) está restringido al creador del almacén de claves, a los administradores y a System. Hay disponible un programa de utilidad (dsmcutil addace) para permitir a los usuarios de Windows modificar fácilmente las listas de control de accesos de archivos de contraseñas. Para obtener más información, consulte ADDACE y DELETEACE.

 Sistemas operativos AIX, Linux, Mac OS X, Oracle Solaris

## Ubicaciones de contraseñas en los clientes UNIX y Linux

En los clientes UNIX y Linux, las contraseñas existentes en los archivos TSM.PWD se migran al nuevo almacén de contraseñas en la misma ubicación. Para usuarios root, la ubicación predeterminada del almacén de contraseñas es /etc/adsm. Para usuarios no root, la ubicación del almacén de contraseñas se especifica mediante la opción passworddir.

El archivo TSM.PWD se suprime tras la migración.

 Sistemas operativos AIX, Linux, Mac OS X, Oracle Solaris

## Trusted Communications Agent ya no está disponible

Trusted Communications Agent (TCA), utilizado anteriormente por los usuarios no root en los clientes de V8.1.0, V7.1.6 y anteriores, ya no está disponible. Los usuarios root pueden utilizar los métodos siguientes para permitir que los usuarios no root gestionen sus

archivos:

#### Método de HelpDesk

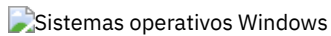
Con el método de HelpDesk, el usuario root ejecuta todas las operaciones de copia de seguridad y restauración. El usuario no root debe ponerse en contacto con el usuario root para solicitar la copia de seguridad o restauración de determinados archivos.

#### Método de usuario autorizado

Con el método de usuario autorizado, se proporciona acceso de lectura y escritura a un usuario no root al almacén de contraseñas utilizando la opción `passworddir` para que apunte a una ubicación de contraseña en la que pueda leer y escribir el usuario no root. Este método permite que los usuarios no root hagan copia de seguridad y restauren sus propios archivos, y que gestionen sus contraseñas con la opción `passwordaccess generate`.

Para obtener más información, consulte el apartado Permitir que los usuarios no root gestionen sus propios datos.

Si ninguno de estos métodos es satisfactorio, debe utilizar los clientes anteriores que incluían TCA.



Sistemas operativos Windows

## Ubicaciones de contraseñas en entornos de clúster

Si utiliza el cliente en un entorno de clúster (CLUSTERNODE YES en el archivo de opciones del cliente), los archivos de contraseñas se almacenan en un subdirectorio de la ubicación del archivo de opciones del cliente. El nombre del subdirectorio es:

```
NODES\NodeName\ServerName
```

En una configuración de clúster, el archivo de opciones se almacena en un disco del clúster de forma que el nodo que toma el control puede tener acceso a él. Los archivos de contraseñas también se deben almacenar en un disco del clúster de forma que, tras un error, la contraseña del cliente de archivado y copia de seguridad generado esté disponible para el nodo que toma el control.

Por ejemplo, si el archivo `dsm.opt` está en el directorio `c:\ClusterStorage\Volume1\SPData`, el nombre de archivo es `Cluster-B` y el nombre del servidor es `Bigdata`, la ubicación de los archivos de contraseñas es:

```
C:\ClusterStorage\Volume1\SPdata\Nodes\Cluster-B\Bigdata
```



Sistemas operativos Windows

## Derechos de seguridad y operaciones del cliente de archivado y copia de seguridad

En este apartado se explican los tipos de operaciones del cliente de copia de seguridad/archivado de IBM Spectrum Protect que pueden realizarse y los derechos de seguridad que se necesitan.

Debe disponer de privilegios de administrador local o del dominio para instalar y configurar los servicios del cliente de IBM Spectrum Protect.

Tabla 1 resume los derechos de seguridad del usuario para las operaciones de copia de seguridad y restauración. La información de la tabla supone los privilegios predeterminados para el grupo de Administradores de Microsoft Windows, grupo de Operadores de copia de seguridad y el grupo de Usuarios no se han alterado.

Tabla 1. Derechos de seguridad de usuario necesarios para los servicios de copia de seguridad y restauración de IBM Spectrum Protect

Sistema operativo	Cuenta	¿De qué elementos puedo realizar una copia de seguridad y restauración?
Clientes de Windows	Miembro del grupo Administradores	<ul style="list-style-type: none"><li>Realizar una copia de seguridad o restaurar todos los objetos de archivo y directorio</li><li>Realizar una copia de seguridad o restaurar el estado del sistema</li><li>Datos de estado del sistema (el grupo de operadores de copia de seguridad no puede realizar una copia de seguridad de los datos del grabador de ASR y no puede restaurar los datos de estado del sistema)</li></ul>

Sistema operativo	Cuenta	¿De qué elementos puedo realizar una copia de seguridad y restauración?
Clientes de Windows	Miembro del grupo de Operadores de copia de seguridad	<ul style="list-style-type: none"> <li>• Realizar una copia de seguridad o restaurar todos los objetos de archivo y directorio</li> <li>• Copia de seguridad del estado del sistema, a excepción de ASR Writer</li> </ul> <p>Nota: Los miembros de grupo de operadores de copia de seguridad no pueden restaurar el estado del sistema.</p>
Clientes de Windows	Miembro del grupo Usuarios u otro grupo	<ul style="list-style-type: none"> <li>• Realizar una copia de seguridad o restaurar todos los objetos de archivo y directorio</li> </ul> <p>Atención: Los usuarios deben tener los siguientes privilegios de seguridad de Microsoft Windows para realizar copias de seguridad y restaurar archivos y directorios:</p> <ul style="list-style-type: none"> <li>◦ Hacer copia de seguridad de archivos y directorios</li> <li>◦ Restaurar archivos y directorios</li> </ul> <p>Estos privilegios representan un riesgo potencial de seguridad desde que se permite al usuario realizar copias de seguridad de cualquier archivo, o restaurar archivos para cualquier copia de seguridad. Los privilegios solo deben otorgarse a usuarios de confianza. Para obtener más información sobre estos privilegios, consulte la documentación de Microsoft Windows.</p> <p>Nota: No se puede realizar ni restaurar el estado del sistema.</p>

De forma predeterminada, los servicios de cliente de IBM Spectrum Protect se ejecutan en la cuenta de sistema local. Sin embargo, la cuenta de sistema local no tiene acceso a las unidades correlacionadas de red y tampoco tiene los mismos permisos y propiedades de conexión que un usuario que esté conectado al sistema. Si experimenta discrepancias entre una copia de seguridad iniciada por un usuario y una copia de seguridad planificada mediante la cuenta de sistema local, tenga en cuenta la posibilidad de cambiar los servicios que se van a ejecutar en la cuenta de usuario.

Consejo: Además de los derechos de seguridad de usuario correspondientes, el cliente de archivado y copia de seguridad de IBM Spectrum Protect requiere que el usuario disponga de permiso de lectura para la raíz de cualquier unidad de la que deba realizarse una copia de seguridad o restauración. Si utiliza la cuenta del sistema para iniciar la sesión para el servicio del planificador de IBM Spectrum Protect asegúrese de otorgar a la cuenta del sistema (SYSTEM) acceso de lectura para la raíz de la unidad. No basta con otorgar a todos los usuarios acceso de lectura para la raíz de la unidad.



Sólo pueden acceder a los recursos del dominio, por ejemplo, las unidades de red, los servicios configurados para ejecutarse bajo una cuenta autorizada de dominio mediante dsmcutil o la aplicación Servicios del Panel de control.


A partir de IBM Spectrum Protect Versión 8.1.2, se aplica un control de accesos más estricto para el almacenamiento de contraseñas de IBM Spectrum Protect en los sistemas operativos Windows. De forma predeterminada, sólo la cuenta de administrador, SYSTEM o LocalSystem tiene acceso al almacén de contraseñas y los certificados SSL.

Puede utilizar el mandato dsmcutil addace para modificar la lista de control de accesos para permitir usuarios adicionales, por ejemplo, usuarios no administrativos o procesos como por ejemplo los procesos de cliente de IBM Spectrum Protect Data Protection para acceder al almacén de contraseñas y los certificados SSL.

Puede utilizar el mandato dsmcutil deleteace para modificar la lista de control de accesos para eliminar el acceso al almacén de contraseñas y los certificados de cliente de los usuarios, como usuarios no administrativos o procesos como por ejemplo los procesos de cliente de IBM Spectrum Protect Data Protection.

Para obtener más información, consulte ADDACE y DELETEACE.

-  Sistemas operativos Windows Operaciones del grupo Operadores de copia de seguridad  
El grupo Operadores de copia de seguridad permite a los usuarios hacer copias de seguridad y restaurar archivos sin tener en cuenta si tienen acceso de lectura o de grabación a los archivos.
-  Sistemas operativos Windows Consideraciones que deben tenerse en cuenta antes de empezar a utilizar una cuenta del grupo de operadores de copia de seguridad  
Debería tener en cuenta los siguientes elementos antes de empezar a utilizar una cuenta del grupo de operadores de copia de seguridad para realizar las operaciones de copia de seguridad, archivado, restauración y recuperación de sus datos.

 Sistemas operativos Windows

## Operaciones del grupo Operadores de copia de seguridad

---

El grupo Operadores de copia de seguridad permite a los usuarios hacer copias de seguridad y restaurar archivos sin tener en cuenta si tienen acceso de lectura o de grabación a los archivos.

Este grupo dispone de un conjunto limitado de derechos de usuario, por lo que algunas funciones no están disponibles para los miembros del grupo Operadores de copia de seguridad.

La lista siguiente contiene las operaciones del cliente de archivado y copia de seguridad que puede realizar un miembro del grupo Operadores de copia de seguridad:

- Realizar una copia de seguridad y la restauración de archivos (consulte Tabla 1)
- Copia de seguridad del estado del sistema

Para realizar copias de seguridad de archivos de grabador ASR, debe ser miembro del grupo Administradores.

- Iniciar el servicio del planificador

La lista siguiente contiene las operaciones del cliente de archivado y copia de seguridad que no puede realizar un miembro del grupo Operadores de copia de seguridad:

- Iniciar ningún otro servicio (aceptación de clientes, agente de cliente remoto y servicio de diario)
- Instalar o configurar servicios del cliente
- Utilizar el soporte de archivos abiertos (OFS)
- Realizar una copia de seguridad o restaurar imágenes
- Realizar una copia de seguridad o restaurar compartimientos de archivos de Windows

 Sistemas operativos Windows

## Consideraciones que deben tenerse en cuenta antes de empezar a utilizar una cuenta del grupo de operadores de copia de seguridad

---

Debería tener en cuenta los siguientes elementos antes de empezar a utilizar una cuenta del grupo de operadores de copia de seguridad para realizar las operaciones de copia de seguridad, archivado, restauración y recuperación de sus datos.

Tenga en cuenta estas consideraciones antes de empezar a utilizar una cuenta del grupo Operadores copia de seguridad para realizar copias de seguridad, archivado, restauración y recuperación de sus datos:

- Si ya ha estado utilizando el cliente de copia de seguridad y archivado con una cuenta del grupo Administradores, es posible que no pueda iniciar el cliente porque no podrá abrir los archivos de anotaciones (por ejemplo, `dsmeerror.log`). Para mitigar este problema, puede otorgar al grupo Operadores de copia de seguridad permisos de lectura y grabación para los archivos de anotaciones o los directorios que contienen estos archivos de anotaciones.
- Si tiene copias de seguridad de un cliente de archivado y copia de seguridad de la versión 5.2 o anterior e intenta realizar una copia de seguridad incremental de un espacio de archivos existente con un miembro del grupo Operadores de copia de seguridad, todos los datos aparecen como modificados y vuelven a enviarse al servidor de IBM Spectrum Protect.
- Es posible que los miembros del grupo Operadores de copia de seguridad no puedan realizar la copia de seguridad o restauración de los datos de los archivos que se han cifrado con una cuenta de Administrador mediante la utilización del sistema de archivos cifrados (EFS) de Windows.
- Los miembros del grupo Operadores de copia de seguridad no disponen de la autorización adecuada para actualizar la hora del último acceso a los archivos que se cifra con el sistema de archivos cifrados (EFS) de Windows. Si un miembro del grupo Operadores de copia de seguridad restaura archivos EFS, no se conservará la hora del último acceso.

 Sistemas operativos Windows



## Permisos necesarios para restaurar archivos que utilizan la copia de seguridad adaptable de subarchivos

---

La copia de seguridad de subarchivos adaptativa está en desuso, pero aún puede restaurar los datos de seguridad de subarchivos creados con la versión 7.1 del cliente, o alguna anterior. Para restaurar archivos que se procesaron mediante la copia de seguridad adaptable de subarchivos, debe ser el propietario de los archivos o tener acceso de lectura.

Estos permisos se agregan a los necesarios para efectuar una restauración normal.

Para obtener información sobre la copia de seguridad de subarchivos adaptativa, consulte el apartado Realización de una copia de seguridad con un ancho de banda limitado de la documentación del cliente de archivado y copia de seguridad, versión 7.1.

 Sistemas operativos Windows

## Permisos necesarios para copias de seguridad, archivado, restauración o recuperación de archivos en recursos de clúster

---

Para realizar una copia de seguridad, archivar o recuperar datos que residan en el MSCS (Microsoft Cluster Server) o los recursos del clúster Veritas Cluster Server, su cuenta de Windows debe pertenecer al grupo de administradores de dominio o al grupo de operadores de copia de seguridad.

Como valor predeterminado, los operadores de copia de seguridad no disponen de los derechos necesarios para llevar a cabo estas tareas en un nodo de clúster. Sin embargo, los operadores de copia de seguridad pueden llevar a cabo este procedimiento si se agrega el grupo al descriptor de seguridad del servicio de clúster. Para ello puede utilizar el administrador de clústeres o ejecutar cluster.exe.

## Autenticación del cliente de IBM Spectrum Protect

---

Si se utiliza la interfaz gráfica de usuario o la interfaz de línea de mandatos del cliente de IBM Spectrum Protect, se puede iniciar la sesión utilizando un nombre de nodo y una contraseña o un ID y una contraseña de usuario de administración.

El cliente solicita el identificador de usuario y lo compara con el nombre de nodo configurado. Si coinciden, el cliente intenta autenticar el identificador de usuario como un nombre de nodo. Si la autenticación falla o si el identificador de usuario no coincide con el nombre de nodo configurado, el cliente intenta autenticar el identificador de usuario como un identificador de usuario de administración.

Para utilizar un identificador de usuario de administración con cualquiera de los clientes de copia de seguridad/archivado, el identificador de usuario debe tener una de las autorizaciones siguientes:

### *Privilegio de sistema*

Autorización en todo el sistema. Un administrador con privilegio de sistema pueden realizar cualquier tarea de administración.

### *Privilegio de política*

Autorización sobre el dominio de políticas del nodo. Permite a un administrador gestionar objetos de políticas, inscribir nodos cliente y planificar operaciones de cliente para los nodos cliente.

### *Propietario de cliente*

Autorización en el nodo cliente de IBM Spectrum Protect inscrito. Puede acceder al cliente por medio del cliente web o del cliente de archivado y copia de seguridad. Puede ser el propietario de datos y tener autorización para acceder físicamente a los datos de forma remota. Puede hacer una copia de seguridad y restaurar archivos en el mismo sistema u otro distinto y puede suprimir espacios de archivos o datos archivados.

### *Acceso a cliente*

Si desea utilizar el cliente web para hacer copias de seguridad y restaurar los archivos en un sistema de cliente remoto, debe disponer de un identificador de usuario de administración con autorización de acceso a cliente en el nombre de nodo para el sistema de cliente remoto. Si no desea que los administradores de IBM Spectrum Protect con autorización de acceso a cliente en el nombre de nodo puedan hacer operaciones de copia de seguridad y restauración de su sistema, especifique la opción `revokeremoteaccess` en el archivo de opciones del cliente.

La autorización de acceso a cliente sólo permite a los administradores de IBM Spectrum Protect hacer copias de seguridad y restaurar archivos en sistemas remotos. No tienen acceso físico a los datos. Es decir, no pueden restaurar en sus propios sistemas los datos que pertenecen al sistema remoto. Para restaurar en el propio sistema los datos que pertenecen a un sistema remoto, debe poseer por lo menos autorización de propietario de cliente.


Para determinar qué autorización tiene, puede utilizar uno de los siguientes métodos:

- En la ventana principal de la GUI de IBM Spectrum Protect, seleccione **Archivo** → **Información acerca de la conexión**.
- Utilice el mandato `QUERY ADMIN` del servidor de IBM Spectrum Protect desde el cliente de línea de mandatos de administración.

**Referencia relacionada:**

Revokeremoteaccess

Mandato QUERY ADMIN


 Sistemas operativos Windows

## Control de cuentas de usuario

El control de cuenta de usuario (UAC) es una característica de seguridad de Windows que ayuda a impedir que cualquier programa malicioso ponga en peligro el sistema operativo. El control de cuenta de usuario limita los programas a los privilegios de usuario estándar.

Si ha habilitado el control de cuenta de usuario (UAC), los programas que requieren privilegios elevados no pueden ejecutarse sin su permiso.

El cliente de archivado y copia de seguridad necesita privilegios elevados. Si ha habilitado el control de cuenta de usuario al ejecutar el cliente, visualizará el cuadro de diálogo Control de cuenta de usuario. El diálogo preguntará si quiere ejecutar el programa. Si no ha iniciado la sesión como administrador, el diálogo también le pedirá sus credenciales de cuenta.









-  Sistemas operativos Windows Habilitar el acceso del cliente a los recursos compartidos de la red cuando está activado UAC. Cuando está activado el Control de cuentas de usuario (UAC), el cliente de archivado y copia de seguridad no puede acceder a las correlaciones de recursos de red existentes. La solución consiste en correlacionar los recursos de la red desde una solicitud de mandato elevado antes de iniciar el cliente.



## Inicio de una sesión en la GUI Java


Los pasos que se utilizan para iniciar el programa de la interfaz gráfica de usuario del cliente de archivado y copia de seguridad depende del sistema operativo.





### Procedimiento

Complete el procedimiento que sea apropiado para que su sistema operativo inicie la interfaz gráfica de usuario de Java™.

Sistema operativo	Procedimiento
 sistemas operativos Mac OS X <b>Mac OS X</b>	 sistemas operativos Mac OS X <ul style="list-style-type: none"> <li>• Pulse dos veces en la aplicación de IBM Spectrum Protect para iniciar el cliente de copia de seguridad y archivado sin privilegios de administrador del sistema. Cuando ejecute el cliente sin privilegios de administrador del sistema, puede gestionar los archivos que posee el usuario actual.</li> <li>• Pulse dos veces IBM Spectrum Protect para administradores y seleccione IBM Spectrum Protect. Después de introducir un nombre de usuario administrador del sistema y una contraseña, se inicia el cliente con privilegios de administrador del sistema. Cuando ejecuta el cliente con privilegios de administrador, puede gestionar los archivos que poseen todos los usuarios en el sistema.</li> <li>• También puede iniciar el cliente de copia de seguridad y archivado utilizando el mandato dsmj. Puede ejecutar el cliente como un proceso en primer plano o en segundo plano. El script dsmj está instalado en /Library/Application Support/tivoli/tsm/client/ba/bin.</li> </ul>
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris <b>AIX, Linux, Solaris</b>	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris <p>En sistemas UNIX distintos a Mac OS X, la interfaz gráfica de usuario del cliente de copia de seguridad y archivado se debe ejecutar desde X Window System. Si ve el icono de IBM Spectrum Protect en el escritorio, significa que ya se está ejecutando el cliente. Efectúe una doble pulsación en el icono para abrir la ventana IBM Spectrum Protect. Si el icono IBM Spectrum Protect no se muestra en el escritorio, inicie la interfaz gráfica del cliente de copia de seguridad y archivado mediante el mandato dsmj. Puede ejecutar el cliente como un proceso en primer plano o en segundo plano.</p>


Sistema operativo	Procedimiento
 Sistemas operativos Windows <b>Windows</b>	 Sistemas operativos Windows Para iniciar la GUI del cliente de copia de seguridad y archivado en un sistema Windows, utilice uno de los siguientes métodos: <ul style="list-style-type: none"> <li>• Pulse Inicio &gt; Programas &gt; IBM Spectrum Protect &gt; GUI de copia de seguridad y archivado.</li> <li>• Pulse Inicio &gt; Ejecutar y escriba la vía de acceso completa al cliente de archivado y copia de seguridad del archivo dsm.exe.</li> <li>• En la línea de mandatos, vaya al directorio de instalación del cliente de copia de seguridad y archivado y escriba dsm.</li> </ul> En sistemas operativos de Windows que tengan la función de control de cuentas de usuario activadas, se le solicitará que permita que se ejecute el programa dsm.exe. Para permitir que el programa continúe y se inicie la GUI del cliente de archivado y copia de seguridad, proporcione las credenciales administrativas.

 Sistemas operativos Windows El cliente de copia de seguridad y archivado localiza y utiliza las opciones que se especifican en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris El cliente de copia de seguridad y archivado localiza y utiliza las opciones que se especifican en el archivo de opciones de sistema del cliente (dsm.sys) y en los archivos de opciones del cliente (dsm.opt).

- contraseña de IBM Spectrum Protect  
El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.
- Asistente para la instalación  
Cuando se inicia el cliente GUI, este comprueba si existe un archivo de opciones del sistema cliente.

#### Tareas relacionadas:

 Sistemas operativos Windows Configuración del idioma para visualizar la GUI de Java

## contraseña de IBM Spectrum Protect

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.

El cliente de IBM Spectrum Protect le solicita la contraseña, en caso de que se necesite una. Póngase en contacto con el administrador de IBM Spectrum Protect si desconoce la contraseña.





#### Tareas relacionadas:


Cambio de la contraseña

## Asistente para la instalación

Cuando se inicia el cliente GUI, este comprueba si existe un archivo de opciones del sistema cliente.

Si no existe el archivo de opciones del cliente (lo cual suele suceder después de haber instalado el cliente por primera vez en el sistema), el asistente para la instalación se iniciará automáticamente para ayudarle a realizar todos los pasos del proceso de configuración.





 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El archivo de opciones del cliente es dsm.sys.


 Sistemas operativos Windows Puede iniciar el asistente para la instalación en cualquier momento para modificar los archivos de configuración del cliente.





 Sistemas operativos Windows El archivo de opciones del cliente es dsm.opt.


## Inicio de una sesión de línea de mandatos

Puede iniciar una sesión de línea de mandatos por medio del mandato dsmc.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota: Si el directorio `/usr/bin` contiene un enlace simbólico al ejecutable de IBM Spectrum Protect y se han establecido todas las variables, puede especificar el mandato dsmc desde cualquier directorio. Sino, especifique la vía de acceso completa del mandato.

 sistemas operativos Mac OS X Nota: En Mac OS X, los administradores del sistema pueden utilizar el mandato sudo para obtener autorización adicional con el fin de que el cliente de copia de seguridad y archivado pueda acceder a los archivos de todos los usuarios del sistema.



 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris En la línea de mandatos, especifique dsmc seguido del mandato (*modalidad por lotes*). Si los directorios `/usr/bin` u `opt/bin` contienen un enlace simbólico al directorio de instalación de IBM Spectrum Protect, puede especificar el mandato dsmc desde cualquier directorio. De lo contrario, puede especificar el nombre completo.

 Sistemas operativos Windows Nota: Si la variable de entorno PATH se ha definido en el directorio de instalación de cliente, puede especificar el mandato dsmc desde cualquier directorio. En caso contrario, especifique la vía de acceso completa.




Solo se puede iniciar el cliente con el mandato "dsmc" en caso de que la variable de entorno PATH se actualice con la vía de acceso a la ubicación del cliente.

 Sistemas operativos Windows Puede abrir el menú de Windows Inicio y seleccionar Programas > IBM Spectrum Protect > Línea de mandatos de copia de seguridad y archivado.

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor. El cliente le solicita la contraseña, si se necesita. Póngase en contacto con el administrador si no conoce la contraseña.

- Utilización de la modalidad por lotes  
Utilice la modalidad *por lotes* para entrar un solo mandato de cliente. Cuando utilice la modalidad por lotes, el mandato debe ir precedido de **dsmc**.
- Emisión de una serie de mandatos mediante la modalidad interactiva  
Utilice la modalidad *interactiva* si desea emitir una serie de mandatos.
-  Sistemas operativos Windows Visualización de caracteres de euro en el indicador de línea de mandatos  
En este tema se explica cómo visualizar el carácter de Euros en el indicador de línea de mandatos de Windows (ventana de consola).
-  Sistemas operativos Windows Utilizar las opciones del mandato DSMC  
En este tema, se muestran algunos ejemplos de cómo utilizar las opciones del mandato dsmc.

#### Conceptos relacionados:

 Sistemas operativos Windows Derechos de seguridad y operaciones del cliente de archivado y copia de seguridad  
Opciones en la modalidad interactiva  
 Sistemas operativos Windows Inicio y finalización de una sesión de mandatos de cliente  
 sistemas operativos Mac OS X Tareas de usuario root y autorizado del cliente de UNIX y Linux  
Utilización de los mandatos

## Utilización de la modalidad por lotes

---

Utilice la modalidad *por lotes* para entrar un solo mandato de cliente. Cuando utilice la modalidad por lotes, el mandato debe ir precedido de **dsmc**.





### Acerca de esta tarea

---

Por ejemplo, para emitir el mandato incremental, escriba lo siguiente en el indicador de mandatos:

```
dsmc incremental
```

Algunos mandatos requieren uno o más argumentos. Por ejemplo, para archivar un archivo:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc archive /home/proj1/file1.txt
```

 Sistemas operativos Windows

```
dsmc archive c:\myfiles\file1.dat
```

En función del valor actual de la opción passwordaccess, puede que el cliente le solicite la contraseña antes de procesar el mandato en una sesión en modalidad por lotes.

Cuando escribe la contraseña, ésta no se visualiza en la pantalla.

#### Referencia relacionada:

Passwordaccess

## Emisión de una serie de mandatos mediante la modalidad interactiva

---

Utilice la modalidad *interactiva* si desea emitir una serie de mandatos.

### Acerca de esta tarea

---


La conexión con el servidor solo se establece una vez para la modalidad interactiva, por lo que podrá procesar una serie de mandatos más deprisa en la modalidad interactiva que en la modalidad por lotes.

Para iniciar una sesión de mandatos de cliente en modalidad interactiva, entre uno de los siguientes mandatos:

- `dsmc`
- `dsmc loop`





Se visualiza el siguiente mensaje en su pantalla:

```
Protect>
```


 Sistemas operativos Windows Si inicia la sesión con un ID de administrador, puede ejecutar las tareas de usuario estándar. Si no ha iniciado una sesión antes de comenzar una tarea desde una ventana de indicador de mandatos, se le solicitará que lo haga..

Si está en la modalidad interactiva, no es necesario escribir `dsmc` delante de los mandatos. Por ejemplo, en lugar de escribir `dsmc archive` para archivar un archivo, escriba solamente **archive**.

Por ejemplo, para archivar un archivo, escriba el mandato con la especificación de archivo:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
archive /home/proj1/file1.txt
```

 Sistemas operativos Windows

```
archive c:\myfiles\file1.dat
```

En función del valor actual de la opción `passwordaccess`, puede que el cliente le solicite la contraseña para que pueda especificar un mandato en una sesión interactiva.

Cuando escribe la contraseña, ésta no se visualiza en la pantalla.

 Sistemas operativos Windows

## Visualización de caracteres de euro en el indicador de línea de mandatos

---

En este tema se explica cómo visualizar el carácter de Euros en el indicador de línea de mandatos de Windows (ventana de consola).

### Procedimiento

---

1. Póngase en contacto con el representante de Microsoft para obtener la página de códigos 858 (el nombre del archivo es `c_858.nls`). Copie el archivo en el directorio `system32` de Windows (por ejemplo, `C:\WINNT\system32`).
2. Edite la clave del registro de Windows mediante este mandato:  
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nls\CodePage\850`, y establezca el valor `c_858.nls`. **Los cambios que haga el editor del registro de Windows no podrán deshacerse.** Los errores generados al editar el registro de Windows pueden provocar anomalías de funcionamiento en el sistema e incluso hacer que éste no se pueda reiniciar. **Tenga cuidado** al editar el registro de Windows. Si no está familiarizado con el uso del editor de registro de Windows, solicite a alguien familiarizado con dicho registro de Windows que le ayude.
3. En Configuración regional, seleccione un país de Europa Occidental (Alemania, Francia, Italia, etc.) como valor local.
4. Salga y reinicie el sistema.

### Resultados

---

Asegúrese de que la fuente que utiliza en la ventana de consola admite el símbolo de euro (como por ejemplo, Lucida Console).

 Sistemas operativos Windows

## Utilizar las opciones del mandato DSMC

---

En este tema, se muestran algunos ejemplos de cómo utilizar las opciones del mandato dsmc.

## Acerca de esta tarea

---

Por ejemplo, suponga que dispone de una estación de trabajo con el nombre de nodo `galaxy1` y de otra estación de trabajo con el nombre de nodo `galaxy2`, y que desea restaurar los datos de `galaxy1` en el sistema `galaxy2`. Para recuperar un archivo de una estación de trabajo (`galaxy1`) mientras se encuentra en la otra estación de trabajo (`galaxy2`), debe acceder a `galaxy1`. Utilice el mandato `set access` para obtener dicho acceso.

Por ejemplo, suponga que el archivo que debe recuperar en `galaxy1` es `c:\universe\saturn.planet`. El propietario de `galaxy1` entra el mandato siguiente:

```
dsmc set access archive c:\universe\saturn.planet galaxy2
```

Una vez otorgado el acceso, deberá recuperar el archivo especificando el mandato:

```
dsmc retrieve -fromnode=galaxy1 \\galaxy1\universe\saturn.planet c:\
```

Nota: También se puede otorgar y obtener acceso a los archivos de otro usuario mediante la GUI.

Si dispone de más de un servidor de copia de seguridad en la organización, puede alternar fácilmente de servidor mediante la opción de línea de mandatos. Para modificar el servidor especificado en `dsm.opt`, puede utilizar un mandato como el siguiente:

```
dsmc -tcpserveraddress=myserver -node=mynode -tcpport=1599
```

### Referencia relacionada:

Fromnode  
Set Access

## Especificación de cadenas de entrada que contengan espacios en blanco o comillas

---

Debe seguir ciertas reglas cuando especifique una cadena de entrada que tenga espacios en blanco o comillas.

Siga estas reglas cuando especifique una cadena de entrada que tenga espacios en blanco o comillas:

- Si la cadena de entrada tiene uno o varios espacios, inclúyala entre comillas simples o dobles. Puede utilizar comillas simples o dobles, siempre y cuando coincidan.
- Si la cadena de entrada contiene alguna comilla simple, inclúyala entre comillas dobles, como en el siguiente ejemplo:

```
-description="Annual backup of the accounting department's monthly reports"
```

- Si la cadena de entrada contiene alguna comilla doble, inclúyala entre comillas simples, como en el siguiente ejemplo:

```
-description='New translations of "The Odyssey" and "The Iliad"'
```

- Si la cadena de entrada tiene espacios y comillas, inclúyala entre comillas. Las comillas externas no pueden ser las mismas que las comillas dentro de la cadena.

Restricción: Una cadena de entrada que contenga comillas simples y dobles no es una cadena válida.

Las siguientes reglas se aplican a estos tipos de datos:

- Nombres completos
- La opción `description` que especifique en el mandato `archive`
- Cualquier valor de opción donde la serie de caracteres incluya espacios o comillas

Importante: No podrá utilizar caracteres de escape con las cadenas de entrada. Los caracteres de escape reciben el mismo tratamiento que los demás caracteres. A continuación, se muestran algunos ejemplos en los que no se reconocen los caracteres de escape:

- Si la serie de caracteres está en un archivo de opciones
- Si la serie de caracteres está en un archivo de lista
- Si la serie de caracteres se especifica en la modalidad interactiva

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Inicio: consideraciones adicionales

---

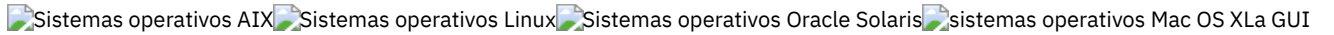
Puede incluir opciones en forma de argumentos para los mandatos **dsmj** y **dsmc**. Por ejemplo, puede utilizar opciones para modificar el formato que muestra fechas, horas y números o para incluir la contraseña para que el cliente de copia de seguridad y archivado no la solicite.

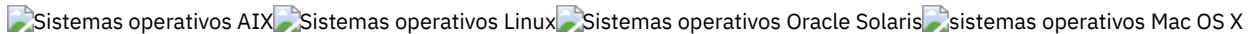
## Acerca de esta tarea

Asimismo, si existe más de un servidor definido en `dsm.sys` y desea establecer contacto con un servidor distinto para hacer uso de los servicios de copia de seguridad/archivado (un servidor distinto del que se ha especificado en el archivo de opciones de usuario `dsm.opt`), especifique el servidor con la opción `servername`.

Por ejemplo:

```
dsmj -servername=server_b
```

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X La GUI Java™ GUI (dsmj) acepta parámetros de línea de mandatos como, por ejemplo, las opciones `-X` de Java. A consecuencia de ello, ahora también puede modificar el tamaño del almacenamiento dinámico de Java. Por ejemplo:

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X


```
dsmj -Xmx512M
```

## Utilización del cliente web en el nuevo entorno de seguridad

A partir de IBM Spectrum Protect Versión 8.1.2, ya no puede utilizar el cliente web para conectarse al servidor de IBM Spectrum Protect V8.1.2 o posterior.

Sin embargo, aún puede utilizar el cliente web para conectarse a los servidores de IBM Spectrum Protect V8.1.1, V8.1.0, V7.1.7 o anteriores.

Si está conectado al servidor de IBM Spectrum Protect V8.1.2 o posterior, utilice las siguientes alternativas al cliente web:

- Para restaurar datos cuya copia de seguridad se ha hecho con el cliente de archivado y copia de seguridad, utilice la GUI Java del cliente de archivado y copia de seguridad (dsmj) o el cliente de línea de mandatos (dsmc). Para obtener más información, consulte:
  - Copia de seguridad de los datos
  - Restauración de los datos
-  Sistemas operativos AIX, Sistemas operativos Oracle Solaris, Sistemas operativos Windows Para hacer copia de seguridad y restaurar servidores de archivos NAS utilizando Network Data Management Protocol (NDMP), utilice los mandatos del servidor de IBM Spectrum Protect en el cliente de línea de mandatos administrativo (dsmadmc). Para obtener más información, consulte la siguiente documentación del servidor:
  - Protección de los servidores de archivos NAS
  - Copia de seguridad y restauración de servidores de archivos NAS mediante NDMP
  - Copia de seguridad y restauración a nivel de archivo para operaciones NDMP
- Inicio de una sesión de cliente web  
El cliente web es una aplicación de inicio de Java™ Web que se puede iniciar y gestionar independientemente del software del navegador web. Después de instalar y configurar el cliente web en la estación de trabajo, puede utilizar el cliente web para obtener acceso remoto y poder ejecutar, de manera remota, operaciones de copia de seguridad, restauración, archivado o recuperación de datos en el nodo de cliente. El cliente web permite la utilización de dispositivos de ayuda para usuarios con discapacidades e incluye mejoras en la navegación con el teclado.


 sistemas operativos Mac OS X, Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, Sistemas operativos Windows

## Iniciar automáticamente el planificador cliente

Puede iniciar el planificador cliente automáticamente al iniciar la estación de trabajo.

Si el administrador de IBM Spectrum Protect ha definido planificaciones para el nodo, el inicio del planificador cliente permite hacer automáticamente copias de seguridad de la estación de trabajo (o realizar otras acciones planificadas).

También puede utilizar el servicio de aceptación de clientes de IBM Spectrum Protect para gestionar el planificador.

 Sistemas operativos Windows IBM Spectrum Protect admite conexiones de red remota al servidor. Con una conexión de red remota, los usuarios móviles ya no se ven obligados a realizar una conexión a la red de la empresa cuando se ha planificado que se ejecute una

copia de seguridad. IBM Spectrum Protect establece una conexión automática antes de que se realice la copia de seguridad planificada. Si la conexión falla, IBM Spectrum Protect vuelve a establecer la conexión antes de intentar realizar la copia de seguridad.

**Tareas relacionadas:**

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

## Cambio de la contraseña

El administrador de IBM Spectrum Protect puede requerir que el usuario utilice una contraseña para conectarse al servidor.







### Acerca de esta tarea

El cliente de copia de seguridad y archivado le solicita la contraseña, en caso de que se necesite una. Póngase en contacto con el administrador de IBM Spectrum Protect si desconoce la contraseña.

Importante: La contraseña mencionada en este tema es distinta de la que se utiliza para los archivos cifrados.






Para cambiar la contraseña desde la GUI:

### Procedimiento


1.  sistemas operativos Mac OS X En clientes Mac OS X, inicie el cliente de copia de seguridad y archivado con las Herramientas de IBM Spectrum Protect para administradores.
2.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows En la ventana principal, abra el menú **Herramientas** y seleccione **Cambiar contraseña**.
3. Entre las contraseñas actual y nueva, y vuelva a entrar la contraseña nueva en el campo **Verificar contraseña**.
4. Pulse **Cambiar**.

### Resultados

Para cambiar la contraseña desde el cliente de línea de mandatos, escriba este mandato:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Para clientes de UNIX, Linux, y Windows:

```
dsmc set password
```

 sistemas operativos Mac OS X Para clientes de Mac OS X, escriba este mandato para cambiar la contraseña desde el cliente de línea de mandatos:

```
sudo dsmc set password
```

A continuación, entre las contraseñas antigua y nueva cuando se le solicite.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de contraseña varían, dependiendo del lugar donde se almacenan y gestionan las contraseñas y en función de la versión del servidor IBM Spectrum Protect al que se conecta el cliente.

Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```



Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9  
\_ - & + .

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Sistemas operativos Windows Recuerde:

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.

Sistemas operativos Windows

En sistemas Windows:

Escriba los parámetros de mandato entre comillas (").

Ejemplo de línea de mandatos:

```
dsmc set password "t67@#$$%^&" "pass2><w0rd"
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris

En sistemas AIX, Linux y Solaris:

Escriba los parámetros de mandato entre comillas simples (').

Ejemplo de línea de mandatos:

```
dsmc set password -type=vmgquest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$$%^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

#### Conceptos relacionados:

Iniciar automáticamente el planificador cliente

#### Tareas relacionadas:

sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Inicio: consideraciones adicionales

#### Referencia relacionada:

Contraseña

Establecer contraseña

## Ordenación de listas de archivos mediante la GUI del cliente de copia de seguridad y archivado

Puede utilizar la interfaz gráfica de usuario del cliente de copia de seguridad y archivado para mostrar, ordenar o seleccionar archivos.

### Acerca de esta tarea

Tabla 1. Trabajar con archivos mediante la GUI del cliente de copia de seguridad y archivado

Tarea	Procedimiento
Visualización de archivos	Para visualizar los archivos de un directorio, pulse en el icono de la carpeta situado junto al nombre de directorio. Los archivos aparecen en el cuadro Lista de archivos de la derecha.
Clasificar la lista de archivos	<ul style="list-style-type: none"><li>Pulse la cabecera de la columna que corresponda en el cuadro Lista de archivos.</li></ul>
Visualizar versiones de copia de seguridad activas e inactivas	<ul style="list-style-type: none"><li>Pulse la opción Visualizar archivos activos/inactivos en el menú Ver.</li><li>Pulse la herramienta Visualizar archivos activos e inactivos en la barra de herramientas.</li></ul>

Tarea	Procedimiento
Visualizar sólo versiones de copia de seguridad activas	Pulse la opción Visualizar sólo archivos activos en el menú Ver.
Seleccionar archivos para restaurar o recuperar	<ul style="list-style-type: none"> <li>• Pulse la casilla situada junto al nombre de directorio o archivo que desea restaurar o recuperar.</li> <li>• Resalte los archivos que desea restaurar o recuperar y pulse la herramienta Seleccionar elementos en la barra de herramientas.</li> <li>• Resalte los archivos que desea restaurar o recuperar y pulse la opción Seleccionar elementos en el menú Editar.</li> </ul>
Deseleccionar archivos	<ul style="list-style-type: none"> <li>• Pulse la casilla marcada situada junto al nombre de directorio o archivo.</li> <li>• Resalte los archivos que desea deseleccionar y pulse la herramienta Deseleccionar elementos en la barra de herramientas.</li> <li>• Resalte los archivos que desea deseleccionar y pulse la opción Deseleccionar elementos en el menú Editar.</li> </ul>
Visualizar información de archivo	<ul style="list-style-type: none"> <li>• Resalte el nombre de archivo y pulse el botón Ver detalles de archivo en la barra de herramientas.</li> <li>• Resalte el nombre de archivo y seleccione Detalles de archivo en el menú Ver.</li> </ul>

Nota:

1. A menos que se indique algo distinto, las tareas y procedimientos de la tabla de arriba se aplican a todas las GUI de cliente.
2. Con las GUI de cliente, puede clasificar una lista de archivos en función de varios atributos, como por ejemplo, nombre, directorio, tamaño o fecha de modificación. La clasificación de archivos en función de la fecha de la última copia de seguridad puede ser útil para determinar la fecha y la hora que se debe utilizar en la función de instante específico.
3. Un archivo *activo* es la versión de copia de seguridad más reciente de un archivo que existía en la estación de trabajo cuando se ejecutó la última copia de seguridad. El resto de versiones de copia de seguridad del archivo están *inactivas*. Sólo se visualizan las versiones de copia de seguridad activas de los archivos, a menos que seleccione la opción de menú Visualizar archivos activos/inactivos. Si suprime el archivo de la estación de trabajo, la versión activa pasa a estar inactiva la siguiente ocasión en que se ejecute una copia de seguridad incremental.

En el cliente de línea de mandatos, puede utilizar los mandatos query con la opción inactive para visualizar los objetos activos e inactivos. Puede utilizar los mandatos restore con las opciones pick e inactive para generar la lista de copias de seguridad activas e inactivas para realizar selecciones.


**Referencia relacionada:**

Inactive  
Pick

## Visualización de ayuda en línea

Puede visualizar la ayuda en línea de cualquiera de los siguientes modos: en la GUI del cliente de copia de seguridad y archivado, desde el cliente web, o desde la línea de mandatos de dsmc.

### Acerca de esta tarea

- En la GUI del cliente de copia de seguridad y archivado:
  - Abra el menú Ayuda. Pulse en Help o pulse en F1.
  - Pulse el botón Ayuda en la ventana actual.
  -  sistemas operativos Mac OS X En sistemas de Mac, pulse en la interrogación de la GUI(?), que muestra la información online sobre la operación actual.
- Desde la línea de mandatos de dsmc: escriba el mandato help. Se visualiza la tabla de contenidos completa para el texto de ayuda que está disponible.

**Referencia relacionada:**





Help




















## Finalización de una sesión


Puede terminar una sesión de cliente desde la GUI del cliente de copia de seguridad y archivado o desde la línea de mandatos dsmc.

## Acerca de esta tarea

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

- Desde la GUI de cliente de copia de seguridad y archivado:
  -  sistemas operativos Mac OS X Abra el menú File (Archivo) y seleccione Quit (Salir).
  -  sistemas operativos Mac OS XPulse Command+Q.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Abra el menú Archivo y seleccione Salir.
  -  sistemas operativos Windows Pulse el icono X del extremo superior derecho.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Abra el menú Sistema y seleccione Cerrar.
  -  Sistemas operativos Windows Pulse **Alt+F4**.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Para el cliente web: abra otro URL o cierre el navegador.
- En la línea de mandatos de DSMC:
  - En la modalidad de proceso por lotes, cada mandato dsmc que introduce es una sesión completa. El cliente finaliza la sesión cuando acaba de procesar el mandato.
  - Para finalizar una sesión interactiva, escriba quit en el indicador `Protect>`.
  - Para interrumpir un mandato dsmc antes de que el cliente haya terminado el proceso, especifique `QQ` en la consola de IBM Spectrum Protect. En la mayoría de los casos, no en todos, ello interrumpirá el mandato. Si no se puede interrumpir el mandato, utilice el mandato kill -9 de UNIX desde un indicador de mandatos disponible. No pulse Control-C ni utilice el mandato kill -15 de UNIX ya que podría producir resultados inesperados.

 Sistemas operativos Windows

- Desde la ventana principal de la GUI de cliente de copia de seguridad y archivado:
  - Pulse Archivo > Salir.
  - Pulse **Alt-X**.
  - Para el cliente web: abra otro URL o cierre el navegador.
- En la línea de mandatos de DSMC:
  - En la modalidad de proceso por lotes, cada mandato dsmc que introduce es una sesión completa. El cliente finaliza la sesión cuando acaba de procesar el mandato.
  - Para finalizar una sesión interactiva, indique quit en el indicador `protect>`.
  - Para interrumpir un mandato dsmc antes de que el cliente haya terminado el proceso, especifique `QQ` en la consola de IBM Spectrum Protect. En la mayoría de los casos, no en todos, ello interrumpirá el mandato. Si no se puede interrumpir el mandato, utilice el gestor de tareas de Windows para finalizar el proceso dsmc. No pulse Control-C porque, aunque finaliza la sesión, puede llevar a resultados inesperados.

### Referencia relacionada:

Loop

## Foros en línea

---

Para participar en debates de usuarios de IBM Spectrum Protect puede inscribirse en el servidor de listas ADSM-L.

## Acerca de esta tarea

---

Se trata de un foro de usuarios administrado por Marist College. Aunque IBM® no le da soporte de forma oficial, los desarrolladores del producto y otros miembros del personal de soporte de IBM también participan de forma informal. Dado que no se trata de un canal oficial de soporte de IBM deberá ponerse en contacto con el servicio de soporte de IBM si necesita obtener una respuesta específica de IBM. De lo contrario, no tiene ninguna garantía de que IBM responda a la pregunta en el servidor de listas.

Puede inscribirse enviando un mensaje a la siguiente dirección de correo electrónico:

`listserv@vm.marist.edu`

El cuerpo del mensaje debe contener la siguiente información:

`SUBSCRIBE ADSM-L mi_nombre mi_apellido`

El servidor de listas le enviará un mensaje solicitando que confirme la solicitud de suscripción. Una vez confirmada la solicitud de suscripción, el servidor de listas le enviará nuevas instrucciones. A continuación, podrá enviar mensajes al servidor de listas escribiendo un correo electrónico a:

`ADSM-L@vm.marist.edu`

Si posteriormente desea borrarse de ADSM-L, puede enviar un mensaje a la siguiente dirección de correo electrónico:

[listserv@vm.marist.edu](mailto:listserv@vm.marist.edu)

El cuerpo del mensaje debe contener la siguiente información:

SIGNOFF ADSM-L

También puede leer y buscar los archivos ADSM-L, participar en foros de debates y acceder a otros recursos en el siguiente URL:

<http://www.adsm.org>

## Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad

---





Si quiere guardar una copia de un archivo desde su ordenador al IBM Spectrum Protect servidor, utilice la función *copia de seguridad*. Si en alguna ocasión se daña o se pierde el archivo original, puede *restaurar* la versión de copia de seguridad del servidor.

- Copia de seguridad de los datos  
Utilice el cliente de copia de seguridad/archivado para almacenar versiones de copia de seguridad de los archivos en un servidor de IBM Spectrum Protect. Estas versiones de copia de seguridad se pueden restaurar en caso de que los archivos originales se pierdan o resulten dañados.
- Restauración de los datos  
Utilice IBM Spectrum Protect para restaurar versiones de copia de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios completos.


## Copia de seguridad de los datos

---


Utilice el cliente de copia de seguridad/archivado para almacenar versiones de copia de seguridad de los archivos en un servidor de IBM Spectrum Protect. Estas versiones de copia de seguridad se pueden restaurar en caso de que los archivos originales se pierdan o resulten dañados.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Todos los procedimientos de copia de seguridad y restauración de cliente también se aplican al cliente web.

Restricción: El cliente web no dispone de un Editor de preferencias para configurar las opciones del cliente.


























 Sistemas operativos Windows Todos los procedimientos de copia de seguridad y restauración de cliente también se aplican al cliente web.



























Restricción: El cliente web no dispone de un Editor de preferencias para configurar las opciones del cliente. El cliente web no ofrece un asistente de configuración, que está disponible en la GUI del cliente de copia de seguridad y archivado en los clientes de Windows. El cliente web no puede examinar recursos de red.

 Sistemas operativos Windows A menos que se indique lo contrario, las referencias a Windows se aplican a todos los sistemas operativos Windows.























 Sistemas operativos Windows El cliente proporciona los servicios de copia de seguridad y archivado para todos los archivos en los siguientes sistemas de archivos: File Allocation Table (FAT), FAT 32, NTFS y ReFS.













A continuación se muestra una lista de las principales tareas de copia de seguridad.


-  Sistemas operativos Windows Planificación de las copias de seguridad (Windows)
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Planificación de las copias de seguridad
-  Sistemas operativos Windows Consideraciones previas a la copia de seguridad (Windows)
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Consideraciones previas a la copia de seguridad (UNIX y Linux)
-  Sistemas operativos Windows Copias de seguridad incrementales, selectivas o incrementales por fecha (Windows)
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)
-  Sistemas operativos Windows Supresión de datos de copia de seguridad
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Supresión de datos de copia de seguridad
-  Sistemas operativos Windows Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (Windows)
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)

-  Sistemas operativos Windows Copia de seguridad del estado del sistema de Windows
-  Sistemas operativos Windows Copia de seguridad de los archivos de Recuperación automática del sistema
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Copia de seguridad de imagen
- Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes
-  Sistemas operativos Windows Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware
-  Sistemas operativos Windows Realización de copias de seguridad de máquinas virtuales en un sistema Hyper-V
-  Sistemas operativos Windows Copia de seguridad de las definiciones de compartición de Net Appliance CIFS
-  Sistemas operativos Windows Planificación de las copias de seguridad (Windows)  
Si es la primera vez que utiliza este producto o si solo realiza copias de seguridad de los archivos de forma ocasional, puede utilizar la tabla que figura en este tema como una lista de comprobación de los pasos previos que deben tenerse en cuenta antes de realizar una copia de seguridad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Planificación de las copias de seguridad  
Si es la primera vez que utiliza este producto o si solo realiza copias de seguridad de los archivos de forma ocasional, puede utilizar la tabla que figura en este tema como lista de comprobación de los pasos previos que deben tenerse en cuenta antes de realizar una copia de seguridad.
- Los archivos de los que se hace copia de seguridad  
Cuando se solicita una copia de seguridad, el cliente realiza una copia de seguridad de un archivo si se cumplen algunos de los requisitos siguientes.
-  Sistemas operativos Windows Soporte de archivos abiertos para las operaciones de copia de seguridad  
El proveedor de instantánea VSS se utiliza para el soporte de archivos abiertos.
-  Sistemas operativos Windows Copia de seguridad de datos mediante la GUI  
Puede utilizar la GUI del cliente de copia de seguridad y archivado para realizar copias de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios enteros.
-  Sistemas operativos Windows Copia de seguridad de datos mediante la línea de mandatos  
Puede utilizar los mandatos incremental o selective para realizar copias de seguridad. En la siguiente tabla se muestran ejemplos de utilización de estos mandatos para realizar diferentes tareas.
-  Sistemas operativos Windows Supresión de datos de copia de seguridad  
Si el administrador le ha otorgado autorización, puede suprimir copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos.
- Cuándo realizar copias de seguridad y cuándo archivar copias  
Cuando el cliente de copia de seguridad/archivado realiza una copia de seguridad o una copia archivada de un archivo, envía una copia de este archivo y sus atributos asociados al servidor. Sin embargo, las operaciones de copia de seguridad y archivado tienen objetivos distintos.
-  Sistemas operativos Windows Consideraciones previas a la copia de seguridad (Windows)  
Diversos factores en el sistema o el entorno pueden afectar la manera en que el cliente de archivado y copia de seguridad procesa los datos. Revise estas consideraciones antes de realizar la copia de seguridad de los datos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Consideraciones previas a la copia de seguridad (UNIX y Linux)  
Diversos factores en el sistema o el entorno pueden afectar la manera en que el cliente de archivado y copia de seguridad procesa los datos. Revise estas consideraciones antes de realizar la copia de seguridad de los datos.
-  Sistemas operativos Windows Copias de seguridad incrementales, selectivas o incrementales por fecha (Windows)  
Es posible que el administrador haya establecido planificaciones para realizar automáticamente copias de seguridad. En esta sección se indica cómo realizar copias de seguridad de archivos sin utilizar una planificación.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)  
Es posible que el administrador haya establecido planificaciones para realizar automáticamente copias de seguridad de archivos de la estación de trabajo. En los apartados siguientes se indica cómo realizar copias de seguridad sin utilizar una planificación.
-  Sistemas operativos Windows Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (Windows)  
Utilice el mandato backup group para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)  
Puede utilizar el mandato backup group para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos desde uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.
-  Sistemas operativos Windows Copia de seguridad de datos con soporte de proxy de nodo cliente (Windows)  
Las copias de seguridad de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad con soporte de proxy de nodo cliente (UNIX y Linux)

Las copias de seguridad de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

-  **Sistemas operativos Windows** Asociar una instantánea local con un espacio de archivos del servidor (Windows)  
Utilice la opción snapshotroot con los mandatos incremental y selective junto con una aplicación suministrada por otro proveedor que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  
Asociar una instantánea local con un espacio de archivos del servidor (UNIX y Linux)  
Utilice la opción snapshotroot con los mandatos incremental y selective junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.
-  **Sistemas operativos Windows** Copia de seguridad del estado del sistema de Windows  
El cliente de copia de seguridad y archivado utiliza VSS para realizar copia de seguridad de todos los componentes de estado del sistema como un solo objeto a fin de proporcionar una instantánea de instante específico coherente del estado del sistema. El estado del sistema consta de todos los componentes de servicios del sistema y de estado del sistema arrancables.
-  **Sistemas operativos Windows** Copia de seguridad de los archivos de Recuperación automática del sistema  
Puede realizar una copia de seguridad de los archivos de Recuperación automática del sistema (ASR) en preparación para la recuperación de la información de configuración del disco de Windows y el estado del sistema si se produce un error muy grave del sistema o de hardware.
-  **Sistemas operativos Windows** Preparación para la recuperación automática del sistema  
Las copias de seguridad específicas y el soporte son necesarios para Windows Automated System Recovery (ASR).
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Windows**  
Copia de seguridad de imagen  
Desde la estación de trabajo local puede hacer una copia de seguridad de un volumen lógico como un solo objeto (copia de seguridad de imagen) del sistema.
-  **Sistemas operativos AIX** Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea  
Para clientes de copia de seguridad y archivado que se ejecutan en AIX 5.3 o sistemas de archivos JFS2 posteriores como usuario root, la copia de seguridad de imágenes basada en instantánea se crea mediante las instantáneas predeterminadas.
-  **Sistemas operativos Linux** Protección de los sistemas de archivos Btrfs  
El sistema de archivos Btrfs debe incluirse como las especificaciones de los archivos para emitir los mandatos de copia de seguridad y restauración, los mandatos de archivado y recuperación y en los mandatos de backup image y restore image. También puede especificar los subvolúmenes Btrfs como la especificación del archivo para realizar la copia de seguridad y restauración y las funciones de archivado y recuperación. No puede utilizar la imagen del cliente de archivado y copia de seguridad o los mandatos de restauración de la imagen en un subvolumen Btrfs.
-  **Sistemas operativos AIX**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Windows** Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes  
Los clientes de archivado y copia de seguridad de Windows, AIX y Solaris pueden utilizar NDMP (Network Data Management Protocol - Protocolo de gestión de datos de redes) para realizar copias de seguridad de imágenes de sistema de archivo de almacenamiento conectado a la red (NAS) y restaurar dichas imágenes de forma eficiente. Las imágenes de sistema de archivo se pueden copiar en, o restaurar desde, bibliotecas o unidades de cinta automatizadas que están conectadas localmente a servidores de archivos NAS de EMC Celerra o de dispositivos de red, o se pueden copiar en, o restaurar desde, unidades de cinta o bibliotecas conectadas de forma local al servidor de IBM Spectrum Protect.
-  **Sistemas operativos Windows** Soporte para Persistent Storage Manager de CDP  
Persistent Storage Manager (PSM) es la tecnología de instantánea que se incluye con un número de cajas de sistemas NAS basados en el Microsoft Server Appliance Kit, que incluye IBM® TotalStorage NAS 200, 300 y 300G.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  
Copia de seguridad de sistemas de archivos de red  
Puede configurar el cliente de archivado y copia de seguridad para proteger archivos a los que se accede con el protocolo NFS (Network File System) o con el protocolo CIFS (Common Internet File System).
-  **Sistemas operativos AIX** Copia de seguridad de los sistemas de archivos con partición de carga de trabajo de AIX  
Mediante la utilización del cliente de archivado y copia de seguridad en AIX, puede realizar la copia de seguridad y restaurar los datos del archivo de partición local dentro de la partición global utilizando el espacio de nombres disponible dentro de la partición global.
-  **Sistemas operativos Oracle Solaris** Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte  
En los sistemas Solaris SPARC y Solaris x86, puede hacer copia de seguridad de los sistemas de archivos Zettabyte (ZFS - Zettabyte file systems), utilizando instantáneas ZFS. La ventaja de este método frente a una copia de seguridad incremental o selectiva ordinaria es que los archivos y carpetas de una instantánea siempre están en estado de sólo lectura, de forma que no se pueden modificar durante una copia de seguridad.
-  **Sistemas operativos AIX** Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX  
Utilice el sistema de archivos cifrados (EFS) de JFS2 de AIX para realizar una copia de seguridad de los archivos en formato de texto legible o sin formato (RAW). Con el formato de texto legible, el archivo se descifra mediante EFS a medida que se va leyendo. Si no se aplica formato, los datos no se descifran. El valor predeterminado es no aplicar formato, pero cuando establece la opción efsdecrypt en yes, obtiene copias de seguridad de texto legible.

-  Sistemas operativos AIX Copia de seguridad de los atributos ampliados de AIX JFS2  
El sistema de archivos de AIX JFS2 (Enhanced Journal File System) proporciona el proceso de copia de seguridad de los atributos ampliados para todos los sistemas de archivos que admiten atributos ampliados con nombre.
-  Sistemas operativos Linux  Sistemas operativos Windows Realización de copia de seguridad de máquinas virtuales VMware  
Puede utilizar el cliente de archivado y copia de seguridad para realizar copias de seguridad y restaurar una máquina virtual (VM) a VMware. Las copias de seguridad completas de la máquina virtual operan a nivel de una imagen de disco. Las copias de seguridad incrementales solo copian los datos modificados desde la última copia de seguridad completa.
-  Sistemas operativos Windows Realización de copias de seguridad de máquinas virtuales en un sistema Hyper-V  
Puede utilizar el cliente de archivado y copia de seguridad para realizar copias de seguridad de máquinas virtuales gestionadas por un servidor de Microsoft Hyper-V.
-  Sistemas operativos Linux  Sistemas operativos Windows Copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack  
Utilice Tivoli Storage Manager FastBack para realizar copias de seguridad y archivado de las instantáneas más recientes para retención a corto plazo.
-  Sistemas operativos Windows Copia de seguridad de las definiciones de compartición de Net Appliance CIFS  
Las definiciones de compartición de Network Appliance (NetApp) CIFS incluyen los permisos de compartición que se han establecido en el servidor de archivos.
- Visualización del estado del proceso de copia de seguridad  
Durante una copia de seguridad, de forma predeterminada, el cliente de copia de seguridad y archivado muestra el estado de cada archivo del que intenta realizar una copia de seguridad.
-  Sistemas operativos Windows Copia de seguridad (Windows): Consideraciones adicionales  
En este apartado trata sobre la información adicional que debe tenerse en cuenta al realizar una copia de seguridad de los datos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copia de seguridad (UNIX y Linux): Consideraciones adicionales  
Hay algunas situaciones especiales que debe tener en cuenta antes de realizar una copia de seguridad de los datos.

 Sistemas operativos Windows

## Planificación de las copias de seguridad (Windows)

Si es la primera vez que utiliza este producto o si solo realiza copias de seguridad de los archivos de forma ocasional, puede utilizar la tabla que figura en este tema como una lista de comprobación de los pasos previos que deben tenerse en cuenta antes de realizar una copia de seguridad.

Lea las tareas enumeradas en esta lista de tareas para determinar si está preparado para realizar una copia de seguridad de los datos.

Tabla 1. Planificación de las copias de seguridad

<input type="checkbox"/>	Debe decidir si desea realizar una copia de seguridad o una copia archivada de los archivos. Para obtener más información, consulte el apartado Cuándo realizar copias de seguridad y cuándo archivar copias.
<input type="checkbox"/>	Consulte el apartado Consideraciones previas a la copia de seguridad (Windows) para obtener información importante acerca de la migración y del modo de aumentar el rendimiento antes de realizar copias de seguridad de archivos y directorios.
<input type="checkbox"/>	Debe crear una lista de inclusión/exclusión para especificar qué archivos y directorios desea excluir de los servicios de copia de seguridad. Para obtener más información, consulte el apartado Proceso de control con una lista de inclusión-exclusión.
<input type="checkbox"/>	Debe decidir el tipo de copia de seguridad que desea en función de lo que necesite. Consulte los apartados siguientes para obtener más información: <ul style="list-style-type: none"> <li>• Copias de seguridad incrementales, selectivas o incrementales por fecha (Windows)</li> <li>• Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (Windows)</li> <li>• Copia de seguridad del estado del sistema de Windows</li> <li>• Copia de seguridad de los archivos de Recuperación automática del sistema</li> <li>• Copia de seguridad de imagen</li> <li>• Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes</li> <li>• Copias de seguridad paralelas de máquinas virtuales</li> </ul>
<input type="checkbox"/>	Si desea obtener más información acerca de las consideraciones que debe tener en cuenta para realizar una copia de seguridad, consulte el apartado Copia de seguridad (Windows): Consideraciones adicionales.

**Conceptos relacionados:**

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

**Tareas relacionadas:**

Configuración de clientes de copia de seguridad/archivado

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Planificación de las copias de seguridad

---

Si es la primera vez que utiliza este producto o si solo realiza copias de seguridad de los archivos de forma ocasional, puede utilizar la tabla que figura en este tema como lista de comprobación de los pasos previos que deben tenerse en cuenta antes de realizar una copia de seguridad.

Lea la lista de tareas para determinar si está preparado para realizar una copia de seguridad de los datos.

- Debe decidir si desea realizar una copia de seguridad o una copia archivada. Consulte *Cuándo realizar copias de seguridad y cuándo archivar copias* para obtener más información.
- En el apartado *Consideraciones previas a la copia de seguridad (UNIX y Linux)* encontrará información importante que debe tenerse en cuenta antes de hacer la copia de seguridad de los archivos y directorios.
- ¿Debe excluir archivos de los servicios de copia de seguridad? Consulte el apartado *Opciones de inclusión/exclusión* para controlar el proceso para obtener más información.

**Conceptos relacionados:**

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

**Tareas relacionadas:**

Configuración de clientes de copia de seguridad/archivado

## Los archivos de los que se hace copia de seguridad

---

Cuando se solicita una copia de seguridad, el cliente realiza una copia de seguridad de un archivo si se cumplen algunos de los requisitos siguientes.

Para hacer copia de seguridad de un archivo, el cliente debe cumplir los siguientes requisitos:

- La clase de gestión seleccionada contiene un grupo de copia de seguridad.
- El archivo cumple con los requisitos de serialización que se definen en el grupo de copia de seguridad. Si el parámetro de serialización del grupo de copia es `static` o `shrstatic` y el archivo cambia durante la copia de seguridad, no se ha realizado la copia de seguridad del archivo.
- El archivo cumple con los requisitos de modo que se definen en el grupo de copia de seguridad. Si el parámetro `mode` del grupo de copia es `modified`, el archivo debe haber cambiado desde la última copia de seguridad. Si `mode` es `absoluta`, puede realizarse una copia de seguridad del archivo aunque este no haya cambiado.
- El archivo cumple con los requisitos de frecuencia que se definen en el grupo de copia de seguridad. El número mínimo especificado de días desde la última copia de seguridad que deben transcurrir antes de que se realice la copia de seguridad del archivo.
- El archivo no se excluye de la copia de seguridad por una sentencia de exclusión.
- El archivo no se excluye de la copia de seguridad por un sistema operativo. Estos archivos excluidos se pueden encontrar en la subclave de registro `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup`.

Los archivos que son parte del estado del sistema de Windows se pueden elegir para realizar la copia de seguridad solo cuando se ha realizado una copia de seguridad del estado del sistema. Puede realizar una copia de seguridad del estado del sistema únicamente como una sola entidad debido a las dependencias entre los componentes de Estado del sistema. No puede realizar la copia de seguridad o restaurar los archivos de forma individual. Por ejemplo, ya que `C:\windows\system32\ntoskrnl.exe` es parte del estado del sistema de Windows, no se realiza la copia de seguridad durante la copia de seguridad incremental o selectiva de la unidad `C:`.

 Sistemas operativos Windows

## Soporte de archivos abiertos para las operaciones de copia de seguridad

---

El proveedor de instantánea VSS se utiliza para el soporte de archivos abiertos.

VSS es el proveedor de instantáneas para Windows.

Algunas aplicaciones pueden crear archivos y abrirlos de manera que no permitan acceder a los mismos a los demás procesos en un sistema operativo Microsoft Windows. Aunque no se trata de una práctica común, a veces la utilizan los proveedores de bases de datos u otras aplicaciones que podrían desear limitar el acceso a determinados archivos. Mediante la restricción del acceso a estos archivos, se impide que los productos de copia de seguridad puedan realizar la copia de seguridad de los datos. Estos archivos bloqueados no



son lo mismo que los archivos que están abiertos o en uso. El cliente de copia de seguridad y archivado, si se ejecuta sin la característica de soporte de archivos abiertos (OFS), puede hacer una copia de seguridad de archivos abiertos o en uso, incluidos los archivos que están abiertos para su lectura o grabación, los archivos que cambian durante la copia de seguridad, los archivos ejecutables y dll que se están ejecutando, los archivos de anotaciones que se adjuntan, etc.

Puede crear copias de seguridad de imágenes activadas o de OFS en estaciones de trabajo con una sola unidad C: basada en NTFS o ReFS.

A continuación se muestra un mensaje de error que aparece en el archivo `dsmerror.log` cuando el cliente encuentra uno de estos archivos bloqueados sin el soporte de OFS activado:

```
ANS4987E Error al procesar '\\machine1\d$\dir1\lockedfile.xyz': otro proceso está utilizando el objeto
```

```
ANS1228E El envío del objeto '\\machine1\d$\dir1\lockedfile.xyz' ha fallado
```

No utilice OFS para realizar la copia de seguridad de los archivos del sistema Windows bloqueados, como el estado del sistema de Windows. El cliente tiene funciones avanzadas para realizar la copia de seguridad de los datos contenida dentro de estos archivos. La copia de seguridad de los datos del sistema que se incluyen en estos archivos requiere un proceso adicional y debe hacerse dentro de un grupo para que la restauración sea satisfactoria. Estos archivos se excluyen de la copia de seguridad a nivel de archivos de IBM Spectrum Protect.

Para las aplicaciones de base de datos que utilizan determinados archivos para mantener la coherencia transaccional (por ejemplo, un archivo de anotaciones de recuperación), es posible que no pueda realizarse la copia de seguridad y restauración de estos archivos sin la coordinación de la base de datos. En estas circunstancias, no haga la copia de seguridad de estos archivos de base de datos con la copia de seguridad normal a nivel de archivos. Puede excluirlos del proceso de copia de seguridad por medio de una exclusión o la opción `excluye.dir`. Dispone de varios clientes de protección de datos (IBM Spectrum Protect for Databases, IBM Spectrum Protect for Mail, etc.) para ofrecer esta coordinación de base de datos y copia de seguridad junto con otras características avanzadas de copia de seguridad de base de datos. Para obtener una lista actualizada de clientes de protección de datos, vaya a este sitio web: <http://www.ibm.com/systems/storage/spectrum/protect/>.

En las aplicaciones privadas o en otros productos de base de datos que no disponen de clientes de Data Protection, puede utilizar la opción `preschedulecmd` para indicar a la base de datos o a la aplicación que realice una de las siguientes acciones:

- Haga lo necesario para que estos archivos adquieran un estado coherente que no sea abierto.
- Detenga la base de datos antes de iniciar la copia de seguridad a nivel de archivos.
- Cree otro método, mediante un programa o un script, para hacer una copia de seguridad de estos datos y exclúyalos de la copia de seguridad a nivel de archivos. En estos casos, la característica OFS no es necesaria puesto que estos archivos no están disponibles ni están bloqueados por la aplicación. Cuando se completa la copia de seguridad a nivel de archivo, utilice la opción `postschedulecmd` para volver a poner en línea de la base de datos o reiniciar la aplicación.

Si el intervalo de tiempo transcurrido para realizar la copia de seguridad a nivel de archivos es demasiado largo para que los archivos abiertos estén fuera de línea (por ejemplo, teniendo la base de datos fuera de línea o conteniendo el proceso de transacciones), utilice la característica OFS para crear una instantánea de instante específico del volumen. En este caso, utilice las opciones `presnapshotcmd` y `postsnapshotcmd` para indicar a la base de datos o a la aplicación que se coordine con la copia de seguridad de estos archivos abiertos. La instantánea, que se produce entre el mandato previo a la instantánea y el mandato posterior a la instantánea, normalmente tarda unos cuantos segundos en crearse. Esto permite que la base de datos o la aplicación reanude rápidamente las aplicaciones a la vez que sigue permitiendo que el cliente lleve a cabo una copia de seguridad incremental completa del volumen, incluidos los archivos bloqueados. Hay otras situaciones en las que se puede hacer de forma segura una copia de seguridad de estos archivos bloqueados de la aplicación y restaurarlos uno por uno. En estas situaciones puede habilitar la característica OFS para dicho volumen en el que están los archivos abiertos. Luego el cliente accede a estos archivos y hace una copia de seguridad de los mismos con las operaciones de copia de seguridad y archivado a nivel de archivos.

Para obtener información sobre las restricciones y los problemas de Open File Support, consulte la nota técnica 1248971.

Si se ha configurado el soporte de archivos abiertos, el cliente realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan). La instantánea permite que la copia de seguridad pueda realizarse a partir de una copia de instante específico que coincida con el sistema de archivos en el momento de tomarse la instantánea. Los cambios que se realicen posteriormente en el sistema de archivos no se incluirán en la operación de copia de seguridad. Puede establecer el parámetro `snapshotproviderfs` de la opción `include.fs` en `none` para especificar qué unidades no utilizan el soporte de archivos abiertos.

Para controlar una operación de soporte de un archivo abierto, puede especificar estas opciones adicionales en su archivo de `dsm.opt` o como valores de la opción `include.fs`: `snapshotproviderfs`, y `presnapshotcmd` y `postsnapshotcmd`.

Nota:

1. Puede utilizar la opción `include.fs` para establecer opciones de instantánea para cada sistema de archivos.

2. El soporte de archivos abiertos se proporciona para la copia de seguridad y el archivado. Para la copia de seguridad incluye la copia de seguridad incremental, la copia de seguridad incremental por fecha, la copia de seguridad selectiva, la copia de seguridad de imagen incremental y la copia de seguridad basada en el diario.
3. El soporte de archivos abiertos solo se admite en volúmenes fijos locales, (montados en letras de unidad o en puntos de montaje de volúmenes) con formato de sistemas de archivos FAT, FAT32, NTFS o ReFS. Este soporte incluye los volúmenes conectados con la SAN que satisfacen estos requisitos.
4. Para habilitar el soporte de OFS en un entorno de clúster, dicho soporte debe estar configurado en todas las estaciones de trabajo del clúster. Defina VSS como proveedor de instantáneas en la opción snapshotproviderfs.


**Conceptos relacionados:**

Opciones de proceso

**Tareas relacionadas:**

Copia de seguridad del estado del sistema de Windows

Configuración del soporte de archivos abiertos

 Sistemas operativos Windows

## Copia de seguridad de datos mediante la GUI

---

Puede utilizar la GUI del cliente de copia de seguridad y archivado para realizar copias de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios enteros.

### Acerca de esta tarea

---

Puede localizar los archivos de los que desea hacer copia de seguridad mediante la búsqueda o el filtrado. El filtrado muestra sólo los archivos que coinciden con los criterios de filtrado de la operación de copia de seguridad. Los archivos que no coinciden con los criterios de filtrado no se visualizan.

Para realizar una copia de seguridad desde la GUI, siga estos pasos:

### Procedimiento

---


1. Pulse Copia de seguridad en la ventana principal de la GUI. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios pulsando el signo más (+). Para visualizar archivos en una carpeta, pulse el icono Carpeta. Para buscar o filtrar los archivos, pulse en el icono de Buscar desde la barra de herramientas.
3. Pulse en las casillas de selección de los objetos de los que desea realizar una copia de seguridad.
4. Seleccione el tipo de copia de seguridad en menú desplegable:
  - a. Para efectuar una copia de seguridad incremental seleccione Incremental (completa).
  - b. Para efectuar una copia de seguridad incremental por fecha, seleccione Incremental (sólo por fecha).
  - c. Para efectuar una copia de seguridad selectiva, seleccione Hacer siempre copia de seguridad.
  - d. Para ejecutar una copia de seguridad incremental sin utilizar la base de datos de registro por diario, seleccione Incremental (sin diario). Si ha instalado el servicio de motor de diario y este está ejecutándose, de forma predeterminada el mandato Incremental realiza automáticamente una copia de seguridad basada en el diario en los sistemas de archivos seleccionados que el servicio de motor de diario está supervisando. Esta opción realiza una copia de seguridad incremental completa tradicional, en lugar de la copia de seguridad basada en el diario predeterminada.
5. Pulse en Copia de seguridad. La ventana Lista de tareas de copia de seguridad visualiza el estado de proceso de copia de seguridad. Cuando se completa el proceso, la ventana Informe de copia de seguridad visualiza los detalles de proceso.

### Resultados

---

A continuación se muestran algunos elementos a tener en cuenta al utilizar la GUI para hacer una copia de seguridad de los datos.

- IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión que se utiliza es una clase de gestión predeterminada seleccionada automáticamente o una clase de gestión que el usuario asigna al archivo utilizando la opción include en la lista de opciones de inclusión/exclusión. Seleccione Herramientas → Ver información de políticas en la GUI de cliente web o cliente de archivado y copia de seguridad para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para el nodo cliente. Seleccione Editar → Preferencias de cliente en la GUI de cliente web o cliente de archivado y copia de seguridad y seleccione el separador Inclusión/Exclusión en el editor de preferencias para visualizar la lista de inclusión/exclusión.
- Si desea modificar opciones de copia de seguridad específicas, pulse el botón Opciones. Cualquier opción que cambie será eficaz solo durante la sesión actual.
- Para realizar más copias de seguridad incrementales, abra el menú Acciones de la ventana principal de IBM Spectrum Protect y seleccione Copia de seguridad del dominio.

- La GUI del cliente web no puede examinar recursos de red para realizar una copia de seguridad. No se listan unidades compartidas si se expande la rama de Red. Es posible realizar una copia de seguridad de un recurso de red desde el cliente web a condición de que se procese el archivo entero. Para ello, se especifica el sistema de archivos utilizando la opción domain en dsm.opt. Por ejemplo, domain all-local \\server\share. Para completar la copia de seguridad, seleccione Copia de seguridad de dominio en el menú Acción. Esto procesa todos los sistemas de archivo que se especifican con la opción de dominio. Alternativamente, puede utilizar el cliente de GUI para realizar la copia de seguridad.
-  Sistemas operativos Windows Especificación de unidades en el dominio  
Al iniciar el cliente, el dominio predeterminado se establece en las unidades que especifica mediante la opción domain del archivo dsm.opt.

**Conceptos relacionados:**

Políticas de gestión de almacenamiento

**Tareas relacionadas:**

Restauración de datos mediante la GUI

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

 Sistemas operativos Windows

## Copia de seguridad de datos mediante la línea de mandatos

Puede utilizar los mandatos incremental o selective para realizar copias de seguridad. En la siguiente tabla se muestran ejemplos de utilización de estos mandatos para realizar diferentes tareas.

### Acerca de esta tarea

Tabla 1. Ejemplos de copia de seguridad desde la línea de mandatos

Tarea	Mandato	Consideraciones
<i>Copias de seguridad incrementales</i>		
Realizar una copia de seguridad incremental del dominio del cliente.	dsmc incremental	Consulte el apartado Incremental para obtener más información sobre el mandato incremental. Consulte el apartado Copia de seguridad incremental completa y parcial para obtener información detallada acerca de las copias de seguridad incrementales.
Realizar una copia de seguridad de las unidades g: y h:, además de las unidades c:, d: y e: definidas en el dominio del cliente.	dsmc incremental -domain="g: h:"	Consulte el apartado Domain para obtener más información sobre la opción domain.
Realizar una copia de seguridad de todos los volúmenes locales definidos en el dominio del cliente <i>salvo</i> la unidad c: y el dominio systemobject.	dsmc incremental -domain="all-local -c: -systemobject"	No es posible utilizar el operador (-) delante de la palabra clave de dominio all-local. Para obtener más información, consulte el apartado Domain. En clientes Windows también puede excluir el estado del sistema del proceso de copia de seguridad de este modo.
Realizar una copia de seguridad de todos los volúmenes locales definidos en el dominio del cliente <i>salvo</i> la unidad c: y el dominio systemstate.	dsmc incremental -domain="all-local -c: -systemstate"	No es posible utilizar el operador (-) delante de la palabra clave de dominio all-local. Para obtener más información, consulte el apartado Domain.
Realizar una copia de seguridad <i>sólo</i> de las unidades g: y h:.	dsmc incremental g: h:	Ninguna
Realizar una copia de seguridad de todos los archivos del directorio c:\Accounting y de todos sus subdirectorios.	dsmc incremental c:\Accounting\* -sub=yes	Consulte el apartado Subdir para obtener más información sobre la opción subdir.

Tarea	Mandato	Consideraciones
Suponiendo que ha iniciado una instantánea de la unidad C: y ha montado la instantánea como volumen lógico \\florence\c\$\snapshots\snapshot.0, ejecute una copia de seguridad incremental de todos los archivos y directorios situados debajo de la instantánea local y gestiónelos en el servidor de IBM Spectrum Protect, debajo del nombre de espacio de archivos C:.	dsmc incremental c: -snapshot=\\florence\c\$\snapshots\snapshot.0	Para obtener más información, consulte el apartado Snapshotroot.
<i>Copia de seguridad incremental por fecha</i>		
Realizar una copia de seguridad incremental por fecha del dominio de cliente predeterminado.	dsmc incremental -incrbydate	Utilice la opción incrbydate con el mandato incremental para hacer una copia de seguridad de los archivos nuevos y modificados con una fecha de modificación posterior a la de la última copia de seguridad incremental almacenada en el servidor. Consulte el apartado Incrbydate para obtener más información sobre la opción incrbydate.
<i>Copias de seguridad selectivas</i>		
Realizar una copia de seguridad de todos los archivos del directorio d:\proj.	dsmc selective d:\proj\	Utilice el mandato selective para efectuar copias de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios vacíos y sus atributos, independientemente de si se realizó una copia de seguridad de dichos archivos o directorios durante la última copia de seguridad incremental y sin que afecte al último recuento de copias de seguridad incrementales del servidor de copia de seguridad. Puede utilizar caracteres comodín para realizar una copia de seguridad de varios archivos a la vez. Consulte el apartado Selective para obtener más información sobre el mandato selective.
Realizar una copia de seguridad del directorio d:\proj y de todos sus subdirectorios.	dsmc selective d:\proj\ -subdir=yes	Consulte el apartado Subdir para obtener más información sobre la opción subdir.
Realizar una copia de seguridad de los archivos d:\h1.doc y d:\test.doc.	dsmc selective d:\h1.doc d:\test.doc	Puede especificar tantas especificaciones de archivo como recursos disponibles existan o como límites del sistema operativo estén permitidos. Separe las especificaciones de los archivos con un espacio en blanco. También puede utilizar la opción filelist para procesar una lista de archivos. El cliente de copia de seguridad y archivado abre el archivo que especifique con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico. Consulte Filelist para obtener más información.
Realizar una copia de seguridad de una lista de archivos en la unidad c:.	dsmc selective -filelist=c:\filelist.txt	Utilice la opción filelist para procesar una lista de archivos. Para obtener más información, consulte el apartado Filelist.

Tarea	Mandato	Consideraciones
Suponiendo que ha iniciado una instantánea de la unidad C: y ha montado la instantánea como volumen lógico \\florence\c\$\snapshots\snapshot.0, ejecute una copia de seguridad selectiva de c:\dir1\sub1 de la instantánea local y gestiónela en el servidor de IBM Spectrum Protect, debajo del nombre de espacio de archivos C:.	dsmc selective c:\dir1\sub1\* - subdir=yes snapshot=\\florence\c\$\snapshots\ snapshot.0	Para obtener más información, consulte el apartado Snapshotroot.

**Conceptos relacionados:**

Copia de seguridad(Windows): Consideraciones adicionales

Utilización de los mandatos

 Sistemas operativos Windows

## Supresión de datos de copia de seguridad

Si el administrador le ha otorgado autorización, puede suprimir copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos.

### Acerca de esta tarea

Por ejemplo, es posible que tenga que suprimir los datos confidenciales de los que se realizó una copia de seguridad (voluntaria o involuntariamente), que ahora tienen que ser eliminados del servidor. También es posible que necesite suprimir los archivos de los que se realizó una copia de seguridad, y en los cuales se encontraron más tarde virus. Para determinar si tiene la autorización necesaria para suprimir las copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos, seleccione **Archivo** → **Información de conexión** en la GUI del cliente de copia de seguridad y archivado o en el menú principal del cliente web. El estado de la autorización se proporciona en el campo Suprimir archivos de copia de seguridad.

**Importante:** si suprime archivos de copia de seguridad, **no podrá restaurarlos**. Antes de suprimirlos, verifique que los archivos de copia de seguridad ya no sean necesarios. IBM Spectrum Protect le solicitará si desea continuar con la operación de supresión. Si especifica **Sí**, los archivos de copia de seguridad especificados se suprimirán inmediatamente y se eliminarán del almacenamiento del servidor de IBM Spectrum Protect.

Para suprimir copias de seguridad mediante la GUI de IBM Spectrum Protect o el cliente web:

### Procedimiento

1. Seleccione **Suprimir datos de copia de seguridad** en el menú **Herramientas**. Aparecerá la ventana Supresión de copia de seguridad.
2. Expanda el árbol de directorios pulsando en el signo más (+) o en el icono de carpeta situado junto al objeto que desea expandir.
3. Seleccione un elemento de la lista desplegable que hay junto a la parte superior de la ventana **Supresión de copia de seguridad** para especificar el tipo de supresión de copia de seguridad que desea realizar. Puede suprimir las versiones de copia de seguridad activas, las versiones de copia de seguridad inactivas o todos los objetos que haya seleccionado en el árbol. Un directorio solo se suprimirá si selecciona **Suprimir todos los objetos**.

### Resultados

Para suprimir copias de seguridad mediante el cliente de línea de mandatos de IBM Spectrum Protect, utilice el mandato delete backup.

**Referencia relacionada:**

Delete Backup

## Cuándo realizar copias de seguridad y cuándo archivar copias

Cuando el cliente de copia de seguridad/archivado realiza una copia de seguridad o una copia archivada de un archivo, envía una copia de este archivo y sus atributos asociados al servidor. Sin embargo, las operaciones de copia de seguridad y archivado tienen objetivos distintos.

Utilice las copias de seguridad como protección en caso de que los archivos se dañen de forma súbita y utilice las copias archivadas para conservar las versiones de los archivos de forma más permanente.

Los datos de copia de seguridad se gestionan por versiones mediante la política predeterminada basada en reglas. Utilizando estas reglas, el administrador de IBM Spectrum Protect puede controlar los procesos siguientes:






- El número de versiones que se mantienen en el servidor de IBM Spectrum Protect
- El número de días que se conserva cada copia adicional de la copia de seguridad
- Lo que ocurre con las versiones de copia de seguridad cuando se suprime el archivo del sistema cliente

Cada copia del archivo se almacena en el servidor se considera una versión independiente y única del archivo.






El archivado es un mecanismo potente y flexible para guardar datos a largo plazo. Los datos archivados, denominados copias de archivado, se guardan durante un número determinado de días. La función de archivado no tiene un concepto o soporte para las versiones. El usuario o el administrador son los responsables de determinar qué archivos se agregan a las copias archivadas.

Consejo: Si se archiva un archivo varias veces mediante la misma descripción de archivo, se añade una copia nueva del archivo al archivado cada vez que se ejecuta la operación. Para simplificar la operación de recuperación, guarde solo una copia de un archivo en cada archivado.

Las copias de seguridad se protegen contra el daño de los archivos o la pérdida que puede ocurrir a través de la supresión accidental, corrupción o anomalías en el disco. El servidor conserva una o varias versiones de copia de seguridad de cada archivo del que se ha realizado una copia de seguridad. Las versiones antiguas se eliminan a medida que se van creando versiones nuevas. El administrador se encarga de establecer el número de versiones de copia de seguridad que el servidor debe conservar.








 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Las copias archivadas se guardan para su almacenamiento a largo plazo. Los administradores pueden limitar el período de tiempo que estas copias deben conservarse. El servidor puede almacenar un número ilimitado de versiones de copias archivadas de un archivo. Las copias de archivado son útiles si desea volver a una versión particular de sus archivos, o si desea suprimir un archivo desde la estación de trabajo y recuperarla más tarde si fuese necesario. Por ejemplo, es posible que deba guardar hojas de cálculo para los impuestos, pero, puesto que no las utiliza, puede que no desee dejarlas en su estación de trabajo.


#### Conceptos relacionados:





 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivar y recuperar datos (UNIX y Linux)  
Restauración de datos desde un conjunto de copias de seguridad  
 Sistemas operativos Windows

## Consideraciones previas a la copia de seguridad (Windows)

Diversos factores en el sistema o el entorno pueden afectar la manera en que el cliente de archivado y copia de seguridad procesa los datos. Revise estas consideraciones antes de realizar la copia de seguridad de los datos.

-  Sistemas operativos Windows Traspaso de datos sin LAN  
El traspaso de datos fuera de la LAN desplaza el traspaso de datos de cliente desde la red de comunicaciones hasta una red de área de almacenamiento (SAN). De esta forma se reduce la carga en el servidor de IBM Spectrum Protect.
-  Sistemas operativos Windows Espacios de archivos Unicode (Windows)  
El cliente Windows está activado para Unicode. Sin embargo, las versiones del cliente anteriores a la versión 4.2 no estaban activadas para Unicode.
-  Sistemas operativos Windows Copias de seguridad incrementales en sistemas con restricción de memoria  
El rendimiento de la copia de seguridad incremental se ve afectado negativamente si la cantidad de memoria disponible en el sistema es baja antes de iniciarse la copia de seguridad.
-  Sistemas operativos Windows Copias de seguridad incrementales en sistemas con un gran número de archivos  
El cliente puede utilizar grandes cantidades de memoria para ejecutar las operaciones de copia de seguridad incremental, en especial en los sistemas de archivos que contienen gran cantidad de archivos.
-  Sistemas operativos Windows Proceso de control con una lista de inclusión-exclusión  
Puede que en el sistema existan archivos cuya copia de seguridad no desea realizar. Pueden ser archivos del sistema operativo o archivos de aplicación, que se pueden recuperar fácilmente volviendo a instalar el programa, o cualquier otro archivo que se pueda volver a crear con facilidad.
-  Sistemas operativos Windows Cifrado de datos durante una operación de copia de seguridad o archivado  
Para un cifrado lo más seguro posible, utilice el estándar de cifrado avanzado (AES) de 256 bits con la opción `encryptiontype`. Actualmente, el valor predeterminado es el cifrado estándar de cifrado avanzado de 128 bits.
-  Sistemas operativos Windows Tamaño máximo de archivo para operaciones  
Los tamaños de archivo máximos para la copia de seguridad y restauración y las operaciones de archivado y recuperación dependen del sistema de archivos de Windows que se utiliza.

- 
 Sistemas operativos Windows Cómo gestiona el cliente los nombres de usuario y de grupo largos  
 El cliente de archivado y copia de seguridad puede gestionar sin problemas nombres de usuario y de grupo con hasta 64 caracteres. Sin embargo, los nombres de más de 64 caracteres requieren un tratamiento especial.





 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 Sistemas operativos Oracle Solaris
 
 Sistemas operativos Windows

## traspaso de datos sin LAN



---





El traspaso de datos fuera de la LAN desplaza el traspaso de datos de cliente desde la red de comunicaciones hasta una red de área de almacenamiento (SAN). De esta forma se reduce la carga en el servidor de IBM Spectrum Protect.

La SAN proporciona una vía de acceso que permite realizar una copia de seguridad, restaurar, archivar y recuperar datos en un dispositivo de almacenamiento conectado a la SAN y desde el mismo. Los datos del cliente se traspasan por la SAN hasta llegar al dispositivo de almacenamiento utilizando el agente de almacenamiento de IBM Spectrum Protect. El agente de almacenamiento debe estar instalado en el mismo sistema que el cliente.


 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 Sistemas operativos Oracle Solaris Los clientes de AIX, Linux y Solaris admiten el movimiento de datos sin LAN.


 Sistemas operativos Windows Todos los clientes Windows aceptan el traspaso de datos fuera de red de área local.

- 
 Sistemas operativos Windows Requisitos previos del soporte para fuera de la LAN  
 Para habilitar el soporte sin LAN, debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.
- 
 Sistemas operativos Windows Opciones de traspaso de datos fuera de la LAN  
 Para habilitar el traspaso de datos fuera de la LAN, puede utilizar varias opciones del cliente. Antes debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.


 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 Sistemas operativos Oracle Solaris
 
 Sistemas operativos Windows





## Requisitos previos del soporte para fuera de la LAN

---

Para habilitar el soporte sin LAN, debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

IBM Spectrum Protect for SAN es un producto separado.

Para obtener más información sobre cómo instalar y configurar el agente de almacenamiento, consulte la documentación de IBM Spectrum Protect for SAN.


 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 Sistemas operativos Oracle Solaris
 
 Sistemas operativos Windows

## Opciones de traspaso de datos fuera de la LAN

---

Para habilitar el traspaso de datos fuera de la LAN, puede utilizar varias opciones del cliente. Antes debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

Utilice las opciones siguientes para habilitar el traspaso de datos fuera de la LAN:

*enablelanfree*

Especifica si se activa una vía de acceso disponible fuera de la LAN para un dispositivo de almacenamiento conectado a SAN.

*lanfreecommmethod*

Especifica un protocolo de comunicaciones entre el cliente y el agente de almacenamiento.

*lanfreshmport*

Especifica el número exclusivo que el cliente y el agente de almacenamiento utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.

*lanfreetcport*

Especifica el número de puerto TCP/IP en el que está conectado el agente de almacenamiento.

*lanfreetcpserveraddress*

Especifica la dirección TCP/IP del agente de almacenamiento.

### Referencia relacionada:

Enablelanfree

Lanfreecommmethod

Lanfreshmport

## Espacios de archivos Unicode (Windows)

---

El cliente Windows está activado para Unicode. Sin embargo, las versiones del cliente anteriores a la versión 4.2 no estaban activadas para Unicode.

Si hace la copia de seguridad de un sistema en el que una vez se utilizó una versión de cliente anterior a la versión 4.2 y los espacios de archivos todavía no se han migrado a Unicode, es necesario planificar la migración de los espacios de archivos a Unicode. Esto implica cambiar el nombre de los espacios de archivos del servidor y crear nuevos espacios de archivos activados para Unicode en el servidor mediante la opción `autofsrename`.

### Conceptos relacionados:

Consideraciones sobre los clientes habilitados para Unicode

### Referencia relacionada:

`Autofsrename`

`Detail`

`Query Filespace`

`Restore`

`Retrieve`

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 Sistemas operativos Windows

## Copias de seguridad incrementales en sistemas con restricción de memoria

---

El rendimiento de la copia de seguridad incremental se ve afectado negativamente si la cantidad de memoria disponible en el sistema es baja antes de iniciarse la copia de seguridad.

Si el sistema tiene restricciones de memoria, especifique la opción `memoryefficientbackup yes` en el archivo de opciones de cliente. Esta opción da lugar a que el cliente de copia de seguridad y archivado sólo procese un único directorio cada vez, lo que reduce el consumo de memoria pero incrementa el tiempo necesario para la realización de la copia de seguridad. Cuando especifica `yes`, el cliente sólo analiza un único directorio cada vez para la realización de la copia de seguridad. Si el rendimiento sigue siendo bajo, compruebe los valores del búfer de comunicación y el enlace de comunicación existente entre el sistema y el servidor de IBM Spectrum Protect. Si el sistema no tiene restricciones de memoria, el establecimiento de la opción `memoryefficientbackup` en `yes` afectará negativamente al rendimiento de la copia de seguridad.

### Referencia relacionada:

`Memoryefficientbackup`

## Copias de seguridad incrementales en sistemas con un gran número de archivos

---

El cliente puede utilizar grandes cantidades de memoria para ejecutar las operaciones de copia de seguridad incremental, en especial en los sistemas de archivos que contienen gran cantidad de archivos.

El término *memoria* tal como se utiliza aquí hace referencia a la memoria direccionable que está disponible para el proceso del cliente. La memoria direccionable es una combinación de la RAM física y de la memoria virtual.

Como término medio, el cliente utiliza aproximadamente 300 bytes de memoria para cada objeto (archivo o directorio). De esta forma, para un sistema de archivos que tenga un millón de archivos y directorios, el cliente necesita, como promedio, 300 MB de memoria aproximadamente. La cantidad exacta de memoria que se utiliza para cada objeto varía en función de la longitud de la vía de acceso del objeto y de la longitud del nombre o de la profundidad de anidamiento de los directorios. El número de bytes de datos no es un factor importante para la determinación del requisito de memoria del cliente de copia de seguridad.







El número máximo de archivos puede determinarse dividiendo la cantidad máxima de memoria virtual disponible para un proceso entre la cantidad media de memoria necesaria para cada objeto.

El requisito de memoria total puede reducirse aplicando cualquiera de los métodos siguientes:

- Utilice la opción del cliente de `memoryefficientbackup diskcachemethod`. Esta opción reduce la utilización de memoria a un mínimo, lo cual se obtiene a expensas del rendimiento y de un incremento significativo del espacio de disco necesario para la



realización de la copia de seguridad. Los datos de descripción de archivo del servidor se almacenan en una base de datos temporal que reside en el disco, no en la memoria. A medida que se exploran los directorios de la estación de trabajo, se consulta la base de datos para determinar si ha de realizarse una operación de copia de seguridad, de actualización o de caducidad para cada objeto. Cuando se ha completado la copia de seguridad, el archivo de base de datos se suprime.

- Utilice la opción del cliente `memoryefficientbackup yes`. El promedio de memoria que utiliza el cliente equivaldrá entonces a 300 bytes multiplicados por el número de directorios más 300 bytes por cada archivo del directorio que está procesándose. Para los sistemas de archivos con números grandes (millones) de directorios, puede que el cliente no pueda alojar suficiente memoria para llevar a cabo la copia de seguridad incremental con `memoryefficientbackup yes`.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los clientes UNIX y los clientes Linux pueden utilizar la opción de cliente `virtualmountpoint` para definir varios puntos de montaje virtuales dentro de un único sistema de archivos, lo que permitirá que el cliente pueda realizar la copia de seguridad de cada uno de estos independientemente.
- Si la opción de cliente `resourceutilization` se establece en un valor mayor que 4 y se desea realizar la copia de seguridad de varios sistemas de archivos, la reducción del valor de la opción `resourceutilization` a 4 o un valor inferior limita el proceso de la copia de seguridad incremental a un único sistema de archivos cada vez. Este ajuste reduce los requisitos de memoria. Si, por razones de rendimiento, debe realizarse la copia de seguridad de varios sistemas de archivos en paralelo, y los requisitos de memoria combinados exceden los límites del proceso, pueden utilizarse varias instancias del cliente de copia de seguridad para realizar la copia de seguridad de varios sistemas de archivos en paralelo. Por ejemplo, si desea realizar la copia de seguridad de dos sistemas de archivos al mismo tiempo, pero los requisitos de memoria de éstos exceden los límites de un único proceso, inicie una instancia del cliente para que realice la copia de seguridad de uno de los sistemas de archivos e inicie una segunda instancia del cliente para que realice la copia de seguridad del otro sistema de archivos.
- Utilice la opción de cliente `- incrbydate` para realizar una copia de seguridad "incremental por fecha".
- Utilice la opción `exclude.dir` del cliente para impedir que el cliente recorra los directorios y realice la copia de seguridad de los directorios cuya copia de seguridad no es necesario realizar.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Excepto para Mac OS X, utilice la función de copia de seguridad de imágenes del cliente para realizar la copia de seguridad del volumen completo. Es posible que una copia de seguridad de imagen que utilice menos recursos del sistema y ejecute más rápidamente que la copia de seguridad incremental de algunos sistemas de archivos con un gran número de pequeños archivos.
- Reduzca el número de archivos por sistema de archivos distribuyendo los datos entre varios sistemas de archivos.

#### Referencia relacionada:

Snapdiff

Opciones `exclude`

`Incrbydate`

`Memoryefficientbackup`

`Resourceutilization`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `Virtualmountpoint`

 Sistemas operativos Windows

## Proceso de control con una lista de inclusión-exclusión

---

Puede que en el sistema existan archivos cuya copia de seguridad no desea realizar. Pueden ser archivos del sistema operativo o archivos de aplicación, que se pueden recuperar fácilmente volviendo a instalar el programa, o cualquier otro archivo que se pueda volver a crear con facilidad.

Utilice las opciones `include` y `exclude` en el archivo de opciones del cliente (`dsm.opt`) para definir qué archivos deben incluirse o excluirse del proceso de copia de seguridad incremental o selectiva. Un archivo es elegible para la copia de seguridad salvo que se excluya por una opción `exclude`. No es necesario utilizar una opción `include` para incluir archivos específicos para la copia de seguridad, a menos que estos archivos estén en un directorio que contenga otros archivos que desea excluir.

Puede que la lista de inclusión/exclusión contenga elementos que especifica el servidor. Para ver el contenido de su lista de inclusión/exclusión, utilice el mandato `query inclexcl`.

IBM Spectrum Protect utiliza *clases de gestión* para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión es una clase de gestión predeterminada que selecciona personalmente o bien una clase de gestión que asigna al archivo mediante la utilización de la opción `include` en la lista de inclusión/exclusión. Si asigna una clase de gestión, ésta deberá contener un grupo de copia de seguridad para el archivo cuya copia de seguridad desea realizarse.

También puede añadir sentencias de inclusión/exclusión en el árbol de directorios de la GUI del cliente de copia de seguridad y archivado. Puede utilizar el mandato `preview` para ver los efectos resultantes de la lista de inclusión/exclusión sin tener que ejecutar una operación de copia de seguridad real.


#### Tareas relacionadas:

Creación de una lista de inclusión/exclusión

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

**Referencia relacionada:**

Previsualizar copia de seguridad

 Sistemas operativos Windows

## Cifrado de datos durante una operación de copia de seguridad o archivado

Para un cifrado lo más seguro posible, utilice el estándar de cifrado avanzado (AES) de 256 bits con la opción `encrypttype`. Actualmente, el valor predeterminado es el cifrado estándar de cifrado avanzado de 128 bits.

Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.

Atención: Si la contraseña de cifrado no se ha guardado en el registro de Windows, y has olvidado la contraseña, los datos no se pueden recuperar.

El cifrado solo puede habilitarse en el cliente de copia de seguridad/archivado mediante la opción `include.encrypt`. Si no se utiliza ninguna sentencia `include.encrypt`, no se realizará el cifrado.

El cifrado no es compatible con las copias de seguridad de la máquina virtual de VMWare que utilizan los modos de copia virtual incremental para siempre (`MODE=IFIncremental` y `MODE=IFFull`). Si el cliente se configura para el cifrado, no se puede utilizar la copia de seguridad siempre incremental.

Para cifrar datos de archivos, debe seleccionar una contraseña de clave de cifrado, que el cliente utiliza para generar la clave de cifrado para cifrar y descifrar los datos de archivos. Puede especificar si la contraseña de clave de cifrado debe guardarse en el registro de Windows mediante la opción `encryptkey`.

El cifrado del cliente de IBM Spectrum Protect permite especificar un valor que tenga un máximo de 63 caracteres de longitud. Esta contraseña de cifrado debe confirmarse al cifrar el archivo para la copia de seguridad y también debe especificarse cuando se realizan restauraciones de archivos cifrados.

Al restaurar un archivo cifrado, se le solicitará la contraseña de clave para descifrar el archivo en los siguientes casos:

- Si la opción `encryptkey` se establece en `Prompt`.
- Si la clave proporcionada por el usuario no coincide.
- Si la opción `encryptkey` se establece en `Save` y la contraseña de clave almacenada localmente no coincide con el archivo.

**Conceptos relacionados:**

Copia de seguridad(Windows): Consideraciones adicionales

**Referencia relacionada:**

`Encrypttype`

`Encryptkey`

Opciones `exclude`

Opciones `include`







 Sistemas operativos Windows


## Tamaño máximo de archivo para operaciones

Los tamaños de archivo máximos para la copia de seguridad y restauración y las operaciones de archivado y recuperación dependen del sistema de archivos de Windows que se utiliza.

La tabla siguiente muestra el tamaño máximo de archivo, en bytes, para las copias de seguridad, restauración y recuperación de datos.

Tabla 1. Tamaño máximo de archivo

Sistema de archivos	Tamaño de archivo máximo (en bytes)
 Sistemas operativos Windows FAT16	 Sistemas operativos Windows 2.147.483.647 (2 GB)
 Sistemas operativos Windows FAT32	 Sistemas operativos Windows 4.294.967.295 (4 GB)
 Sistemas operativos Windows NTFS y ReFS	 Sistemas operativos Windows 17.592.185.978.880 (16 TB-64 K)

 Sistemas operativos Windows

## Cómo gestiona el cliente los nombres de usuario y de grupo largos





El cliente de archivado y copia de seguridad puede gestionar sin problemas nombres de usuario y de grupo con hasta 64 caracteres. Sin embargo, los nombres de más de 64 caracteres requieren un tratamiento especial.

Restricción: No exceda el límite de 64 caracteres para los nombres de usuario y de grupo. El cliente acorta el nombre para que se ajuste a este límite utilizando el siguiente algoritmo: utilizar los 53 primeros caracteres y añadir una barra inclinada (/) para, a continuación, utilizar el ID numérico como una serie de caracteres.

Se anota un mensaje de error que contiene el nombre largo y la serie de caracteres acortada resultante. Para ejecutar la mayoría de las funciones no será necesario que conozca el nombre abreviado. Las excepciones son:



































- El mandato set access
- La opción fromowner
- Las opciones users y groups (autorización)

En cada uno de estos casos, cuando tenga que especificar un nombre, deberá buscar el mensaje de error que contiene la transformación o bien construir el nombre utilizando la regla que se describe aquí.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris





## Consideraciones previas a la copia de seguridad (UNIX y Linux)

Diversos factores en el sistema o el entorno pueden afectar la manera en que el cliente de archivado y copia de seguridad procesa los datos. Revise estas consideraciones antes de realizar la copia de seguridad de los datos.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Traspaso de datos sin LAN  
El traspaso de datos fuera de la LAN desplaza el traspaso de datos de cliente desde la red de comunicaciones hasta una red de área de almacenamiento (SAN). De esta forma se reduce la carga en el servidor de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copias de seguridad incrementales en sistemas con restricción de memoria  
El rendimiento de la copia de seguridad incremental se ve afectado negativamente si la cantidad de memoria disponible en el sistema es baja antes de iniciarse la copia de seguridad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copias de seguridad incrementales en sistemas con un gran número de archivos  
El cliente puede utilizar grandes cantidades de memoria para ejecutar las operaciones de copia de seguridad incremental, en especial en los sistemas de archivos que contienen gran cantidad de archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Opciones de inclusión/exclusión para controlar el proceso  
Puede que tenga archivos en los sistemas de archivos cuya copia de seguridad no desee realizar. Estos archivos podrían ser archivos del núcleo, cachés locales de los sistemas de archivos de red, archivos del sistema operativo o de aplicaciones que podrían recuperarse fácilmente si se volviera a instalar el programa o cualquier otro archivo que pueda volver a crearse con facilidad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Cifrado de datos durante una operación de copia de seguridad o archivado  
La manera de garantizar la seguridad de datos consiste en cifrar los datos. Utilice el cifrado de datos para proteger los datos durante una operación de copia de seguridad o archivado. El cifrado AES (Advanced Encryption Standard - Estándar de cifrado avanzado) de 128 bits es la opción de cifrado predeterminada. Para obtener el nivel más alto de cifrado de datos, utilice el cifrado de datos AES (Estándar de cifrado avanzado) de 256 bits especificando la opción encryptiontype.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Soporte para sistemas de archivos y ACL  
Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. Los clientes UNIX y Linux pasan por alto los sistemas de archivos especiales y su contenido.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Tamaño máximo de archivo para operaciones  
El tamaño máximo de archivo depende del tipo de sistema de archivos. El cliente de copia de seguridad y archivado no comprueba ningún límite de tamaño de archivo durante las operaciones de copia de seguridad, archivado, restauración o recuperación
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows  
Nombres de usuario y de grupo largos  
El cliente de archivado y copia de seguridad puede gestionar sin problemas nombres de usuario y de grupo con hasta 64 caracteres. Sin embargo, los nombres de más de 64 caracteres requieren un manejo especial por parte de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  
Nombres de volumen en Mac OS X  
El cliente de copia de seguridad y archivado hace copias de seguridad de los volúmenes en función de su nombre de punto de montaje UNIX.
-  sistemas operativos Mac OS X  
Habilitación de Unicode para Mac OS X  
El cliente Mac OS X está habilitado para Unicode. Los clientes nuevos que almacenen datos en el servidor por primera vez no

requieren una configuración especial.

-  sistemas operativos Mac OS X Disco de copia de seguridad Time Machine de Mac OS X  
Time Machine es la aplicación de copia de seguridad disponible con Mac OS X.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## traspaso de datos sin LAN







---





El traspaso de datos fuera de la LAN desplaza el traspaso de datos de cliente desde la red de comunicaciones hasta una red de área de almacenamiento (SAN). De esta forma se reduce la carga en el servidor de IBM Spectrum Protect.

La SAN proporciona una vía de acceso que permite realizar una copia de seguridad, restaurar, archivar y recuperar datos en un dispositivo de almacenamiento conectado a la SAN y desde el mismo. Los datos del cliente se traspasan por la SAN hasta llegar al dispositivo de almacenamiento utilizando el agente de almacenamiento de IBM Spectrum Protect. El agente de almacenamiento debe estar instalado en el mismo sistema que el cliente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los clientes de AIX, Linux y Solaris admiten el movimiento de datos sin LAN.

 Sistemas operativos Windows Todos los clientes Windows aceptan el traspaso de datos fuera de red de área local.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Requisitos previos del soporte para fuera de la LAN  
Para habilitar el soporte sin LAN, debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Opciones de traspaso de datos fuera de la LAN  
Para habilitar el traspaso de datos fuera de la LAN, puede utilizar varias opciones del cliente. Antes debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows





## Requisitos previos del soporte para fuera de la LAN

---

Para habilitar el soporte sin LAN, debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

IBM Spectrum Protect for SAN es un producto separado.

Para obtener más información sobre cómo instalar y configurar el agente de almacenamiento, consulte la documentación de IBM Spectrum Protect for SAN.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Opciones de traspaso de datos fuera de la LAN

---

Para habilitar el traspaso de datos fuera de la LAN, puede utilizar varias opciones del cliente. Antes debe instalar y configurar el agente de almacenamiento de IBM Spectrum Protect for SAN en la estación de trabajo cliente.

Utilice las opciones siguientes para habilitar el traspaso de datos fuera de la LAN:

*enablelanfree*

Especifica si se activa una vía de acceso disponible fuera de la LAN para un dispositivo de almacenamiento conectado a SAN.

*lanfreecommmethod*

Especifica un protocolo de comunicaciones entre el cliente y el agente de almacenamiento.

*lanfreeshmport*

Especifica el número exclusivo que el cliente y el agente de almacenamiento utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.

*lanfreetcport*

Especifica el número de puerto TCP/IP en el que está conectado el agente de almacenamiento.

*lanfreetcserveraddress*

Especifica la dirección TCP/IP del agente de almacenamiento.

### Referencia relacionada:

Enablelanfree

Lanfreecommmethod  
Lanfreeshmport  
Lanfreessl  
Lanfreetcppport  
Lanfreetcpsrserveraddress

 Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

## Copias de seguridad incrementales en sistemas con restricción de memoria

El rendimiento de la copia de seguridad incremental se ve afectado negativamente si la cantidad de memoria disponible en el sistema es baja antes de iniciarse la copia de seguridad.

Si el sistema tiene restricciones de memoria, especifique la opción `memoryefficientbackup yes` en el archivo de opciones de cliente. Esta opción da lugar a que el cliente de copia de seguridad y archivado sólo procese un único directorio cada vez, lo que reduce el consumo de memoria pero incrementa el tiempo necesario para la realización de la copia de seguridad. Cuando especifica `yes`, el cliente sólo analiza un único directorio cada vez para la realización de la copia de seguridad. Si el rendimiento sigue siendo bajo, compruebe los valores del búfer de comunicación y el enlace de comunicación existente entre el sistema y el servidor de IBM Spectrum Protect. Si el sistema no tiene restricciones de memoria, el establecimiento de la opción `memoryefficientbackup` en `yes` afectará negativamente al rendimiento de la copia de seguridad.

### Referencia relacionada:

`Memoryefficientbackup`

## Copias de seguridad incrementales en sistemas con un gran número de archivos




El cliente puede utilizar grandes cantidades de memoria para ejecutar las operaciones de copia de seguridad incremental, en especial en los sistemas de archivos que contienen gran cantidad de archivos.

El término *memoria* tal como se utiliza aquí hace referencia a la memoria direccionable que está disponible para el proceso del cliente. La memoria direccionable es una combinación de la RAM física y de la memoria virtual.




Como término medio, el cliente utiliza aproximadamente 300 bytes de memoria para cada objeto (archivo o directorio). De esta forma, para un sistema de archivos que tenga un millón de archivos y directorios, el cliente necesita, como promedio, 300 MB de memoria aproximadamente. La cantidad exacta de memoria que se utiliza para cada objeto varía en función de la longitud de la vía de acceso del objeto y de la longitud del nombre o de la profundidad de anidamiento de los directorios. El número de bytes de datos no es un factor importante para la determinación del requisito de memoria del cliente de copia de seguridad.

El número máximo de archivos puede determinarse dividiendo la cantidad máxima de memoria virtual disponible para un proceso entre la cantidad media de memoria necesaria para cada objeto.

El requisito de memoria total puede reducirse aplicando cualquiera de los métodos siguientes:

- Utilice la opción del cliente de `memoryefficientbackup diskcachemethod`. Esta opción reduce la utilización de memoria a un mínimo, lo cual se obtiene a expensas del rendimiento y de un incremento significativo del espacio de disco necesario para la realización de la copia de seguridad. Los datos de descripción de archivo del servidor se almacenan en una base de datos temporal que reside en el disco, no en la memoria. A medida que se exploran los directorios de la estación de trabajo, se consulta la base de datos para determinar si ha de realizarse una operación de copia de seguridad, de actualización o de caducidad para cada objeto. Cuando se ha completado la copia de seguridad, el archivo de base de datos se suprime.
- Utilice la opción del cliente `memoryefficientbackup yes`. El promedio de memoria que utiliza el cliente equivaldrá entonces a 300 bytes multiplicados por el número de directorios más 300 bytes por cada archivo del directorio que está procesándose. Para los sistemas de archivos con números grandes (millones) de directorios, puede que el cliente no pueda alojar suficiente memoria para llevar a cabo la copia de seguridad incremental con `memoryefficientbackup yes`.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los clientes UNIX y los clientes Linux pueden utilizar la opción de cliente `virtualmountpoint` para definir varios puntos de montaje virtuales dentro de un único sistema de archivos, lo que permitirá que el cliente pueda realizar la copia de seguridad de cada uno de estos independientemente.
- Si la opción de cliente `resourceutilization` se establece en un valor mayor que 4 y se desea realizar la copia de seguridad de varios sistemas de archivos, la reducción del valor de la opción `resourceutilization` a 4 o un valor inferior limita el proceso de la copia de seguridad incremental a un único sistema de archivos cada vez. Este ajuste reduce los requisitos de memoria. Si, por razones de rendimiento, debe realizarse la copia de seguridad de varios sistemas de archivos en paralelo, y los requisitos de memoria combinados exceden los límites del proceso, pueden utilizarse varias instancias del cliente de copia de seguridad para realizar la copia de seguridad de varios sistemas de archivos en paralelo. Por ejemplo, si desea realizar la copia de seguridad de dos

sistemas de archivos al mismo tiempo, pero los requisitos de memoria de éstos exceden los límites de un único proceso, inicie una instancia del cliente para que realice la copia de seguridad de uno de los sistemas de archivos e inicie una segunda instancia del cliente para que realice la copia de seguridad del otro sistema de archivos.

- Utilice la opción de cliente - `incrbydate` para realizar una copia de seguridad "incremental por fecha".
- Utilice la opción `exclude.dir` del cliente para impedir que el cliente recorra los directorios y realice la copia de seguridad de los directorios cuya copia de seguridad no es necesario realizar.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Excepto para Mac OS X, utilice la función de copia de seguridad de imágenes del cliente para realizar la copia de seguridad del volumen completo. Es posible que una copia de seguridad de imagen que utilice menos recursos del sistema y ejecute más rápidamente que la copia de seguridad incremental de algunos sistemas de archivos con un gran número de pequeños archivos.
- Reduzca el número de archivos por sistema de archivos distribuyendo los datos entre varios sistemas de archivos.

#### Referencia relacionada:

`Snapdiff`

Opciones `exclude`

`Incrbydate`

`Memoryefficientbackup`

`Resourceutilization`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `Virtualmountpoint`

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Opciones de inclusión/exclusión para controlar el proceso

Puede que tenga archivos en los sistemas de archivos cuya copia de seguridad no desee realizar. Estos archivos podrían ser archivos del núcleo, cachés locales de los sistemas de archivos de red, archivos del sistema operativo o de aplicaciones que podrían recuperarse fácilmente si se volviera a instalar el programa o cualquier otro archivo que pueda volver a crearse con facilidad.

Puede utilizar las opciones `exclude` e `include` de la lista de opciones de inclusión/exclusión para especificar los archivos que deben excluirse del proceso de copia de seguridad.





Utilice las opciones `include` y `exclude` de `dsm.sys` para definir qué archivos deben incluirse o excluirse del proceso de copia de seguridad incremental o selectiva. Un archivo es elegible para la copia de seguridad salvo que se excluya por una opción `exclude`. No es necesario utilizar una opción `include` para incluir archivos específicos para la copia de seguridad, a menos que estos archivos estén en un directorio que contenga otros archivos que desea excluir.

IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión es una clase de gestión predeterminada que selecciona personalmente o bien una clase de gestión que asigna al archivo mediante la utilización de la opción `include` en la lista de inclusión/exclusión. Si asigna una clase de gestión, ésta deberá contener un grupo de copia de seguridad para el archivo cuya copia de seguridad desea realizarse.

#### Tareas relacionadas:

Creación de una lista de inclusión/exclusión

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Cifrado de datos durante una operación de copia de seguridad o archivado

La manera de garantizar la seguridad de datos consiste en cifrar los datos. Utilice el cifrado de datos para proteger los datos durante una operación de copia de seguridad o archivado. El cifrado AES (Advanced Encryption Standard - Estándar de cifrado avanzado) de 128 bits es la opción de cifrado predeterminada. Para obtener el nivel más alto de cifrado de datos, utilice el cifrado de datos AES (Estándar de cifrado avanzado) de 256 bits especificando la opción `encryptiontype`.

Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos.

El cifrado sólo puede habilitarse en el cliente de copia de seguridad/archivado mediante la opción `include.encrypt`. Si no se utilizan sentencias `include.encrypt`, no se puede producir el cifrado.

 Sistemas operativos Linux El cifrado no es compatible con las copias de seguridad de la máquina virtual de VMWare que utilizan los modos de copia virtual incremental para siempre (`MODE=IFIncremental` y `MODE=IFFull`). Si el cliente se configura para el cifrado, no se puede utilizar la copia de seguridad siempre incremental.

Utilice las opciones `include` y `exclude` en `dsm.sys` para definir qué archivos incluir o excluir del proceso de copias de seguridad incrementales o selectivas. Un archivo es elegible para la copia de seguridad salvo que se excluya por una opción `exclude`. No es

necesario utilizar una opción include para incluir archivos específicos para la copia de seguridad, a menos que estos archivos estén en un directorio que contenga otros archivos que desea excluir.

Para cifrar datos de archivos, debe seleccionar una contraseña de clave de cifrado, que el cliente utiliza para generar la clave de cifrado para cifrar y descifrar los datos de archivos. Guarde la contraseña de clave de cifrada para utilizarla posteriormente. Puede especificar si se debe guardar la contraseña de clave de cifrado en un archivo que se denomina TSM.sth mediante la opción encryptkey.

El cifrado del cliente de IBM Spectrum Protect permite especificar un valor que tenga un máximo de 63 caracteres de longitud. Esta contraseña de cifrado debe confirmarse al cifrar el archivo para la copia de seguridad y también debe especificarse cuando se realizan restauraciones de archivos cifrados.

Al restaurar el archivo cifrado, el cliente solicitará al usuario la contraseña de clave para descifrar el archivo en los casos siguientes:

- La opción encryptkey se ha establecido en `Prompt`.
- La clave proporcionada por el usuario en el caso anterior no coincide.
- La opción encryptkey se ha establecido en `Save` y la contraseña de clave guardada localmente no coincide con el archivo cifrado.

**Referencia relacionada:**

Encryptiontype

Encryptkey

Opciones exclude

Opciones include

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Soporte para sistemas de archivos y ACL

Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. Los clientes UNIX y Linux pasan por alto los sistemas de archivos especiales y su contenido.







Los sistemas de archivos especiales incluyen los siguientes tipos:













- El sistema de archivos `/proc` en la mayoría de las plataformas UNIX
- El sistema de archivos `/dev/fd` en Solaris
- El `/dev/pts` en Linux



El cliente de copia de seguridad y archivado puede trabajar en tipos de sistema de archivos específicos que se utilizan habitualmente. Para obtener una lista de los tipos de sistemas de archivos admitidos, consulte la Tabla 1.




Restricción: La tabla muestra el soporte completo de NFS en AIX, incluida la conservación de ACL y atributos ampliados. En otros sistemas operativos, se admiten las copias de seguridad de NFS, pero dichas copias de seguridad sólo incluyen metadatos POSIX estándares (permisos de acceso, fecha de creación, etc.). Para obtener más información sobre cómo realizar copias de seguridad de sistemas NFS, consulte Copia de seguridad de sistemas de archivos de red.

Tabla 1. Sistemas de archivos admitidos y soporte para ACL

Plataforma	Sistema de archivos	Soporte de ACL
 Sistemas operativos AIX	 Sistemas operativos AIX GPFS JFS JFS2 JFS2 NFSV4 VxFS	 Sistemas operativos AIX yes yes yes yes yes
 Sistemas operativos Linux Linux x86_64	 Sistemas operativos Linux Btrfs XFS EXT2 EXT3 EXT4 ReiserFS GPFS JFS VxFS NSS	 Sistemas operativos Linux yes yes yes yes yes yes no no yes




Plataforma	Sistema de archivos	Soporte de ACL
 Sistemas operativos Linux Linux en servidores de Power Systems	 Sistemas operativos Linux  Btrfs XFS EXT2 EXT3 EXT4 ReiserFS JFS GPFS	 Sistemas operativos Linux  yes yes yes yes yes yes no yes
 Sistemas operativos Linux Linux en z Systems	 Sistemas operativos Linux  Btrfs EXT2 EXT3 EXT4 ReiserFS JFS GPFS	 Sistemas operativos Linux  yes yes yes yes yes no yes
 sistemas operativos Mac OS X macOS	 sistemas operativos Mac OS X  HFS estándar (HFS) HFS extendido (HFS+) HFS extendido y sensible a mayúsculas/minúsculas (HFSX+) Xsan (XSAN) Formato de disco universal (UDF) ISO9660	 sistemas operativos Mac OS X  yes yes yes yes yes yes yes
 Sistemas operativos Oracle Solaris Solaris	 Sistemas operativos Oracle Solaris  UFS VxFS QFS ZFS	 Sistemas operativos Oracle Solaris  yes yes no yes

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris En los sistemas de archivos en los que se han definido y utilizado las ACL NFS V4 (Solaris ZFS y AIX JFS2 Versión 2), incluso si sólo se han modificado los permisos de UNIX estándar o las ACL, por ejemplo, con el mandato CHMOD, se vuelve a realizar una copia de seguridad completa del archivo o del directorio. Con el resto de sistemas de archivos, este tipo de cambio sólo hace que se actualice un atributo en el servidor de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Para poder procesar todos los demás sistemas de archivos, utilice la opción virtualmountpoint para habilitar el soporte de los siguientes elementos:

- Para realizar una copia de seguridad, restaurar, archivar y recuperar datos de archivos
- Permisos básicos de UNIX y Linux
- Para cambiar, acceder y modificar indicaciones de fecha y hora y la estructura del árbol de directorio


No son válidos los atributos específicos de sistema de archivos, como ACL. El tipo de sistema de archivos para dichos sistemas de archivos debe establecerse en "UNKNOWN".

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Por ejemplo, si el sistema de archivos /media/abc/DATA1 no es compatible con el cliente, añada la siguiente sentencia a dsm.sys para realizar la copia de seguridad o archivar los datos en este sistema de archivos:

```
VIRTUALMOUNTPOINT /media/abc/DATA1
```

Este soporte sólo está disponible si el sistema de archivos puede utilizar llamadas al sistema POSIX, como el proceso de lectura o de grabación en el sistema.




No se admite la copia de seguridad entre plataformas ni la restauración. Por ejemplo, los datos cuya copia de seguridad ha realizado un cliente AIX no están disponibles para que los restaure un cliente Windows y viceversa.

 sistemas operativos Mac OS X Nota: Los datos copiados o archivados mediante el cliente de Mac OS X no pueden restaurarse mediante otro cliente. Además, el cliente de Mac OS X no puede restaurar ni recuperar datos de otros clientes.




Podrá utilizar el método de restauración o recuperación de la información de ACL en sistemas de archivos distintos solo si tanto el sistema de archivos original como el de destino admiten listas ACL compatibles. Por ejemplo, en Solaris, la información de ACL cuya copia de seguridad se ha realizado desde un sistema de archivos VxFS se restaura en un sistema de archivos UFS porque estos sistemas de archivos admiten listas ACL compatibles. La información de ACL no se restaura durante las operaciones de restauración o recuperación en sistemas de archivos distintos si el sistema de archivos original y el de destino no admiten listas ACL.


El paquete autónomo LSCqfs 3.5.0 es la única versión admitida de QFS. Asimismo, el sistema de archivos QFS tendrá las siguientes restricciones:



-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris No se admite la copia de seguridad de imagen en los sistemas de archivos QFS.
- El cliente de copia de seguridad/archivado de Solaris no admite la combinación de QFS y SAM que es necesaria para archivar copias en almacenamiento subordinado terciario, como por ejemplo cintas. En su lugar, recupera automáticamente archivos de cinta a disco, si encuentra archivos migrados mientras realiza una copia de seguridad.
- Un sistema de archivos QFS contiene dos archivos de sistema ocultos y un directorio de sistema del que no se puede realizar una copia de seguridad; y es aceptable porque no se necesita una copia de seguridad de estos archivos. Contienen datos internos para gestionar el sistema de archivos. Los datos internos se excluyen de forma automática desde una copia de seguridad y se recrean de forma automática mediante el sistema de archivos en sí mismo si se completa una restauración de archivos en ese sistema de archivos.

En AIX se admiten la copia de seguridad incremental, la copia de seguridad selectiva, la copia de seguridad de lista de archivos, la operación de archivado, la restauración y el proceso de recuperación del sistema de archivos de Veritas y sus ACL. La restauración de un volumen de Veritas en un volumen del gestor de volúmenes lógicos, y viceversa, está admitida siempre que ambos tengan el mismo tipo de sistema de archivos.

 sistemas operativos Mac OS X La siguiente información solo pertenece a sistemas Mac OS:

- En sistemas Mac OS X, los sistemas de archivos UFS y HFSX son sensibles a mayúsculas mientras que el sistema de archivos HFS+ no distingue entre mayúsculas y minúsculas pero las preserva. Es posible que las copias de seguridad de archivos de un sistema de archivos UFS o HFSX (sensible a mayúsculas/minúsculas) no se restauren correctamente en un sistema de archivos HFS+ (no sensible a mayúsculas/minúsculas). Por ejemplo, en un sistema de archivos UFS, los archivos `Afile` y `afile` se consideran archivos distintos. Sin embargo, en un sistema de archivos HFS+ los dos archivos se ven como idénticos.
- En Mac OS X, si se utilizan los sistemas de archivos HFS+ o UFS sensibles a mayúsculas, es importante que la copia de seguridad de los datos del sistema de archivos HFSX o UFS no se realice en un sistema de archivos HFS+ en el servidor de IBM Spectrum Protect. Debe utilizarse un nombre nuevo en el sistema o bien renombrar el espacio de archivos existente en el servidor de IBM Spectrum Protect. Por ejemplo, imagine un sistema que tiene un sistema de archivos llamado `/Volumes/fs2` y que éste se reparticiona con un sistema de archivos HFS+ que distingue entre mayúsculas y minúsculas. Bien el sistema de archivos `/Volumes/fs2` en el servidor de IBM Spectrum Protect debe cambiarse de nombre, bien el nombre nuevo debe utilizarse en el sistema local. De lo contrario, los datos que distinguen entre mayúsculas y minúsculas de HFSX se combinarán con los datos que no distinguen entre mayúsculas y minúsculas de HFS+ ya almacenados en el servidor de IBM Spectrum Protect.
- En Mac OS X, se realiza una copia de seguridad de los alias y de los enlaces simbólicos. Sin embargo, el cliente no lleva a cabo copias de seguridad de los datos a los que hacen referencia los enlaces simbólicos.
- En Mac OS X, cuando se realiza la copia de seguridad de los archivos desde un volumen HFS se restauran a un volumen UFS, los `resource forks` no se asignan al propietario correcto. Corrija este problema utilizando el mandato `chown` en el archivo del `resource fork` para cambiar el propietario. El almacén de archivos del `resource fork` almacena los datos estructurados en un archivo.

 Sistemas operativos Linux En Linux en POWER y Linux en System z, debe instalar `libacl.so` para que el cliente realice copias de seguridad de ACL.

 Sistemas operativos AIX  Sistemas operativos Linux Importante: Si está ejecutando GPFS para AIX, GPFS para Linux x86\_64 o GPFS para Linux en z Systems en un clúster multinodo y todos los nodos comparten un sistema de archivos GPFS montado, el cliente procesa este sistema de archivos como un sistema de archivos local. El cliente realiza copias de seguridad del sistema de archivos en cada nodo durante una copia de seguridad incremental. Para evitar esto, puede realizar una de las siguientes tareas:

- Configure explícitamente la sentencia `domain` en el archivo de opciones de usuario de cliente (`dsm.opt`) para enumerar los sistemas de archivos de los que desea que dicho nodo realice una copia de seguridad.
- Establezca la opción `exclude.fs` en el archivo `dsm.sys` para excluir el sistema de archivos GPFS de los servicios de copia de seguridad.

Si el clúster GPFS contiene diferentes plataformas, debe utilizar los clientes de copia de seguridad y archivado sólo en una plataforma para proteger un solo sistema de archivos. No utilice clientes de copia de seguridad y archivado en más de una plataforma para proteger un sistema de archivos GPFS que se comparta entre más de una plataforma

Por ejemplo, supongamos que un clúster contiene nodos en sistemas AIX, Linux x86 y Linux zSeries. Puede proteger el sistema de archivos A con clientes de copia de seguridad y archivado AIX y el sistema B con clientes de copia de seguridad y archivado Linux zSeries. También puede proteger el sistema de archivos A y el sistema de archivos B con clientes de copia de seguridad y archivado AIX.

Si protege el sistema de archivos A con un cliente de copia de seguridad y archivado AIX, no debe proteger el sistema de archivos A con un cliente de copia de seguridad y archivado de ninguna plataforma que no sea AIX.

## Soporte para la recuperación entre sistemas operativos de archivos almacenados en sistemas de archivos IBM Spectrum Scale

En un clúster IBM Spectrum Scale con varios tipos de sistema operativo, un archivo que contiene la ACL o metadatos de atributos ampliados y cuya copia de seguridad se ha realizado en un sistema operativo de origen se puede restaurar en un sistema operativo de destino. La ACL o los metadatos de atributos ampliados se restauran correctamente si los dos tipos de sistema operativo en el origen y destino utilizan la misma versión de IBM Spectrum Scale.

Se da soporte a los siguientes sistemas operativos de origen:

- AIX
- Linux para IBM System Power big endian (pBE)
- Linux x86
- Linux para IBM System z

Se da soporte a los siguientes tipos de sistema operativo de destino:

- Linux para IBM System Power little endian (pLE)
- Linux x86
- Linux para IBM System z

Los valores de seguridad de los usuarios y grupos afectados deben ser los mismos en los sistemas de origen y destino.

No mezcle tipos de sistema operativo para la actividad de copia de seguridad. Elija únicamente un solo tipo de sistema operativo disponible en el clúster de IBM Spectrum Scale y utilícelo para todas las operaciones de copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris











## Tamaño máximo de archivo para operaciones






El tamaño máximo de archivo depende del tipo de sistema de archivos. El cliente de copia de seguridad y archivado no comprueba ningún límite de tamaño de archivo durante las operaciones de copia de seguridad, archivado, restauración o recuperación.

Si el sistema de archivos permite crear el archivo, el cliente realiza la copia de seguridad o el archivado de dicho archivo.

En la tabla siguiente se especifican los tamaños máximos de archivos para sistemas de archivos nativos en las plataformas cliente UNIX y Linux.

Tabla 1. Tamaño máximo de archivo

Plataforma	Tamaño máximo de archivo (en bytes)
 Sistemas operativos AIX Limitaciones de tamaño para AIX 6.1 (JFS2)	 Sistemas operativos AIX Tamaño máximo del sistema de archivos JFS2: 32 TB Tamaño máximo del sistema de archivos JFS2: 16 TB Tamaño mínimo del sistema de archivos JFS2: 16 MB
 Sistemas operativos Linux Todos los clientes Linux	 Sistemas operativos Linux 9.223.372.036.854.775.807 (8 EB-1)
 sistemas operativos Mac OS X Mac OS X	 sistemas operativos Mac OS X HFS - 2.147.485.648 (2GB) HFS+, HFSX, XSAN y UFS - 9.223.372.036.854.775.808 (8EB)
 Sistemas operativos Oracle Solaris Solaris	 Sistemas operativos Oracle Solaris 1.099.511.627.775 (1 TB-1)
 Sistemas operativos Oracle Solaris Solaris (ZFS)	 Sistemas operativos Oracle Solaris 18.446.744.073.709.551.616 (16 EB)

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Nombres de usuario y de grupo largos

---

El cliente de archivado y copia de seguridad puede gestionar sin problemas nombres de usuario y de grupo con hasta 64 caracteres. Sin embargo, los nombres de más de 64 caracteres requieren un manejo especial por parte de IBM Spectrum Protect.

Importante: No exceda el límite de 64 caracteres para los nombres de usuario y de grupo. Si lo hace, el cliente acorta el nombre para que se ajuste a este límite mediante la utilización de las transformaciones siguientes: se tomarán los 53 primeros caracteres y se añadirán una barra inclinada (/) y, a continuación, el ID numérico como serie de caracteres.

Se anota un mensaje de error que contiene el nombre largo y la serie de caracteres acortada resultante. Para ejecutar la mayoría de las funciones no será necesario que conozca el nombre abreviado. Las excepciones son:

- El mandato set access
- La opción fromowner
- Las opciones users y groups (autorización)

En cada uno de estos casos, cuando tenga que especificar un nombre, deberá buscar el mensaje de error que contiene la transformación o bien construir el nombre utilizando la regla que se describe aquí.

 sistemas operativos Mac OS X



## Nombres de volumen en Mac OS X

---

El cliente de copia de seguridad y archivado hace copias de seguridad de los volúmenes en función de su nombre de punto de montaje UNIX.

IBM Spectrum Protect mantiene cada uno de los nombres de un volumen como una restauración aparte o volumen recuperado. Estos nombres de volumen se convierten en los nombres de los espacios de archivo en un servidor.

Si se cambia el nombre de un volumen del que ya se ha efectuado copia de seguridad, el cliente la considera como un volumen nuevo y no lo relaciona con el anterior. Cualquiera copia de seguridad de un volumen hace copia de seguridad de los archivos con un nombre nuevo. Se puede producir una discrepancia si cambia el nombre de los volúmenes, o si accede a IBM Spectrum Protect desde una estación de trabajo distinta de la utilizada para realizar la copia de seguridad de los archivos.

-  sistemas operativos Mac OS X Precauciones respecto a la asignación de nombres de volumen en Mac OS X  
IBM Spectrum Protect crea todos los espacios de archivos nuevos en el servidor con el punto de montaje UNIX del volumen.
-  sistemas operativos Mac OS X Precauciones respecto a la asignación de nombres de volumen en Mac OS X en sistemas de arranque dual  
Si dispone de más de una versión de Mac OS X que utiliza de manera alternativa, es fundamental que comprenda cómo el cliente utiliza las vías de acceso de montaje de UNIX con los nombres de espacios de archivos del servidor de IBM Spectrum Protect.

 sistemas operativos Mac OS X

## Precauciones respecto a la asignación de nombres de volumen en Mac OS X

---

IBM Spectrum Protect crea todos los espacios de archivos nuevos en el servidor con el punto de montaje UNIX del volumen.

Si hay dos volúmenes que se llaman "La Pomme" y "la pomme", se crearán dos puntos de montaje UNIX únicos.

Los ejemplos siguientes muestran los dos puntos de montaje que se crean:

```
/Volumes/La Pomme  
/Volumes/la pomme
```

Si existen volúmenes duplicados en su escritorio, es posible que los puntos de montaje UNIX no sean los mismos que la última vez que el cliente realizó una copia de seguridad. El cliente podría no hacer copia de seguridad de los datos en el sistema de archivos correcto en el servidor de IBM Spectrum Protect.

Puede comprobar el sistema de archivos en el que el cliente realiza una copia de seguridad de los datos:


1. En la ventana de copia de seguridad, seleccione un sistema de archivos.
2. Pulse **Archivo** → **Mostrar Info**.

El punto de montaje de UNIX está en el diálogo de Información.

La mejor manera de evitar problemas potenciales con la asignación de nombres es asegurarse de que los nombres de volumen sean únicos.

Importante:

- El cliente continuará utilizando los nombres de espacio de archivos existentes en el servidor de IBM Spectrum Protect. Solo los nuevos espacios de archivos utilizarán el punto de montaje UNIX para el nombre.
- No incluya puntos cuando especifique el nombre de los volúmenes (...). El cliente utiliza la secuencia de puntos como parte del proceso de inclusión/exclusión. El cliente informará de la existencia de una sentencia de inclusión/exclusión no válida si un nombre de volumen contiene puntos. *Debe* cambiarse el nombre del volumen.

 sistemas operativos Mac OS X

## Precauciones respecto a la asignación de nombres de volumen en Mac OS X en sistemas de arranque dual

---

Si dispone de más de una versión de Mac OS X que utiliza de manera alternativa, es fundamental que comprenda cómo el cliente utiliza las vías de acceso de montaje de UNIX con los nombres de espacios de archivos del servidor de IBM Spectrum Protect.

Por ejemplo, supongamos que dispone de un sistema de arranque dual con dos volúmenes, *El Capitan* y *Sierra*. El buscador y la GUI del cliente de archivado y copia de seguridad los muestran como *El Capitan* y *Sierra*. Sin embargo, los puntos de montaje de UNIX dependen de la versión de Mac OS que se esté ejecutando. Si *El Capitan* es el disco de inicio, las vías de acceso de UNIX serán:

```
/
/Volumes/Sierra
```

Si *Sierra* es el disco de inicio, las vías de acceso de UNIX serán:

```
/
/Volumes/El Capitan
```

Cuando se ejecute una operación de copia de seguridad o de archivado, los nombres de espacios de archivos dependerán también de la versión de Mac OS X que se esté ejecutando.

Las dos versiones de Mac OS X realizarán una copia de seguridad en el sistema de archivos / del servidor de IBM Spectrum Protect. Si esto sucede, los archivos de sistema se entremezclan.

Para evitar posibles problemas con los sistemas de arranque dual, realice una de las siguientes tareas:

1. Seleccione una versión de Mac OS X para instalar y ejecutar IBM Spectrum Protect. De este modo se asegura de que los puntos de montaje de UNIX son los mismos cada vez que el cliente realiza una copia de seguridad.
2. Configure cada una de las versiones de Mac OS X con un nombre de nodo de IBM Spectrum Protect único. A continuación, excluya la otra versión de Mac OS X del proceso de copia de seguridad con una sentencia de dominio en el archivo de opciones del sistema. Por ejemplo, si el volumen *Sierra* es el disco de inicio, añada esta opción al archivo de opciones del sistema:

```
DOMAIN -/Volumes/El Capitan
```

Si el volumen *El Capitan* es el disco de inicio, añada esto al archivo de opciones del sistema:

```
DOMAIN -/Volumes/Sierra
```

 sistemas operativos Mac OS X

## Habilitación de Unicode para Mac OS X

---

El cliente Mac OS X está habilitado para Unicode. Los clientes nuevos que almacenen datos en el servidor por primera vez no requieren una configuración especial.

El servidor almacena automáticamente archivos y directorios activados para Unicode. Sin embargo, si desea actualizar al cliente activado para Unicode, tiene que planificar la migración de los espacios de archivos existentes para que puedan admitir Unicode.

Se tiene que cambiar el nombre de los espacios de archivos que ya están en el servidor para que se puedan crear espacios de archivos activados para Unicode. Utilice la opción `autofsrename` para cambiar el nombre a los espacios de archivos existentes.

### Referencia relacionada:

Autofsrename

 sistemas operativos Mac OS X

## Disco de copia de seguridad Time Machine de Mac OS X

---

Time Machine es la aplicación de copia de seguridad disponible con Mac OS X.

IBM Spectrum Protect se puede utilizar al mismo tiempo que la aplicación Mac OS X Time Machine. Debido a la forma única en que Time Machine de Mac OS X realiza copias de seguridad de los datos, tenga en cuenta algunas cuestiones antes de utilizar el cliente de copia de seguridad y archivado para realizar una copia de seguridad de los datos de Time Machine de Mac OS X:

- El disco de copia de seguridad de Time Machine de Mac OS X hace un uso amplio de los enlaces fijos de directorio y de archivo para minimizar la utilización del disco. Por ejemplo, si el disco objeto de la copia de seguridad con Time Machine de Mac OS X tiene 5 GB, la primera copia de seguridad copiará los 5 GB de datos en el disco de copia de seguridad de Time Machine de Mac OS X.

Las copias de seguridad subsiguientes copiarán únicamente los archivos que hayan cambiado desde la copia de seguridad anterior. Todos los archivos y directorios que no hayan cambiado se enlazarán de forma fija con la versión que se ha copiado durante la copia de seguridad anterior.

El Finder mostrará cada copia de seguridad como de 5 GB, para un tamaño total de 10 GB. Sin embargo, debido al uso de enlaces fijos, el uso total del disco será ligeramente superior a 5 GB.

Se realiza una copia de seguridad de todos los objetos enlazados de forma fija que no se encuentren en el servidor de IBM Spectrum Protect.


Por ejemplo, se enviarían 10 GB de datos al servidor de IBM Spectrum Protect.

- Cuando los archivos que están restaurados son enlaces fijos, el cliente vuelve a crear el enlace fijo original. La recreación del enlace fijo original solo se puede hacer si *todos* los archivos que están enlazados de forma fija se restauran al mismo tiempo. La restauración de todos los archivos con enlaces fijos no es un método práctico para un disco de copias de seguridad grande que utiliza la aplicación Time Machine de Mac OS X.
- Cuando Time Machine de Mac OS X copia los archivos en el disco de copia de seguridad, se añaden ACL a los archivos para evitar que puedan eliminarse. El cliente de copia de seguridad y archivado puede realizar copias de seguridad de los archivos y restaurarlos con las listas de control de acceso (ACL). Sin embargo, todos los archivos que se restauren seguirán teniendo estas ACL restrictivas.

**Sugerencia:** Para obtener mejores resultados, excluya los datos de la copia de seguridad de la aplicación Time Machine. Todos los datos de Time Machine se encuentran en un directorio denominado `Backups.backupdb`.

#### Conceptos relacionados:

Archivos del sistema a excluir

 Sistemas operativos Windows






## Copias de seguridad incrementales, selectivas o incrementales por fecha (Windows)

---

Es posible que el administrador haya establecido planificaciones para realizar automáticamente copias de seguridad. En esta sección se indica cómo realizar copias de seguridad de archivos sin utilizar una planificación.



Existen tres tipos de copia de seguridad incremental: *completa*, *parcial* e *incremental por fecha*.

Si migra archivos con IBM Spectrum Protect HSM for Windows, puede haber consecuencias en las operaciones de copia de seguridad.

-  Sistemas operativos Windows Copia de seguridad incremental completa y parcial  
Una copia de seguridad incremental sólo copia los archivos nuevos y modificados. El tipo de copia de seguridad incremental depende de los objetos que selecciona para realizar la copia de seguridad.
-  Sistemas operativos Windows Copia de seguridad incremental por fecha  
Para que un sistema de archivos sea elegible para copias de seguridad incrementales por fecha, debe haberse realizado como mínimo una copia de seguridad incremental completa de todo el sistema de archivos. Si ejecuta una copia de seguridad incremental de sólo una rama de directorios o un archivo individual, el sistema de archivos no será elegible para realizar copias de seguridad incrementales por fecha.
-  Sistemas operativos Windows Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales  
Los métodos incrementales por fecha, con registro por diario y diferenciales de instantánea de NetApp son alternativas a los métodos de copia de seguridad incremental completa y parcial.
-  Sistemas operativos Windows Copia de seguridad diferencial de la instantánea con una conexión HTTPS  
Puede utilizar una conexión segura HTTPS para que el cliente de archivado y copia de seguridad se comunique con un archivador NetApp durante una copia de seguridad diferencial de una instantánea.
-  Sistemas operativos Windows Copia de seguridad selectiva  
Utilice la copia de seguridad selectiva para realizar copias de seguridad de archivos específicos o directorios

independientemente de si ya existe una copia de seguridad de dichos archivos en el servidor.

#### Conceptos relacionados:





 Sistemas operativos Windows  Copia de seguridad y restauración de los archivos migrados


#### Tareas relacionadas:

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar






## Copia de seguridad incremental completa y parcial






Una copia de seguridad incremental sólo copia los archivos nuevos y modificados. El tipo de copia de seguridad incremental depende de los objetos que selecciona para realizar la copia de seguridad.






 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si selecciona los sistemas de archivos completos, la copia de seguridad es una copia de seguridad incremental completa. Si selecciona un árbol de directorio o archivos individuales, la copia de seguridad es una copia de seguridad incremental parcial.

 Sistemas operativos Windows Si selecciona las unidades completas, la copia de seguridad es una copia de seguridad incremental completa. Si selecciona un árbol de directorio o archivos individuales, la copia de seguridad es una copia de seguridad incremental parcial.


La primera vez que se ejecuta una copia de seguridad incremental completa, el cliente de copia de seguridad y archivado realiza una copia de seguridad de todos los archivos y directorios que especifique. La operación de copia de seguridad puede llevar mucho tiempo si el número de archivos es grande o si uno o más archivos grandes deben copiarse. Las posteriores copias de seguridad incrementales completas sólo realizan copias de seguridad de los archivos nuevos y modificados. El servidor de copia de seguridad mantiene las versiones actuales de sus archivos sin tener que perder tiempo o espacio realizando la copia de seguridad de los archivos que existen en el almacenamiento del servidor de IBM Spectrum Protect.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Dependiendo de las políticas de gestión de almacenamiento, es posible que el servidor de IBM Spectrum Protect tenga más espacio que una versión de sus archivos en el almacenamiento. Las últimas copias de seguridad realizadas son versiones de copia de seguridad activas. Las copias de archivos más antiguas son versiones inactivas. Sin embargo, si suprime un archivo de la estación de trabajo, la siguiente copia de seguridad incremental completa hace que la versión de copia de seguridad activa del archivo pase a ser inactiva. Puede restaurar la versión inactiva de un archivo. El número de versiones inactivas que mantiene el servidor y cuánto tiempo se gobiernan mediante las políticas de gestión definidas por el administrador del servidor de IBM Spectrum Protect. Las versiones activas representan los archivos que existían en el sistema de archivos cuando se realizó la última copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para iniciar una copia de seguridad incremental completa o parcial mediante la GUI del cliente, seleccione Backup, y después seleccione la opción Incremental (complete). Desde la línea de mandatos, utilice el mandato incremental y especifique los sistemas de archivos, los árboles del directorio o los archivos individuales que se incluyen en la copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Durante una copia de seguridad incremental, el cliente consulta al servidor o la base de datos de diario para determinar cuál es el estado exacto de los archivos desde la última copia de seguridad incremental realizada. El cliente utiliza esta información para las siguientes tareas:

- Realizar copias de seguridad de archivos nuevos.
- Realizar copias de seguridad de archivos cuyo contenido ha cambiado desde la última copia de seguridad.




 Sistemas operativos Windows Se realiza la copia de seguridad de los archivos cuando cualquiera de los siguientes atributos cambia:

- Tamaño del archivo
- Fecha u hora de la última modificación
- Atributos ampliados
- La lista de control de accesos.
- Atributos de archivo esparcido, de punto de reanálisis o cifrado.
- Descriptores de seguridad del archivo NTFS o ReFS: identificador de seguridad del propietario (SID), SID de grupo, Lista de control de acceso discrecional (ACL), y ACL de sistema.
- Atributos de directorios

Si los siguientes atributos cambian, los atributos se actualizan en el servidor de IBM Spectrum Protect, pero no se realiza la copia de seguridad del archivo:





- Solo lectura o lectura y grabación
- Oculto o descubierto
- Comprimido o no comprimido






IBM Spectrum Protect no examina el atributo de archivo al determinar los archivos modificados.






 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Se realiza la copia de seguridad de los archivos cuando cualquiera de los siguientes atributos cambia:

- o Tamaño del archivo
- o Fecha u hora de la última modificación
- o Atributos ampliados
- o La lista de control de accesos.

Si los siguientes atributos cambian, los atributos se actualizan en el servidor de IBM Spectrum Protect, pero no se realiza la copia de seguridad del archivo:

- o Propietario del archivo
  - o Permisos del archivo
  - o Inodo
  - o ID de grupo
  - o  Sistemas operativos AIX  Sistemas operativos Linux Atributo de hora del cambio (`ctime`) (sólo para objetos en sistemas de archivos GPFS y si la opción `updatectime` está establecida en yes). Para obtener más información, consulte la opción `updatectime`.
  - o Ubicación del icono (sólo Mac OS X)
  - o Tipo o creador (sólo Mac OS X)
- Realizar copias de los directorios.  
Se realiza una copia de seguridad de un directorio en cualquiera de las siguientes circunstancias:
    - o No se ha realizado una copia de seguridad previa del directorio.
    - o Los permisos del directorio han cambiado desde la última copia de seguridad.
    - o El directorio de la lista de control de acceso ha cambiado desde la última copia de seguridad.
    - o El directorio de atributos ampliados ha cambiado desde la última copia de seguridad.
    - o  Sistemas operativos AIX  Sistemas operativos Linux El atributo de cambio de hora (`ctime`) se actualiza desde la última copia de seguridad (sólo para sistemas de archivos GPFS). Para obtener más información, consulte la opción `updatectime`.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Los directorios se enumeran de acuerdo con el número de objetos de copia de seguridad. Para excluir directorios y el contenido de los mismos del proceso de copia de seguridad, utilice la opción `exclude.dir`.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Hacer caducar las versiones de copia de seguridad de los archivos del servidor que no tienen archivos correspondientes en la estación de trabajo. El resultado es que los archivos que ya no existen en la estación de trabajo no tienen versiones de copia de seguridad activas en el servidor. Sin embargo, las versiones inactivas se conservan en función de las reglas definidas por el administrador de IBM Spectrum Protect.
- Volver a vincular las versiones de copia de seguridad si han cambiado las asignaciones de clase de gestión. Sólo volverán a enlazarse los objetos que tengan versiones de copia de seguridad activas. Los objetos para los que sólo existan versiones de copia de seguridad inactivas no volverán a enlazarse.  
Durante una operación de copia de seguridad incremental, los objetos se vuelven a enlazar o caducan de la siguiente manera:






Si la especificación de archivo coincide con todos los archivos en una vía de acceso:


El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Éste sería el caso de un mandato incremental como `dsmc incr c:\mydir\* -subdir=yes`.

Si la especificación de archivo no coincide con todos los archivos en una vía de acceso:

El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Sin embargo, las versiones de copia de seguridad seleccionables no caducan ni se vuelven a enlazar si se encuentran en un directorio que ya no existe en el sistema de archivos del cliente.

Pongamos por ejemplo un mandato incremental como `dsmc incr c:\mydir\*.txt -subdir=yes`. Supongamos que algunos archivos en `c:\mydir\` no tienen el tipo de archivo `txt`. El reenlace y la caducidad sólo se produce para archivos que coinciden con la especificación `*.txt` y cuyos directorios aún existen en el sistema de archivos del cliente.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Puede utilizar la opción `preservelastaccessdate` para especificar si va a modificar la última fecha de acceso después de realizar una operación de copia de seguridad o archivado. De forma predeterminada, la fecha de acceso cambia después de una operación de copia de seguridad o archivado predeterminada.

-  Sistemas operativos Windows  
Copia de seguridad con registro por diario  
La copia de seguridad con registro por diario es un método alternativo de copia de seguridad que utiliza un diario de cambios mantenido por el proceso del servicio de diario de IBM Spectrum Protect.

#### Conceptos relacionados:

Políticas de gestión de almacenamiento


#### Referencia relacionada:

Opciones `exclude`

## Copia de seguridad incremental por fecha

---

Para que un sistema de archivos sea elegible para copias de seguridad incrementales por fecha, debe haberse realizado como mínimo una copia de seguridad incremental completa de todo el sistema de archivos. Si ejecuta una copia de seguridad incremental de sólo una rama de directorios o un archivo individual, el sistema de archivos no será elegible para realizar copias de seguridad incrementales por fecha.

 Sistemas operativos Windows Para realizar una copia de seguridad incremental por fecha mediante la utilización de la GUI, seleccione la opción incremental (sólo por fecha) del menú desplegable *Tipo de copia de seguridad* o bien utilice la opción `incrbydate` con el mandato incremental.








El cliente realiza una copia de seguridad sólo de aquellos archivos cuya fecha y hora de modificación es posterior a la fecha y hora de la última copia de seguridad incremental del sistema de archivos en el que se encuentra el archivo. Los archivos que agregue el cliente después de la última copia de seguridad incremental, pero cuya fecha de modificación sea anterior a la última copia de seguridad incremental, no se incluyen en la operación de copia de seguridad.

Los archivos cuyo nombre se ha cambiado después de la última copia de seguridad incremental, pero que no se han modificado, no se incluirán en la copia de seguridad. El cambio de nombre de un archivo no hace cambiar la fecha ni la hora de modificación del archivo. No obstante, si se cambia el nombre de un archivo sí se cambia la fecha de modificación del directorio en el que se encuentra. En este caso, se hace la copia de seguridad del directorio, pero no de los archivos que contiene.

Si ejecuta una copia de seguridad incremental por fecha de todo un sistema de archivos, el servidor actualiza la fecha y hora de la última copia de seguridad incremental. Si efectúa una copia de seguridad incremental por fecha sólo en una parte de un sistema de archivos, el servidor no actualiza la fecha de la última copia de seguridad incremental completa. En este caso, la siguiente copia de seguridad incremental por fecha vuelve a copiar estos archivos.

Nota: A diferencia de la copia de seguridad incremental, la copia de seguridad incremental por fecha no hace caducar los archivos suprimidos o vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.

### Tareas relacionadas:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Copia de seguridad de datos mediante la GUI Java  
 Sistemas operativos Windows  Sistemas operativos AIX  Sistemas operativos Linux

## Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales











---

Los métodos incrementales por fecha, con registro por diario y diferenciales de instantánea de NetApp son alternativas a los métodos de copia de seguridad incremental completa y parcial.

### Copia de seguridad incremental por fecha




Una copia incremental por fecha tarda menos tiempo en procesarse que una copia incremental completa y requiere menos memoria.




Puede ser que una copia de seguridad incremental por fecha no coloque exactamente los mismos archivos de copia de seguridad en el almacenamiento del servidor, ya que la copia de seguridad incremental por fecha:



-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No hace caducar las versiones de copia de seguridad de aquellos archivos que se han suprimido de la estación de trabajo.
- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.
- No efectúa copias de seguridad de archivos cuyos atributos cambian, a menos que también se hayan modificado la fecha y la hora de modificación.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión (las copias de seguridad con registro por diario tampoco tienen en cuenta este atributo).

Copia de seguridad con registro por diario







 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Los requisitos de memoria para un entorno de registro por diario inicial son los mismos que los requisitos de memoria necesarios para una copia de seguridad incremental de espacio de archivos completa, pues las copias de seguridad con registro por diario deben completar la copia de seguridad incremental de espacio de archivos completa para poder establecer la base de datos de diario como válida y para poder establecer la línea de base para el registro por diario.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Los requisitos de memoria para las posteriores copias de seguridad con registro por diario serán mucho menores. Las sesiones de copia de seguridad con registro por diario se ejecutan en paralelo y las rige la opción de cliente resourceutilization, de la misma forma que las sesiones de copia de seguridad normales. El tamaño del archivo de base de datos de diario vuelve a adquirir un tamaño mínimo (menos de 1 KB) cuando se ha suprimido la última entrada del diario. Puesto que las entradas se suprimen del diario a medida que el cliente las procesa, el tamaño de disco que ocupa el diario debería ser el mínimo después de haberse realizado una copia de seguridad con registro por diario completa. Una copia de seguridad incremental completa con el registro por diario activo necesita menos tiempo para procesarse que una copia de seguridad incremental por fecha.

 Sistemas operativos AIX  Sistemas operativos Linux En AIX y Linux, la copia de seguridad con registro por diario tiene algunas limitaciones. Para obtener más información, consulte el apartado Copia de seguridad basada en el diario en AIX y Linux.


#### Diferencial de instantánea de NetApp

 Sistemas operativos Linux  Sistemas operativos Windows Para servidores de archivos NAS y N-Series que se ejecuten en ONTAP 7.3.0, o superior, puede utilizar la opción snapdiff para invocar la copia de seguridad de diferencia de instantáneas NetApp cuando se realice una copia incremental de volumen completa. Esta opción reduce el uso de memoria y es más rápida.

 Sistemas operativos Linux  Sistemas operativos Windows Tenga en cuenta las siguientes limitaciones cuando ejecute una copia de seguridad incremental de volúmenes completos mediante la opción snapdiff para garantizar que se realiza una copia de seguridad de los datos en el momento adecuado.


- Un archivo se excluye debido a una regla de exclusión en el archivo de inclusión/exclusión. El cliente realiza una copia de seguridad de la instantánea actual con la regla de exclusión en vigor. Esto ocurre cuando no se han realizado cambios en el archivo, pero se ha eliminado la regla que excluía el archivo. NetApp no detecta este cambio de inclusión/exclusión, porque sólo detecta los cambios de los archivos entre dos instantáneas.
- Si ha añadido una sentencia de inclusión en el archivo de opciones, esta opción de inclusión solo entra en vigor cuando NetApp detecta que el archivo se ha modificado. El cliente no inspecciona cada uno de los archivos del volumen durante la copia de seguridad.
- Si ha utilizado el mandato dsmc delete backup para suprimir explícitamente un archivo del inventario de IBM Spectrum Protect, NetApp no puede detectar que se ha eliminado manualmente un archivo del almacenamiento de IBM Spectrum Protect. Por consiguiente, el archivo sigue sin protección en el almacenamiento de IBM Spectrum Protect hasta que se cambia en el volumen y NetApp detecta el cambio, señalando al cliente que vuelva a hacer una copia de seguridad del mismo.
- Los cambios de políticas como, por ejemplo, de mode=modified a mode=absolute no se detectan.
- El espacio de archivo entero se suprime del inventario IBM Spectrum Protect. Esta acción provoca que la opción snapdiff cree una instantánea para utilizar como origen y una copia de seguridad incremental completa para ejecutarse.

El software de NetApp determina qué es un objeto cambiado, no IBM Spectrum Protect.

 Sistemas operativos Linux Si ejecuta una copia de seguridad de volumen completa de un NFS-mounted NetApp o N-Series, es posible que también se realice una copia de seguridad de todas las instantáneas del directorio de instantáneas.

Para evitar realizar la copia de seguridad de todas las instantáneas del directorio de instantánea realice una de las siguientes acciones:

- Ejecutar copias de seguridad NDMP
- Ejecutar copias de seguridad utilizando la opción snapshotroot
- Ejecutar copias de seguridad incrementales utilizando la opción snapdiff  
Consejo: Si ejecuta una copia de seguridad incremental mediante la opción snapdiff y planifica copias de seguridad incrementales periódicas, utilice la opción createnewbase=yes junto con la opción snapdiff para crear una instantánea base y utilizarla como origen para ejecutar una copia de seguridad incremental.
- Excluir el directorio de instantáneas desde las copias de seguridad.

 Sistemas operativos Linux En sistemas Linux, el directorio de instantáneas está en .snapshot.

Nota: En algunas versiones de Red Hat Linux, no se realiza una copia de seguridad del directorio .snapshot, por lo que no necesita excluirlo.

 Sistemas operativos Windows En sistemas Windows, el directorio de instantáneas está en ~snapshot.

 Sistemas operativos Windows

## Copia de seguridad diferencial de la instantánea con una conexión HTTPS

---

Puede utilizar una conexión segura HTTPS para que el cliente de archivado y copia de seguridad se comuniquen con un archivador NetApp durante una copia de seguridad diferencial de una instantánea.


El protocolo HTTPS está habilitado en los archivadores NetApp de forma predeterminada y no puede desactivarse.

Cuando ejecuta una copia de seguridad diferencial de instantánea, el cliente de archivado y copia de seguridad establece una sesión administrativa con un archivador NetApp. Las credenciales del archivador, como el nombre de host del archivador o la dirección IP, el nombre de usuario que se utiliza para conectar el archivador y la contraseña del archivador se almacenan localmente en el cliente de archivado y copia de seguridad. Esta información debe transmitirse al archivador para establecer la sesión administrativa autenticada. Es importante utilizar una conexión segura porque autenticar la sesión del archivador administrativo requiere que el cliente transmita la contraseña del archivador en texto claro.


Para establecer una conexión segura mediante el protocolo de comunicación HTTPS, debe utilizar la opción `snapdiffhttps` cuando ejecuta una copia de seguridad de diferencial de instantánea. Sin la opción `snapdiffhttps`, el cliente de archivado y copia de seguridad puede establecer sesiones de gestor de archivos solo con el protocolo HTTP, que requeriría acceso administrativo HTTP para habilitarse en el gestor de archivos. Con la opción `snapdiffhttps`, puede establecer una sesión de administración segura con el archivador NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador NetApp.

Restricciones:

Las siguientes restricciones se aplican a copias de seguridad diferencias instantáneas con HTTPS:


- La conexión HTTPS sólo se utiliza para transmitir datos de forma segura a través de la sesión de administración entre el cliente de archivado de copia de seguridad y el archivador de NetApp. Los datos de la sesión de administración incluyen información como credenciales del archivador, información de instantánea y los nombres de archivo y los atributos que se generan mediante el proceso de diferenciación de instantáneas. La conexión HTTPS no se utiliza para transmitir datos de archivos normales a los que se accede en el archivador mediante el cliente a través de la compartición de archivos. La conexión HTTPS tampoco se aplica a los datos de archivos normales transmitidos mediante el cliente al servidor de IBM Spectrum Protect a través del protocolo cliente/servidor de IBM Spectrum Protect normal.
- La opción `snapdiffhttps` no se aplica a vFilers porque el protocolo HTTPS no está admitido en NetApp vFiler.
- La opción `snapdiffhttps` sólo está disponible utilizando la interfaz de línea de mandatos. No está disponible para su utilización con la GUI del cliente de archivado de copia de seguridad.
-  **Sistemas operativos Windows** Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS  
Cuando ejecuta una copia de seguridad diferencial de una instantánea, puede utilizar la opción `snapdiffhttps` para crear una conexión HTTPS segura entre el cliente de archivado y copia de seguridad y el archivador NetApp.


### Conceptos relacionados:

 **Sistemas operativos Windows** Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales

### Tareas relacionadas:

Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea

 **Sistemas operativos Windows** Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS

 **Sistemas operativos Linux** Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS

### Referencia relacionada:

`Snapdiffhttps`

`Snapdiff`

## Copia de seguridad selectiva

---

Utilice la copia de seguridad selectiva para realizar copias de seguridad de archivos específicos o directorios independientemente de si ya existe una copia de seguridad de dichos archivos en el servidor.






Las copias de seguridad incrementales suelen formar parte de un sistema automatizado para hacer copia de seguridad de todos los sistemas de archivos. Por el contrario, las copias de seguridad selectivas permiten seleccionar manualmente un juego de archivos de los que se debe realizar una copia de seguridad, independientemente de si dichos archivos han cambiado desde la última copia de seguridad incremental.

A diferencia de la copia de seguridad incremental, una copia de seguridad selectiva:

- No provoca que el servidor actualice la fecha y la hora de la última copia incremental.
- Realiza copias de seguridad de entradas de archivos y directorios aunque el tamaño, indicación de la hora de modificación o los permisos no hayan cambiado.
- No hace caducar los archivos suprimidos.

- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.

**Tareas relacionadas:**

 Sistemas operativos Windows Copia de seguridad de datos mediante la GUI  
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad de datos mediante la GUI Java

**Referencia relacionada:**










































Selective

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

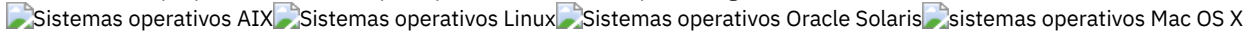



## Realización de una copia de seguridad incremental selectiva o incremental por fecha (UNIX y Linux)

Es posible que el administrador haya establecido planificaciones para realizar automáticamente copias de seguridad de archivos de la estación de trabajo. En los apartados siguientes se indica cómo realizar copias de seguridad sin utilizar una planificación.

Existen dos tipos de copia de seguridad incremental: *incremental completa* e *incremental parcial*.

-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Copia de seguridad incremental completa y parcial  
Una copia de seguridad incremental sólo copia los archivos nuevos y modificados. El tipo de copia de seguridad incremental depende de los objetos que selecciona para realizar la copia de seguridad.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Copia de seguridad incremental por fecha  
Para que un sistema de archivos sea elegible para copias de seguridad incrementales por fecha, debe haberse realizado como mínimo una copia de seguridad incremental completa de todo el sistema de archivos. Si ejecuta una copia de seguridad incremental de sólo una rama de directorios o un archivo individual, el sistema de archivos no será elegible para realizar copias de seguridad incrementales por fecha.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales  
Los métodos incrementales por fecha, con registro por diario y diferenciales de instantánea de NetApp son alternativas a los métodos de copia de seguridad incremental completa y parcial.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Copia de seguridad diferencial de la instantánea con una conexión HTTPS  
Puede utilizar una conexión segura HTTPS para que el cliente de archivado y copia de seguridad se comuniquen con un archivador NetApp durante una copia de seguridad diferencial de una instantánea.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Copia de seguridad selectiva  
Utilice la copia de seguridad selectiva para realizar copias de seguridad de archivos específicos o directorios independientemente de si ya existe una copia de seguridad de dichos archivos en el servidor.
-  Sistemas operativos Oracle Solaris Zona global Solaris y copias de seguridad de zonas no globales  
Para zonas de Solaris, realice copias de seguridad selectivas e incrementales de sistemas de archivos dentro de la zona en la que se han creado dichos sistemas de archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Cómo guardar permisos de acceso  
Al realizar copias de seguridad de archivos, el cliente de copia de seguridad y archivado también guarda los permisos de acceso UNIX estándar asignados a los archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Establecimiento de un punto de montaje virtual  
Si es un usuario autorizado y desea realizar copias de seguridad de archivos que empiecen por un directorio específico del sistema de archivos, puede definir dicho directorio como punto de montaje virtual.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copia de seguridad de datos mediante la GUI Java  
Puede realizar copias de seguridad de archivos específicos, de directorios enteros o de sistemas de archivos enteros del árbol de directorios.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copia de seguridad de datos mediante la línea de mandatos  
Puede utilizar los mandatos incremental o selective para realizar copias de seguridad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Supresión de datos de copia de seguridad  
Si el administrador le ha otorgado autorización, puede suprimir copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos. Para determinar si tiene esta autorización, seleccione Archivo > Información de

conexión en la GUI de cliente de copia de seguridad y archivado o en el menú principal del cliente web. El estado de la autorización se proporciona en el campo Suprimir archivos de copia de seguridad.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Supresión de espacios de archivos





Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor. Cuando se suprime un espacio de archivos, está suprimiendo todos los archivos y las imágenes, tanto las versiones de copia de seguridad como las de copias archivadas que hay en ese espacio de archivos. Por ejemplo, si suprime el espacio de archivos /tmp, está suprimiendo todas las copias de seguridad de cada uno de los archivos de ese sistema de archivos y de cada uno de los archivos que ha archivado desde ese sistema de archivos. Considere detenidamente si desea suprimir un espacio de archivos.


#### Tareas relacionadas:

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar






## Copia de seguridad incremental completa y parcial






Una copia de seguridad incremental sólo copia los archivos nuevos y modificados. El tipo de copia de seguridad incremental depende de los objetos que selecciona para realizar la copia de seguridad.






 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si selecciona los sistemas de archivos completos, la copia de seguridad es una copia de seguridad incremental completa. Si selecciona un árbol de directorio o archivos individuales, la copia de seguridad es una copia de seguridad incremental parcial.


 Sistemas operativos Windows Si selecciona las unidades completas, la copia de seguridad es una copia de seguridad incremental completa. Si selecciona un árbol de directorio o archivos individuales, la copia de seguridad es una copia de seguridad incremental parcial.

La primera vez que se ejecuta una copia de seguridad incremental completa, el cliente de copia de seguridad y archivado realiza una copia de seguridad de todos los archivos y directorios que especifique. La operación de copia de seguridad puede llevar mucho tiempo si el número de archivos es grande o si uno o más archivos grandes deben copiarse. Las posteriores copias de seguridad incrementales completas sólo realizan copias de seguridad de los archivos nuevos y modificados. El servidor de copia de seguridad mantiene las versiones actuales de sus archivos sin tener que perder tiempo o espacio realizando la copia de seguridad de los archivos que existen en el almacenamiento del servidor de IBM Spectrum Protect.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Dependiendo de las políticas de gestión de almacenamiento, es posible que el servidor de IBM Spectrum Protect tenga más espacio que una versión de sus archivos en el almacenamiento. Las últimas copias de seguridad realizadas son versiones de copia de seguridad activas. Las copias de archivos más antiguas son versiones inactivas. Sin embargo, si suprime un archivo de la estación de trabajo, la siguiente copia de seguridad incremental completa hace que la versión de copia de seguridad activa del archivo pase a ser inactiva. Puede restaurar la versión inactiva de un archivo. El número de versiones inactivas que mantiene el servidor y cuánto tiempo se gobiernan mediante las políticas de gestión definidas por el administrador del servidor de IBM Spectrum Protect. Las versiones activas representan los archivos que existían en el sistema de archivos cuando se realizó la última copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para iniciar una copia de seguridad incremental completa o parcial mediante la GUI del cliente, seleccione Backup, y después seleccione la opción Incremental (complete). Desde la línea de mandatos, utilice el mandato incremental y especifique los sistemas de archivos, los árboles del directorio o los archivos individuales que se incluyen en la copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Durante una copia de seguridad incremental, el cliente consulta al servidor o la base de datos de diario para determinar cuál es el estado exacto de los archivos desde la última copia de seguridad incremental realizada. El cliente utiliza esta información para las siguientes tareas:





- Realizar copias de seguridad de archivos nuevos.
- Realizar copias de seguridad de archivos cuyo contenido ha cambiado desde la última copia de seguridad.
-  Sistemas operativos Windows Se realiza la copia de seguridad de los archivos cuando cualquiera de los siguientes atributos cambia:
  - Tamaño del archivo
  - Fecha u hora de la última modificación
  - Atributos ampliados
  - La lista de control de accesos.
  - Atributos de archivo esparcido, de punto de reanálisis o cifrado.
  - Descriptores de seguridad del archivo NTFS o ReFS: identificador de seguridad del propietario (SID), SID de grupo, Lista de control de acceso discrecional (ACL), y ACL de sistema.

- Atributos de directorios

Si los siguientes atributos cambian, los atributos se actualizan en el servidor de IBM Spectrum Protect, pero no se realiza la copia de seguridad del archivo:

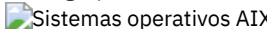
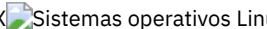
- Solo lectura o lectura y grabación
- Oculto o descubierto
- Comprimido o no comprimido

IBM Spectrum Protect no examina el atributo de archivo al determinar los archivos modificados.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Se realiza la copia de seguridad de los archivos cuando cualquiera de los siguientes atributos cambia:

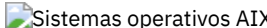
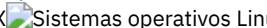
- Tamaño del archivo
- Fecha u hora de la última modificación
- Atributos ampliados
- La lista de control de accesos.


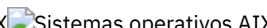
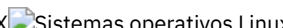
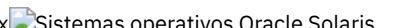
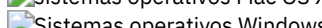
Si los siguientes atributos cambian, los atributos se actualizan en el servidor de IBM Spectrum Protect, pero no se realiza la copia de seguridad del archivo:





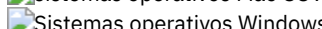
- Propietario del archivo
- Permisos del archivo
- Inodo
- ID de grupo
-  Sistemas operativos AIX  Sistemas operativos Linux Atributo de hora del cambio (`ctime`) (sólo para objetos en sistemas de archivos GPFS y si la opción `updatectime` está establecida en yes). Para obtener más información, consulte la opción `updatectime`.
- Ubicación del icono (sólo Mac OS X)
- Tipo o creador (sólo Mac OS X)

- Realizar copias de los directorios.

Se realiza una copia de seguridad de un directorio en cualquiera de las siguientes circunstancias:

- No se ha realizado una copia de seguridad previa del directorio.
- Los permisos del directorio han cambiado desde la última copia de seguridad.
- El directorio de la lista de control de acceso ha cambiado desde la última copia de seguridad.
- El directorio de atributos ampliados ha cambiado desde la última copia de seguridad.
-  Sistemas operativos AIX  Sistemas operativos Linux El atributo de cambio de hora (`ctime`) se actualiza desde la última copia de seguridad (sólo para sistemas de archivos GPFS). Para obtener más información, consulte la opción `updatectime`.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Los directorios se enumeran de acuerdo con el número de objetos de copia de seguridad. Para excluir directorios y el contenido de los mismos del proceso de copia de seguridad, utilice la opción `exclude.dir`.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Hacer caducar las versiones de copia de seguridad de los archivos del servidor que no tienen archivos correspondientes en la estación de trabajo. El resultado es que los archivos que ya no existen en la estación de trabajo no tienen versiones de copia de seguridad activas en el servidor. Sin embargo, las versiones inactivas se conservan en función de las reglas definidas por el administrador de IBM Spectrum Protect.
- Volver a vincular las versiones de copia de seguridad si han cambiado las asignaciones de clase de gestión. Sólo volverán a enlazarse los objetos que tengan versiones de copia de seguridad activas. Los objetos para los que sólo existan versiones de copia de seguridad inactivas no volverán a enlazarse.

Durante una operación de copia de seguridad incremental, los objetos se vuelven a enlazar o caducan de la siguiente manera:





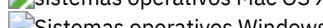
Si la especificación de archivo coincide con todos los archivos en una vía de acceso:

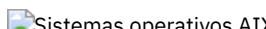
El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Éste sería el caso de un mandato incremental como `dsmc incr c:\mydir\* -subdir=yes`.

Si la especificación de archivo no coincide con todos los archivos en una vía de acceso:

El reenlace y la caducidad se produce para todas las versiones de copia de seguridad seleccionables que coinciden con la especificación de archivo. Sin embargo, las versiones de copia de seguridad seleccionables no caducan ni se vuelven a enlazar si se encuentran en un directorio que ya no existe en el sistema de archivos del cliente.

Pongamos por ejemplo un mandato incremental como `dsmc incr c:\mydir\*.txt -subdir=yes`. Supongamos que algunos archivos en `c:\mydir\` no tienen el tipo de archivo `txt`. El reenlace y la caducidad sólo se produce para archivos que coinciden con la especificación `*.txt` y cuyos directorios aún existen en el sistema de archivos del cliente.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Puede utilizar la opción `preserveaccessdate` para especificar si va a modificar la última fecha de acceso después de realizar una operación de copia de seguridad o archivado. De forma predeterminada, la fecha de acceso cambia después de una operación de copia de seguridad o archivado predeterminada.

-  Sistemas operativos AIX Copia de seguridad basada en el diario en AIX y Linux

La copia de seguridad con registro por diario es un método alternativo de copia de seguridad que utiliza un diario de cambios








mantenido por el proceso del daemon de registro por diario de IBM Spectrum Protect.

**Conceptos relacionados:**

Políticas de gestión de almacenamiento

**Referencia relacionada:**


Opciones exclude

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows *Preservelastaccessdate*  
 Sistemas operativos AIX  Sistemas operativos Linux *Updatectime*

## Copia de seguridad incremental por fecha

---

Para que un sistema de archivos sea elegible para copias de seguridad incrementales por fecha, debe haberse realizado como mínimo una copia de seguridad incremental completa de todo el sistema de archivos. Si ejecuta una copia de seguridad incremental de sólo una rama de directorios o un archivo individual, el sistema de archivos no será elegible para realizar copias de seguridad incrementales por fecha.

 Sistemas operativos Windows Para realizar una copia de seguridad incremental por fecha mediante la utilización de la GUI, seleccione la opción incremental (sólo por fecha) del menú desplegable *Tipo de copia de seguridad* o bien utilice la opción *incrbydate* con el mandato incremental.








El cliente realiza una copia de seguridad sólo de aquellos archivos cuya fecha y hora de modificación es posterior a la fecha y hora de la última copia de seguridad incremental del sistema de archivos en el que se encuentra el archivo. Los archivos que agregue el cliente después de la última copia de seguridad incremental, pero cuya fecha de modificación sea anterior a la última copia de seguridad incremental, no se incluyen en la operación de copia de seguridad.

Los archivos cuyo nombre se ha cambiado después de la última copia de seguridad incremental, pero que no se han modificado, no se incluirán en la copia de seguridad. El cambio de nombre de un archivo no hace cambiar la fecha ni la hora de modificación del archivo. No obstante, si se cambia el nombre de un archivo sí se cambia la fecha de modificación del directorio en el que se encuentra. En este caso, se hace la copia de seguridad del directorio, pero no de los archivos que contiene.

Si ejecuta una copia de seguridad incremental por fecha de todo un sistema de archivos, el servidor actualiza la fecha y hora de la última copia de seguridad incremental. Si efectúa una copia de seguridad incremental por fecha sólo en una parte de un sistema de archivos, el servidor no actualiza la fecha de la última copia de seguridad incremental completa. En este caso, la siguiente copia de seguridad incremental por fecha vuelve a copiar estos archivos.

Nota: A diferencia de la copia de seguridad incremental, la copia de seguridad incremental por fecha no hace caducar los archivos suprimidos o vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.

**Tareas relacionadas:**

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris *Copia de seguridad de datos mediante la GUI Java*  
 Sistemas operativos Windows  Sistemas operativos AIX  Sistemas operativos Linux

## Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales






---






Los métodos incrementales por fecha, con registro por diario y diferenciales de instantánea de NetApp son alternativas a los métodos de copia de seguridad incremental completa y parcial.

**Copia de seguridad incremental por fecha**




Una copia incremental por fecha tarda menos tiempo en procesarse que una copia incremental completa y requiere menos memoria.

Puede ser que una copia de seguridad incremental por fecha no coloque exactamente los mismos archivos de copia de seguridad en el almacenamiento del servidor, ya que la copia de seguridad incremental por fecha:




-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No hace caducar las versiones de copia de seguridad de aquellos archivos que se han suprimido de la estación de trabajo.
- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.
- No efectúa copias de seguridad de archivos cuyos atributos cambian, a menos que también se hayan modificado la fecha y la hora de modificación.

-  sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  Sistemas operativos Windows
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión (las copias de seguridad con registro por diario tampoco tienen en cuenta este atributo).



#### Copia de seguridad con registro por diario

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Windows

Los requisitos de memoria para un entorno de registro por diario inicial son los mismos que los requisitos de memoria necesarios para una copia de seguridad incremental de espacio de archivos completa, pues las copias de seguridad con registro por diario deben completar la copia de seguridad incremental de espacio de archivos completa para poder establecer la base de datos de diario como válida y para poder establecer la línea de base para el registro por diario.



 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Windows

Los requisitos de memoria para las posteriores copias de seguridad con registro por diario serán mucho menores. Las sesiones de copia de seguridad con registro por diario se ejecutan en paralelo y las rige la opción de cliente resourceutilization, de la misma forma que las sesiones de copia de seguridad normales. El tamaño del archivo de base de datos de diario vuelve a adquirir un tamaño mínimo (menos de 1 KB) cuando se ha suprimido la última entrada del diario. Puesto que las entradas se suprimen del diario a medida que el cliente las procesa, el tamaño de disco que ocupa el diario debería ser el mínimo después de haberse realizado una copia de seguridad con registro por diario completa. Una copia de seguridad incremental completa con el registro por diario activo necesita menos tiempo para procesarse que una copia de seguridad incremental por fecha.



 Sistemas operativos AIX
  Sistemas operativos Linux

En AIX y Linux, la copia de seguridad con registro por diario tiene algunas limitaciones. Para obtener más información, consulte el apartado Copia de seguridad basada en el diario en AIX y Linux.

#### Diferencial de instantánea de NetApp

 Sistemas operativos Linux
  Sistemas operativos Windows


Para servidores de archivos NAS y N-Series que se ejecuten en ONTAP 7.3.0, o superior, puede utilizar la opción snapdiff para invocar la copia de seguridad de diferencia de instantáneas NetApp cuando se realice una copia incremental de volumen completa. Esta opción reduce el uso de memoria y es más rápida.

 Sistemas operativos Linux
  Sistemas operativos Windows

Tenga en cuenta las siguientes limitaciones cuando ejecute una copia de seguridad incremental de volúmenes completos mediante la opción snapdiff para garantizar que se realiza una copia de seguridad de los datos en el momento adecuado.

- Un archivo se excluye debido a una regla de exclusión en el archivo de inclusión/exclusión. El cliente realiza una copia de seguridad de la instantánea actual con la regla de exclusión en vigor. Esto ocurre cuando no se han realizado cambios en el archivo, pero se ha eliminado la regla que excluía el archivo. NetApp no detecta este cambio de inclusión/exclusión, porque sólo detecta los cambios de los archivos entre dos instantáneas.
- Si ha añadido una sentencia de inclusión en el archivo de opciones, esta opción de inclusión solo entra en vigor cuando NetApp detecta que el archivo se ha modificado. El cliente no inspecciona cada uno de los archivos del volumen durante la copia de seguridad.
- Si ha utilizado el mandato dsmc delete backup para suprimir explícitamente un archivo del inventario de IBM Spectrum Protect, NetApp no puede detectar que se ha eliminado manualmente un archivo del almacenamiento de IBM Spectrum Protect. Por consiguiente, el archivo sigue sin protección en el almacenamiento de IBM Spectrum Protect hasta que se cambia en el volumen y NetApp detecta el cambio, señalando al cliente que vuelva a hacer una copia de seguridad del mismo.
- Los cambios de políticas como, por ejemplo, de mode=modified a mode=absolute no se detectan.
- El espacio de archivo entero se suprime del inventario IBM Spectrum Protect. Esta acción provoca que la opción snapdiff cree una instantánea para utilizar como origen y una copia de seguridad incremental completa para ejecutarse.


El software de NetApp determina qué es un objeto cambiado, no IBM Spectrum Protect.

 Sistemas operativos Linux


Si ejecuta una copia de seguridad de volumen completa de un NFS-mounted NetApp o N-Series, es posible que también se realice una copia de seguridad de todas las instantáneas del directorio de instantáneas.


Para evitar realizar la copia de seguridad de todas las instantáneas del directorio de instantánea realice una de las siguientes acciones:

- Ejecutar copias de seguridad NDMP
  - Ejecutar copias de seguridad utilizando la opción snapshotroot
  - Ejecutar copias de seguridad incrementales utilizando la opción snapdiff
- Consejo: Si ejecuta una copia de seguridad incremental mediante la opción snapdiff y planifica copias de seguridad incrementales periódicas, utilice la opción createnewbase=yes junto con la opción snapdiff para crear una instantánea base y utilizarla como origen para ejecutar una copia de seguridad incremental.

- Excluir el directorio de instantáneas desde las copias de seguridad.
-  Sistemas operativos Linux
- En sistemas Linux, el directorio de instantáneas está en .snapshot.

Nota: En algunas versiones de Red Hat Linux, no se realiza una copia de seguridad del directorio .snapshot, por lo que no necesita excluirlo.

 Sistemas operativos Windows En sistemas Windows, el directorio de instantáneas está en ~snapshot.

 Sistemas operativos Linux

## Copia de seguridad diferencial de la instantánea con una conexión HTTPS

---

Puede utilizar una conexión segura HTTPS para que el cliente de archivado y copia de seguridad se comuniquen con un archivador NetApp durante una copia de seguridad diferencial de una instantánea.





El protocolo HTTPS está habilitado en los archivadores NetApp de forma predeterminada y no puede desactivarse.

Cuando ejecuta una copia de seguridad diferencial de instantánea, el cliente de archivado y copia de seguridad establece una sesión administrativa con un archivador NetApp. Las credenciales del archivador, como el nombre de host del archivador o la dirección IP, el nombre de usuario que se utiliza para conectar el archivador y la contraseña del archivador se almacenan localmente en el cliente de archivado y copia de seguridad. Esta información debe transmitirse al archivador para establecer la sesión administrativa autenticada. Es importante utilizar una conexión segura porque autenticar la sesión del archivador administrativo requiere que el cliente transmita la contraseña del archivador en texto claro.


Para establecer una conexión segura mediante el protocolo de comunicación HTTPS, debe utilizar la opción `snapdiffhttps` cuando ejecuta una copia de seguridad diferencial de instantánea. Sin la opción `snapdiffhttps`, el cliente de archivado y copia de seguridad puede establecer sesiones de gestor de archivos solo con el protocolo HTTP, que requeriría acceso administrativo HTTP para habilitarse en el gestor de archivos. Con la opción `snapdiffhttps`, puede establecer una sesión de administración segura con el archivador NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador NetApp.

Restricciones:

Las siguientes restricciones se aplican a copias de seguridad diferencias instantáneas con HTTPS:


- La conexión HTTPS sólo se utiliza para transmitir datos de forma segura a través de la sesión de administración entre el cliente de archivado y copia de seguridad y el archivador de NetApp. Los datos de la sesión de administración incluyen información como credenciales del archivador, información de instantánea y los nombres de archivo y los atributos que se generan mediante el proceso de diferenciación de instantáneas. La conexión HTTPS no se utiliza para transmitir datos de archivos normales a los que se accede en el archivador mediante el cliente a través de la compartición de archivos. La conexión HTTPS tampoco se aplica a los datos de archivos normales transmitidos mediante el cliente al servidor de IBM Spectrum Protect a través del protocolo cliente/servidor de IBM Spectrum Protect normal.
- La opción `snapdiffhttps` no se aplica a vFilers porque el protocolo HTTPS no está admitido en NetApp vFiler.
- La opción `snapdiffhttps` sólo está disponible utilizando la interfaz de línea de mandatos. No está disponible para su utilización con la GUI del cliente de archivado de copia de seguridad.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS  
Cuando ejecuta una copia de seguridad diferencial de una instantánea, puede utilizar la opción `snapdiffhttps` para crear una conexión HTTPS segura entre el cliente de archivado y copia de seguridad y el archivador NetApp.


### Conceptos relacionados:

 Sistemas operativos Windows Comparación de copias de seguridad incrementales por fecha, con registro por diario y copias de seguridad diferenciales de instantánea de NetApp con las copias de seguridad incrementales completas y parciales

### Tareas relacionadas:

Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea

 Sistemas operativos Windows Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS

 Sistemas operativos Linux Ejecutar una instantánea de la copia de seguridad diferencial con una conexión HTTPS

### Referencia relacionada:

`Snapdiffhttps`

`Snapdiff`

## Copia de seguridad selectiva

---

Utilice la copia de seguridad selectiva para realizar copias de seguridad de archivos específicos o directorios independientemente de si ya existe una copia de seguridad de dichos archivos en el servidor.

Las copias de seguridad incrementales suelen formar parte de un sistema automatizado para hacer copia de seguridad de todos los sistemas de archivos. Por el contrario, las copias de seguridad selectivas permiten seleccionar manualmente un juego de archivos de








los que se debe realizar una copia de seguridad, independientemente de si dichos archivos han cambiado desde la última copia de seguridad incremental.

A diferencia de la copia de seguridad incremental, una copia de seguridad selectiva:

- No provoca que el servidor actualice la fecha y la hora de la última copia incremental.
- Realiza copias de seguridad de entradas de archivos y directorios aunque el tamaño, indicación de la hora de modificación o los permisos no hayan cambiado.
- No hace caducar los archivos suprimidos.
- No vuelve a vincular las versiones de copia de seguridad a una nueva clase de gestión si ésta se ha modificado.


**Tareas relacionadas:**

 Sistemas operativos WindowsCopia de seguridad de datos mediante la GUI

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle SolarisCopia de seguridad de datos mediante la GUI Java

**Referencia relacionada:**

Selective

 Sistemas operativos Oracle Solaris

## Zona global Solaris y copias de seguridad de zonas no globales

---

Para zonas de Solaris, realice copias de seguridad selectivas e incrementales de sistemas de archivos dentro de la zona en la que se han creado dichos sistemas de archivos.

Trate cada zona no global como un sistema independiente que tiene su propio nombre de nodo de IBM Spectrum Protect y que ejecuta copias de seguridad desde dentro de cada una de las zonas.

Si ejecuta copias de seguridad incrementales o selectivas de zonas no globales desde la zona no global, el administrador de la zona global debe decidir qué archivos de la zona no global deben incluirse o excluirse de las copias de seguridad. Por ejemplo, los archivos kernel, de sistema o dispositivo de las zonas no globales no se excluyen automáticamente de las copias de seguridad, pero no debe realizarse ninguna copia de seguridad de los mismos. La restauración de tales archivos puede inutilizar una zona no global.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Cómo guardar permisos de acceso

---

Al realizar copias de seguridad de archivos, el cliente de copia de seguridad y archivado también guarda los permisos de acceso UNIX estándar asignados a los archivos.

En función del sistema operativo, también guarda permisos ampliados. Por ejemplo, para archivos de una estación de trabajo AIX, el cliente guarda listas de control de accesos.

Un usuario autorizado puede realizar copias de seguridad para otro usuario, sin que ello provoque conflictos de propiedad. El servidor de copia de seguridad registra que el archivo pertenece al propietario original. No es necesario que el usuario autorizado conceda al usuario original acceso a las versiones de copia de seguridad.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris





## Establecimiento de un punto de montaje virtual

---

Si es un usuario autorizado y desea realizar copias de seguridad de archivos que empiecen por un directorio específico del sistema de archivos, puede definir dicho directorio como punto de montaje virtual.

Al definir un punto de montaje virtual en un sistema de archivos, se proporciona una vía de acceso directa a los archivos de los que se desea realizar una copia de seguridad, lo que ahorra tiempo de proceso. Es más eficaz que definir el sistema de archivos con la opción domain y utilizar posteriormente una opción exclude para excluir los archivos que no desea que se tengan en cuenta para la copia de seguridad. También permite almacenar copias de seguridad y copias archivadas de directorios específicos en espacios de archivos de almacenamiento separados.

**Referencia relacionada:**

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Virtualmountpoint

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad de datos mediante la GUI Java

---

Puede realizar copias de seguridad de archivos específicos, de directorios enteros o de sistemas de archivos enteros del árbol de directorios.

### Acerca de esta tarea

---

Puede localizar los archivos de los que desea realizar una copia de seguridad mediante las operaciones de búsqueda y filtrado. El filtrado muestra sólo los archivos que coinciden con los criterios de filtrado de la operación de copia de seguridad.

Utilice la GUI Java™ del cliente de copia de seguridad y archivado para realizar copias de seguridad de los datos tal como se indica a continuación:

### Procedimiento

---

1. Pulse **Copia de seguridad** en la ventana IBM Spectrum Protect. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios si es preciso. Pulse las casillas situadas junto al objeto u objetos de los que desea realizar la copia de seguridad. Para buscar o filtrar archivos, pulse el icono **Buscar** de la barra de herramientas.
3. Escriba los criterios de búsqueda en la ventana Buscar archivos (Copia de seguridad).
4. Pulse el botón **Buscar**. Aparecerá la ventana Archivos coincidentes (Copia de seguridad).
5. Pulse las casillas situadas junto a los archivos de los que desea realizar la copia de seguridad y cierre la ventana Archivos coincidentes (Copia de seguridad).
6. Escriba los criterios de filtrado en la ventana Buscar archivos (Copia de seguridad).
7. Pulse el botón **Filtrar**. La ventana Copia de seguridad muestra los archivos filtrados.
8. Pulse las casillas situadas junto a los archivos o directorios filtrados de los que desea realizar la copia de seguridad.
9. Seleccione uno de los tipos de copia de seguridad siguientes del menú desplegable: (1) Para efectuar una copia de seguridad incremental, pulse **Incremental (completa)**, (2) Para ejecutar una copia de seguridad incremental por fecha, pulse **Incremental (sólo por fecha)**, (3) Para efectuar una copia de seguridad selectiva, pulse **Hacer siempre copia de seguridad**.
10. Pulse **Copia de seguridad**. La ventana **Lista de tareas** de copia de seguridad muestra el estado del proceso de la copia de seguridad.

### Resultados

---

Tenga en cuenta los siguientes elementos cuando haga copia de seguridad de sus datos mediante la GUI de Java.

- Si desea modificar opciones de copia de seguridad específicas, pulse el botón **Opciones**. Las opciones que seleccione estarán en vigor *únicamente* durante la sesión actual.
- IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor. Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión utilizada es una clase de gestión predeterminada seleccionada o la que el usuario asigne al archivo con la opción **include** en la lista de opciones de inclusión/exclusión. Seleccione **Programas de utilidad** → **Ver información de políticas** en la GUI Java del cliente de copia de seguridad/archivado o en la GUI del cliente web para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para su nodo cliente.
- Para realizar una copia de seguridad incremental automática del dominio predeterminado, seleccione **Acciones** → **Copia de seguridad del dominio**. El dominio predeterminado tiene establecida la opción **domain** en el archivo de opciones del usuario cliente (dsm.opt). Si la opción **domain** no está establecida, el dominio predeterminado comprende *todos los sistemas de archivos locales*.
- Puede utilizar el editor de preferencias para excluir del proceso de copia de seguridad sistemas de archivos del dominio predeterminado.

#### Conceptos relacionados:

Políticas de gestión de almacenamiento

#### Referencia relacionada:

Domain

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad de datos mediante la línea de mandatos

---

Puede utilizar los mandatos incremental o selective para realizar copias de seguridad.

En la siguiente tabla se muestran ejemplos de utilización de estos mandatos para realizar diferentes tareas.

Tabla 1. Ejemplos de copia de seguridad desde la línea de mandatos

Tarea	Mandato	Consideraciones
<i>Copias de seguridad incrementales</i>		
Realizar una copia de seguridad incremental del dominio del cliente.	<code>dsmc incremental</code>	Consulte el apartado Incremental para obtener más información sobre el mandato incremental.
Realizar una copia de seguridad de los sistemas de archivos /fs1 y /fs2 además de los sistemas de archivos /home, /usr, y /datasave definidos en el dominio de cliente.	<code>dsmc incremental -domain="/fs1 /fs2"</code>	Consulte el apartado Domain para obtener más información sobre la opción domain.
Realizar una copia de seguridad de los sistemas de archivos /Volumes/fs1 y /Volumes/fs2 además de los volúmenes definidos en el dominio de cliente.	<code>dsmc incremental -domain="/Volumes/fs1 /Volumes/fs2"</code>	Consulte el apartado Domain para obtener más información sobre la opción domain.
Realizar una copia de seguridad de todos los sistemas de archivos locales definidos en el dominio de cliente salvo el sistema de archivos /home.	<code>dsmc incremental -domain="all-local -/home"</code>	No es posible utilizar el operador (-) delante de la palabra clave de dominio all-local. Para obtener más información, consulte el apartado Domain. Para Los clientes Windows también pueden excluir el dominio del estado del sistema del proceso de copia de seguridad de este modo.
Realizar la copia de seguridad de los sistemas de archivos /fs1 y /fs2.	<code>dsmc incremental /fs1 /fs2</code>	Ninguna
Realizar una copia de seguridad de los archivos del directorio /home y todos sus subdirectorios.	<code>dsmc incremental /home/ -subdir=yes</code>	Consulte el apartado Subdir para obtener más información sobre la opción subdir.
Realizar una copia de seguridad de todos los archivos del directorio /Users y todos sus subdirectorios.	<code>dsmc incremental /Users/ -subdir=yes</code>	Consulte el apartado Subdir para obtener más información sobre la opción subdir.
Ejecutar una copia de seguridad incremental, dándose por supuesto que ha iniciado una instantánea del sistema de archivos /usr y que ha montado la instantánea como /snapshot/day1, de todos los archivos y directorios de la instantánea local y gestionar éstos en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos /usr.	<code>dsmc incremental /usr -snapshotroot=/snapshot/day1</code>	El cliente de copia de seguridad y archivado considera el valor de snapshotroot como el nombre del espacio de archivos. Para obtener más información, consulte el apartado Snapshotroot.
<i>Copia de seguridad incremental por fecha</i>		
Realizar una copia de seguridad incremental por fecha del dominio de cliente predeterminado.	<code>dsmc incremental -incrbydate</code>	Utilice la opción incrbydate con el mandato incremental para hacer una copia de seguridad de los archivos nuevos y modificados con una fecha de modificación posterior a la de la última copia de seguridad incremental almacenada en el servidor. Consulte el apartado Incrbydate para obtener más información sobre la opción incrbydate.
<i>Copias de seguridad selectivas</i>		

Tarea	Mandato	Consideraciones
Realizar una copia de seguridad del directorio /home/proj o /Users/van/Documents.	dsmc selective /home/proj/ o dsmc selective /Users/van/Documents/	Utilizar el mandato selective para hacer copia de seguridad de archivos o directorios específicos sin tener en cuenta si han cambiado desde la última copia de seguridad incremental. Puede utilizar caracteres comodín para realizar una copia de seguridad de varios archivos a la vez. Consulte el apartado Selective para obtener más información sobre el mandato selective.
Realizar una copia de seguridad de todos los archivos del directorio /home/proj y todos sus subdirectorios.	dsmc selective /home/proj/ -subdir=yes	Si especifica -subdir=yes al realizar una copia de seguridad de un vía de acceso y archivo específico, el cliente realiza la copia de seguridad de todos los subdirectorios de esta vía de acceso y de todas las instancias del archivo especificado que existan bajo cualquiera de estos subdirectorios.  Si un subdirectorio es un sistema de archivos montado, el cliente no realiza la copia de seguridad de los archivos de dicho subdirectorio si se utiliza la opción subdir=yes. Consulte el apartado Subdir para obtener más información sobre la opción subdir.
Realizar una copia de seguridad de todos los archivos del directorio /Users/van/Documents y todos sus subdirectorios.	dsmc selective /Users/van/Documents/ -subdir=yes	Si especifica -subdir=yes al realizar la copia de seguridad de una vía de acceso y archivo específicos, el cliente realiza una copia de seguridad de forma recursiva de todos los subdirectorios de esa vía de acceso, y todas las instancias del archivo especificado que existen en todos esos subdirectorios.  Si un subdirectorio es un sistema de archivos montado, el cliente no realiza la copia de seguridad de los archivos de dicho subdirectorio si se utiliza la opción subdir=yes. Consulte el apartado Subdir para obtener más información sobre la opción subdir.
Realizar una copia de seguridad de los archivos /home/dir1/h1.doc y /home/dir1/test.doc.	dsmc selective /home/dir1/h1.doc /home/dir1/test.doc	Si especifica la opción removeoperandlimit con los mandatos incremental o selective, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo. Esto permite especificar más de 20 archivos en un único mandato. Consulte el apartado Removeoperandlimit para obtener más información acerca de esta opción.
Realizar una copia de seguridad de los archivos /Users/ann/Documents/h1.doc y /Users/ann/Documents/test.doc.	dsmc selective /Users/ann/Documents/h1.doc /Users/ann/Documents/test.doc	Si especifica la opción removeoperandlimit con los mandatos incremental o selective, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo. Esto permite especificar más de 20 archivos en un único mandato. Consulte el apartado Removeoperandlimit para obtener más información acerca de esta opción.
Realizar una copia de seguridad de una lista de archivos del archivo /home/filelist.txt.	selective -filelist=/home/filelist.txt	Utilice la opción filelist para procesar una lista de archivos. Para obtener más información, consulte el apartado Filelist.
Realizar una copia de seguridad de todos los archivos indicados en el archivo /Users/filelist.txt.	dsmc selective -filelist=/Users/filelist.txt	Utilice la opción filelist para procesar una lista de archivos. Para obtener más información, consulte el apartado Filelist.

Tarea	Mandato	Consideraciones
Suponiendo que ha iniciado una instantánea del sistema de archivos /usr y ha montado la instantánea como /snapshot/day1, ejecute una copia de seguridad selectiva del árbol de directorios /usr/dir1/sub1 desde la instantánea local y gestiónelo en el servidor de IBM Spectrum Protect debajo del nombre de espacio de archivos /usr.	dsmc selective /usr/dir1/sub1/ - subdir=yes - snapshotroot=/snapshot/day1	El cliente considera el valor de snapshotroot como el nombre del espacio de archivos. Para obtener más información, consulte el apartado Snapshotroot.

**Referencia relacionada:**

Incremental

Selective

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Supresión de datos de copia de seguridad

Si el administrador le ha otorgado autorización, puede suprimir copias de seguridad individuales del servidor de IBM Spectrum Protect sin suprimir todo el espacio de archivos. Para determinar si tiene esta autorización, seleccione Archivo > Información de conexión en la GUI de cliente de copia de seguridad y archivado o en el menú principal del cliente web. El estado de la autorización se proporciona en el campo Suprimir archivos de copia de seguridad.

### Acerca de esta tarea

**Importante:** si suprime archivos de copia de seguridad, **no podrá restaurarlos**. Antes de suprimirlos, verifique que los archivos de copia de seguridad ya no sean necesarios. El cliente le solicitará si desea continuar con la operación de supresión. Si especifica *Sí*, los archivos de copia de seguridad especificados se suprimirán inmediatamente y se eliminarán del almacenamiento del servidor de IBM Spectrum Protect.

Para suprimir copias de seguridad mediante la GUI de cliente de copia de seguridad y archivado o el cliente web:

### Procedimiento

1. Seleccione **Suprimir datos de copia de seguridad** en el menú **Herramientas**. Aparecerá la ventana Supresión de copia de seguridad.
2. Expanda el árbol de directorios pulsando en el signo más (+) o en el icono de carpeta situado junto al objeto que desea expandir.
3. Pulse en las casillas que se encuentran junto a los objetos que desee suprimir.
4. Seleccione un elemento de la lista desplegable que hay junto a la parte superior de la ventana **Supresión de copia de seguridad** para especificar el tipo de supresión de copia de seguridad que desea realizar. Puede suprimir las versiones de copia de seguridad activas, las versiones de copia de seguridad inactivas o todos los objetos que haya seleccionado en el árbol.

### Resultados

Nota:

1. Un directorio solo se suprimirá si selecciona **Suprimir todos los objetos**.
2. Para suprimir copias de seguridad mediante el cliente de línea de mandatos, utilice el mandato delete backup.

**Referencia relacionada:**

Delete Backup

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Supresión de espacios de archivos

Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor. Cuando se suprime un espacio de archivos, está suprimiendo todos los archivos y las imágenes, tanto las versiones de copia de seguridad como las de copias archivadas que hay en ese espacio de archivos. Por ejemplo, si suprime el espacio de archivos /tmp, está suprimiendo todas las copias de seguridad de cada uno de los archivos de ese sistema de archivos y de cada uno de los archivos que ha archivado desde ese sistema de archivos. Considere detenidamente si desea suprimir un espacio de archivos.

## Acerca de esta tarea

---

También puede suprimir un espacio de archivos con el mandato delete filepace. Utilice la opción class con el mandato delete filepace para suprimir espacios de archivos NAS.

Puede suprimir las versiones individuales de copia de seguridad utilizando el mandato delete backup.

Puede suprimir espacios de archivos mediante la GUI del cliente de copia de seguridad y archivado o mediante clientes de línea de mandatos. Para suprimir espacios de archivos NAS, utilice el cliente web o el cliente de línea de mandatos.

Para suprimir un espacio de archivos mediante la GUI, siga estos pasos:

## Procedimiento

---

1. Seleccione Herramientas > Suprimir espacios de archivos en la ventana principal.
2. Pulse en las casillas que se encuentran junto a los espacios de archivos que desea eliminar.
3. Pulse el botón Suprimir. El cliente le pedirá una confirmación antes de eliminarlos.

### Referencia relacionada:

Class

Delete Backup

Delete Filespace

 Sistemas operativos Windows

## Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (Windows)

---

Utilice el mandato backup group para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.

## Acerca de esta tarea

---

Una *copia de seguridad de grupo* crea una copia de seguridad de instante específico coherente de un grupo de archivos que se gestiona como si se tratara de una entidad lógica única:

- Todos los objetos del grupo se asignan a la misma clase de gestión. Utilice la opción include vincular un grupo a una clase de gestión.
- Las sentencias exclude existentes que se aplican a cualquier archivo del grupo se pasan por alto.
- Todos los objetos del grupo se exportan juntos.
- Todos los objetos del grupo caducan al mismo tiempo, tal como se ha especificado en la clase de gestión. Ninguno de los objetos de un grupo caduca hasta que caducan los demás objetos del grupo, incluso cuando caduque otro grupo al que pertenecen.

Una copia de seguridad de grupo se puede agregar a un juego de copias de seguridad.

Puede realizar una copia de seguridad completa o diferencial con la opción mode.

## Procedimiento

---

Especifique el mandato backup group para iniciar una copia de seguridad de grupo.

Por ejemplo, para realizar una copia de seguridad completa de todos los archivos incluidos en el archivo c:\dir1\filelist1 en el espacio de archivos virtual \virtfs, que contiene el archivo de líder de grupo c:\group1, especifique el mandato siguiente:

```
dsmc backup group -filelist=c:\dir1\filelist1 -groupname=group1 -virtualfsname=\virtfs -mode=full
```

### Conceptos relacionados:

Restauración de datos desde un conjunto de copias de seguridad

### Referencia relacionada:

Backup Group

Opciones include

Mode

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad de archivos desde uno o varios espacios de archivos para una copia de seguridad de grupo (UNIX y Linux)

---

Puede utilizar el mandato `backup group` para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos desde uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.

**Restricción:** el mandato `backup group` no se aplica a Mac OS X.

Una *copia de seguridad de grupo* permite crear una copia de seguridad de instante específico coherente de un grupo de archivos que se gestiona como si se tratara de una entidad lógica única:

- Todos los objetos del grupo se asignan a la misma clase de gestión.
- Las sentencias *exclude* existentes que se aplican a cualquier archivo del grupo se pasan por alto.
- Todos los objetos del grupo se exportan juntos.
- Todos los objetos del grupo caducan al mismo tiempo, tal como se ha especificado en la clase de gestión. Ninguno de los objetos de un grupo caduca hasta que caducan los demás objetos del grupo, incluso cuando caduque otro grupo al que pertenecen.

Se puede añadir una copia de seguridad de grupo a un conjunto de copias de seguridad.

Puede realizar una copia de seguridad completa o diferencial mediante la opción `mode`.

Por ejemplo, para realizar una copia de seguridad completa de todos los archivos indicados en el archivo `/home/dir1/filelist1` en el espacio de archivos virtual `/virtfs` que contiene el archivo de líder de grupo `/home/group1`, especifique:

```
dsmc backup group -filelist=/home/dir1/filelist1 -groupname=group1 -virtualfsname=/virtfs -mode=full
```

### Conceptos relacionados:

Restauración de datos desde un conjunto de copias de seguridad

### Referencia relacionada:

Backup Group

Opciones include

Mode

 Sistemas operativos Windows

## Copia de seguridad de datos con soporte de proxy de nodo cliente (Windows)

---

Las copias de seguridad de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

### Antes de empezar

---

Se aplican las siguientes consideraciones cuando utiliza un nodo proxy para realizar una copia de seguridad o restaurar datos en otros nodos:

- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- No puede utilizar `asnodename` con el mandato `backup nas`.
- No puede utilizar `asnodename` con la opción `fromnode`.
- Si utiliza `asnodename` para realizar copias de seguridad y restaurar volúmenes que se encuentran en una configuración de clúster, no utilice `clusternode yes`.
- No puede utilizar `asnodename` para realizar la copia de seguridad o restaurar el estado del sistema.
- Si un nodo de agente restaura los datos de un conjunto de copias de seguridad, no se restaura el objeto de estado del sistema en el conjunto de copias de seguridad.
- Puede utilizar `asnodename` con el mandato `backup image`, pero debe especificar el volumen mediante un nombre UNC. No puede utilizar la letra de unidad.
- Si utiliza los mismos valores `asnodename` para realizar la copia de seguridad de archivos de distintas máquinas, necesitará realizar un seguimiento de qué archivos o volúmenes tienen una copia de seguridad de cada sistema para que pueda restaurarlos en la ubicación correcta.
- Todos los nodos de agente de un entorno de varios nodos deben tener el mismo tipo de plataforma.
- No utilice nodos de destino como nodos tradicionales, especialmente si cifra los archivos antes de hacer una copia de seguridad en el servidor.

## Acerca de esta tarea

---

Un *nodo de agente* es un nodo cliente al que se ha otorgado autorización para realizar operaciones de cliente en nombre de un nodo de destino.

Un *nodo de destino* es un nodo cliente que otorga autorización a uno (o más) nodos agente para realizar operaciones de cliente en su nombre.

La utilización de un nodo de agente para realizar copias de seguridad de nodos de destino resulta útil cuando la estación de trabajo responsable de realizar la copia de seguridad puede cambiar con el tiempo, como sucede con una configuración de clúster.




La opción `asnodename` permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad.

Utilice la opción `asnodename` con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor de IBM Spectrum Protect. Este soporte está sólo disponible con servidores y clientes IBM Spectrum Protect Versión 5.3 y posterior.

## Procedimiento






---

Si desea activar esta opción, realice estos pasos:

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
  2. Registre cada nodo con el servidor de IBM Spectrum Protect, si éste no existe. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.
  3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Éste es el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenarán con el nombre de nodo cuando se utilice la opción `asnodename`.
  4. Otorgue la autorización de proxy a todos los nodos del entorno compartido para acceder al nombre de nodo de destino en el servidor de IBM Spectrum Protect, mediante el uso del mandato `GRANT PROXYNODE` (administrador de IBM Spectrum Protect).
  5. Utilice el mandato de cliente de administración `QUERY PROXYNODE` para visualizar los nodos de cliente del usuario autorizado, otorgados mediante el mandato `GRANT PROXYNODE`.
-  Sistemas operativos WindowsHabilitación de varias operaciones de nodos desde la GUI  
Para habilitar operaciones multinodo en la GUI, utilice el editor Preferencias para especificar el nombre del nodo de destino al que se ha otorgado autoridad de proxy.
  -  Sistemas operativos WindowsConfiguración del cifrado  
En este tema se enumeran los pasos que debe seguir para configurar el cifrado con la opción `encryptkey`.
  -  Sistemas operativos WindowsCopias de seguridad de planificación con soporte de proxy de nodo cliente  
Se pueden utilizar varios nodos para realizar operaciones de copia de seguridad mediante un planificador.

### Referencia relacionada:

`Asnodename`

-  Sistemas operativos Windows
-  sistemas operativos Mac OS X
-  Sistemas operativos AIX
-  Sistemas operativos Linux
-  Sistemas operativos Oracle Solaris

## Habilitación de varias operaciones de nodos desde la GUI

---

Para habilitar operaciones multinodo en la GUI, utilice el editor Preferencias para especificar el nombre del nodo de destino al que se ha otorgado autoridad de proxy.

## Procedimiento

---

1. Compruebe que el nodo cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) mediante el uso del mandato de cliente de administración `QUERY PROXYNODE`.
2. Seleccione `Editar > Preferencias de cliente` para abrir la ventana de preferencias.
3. Seleccione la ficha `General` y rellene el campo `Como nombre de nodo` con el nombre de nodo de destino.
4. Pulse `Aplicar y, a continuación, Aceptar` para cerrar la ventana de preferencias.

## Qué hacer a continuación


---

Realice uno de estos pasos para comprobar que el nodo cliente acceda ahora al servidor como nodo de destino:

- Abra la ventana de árbol y compruebe que aparece el nombre de nodo de destino especificado por el campo `Como nombre de nodo`.
- Compruebe el nombre de nodo de destino del campo `Acceder como nodo` de la ventana `Información de conexión`.



Para volver a la operación de nodo único, suprima Como nombre de nodo desde el campo Acceso como nodo en el separador General > Preferencias.

 Sistemas operativos Windows

## Configuración del cifrado

---

En este tema se enumeran los pasos que debe seguir para configurar el cifrado con la opción `encryptkey`.

### Procedimiento

---

1. Especifique `encryptkey=save` en el archivo de opciones.
2. Realice la copia de seguridad de un archivo como mínimo con `asnode=ProxyNodeName` para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

### Resultados


---

Efectúe estos pasos para configurar el cifrado con la opción `encryptkey=prompt`:

1. Especifique `encryptkey=prompt` en el archivo de opciones.
2. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.

#### Importante:

- Si cambia la clave de cifrado, deberá repetir los pasos anteriores.
- Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

 Sistemas operativos Windows

## Copias de seguridad de planificación con soporte de proxy de nodo cliente

---

Se pueden utilizar varios nodos para realizar operaciones de copia de seguridad mediante un planificador.

### Acerca de esta tarea

---

Cuando se otorga autorización de proxy a los nodos agente, éstos efectúan la operación de copia de seguridad programada en nombre del nodo de destino. Cada nodo agente debe utilizar la opción `asnodename` en su planificación para realizar copias de seguridad de varios nodos para el nodo agente.

Siga estos pasos para activar la planificación de varios nodos:

1. Asegúrese de que todos los nodos agente tengan una autorización de proxy sobre el nodo de destino común
2. Asegúrese de que todos los nodos agente tengan una planificación definida en el servidor:

```
def sched domain_name sched_name options='-asnode=target'
```

3. Asegúrese de que cada nodo agente tenga la planificación asociada con un nodo:

```
def association domain_name schedule_name <agentnodename>
```

En los siguientes ejemplos se muestran los mandatos del servidor de clientes de administración mediante el uso del planificador en varios nodos.

- El administrador registra todos los nodos que van a utilizarse emitiendo los siguientes mandatos:
  - `register node NODE-A`
  - `register node NODE-B`
  - `register node NODE-C`
- El administrador concede autoridad de proxy a cada nodo de agente utilizando los siguientes mandatos:
  - `grant proxynode target=NODE-Z agent=NODE-A`
  - `grant proxynode target=NODE-Z agent=NODE-B`
  - `grant proxynode target=NODE-Z agent=NODE-C`
- El administrador define las planificaciones utilizando los siguientes mandatos:
  - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnode=NODE-Z" objects=C: startdate=05/21/2005 starttime=01:00`

- `define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnode=NODE-Z" objects=D: startdate=05/21/2005 starttime=01:00`
- `define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnode=NODE-Z" objects=E: startdate=05/21/2005 starttime=01:00`

Nota: Coloque la opción `asnodename` únicamente en la definición de la planificación. No la coloque en el archivo de opciones del cliente, en la línea de mandatos, ni en ninguna otra ubicación.

Inicie las planificaciones configurando un servicio de planificador o utilizando el siguiente mandato de cliente: `dsmc sched`

También puede utilizar el aceptador de cliente, con la opción `managedservices` establecida para la planificación en el archivo de opciones de sistemas.

Importante:

- Cada planificación se puede iniciar desde una LPAR o estación de trabajo distinta.
- Tras ejecutar las planificaciones, cualquier cliente con proxy puede solicitar y restaurar todos los datos con copia de seguridad.
- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.

#### Referencia relacionada:

`Asnodename`

Valores de sesión y planificaciones de una operación de proxy

Mandato `DEFINE SCHEDULE`

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad con soporte de proxy de nodo cliente (UNIX y Linux)

Las copias de seguridad de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

La consolidación de copias de seguridad de varios nodos en un nombre de nodo de destino común en el servidor es útil en configuraciones en las que la estación de trabajo responsable de realizar las copias de seguridad pudiera cambiar con el tiempo, como dentro de un clúster.

Un nodo de agente es un nodo cliente al que se otorga autorización para realizar operaciones de cliente en nombre de un nodo de destino.

Un nodo de destino es un nodo cliente que otorga autorización a uno o varios nodos de agente para realizar operaciones en nombre de éste.

Utilice la opción `asnodename` con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor.













La opción `asnodename` también permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad.

Tenga en cuenta las siguientes características cuando utilice un nodo proxy para realizar una copia de seguridad o una restauración de datos en otros nodos:

- Una operación de proxy utiliza los valores del nodo de destino (como `maxnummp` y `deduplication`) y las planificaciones definidas en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- Todos los nodos agente del entorno de varios nodos deberían ejecutar el mismo tipo de sistema operativo.
- No utilice nodos de destino como nodos tradicionales, especialmente si cifra los archivos antes de hacerles una copia de seguridad en el servidor.
- No puede acceder a otro nodo (ya sea desde el desplegable de la GUI o mediante la opción `fromnode`).
- No se puede llevar a cabo una copia de seguridad o una restauración de NAS.






### Procedimiento

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
2. Registre cada nodo con el servidor IBM Spectrum Protect. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.

3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Registre el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenan en el servidor, bajo dicho nombre de nodo, cuando se utiliza la opción `asnodename`.
  4. El administrador del servidor IBM Spectrum Protect debe otorgar autoridad de proxy a todos los nodos del entorno compartido para el acceso al nombre de nodo de destino, con el mandato `GRANT PROXYNODE`.
  5. Utilice el mandato `QUERY PROXYNODE` del cliente administrativo para mostrar los nodos de cliente del usuario autorizado al que se le ha otorgado permiso mediante el mandato `GRANT PROXYNODE`.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Habilitación de varias operaciones de nodos desde la GUI  
Para habilitar operaciones multinodo en la GUI, utilice el editor Preferencias para especificar el nombre del nodo de destino al que se ha otorgado autoridad de proxy.
  -  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Configuración del cifrado  
En este tema se enumeran los pasos que debe seguir para configurar el cifrado con la opción `encryptkey`.
  -  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copias de seguridad de planificación con soporte de proxy de nodo cliente  
Se pueden utilizar varios nodos para realizar operaciones de copia de seguridad mediante un planificador.

#### Referencia relacionada:

`Asnodename`

 Sistemas operativos Windows  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  
 Sistemas operativos Oracle Solaris

## Habilitación de varias operaciones de nodos desde la GUI

---

Para habilitar operaciones multinodo en la GUI, utilice el editor Preferencias para especificar el nombre del nodo de destino al que se ha otorgado autoridad de proxy.

### Procedimiento

---

1. Compruebe que el nodo cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) mediante el uso del mandato de cliente de administración `QUERY PROXYNODE`.
2. Seleccione `Editar > Preferencias de cliente` para abrir la ventana de preferencias.
3. Seleccione la ficha `General` y rellene el campo `Como nombre de nodo` con el nombre de nodo de destino.
4. Pulse `Aplicar y, a continuación, Aceptar` para cerrar la ventana de preferencias.

### Qué hacer a continuación

---

Realice uno de estos pasos para comprobar que el nodo cliente acceda ahora al servidor como nodo de destino:

- Abra la ventana de árbol y compruebe que aparece el nombre de nodo de destino especificado por el campo `Como nombre de nodo`.
- Compruebe el nombre de nodo de destino del campo `Acceder como nodo` de la ventana `Información de conexión`.

Para volver a la operación de nodo único, suprima `Como nombre de nodo` desde el campo `Acceso como nodo` en el separador `General > Preferencias`.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Configuración del cifrado

---

En este tema se enumeran los pasos que debe seguir para configurar el cifrado con la opción `encryptkey`.

### Procedimiento

---

1. Especifique `encryptkey=save` en el archivo de opciones.
2. Realice la copia de seguridad de un archivo como mínimo con `asnode=ProxyNodeName` para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

### Resultados

---

Efectúe estos pasos para configurar el cifrado con la opción `encryptkey=prompt`:

1. Especifique `encryptkey=prompt` en el archivo de opciones.
2. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.

Importante:

- Si cambia la clave de cifrado, deberá repetir los pasos anteriores.
- Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copias de seguridad de planificación con soporte de proxy de nodo cliente






Se pueden utilizar varios nodos para realizar operaciones de copia de seguridad mediante un planificador.

### Acerca de esta tarea

Quando se otorga autorización de proxy a los nodos agente, estos efectúan las operaciones de copia de seguridad programada en nombre del nodo de destino. Cada nodo agente debe utilizar la opción `asnodename` en su planificación para realizar copias de seguridad de varios nodos para el nodo agente.

Inicie las planificaciones mediante el mandato del cliente `dsmc sched:`







En los siguientes ejemplos se muestran los mandatos del servidor de clientes de administración mediante el uso del planificador en varios nodos.

- El administrador registra todos los nodos que van a utilizarse emitiendo los siguientes mandatos:
  - `register node NODE-A`
  - `register node NODE-B`
  - `register node NODE-C`
- El administrador concede autoridad de proxy a cada nodo de agente utilizando los siguientes mandatos:
  - `grant proxynode target=NODE-Z agent=NODE-A`
  - `grant proxynode target=NODE-Z agent=NODE-B`
  - `grant proxynode target=NODE-Z agent=NODE-C`
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris   
 sistemas operativos Mac OS X El administrador define las planificaciones utilizando los siguientes mandatos:
  - `define schedule standard proxy1 description="NODE-A proxy schedule" action=incremental options="-asnodel=NODE-Z" objects=/Volumes/Xsan1 startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy2 description="NODE-B proxy schedule" action=incremental options="-asnodel=NODE-Z" objects=/Volumes/Xsan2 startdate=05/21/2005 starttime=01:00`
  - `define schedule standard proxy3 description="NODE-C proxy schedule" action=incremental options="-asnodel=NODE-Z" objects=/Volumes/Xsan3 startdate=05/21/2005 starttime=01:00`

Nota: Coloque la opción `asnodel` únicamente en la definición de la planificación. No la coloque en el archivo de opciones del cliente, en la línea de mandatos, ni en ninguna otra ubicación.

También puede utilizar el daemon de aceptación del cliente (`dsmcad`), con `managedservices` definida como `schedule` en el archivo de opciones del sistema.

Nota:

- Cada planificación se puede iniciar desde una LPAR o estación de trabajo distinta.
- Tras ejecutar las planificaciones, cualquier cliente con proxy puede solicitar y restaurar todos los datos con copia de seguridad.
- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris   
Ejemplos de cómo planificar una copia de seguridad de un clúster de IBM PowerHA SystemMirror   
Esta sección muestra algunos ejemplos de cómo realizar una copia de seguridad de un clúster de IBM® PowerHA SystemMirror.
-  Sistemas operativos AIX  Sistemas operativos Linux Planificar una copia de seguridad de un sistema de archivos de GPFS   
Utilice el planificador y las relaciones de proxy para realizar la copia de seguridad de un sistema de GPFS.

#### Referencia relacionada:

Asnodename

Valores de sesión y planificaciones de una operación de proxy

Mandato DEFINE SCHEDULE

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

# Ejemplos de cómo planificar una copia de seguridad de un clúster de IBM PowerHA SystemMirror

Esta sección muestra algunos ejemplos de cómo realizar una copia de seguridad de un clúster de IBM® PowerHA SystemMirror.

## Acerca de esta tarea

Siga estos pasos para activar la planificación de varios nodos:

1. Asegúrese de que todos los nodos agente tengan una autorización de proxy sobre el nodo de destino común
2. Asegúrese de que todos los nodos agente tengan una planificación definida en el servidor:

```
def sched domain_name sched_name options='-asnode=target'
```

3. Asegúrese de que cada nodo agente tenga la planificación asociada con un nodo:

```
def association domain_name schedule_name <agentnodename>
```

En los ejemplos siguientes, IBM PowerHA SystemMirror está configurado para dos hosts de AIX, `host_a` y `host_b`. Junto con sus propios datos locales, los hosts comparten el almacenamiento de disk, que tiene dos espacios de archivos: `/disk1` y `/disk2`.

En el ejemplo del CLUSTERNODE se muestra cómo la opción `clusternode` se utiliza en un entorno IBM PowerHA SystemMirror actual.

- El administrador define 3 nodos en el servidor IBM Spectrum Protect: `host_a`, `host_b`, `cluster_group`, mediante los mandatos siguientes: (1) `REGISTER NODE host_a mysecretpa5s`, (2) `REGISTER NODE host_b mysecretpa5s`, (3) `REGISTER NODE cluster_group mysecretpa5s`.
- El administrador define un archivo `dsm.opt` en `host_a` y `host_b` (tenga en cuenta que los archivos `opt` son distintos en cada host), utilizando los siguientes mandatos: (1) `NODENAME host_a` (la opción se puede dejar como valor predeterminado), (2) `DOMAIN /home /usr ... etc..`
- El administrador define un archivo `dsm.opt` ubicado en algún sitio de uno de los grupos de disco de clúster, p.ej. `/disk1/tsm/dsm/dsm.opt`, utilizando los siguientes mandatos: (1) `NODENAME cluster_group`, (2) `DOMAIN /disk1 /disk2`, (3) `CLUSTERNODE YES`.
- El administrador define una planificación en el servidor de IBM Spectrum Protect, utilizando el mandato `DEFINE SCHEDULE STANDARD CLUSTER_BACKUP`.
- El administrador define asociaciones para cada uno de los 3 nodos, utilizando el mandato `DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group`. En un momento dado, se ejecutan tres instancias de la planificación del cliente de archivado y copia de seguridad. (El planificador para `cluster_group` formará parte de los recursos del clúster que se sustituyen siempre que se sustituyan los recursos de disco del grupo de clúster. Por lo tanto, se ejecutará en el `host_a` o el `host_b`, pero no en los dos a la vez.)
- Los tres nombres de nodo contienen datos en el servidor de IBM Spectrum Protect.

En el ejemplo de `ASNODE` se muestra cómo se puede configurar sin utilizar `CLUSTERNODE`; se trata de una solución global que se podría aplicar a las soluciones de clúster de UNIX a las que no damos soporte, p.ej. Veritas Cluster Server for Solaris.

- El administrador define 3 nodos en el servidor de IBM Spectrum Protect, `host_a`, `host_b`, `cluster_group`:

```
REGISTER NODE host_a mysecretpa5s
REGISTER NODE host_b mysecretpa5s
REGISTER NODE cluster_group mysecretpa5s
```

- El administrador define una relación de nodo proxy entre `host_a` y `host_b` con `hacmp_cluster`

```
GRANT PROXYNODE TARGET=cluster_group AGENT=host_a,host_b
```

- El administrador define un archivo `dsm.opt` en `host_a` y `host_b` para manejar los sistemas de archivos locales:

```
NODENAME      host_a (la opción se puede dejar como valor predeterminado)
DOMAIN        /home /usr ... etc.
```

```
NODENAME      host_b (la opción se puede dejar como valor predeterminado)
DOMAIN        /home /usr ... etc.
```

- El administrador define un archivo `dsm.opt` en el recurso de clúster para gestionar la copia de seguridad de los recursos en clúster, por ejemplo: `/disk1/tsm/dsmcluster.opt` (el nombre de nodo es el nombre de nodo predeterminado, que es `host_a` o `host_b`, según la máquina que contenga el grupo de clúster en cada momento):

```
DOMAIN        /disk1 /disk2
ASNODE        cluster_group
```

- El administrador define una planificación en el servidor de IBM Spectrum Protect:

```
DEFINE SCHEDULE STANDARD CLUSTER_BACKUP
```

- El administrador define asociaciones para cada uno de los 3 nodos.

```
DEFINE ASSOC STANDARD CLUSTER_BACKUP host_a,host_b,cluster_group
```

- En un momento dado, se ejecutarán tres instancias de la planificación del cliente copia de seguridad/archivado estando en ejecución el planificador para el nodo `hacmp_cluster` del `host_a` o el `host_b`, pero no en ambos (se incluye en los recursos de clúster que se sustituirían por anomalía). Este planificador indicaría al archivo `dsmcluster.opt` que está definido en cada host. Las tres instancias se iniciarían como:

```
[host_a]                dsmc sched
[host_b]                dsmc sched
[cluster_group] dsmc sched -optfile=/disk/tsm/dsmcluster.opt
```

- Los tres nombres de nodo contienen datos en el servidor de IBM Spectrum Protect.

Para obtener más información sobre los mandatos del planificador del servidor, consulte la documentación del mismo.

 Sistemas operativos AIX  Sistemas operativos Linux

## Planificar una copia de seguridad de un sistema de archivos de GPFS

Utilice el planificador y las relaciones de proxy para realizar la copia de seguridad de un sistema de GPFS.

### Acerca de esta tarea

Supongamos que los tres nodos de un clúster GPFS participan en la operación de copia de seguridad. Los nodos `node_1`, `node_2` y `node_3` se utilizan solo para autenticación. Se realiza la copia de seguridad de los espacios de archivo que pertenecen al nodo `node_gpfs`.

### Procedimiento

1. Defina cuatro nodos en el servidor de IBM Spectrum Protect.

```
REGISTER NODE node_1 mysecretpa5s
REGISTER NODE node_2 mysecretpa5s
REGISTER NODE node_3 mysecretpa5s
REGISTER NODE node_gpfs mysecretpa5s
```

2. Defina una relación de proxy entre los nodos.

```
GRANT PROXYNODE TARGET=node_gpfs AGENT=node_1,node_2,node_3
```

3. Defina una planificación.

```
DEFINE SCHEDULE STANDARD GPFS_SCHEDULE ACTION=incremental
OBJECTS="/gpfs"

DEFINE ASSOCIATION STANDARD GPFS_SCHEDULE node_gpfs
```

4. Elija uno de los sistemas GPFS para ejecutar la planificación. Especifique las opciones `nodename` y `asnodename` en el archivo de opciones `dsm.sys` en todos los sistemas del clúster de GPFS. El valor para la opción `asnodename` debe ser el mismo en todos los sistemas.

Definiciones en el archivo de opciones `dsm.sys` en el nodo 1:

```
nodename node_1
asnodename node_gpfs
```

Definiciones en el archivo de opciones `dsm.sys` en el nodo 2:

```
nodename node_2
asnodename node_gpfs
```











Definiciones en el archivo de opciones `dsm.sys` en el nodo 3:

```
nodename node_3
asnodename node_gpfs
```

5. Inicie el planificador en el sistema que se elige para ejecutar la planificación.

```
DSMC SCHED
```

**Información relacionada:**

-  [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)  [Mandato mmbackup: Requisitos de IBM Spectrum Protect](#)
-  [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)  [Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect](#)
-  [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)  [Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale](#)
-  [Sistemas operativos Windows](#)

## Asociar una instantánea local con un espacio de archivos del servidor (Windows)

---

Utilice la opción snapshotroot con los mandatos incremental y selective junto con una aplicación suministrada por otro proveedor que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción snapshotroot no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

**Referencia relacionada:**

- [Snapshotroot](#)
-  [sistemas operativos Mac OS X](#)  [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)  [Sistemas operativos Oracle Solaris](#)


## Asociar una instantánea local con un espacio de archivos del servidor (UNIX y Linux)

---

Utilice la opción snapshotroot con los mandatos incremental y selective junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción snapshotroot no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

**Referencia relacionada:**

- [Snapshotroot](#)
-  [Sistemas operativos Windows](#)

## Copia de seguridad del estado del sistema de Windows

---

El cliente de copia de seguridad y archivado utiliza VSS para realizar copia de seguridad de todos los componentes de estado del sistema como un solo objeto a fin de proporcionar una instantánea de instante específico coherente del estado del sistema. El estado del sistema consta de todos los componentes de servicios del sistema y de estado del sistema arrancables.

### Acerca de esta tarea

---

El cliente admite el servicio de instantáneas de volumen (VSS) de the Microsoft en clientes de Windows soportados.

El estado del sistema se representa mediante varios grabadores VSS de tipo "estado del sistema arrancable" y "servicio del sistema". De estos, System Writer es la mayor parte del estado del sistema en términos de número de archivos y tamaño de datos. De forma predeterminada, la copia de seguridad de System Writer es incremental. Puede utilizar la opción systemstatebackupmethod para realizar copias de seguridad completas de System Writer. Para obtener más información sobre esta opción, consulte Systemstatebackupmethod. El cliente siempre realizará la copia de seguridad completa de todas las demás grabadoras.

La lista de componentes de servicios del sistema y de estado del sistema arrancables es dinámica y puede cambiar en función del paquete de servicio y de las funciones del sistema operativo que se hayan instalado. El cliente permite la recuperación dinámica y la copia de seguridad de estos componentes.

Para realizar una copia de seguridad de los datos de estado del sistema, debe ser miembro del grupo de administradores o de operadores de copia de seguridad.

Para realizar una copia de seguridad del estado del sistema mediante la línea de mandatos:

1. En la línea de mandatos, utilice el mandato **backup systemstate** para realizar copia de seguridad de todos los componentes de estado del sistema o de servicios del sistema como un solo objeto.
2. Utilice el mandato **query systemstate** para que se visualice información acerca de una copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect.

Para realizar una copia de seguridad del estado del sistema mediante la GUI:

1. Pulse **Copia de seguridad** en la ventana principal de la GUI. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios pulsando el signo más (+). Para visualizar los archivos de una carpeta, pulse el icono de la carpeta.
3. Localice el nodo estado del sistema en el árbol de directorios. Expanda el nodo estado del sistema para ver sus componentes.
4. Pulse la casilla situada junto al nodo de estado del sistema para realizar una copia de seguridad de todo el estado del sistema. Puede realizar una copia de seguridad del nodo de estado del sistema únicamente como una sola entidad debido a las dependencias entre los componentes de Estado del sistema. De forma predeterminada, se seleccionan todos los componentes; no es posible realizar una copia de seguridad de componentes del estado del sistema individuales.
5. Pulse **Copia de seguridad**. La ventana Lista de tareas de copia de seguridad muestra el estado del proceso de copia de seguridad. Cuando finaliza el proceso, la ventana Informe de copia de seguridad muestra los detalles del mismo.

La copia de seguridad de los archivos de arranque y del sistema se realiza únicamente como grupo si se modifica uno de los miembros del grupo (uno de los archivos). Si los archivos no se han modificado desde la última copia de seguridad, no se hace otra copia de seguridad de los archivos de arranque y del sistema.

De forma predeterminada, las copias de seguridad de estado del sistema están vinculadas a la clase de gestión predeterminada. Para vincularlas a una clase de gestión diferente, utilice la opción `include.systemstate`; especifique `all` como el patrón, y especifique el nombre de la nueva clase de gestión.

Puede utilizar la opción `domain` para excluir todo el estado del sistema de la copia de seguridad incremental del dominio.

Ahora, el directorio `dllcache` del sistema está incluido en la copia de seguridad de la partición de arranque de los sistemas Windows. Cuando los archivos de `dllcache` no están disponibles al restaurar un sistema Windows, es posible que la recuperación del sistema requiera la disponibilidad del soporte de instalación del sistema operativo. La realización de la copia de seguridad del directorio `dllcache` puede evitar la necesidad de tener que utilizar los medios de instalación durante las restauraciones del sistema.

Si no desea incluir el directorio `dllcache` en la copia de seguridad de la partición de arranque, y entiende las limitaciones que implica no realizar la copia de seguridad del directorio `dllcache`, puede utilizar la sentencia `exclude.dir` para que no se realice la copia de seguridad de esos archivos. Por ejemplo:

```
exclude.dir c:\windows\system32\dllcache
```

En clientes de Windows, `backup systemstate` también realiza copias de seguridad de datos ASR.

#### **Tareas relacionadas:**

Restauración del estado del sistema de Windows

#### **Referencia relacionada:**

Backup Systemstate

Domain

Opciones exclude

Opciones include

Query Systemstate

Restore Systemstate

 Sistemas operativos Windows

## **Copia de seguridad de los archivos de Recuperación automática del sistema**

Puede realizar una copia de seguridad de los archivos de Recuperación automática del sistema (ASR) en preparación para la recuperación de la información de configuración del disco de Windows y el estado del sistema si se produce un error muy grave del sistema o de hardware.

### **Acerca de esta tarea**

El cliente de archivado y copia de seguridad realiza la copia de seguridad de los datos ASR cuando el cliente de archivado y copia de seguridad copia el estado del sistema de Windows.



## Procedimiento

---

Para realizar la copia de seguridad de los archivos ASR en los sistemas operativos de Windows, utilice el mandato backup systemstate.

## Resultados

---

El cliente genera los archivos ASR en el directorio intermedio \adsm.sys\ASR en la unidad del sistema de su estación de trabajo local y guarda estos archivos en el espacio de archivos ASR en el servidor de IBM Spectrum Protect.

### Conceptos relacionados:

Preparación para la recuperación automática del sistema

### Tareas relacionadas:

Restauración de los archivos de Recuperación automática del sistema

### Referencia relacionada:



Backup Systemstate

 Sistemas operativos Windows

## Preparación para la recuperación automática del sistema

---

Las copias de seguridad específicas y el soporte son necesarios para Windows Automated System Recovery (ASR).

-  Sistemas operativos Windows Crear un archivo de opciones del cliente para la recuperación automática del sistema  
Para poder recuperar un sistema Windows con la Recuperación automática del sistema (ASR), debe crear un archivo de opciones. El archivo de opciones es único para cada sistema.
-  Sistemas operativos Windows Realizar la copia de seguridad de la unidad de arranque y de la unidad del sistema para Automated System Recovery  
Antes de poder recuperar el sistema Windows mediante Automated System Recovery (ASR), debe tener una copia de seguridad completa de la unidad de arranque y de la unidad del sistema.

 Sistemas operativos Windows

## Crear un archivo de opciones del cliente para la recuperación automática del sistema

---

Para poder recuperar un sistema Windows con la Recuperación automática del sistema (ASR), debe crear un archivo de opciones. El archivo de opciones es único para cada sistema.

## Acerca de esta tarea

---

En esta tarea se da por sentado que ha creado un CD o DVD WinPE arrancable. Un CD WinPE arrancable no contiene el archivo de opciones del cliente (dsm.opt), porque este archivo es exclusivo de cada sistema. Esta tarea le ayuda a crear un archivo de opciones específico del sistema.

El entorno de preinstalación de Windows (WinPE) requiere determinados valores de opciones.

## Procedimiento

---

1. Localice una copia del archivo de opciones del cliente. Podrá encontrar el archivo en distintas ubicaciones:
  - Existe un archivo de opciones en el directorio de instalación de un cliente de IBM Spectrum Protect instalado. La ubicación predeterminada es C:\Archivos de programa\Tivoli\TSM\baclient\dsm.opt. Si tiene el archivo de opciones para el sistema que desea restaurar, este archivo de opciones necesita modificaciones ínfimas.
  - Hay un ejemplo de un archivo de opciones en el paquete de instalación del cliente. La vía de acceso al paquete es TSM\_BA\_Client\program files\Tivoli\TSM\config\dsm.smp. Renombre el archivo como dsm.opt.
2. Edite dsm.opt.
  - a. Especifique una ubicación de escritura para el registro cronológico de errores. El cliente de archivado y copia de seguridad crea varios archivos de registro. Utilice la opción errorlogname para especificar la ubicación del archivo de registro. Por ejemplo, en el archivo dsm.opt, especifique `errorlogname x:\dsmerror.log`.  
Nota: Este ejemplo utiliza x: porque en modo WinPE, la unidad del sistema predeterminada es x:.
  - b. Especifique el nombre del nodo del cliente con la opción nodename.
  - c. Opcional: Si planea restaurar el estado del sistema a partir de archivos guardados en el servidor de IBM Spectrum Protect, especifique la información de conexión del servidor. Especifique los valores apropiados para las opciones commethod y tcpserveraddress.

- d. Opcional: Si conoce la contraseña para el nodo, especifíquela con la opción password.
3. Copie el archivo dsm.opt en el soporte que pueda leer el sistema de llegada durante la Recuperación Automática del sistema.
  4. Opcional: Copie la información del registro del cliente de IBM Spectrum Protect en un medio que el sistema de destino pueda leer durante la Recuperación automática del sistema. Utilice el programa de utilidad regedit.exe para exportar entradas del registro del cliente de IBM Spectrum Protect desde la clave HKLM\SOFTWARE\IBM. Por ejemplo, desde un indicador de mandatos, ejecute este mandato:

```
regedit /e tsmregistry.out "HKEY_LOCAL_MACHINE\SOFTWARE\IBM"
```

Copie el archivo tsmregistry.out en un soporte que pueda leer el sistema de llegada durante la ASR.

Durante el proceso de ASR, puede importar las entradas del registro desde el archivo tsmregistry.out. El cliente de copia de seguridad y archivado puede utilizar las entradas del registro en el entorno de WinPE para acceder a las copias de seguridad del servidor de IBM Spectrum Protect.

Nota: Guardar las entradas del registro es opcional porque hay otras formas de acceder al servidor protegido por contraseña de IBM Spectrum Protect. Puede acceder al servidor mediante los siguientes métodos:

- Si conoce la contraseña del nodo, puede escribir la contraseña cuando se le solicite durante la recuperación.
- Solicite al administrador de IBM Spectrum Protect que cambie la contraseña del nodo y que le proporcione la nueva contraseña durante la recuperación.
- Proporcione la información de contraseña en el archivo dsm.opt.

Si los archivos que desea restaurar están incluidos en un conjunto de copias de seguridad o en un CD o DVD, no necesitará acceder al servidor de IBM Spectrum Protect.


## Resultados

---

Ha creado un archivo de opciones que contiene información de configuración del cliente que es exclusiva para cada sistema. Esta información complementa el CD de WinPE arrancable genérico.

### Tareas relacionadas:

Crear un CD arrancable WinPE

 Sistemas operativos Windows

## Realizar la copia de seguridad de la unidad de arranque y de la unidad del sistema para Automated System Recovery

---

Antes de poder recuperar el sistema Windows mediante Automated System Recovery (ASR), debe tener una copia de seguridad completa de la unidad de arranque y de la unidad del sistema.

## Procedimiento

---

1. Lleve a cabo una copia de seguridad incremental completa del sistema y de las unidades de arranque. Suponiendo que su sistema y los archivos de arranque están en la siguiente unidad c:, escriba el siguiente mandato:

```
dsmc incremental c:
```

2. Realizar la copia de seguridad del estado del sistema. Para hacer una copia de seguridad del estado del sistema, escriba el siguiente mandato:

```
dsmc backup systemstate
```

Para verificar que se ha realizado una copia de seguridad del estado del sistema, escriba el siguiente mandato:

```
dsmc query systemstate
```





Puede especificar `-showmembers=yes` para mostrar los detalles a nivel de archivo.

### Conceptos relacionados:

Copia de seguridad incremental completa y parcial

### Tareas relacionadas:

Copia de seguridad del estado del sistema de Windows


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows


## Copia de seguridad de imagen


---


Desde la estación de trabajo local puede hacer una copia de seguridad de un volumen lógico como un solo objeto (copia de seguridad de imagen) del sistema.


La copia de seguridad de imagen estática tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris Debe ser usuario root para realizar esta tarea y la copia de seguridad de imágenes no se aplica a Mac OS X.

 Sistemas operativos Windows Estos volúmenes se pueden formatear como NTFS o ReFS, o se pueden dejar como RAW. Si un volumen tiene formato NTFS, solo se realiza la copia de seguridad de los bloques que utiliza el sistema de archivo o el parámetro menor que `imagegapsize`.


 Sistemas operativos Windows Por lo general, no podrá restaurar una copia de seguridad de imagen de la unidad del sistema sobre sí misma, pues no es posible obtener un bloqueo exclusivo de la unidad del sistema. Sin embargo, en un entorno de Windows preinstalado (WinPE), se puede realizar una restauración de la imagen de la unidad del sistema. Para obtener información sobre cómo restaurar datos en un entorno WinPE, consulte la nota técnica 7005028.


 Sistemas operativos Windows No puede restaurar una copia de seguridad de una imagen en el volumen en el que se está ejecutando el cliente. Plantéese la instalación del cliente de copia de seguridad y archivado en la unidad del sistema.

 Sistemas operativos Windows La copia de seguridad de imágenes no garantiza la coherencia de los objetos del sistema como, por ejemplo, Active Directory. Los objetos del sistema pueden extenderse por varios volúmenes y debería realizarse una copia de seguridad utilizando el mandato `backup systemstate`.


Una copia de seguridad de imagen proporciona las ventajas siguientes:


- La copia de seguridad de sistemas de archivos que contienen un gran número de archivos es más rápida que la copia de seguridad incremental completa de un sistema de archivos.
- Mejora la velocidad con la que el cliente restaura los archivos del sistema que contienen muchos archivos pequeños.
- Conserva los recursos del servidor durante las copias de seguridad ya que solamente es necesaria una entrada para la imagen.
- Proporciona una imagen de un instante específico del volumen lógico, que puede resultarle útil si la empresa debe recuperar esta información.
- Restaura un sistema de archivos corrupto o un volumen lógico RAW. Los datos se restauran en el mismo estado que estaban cuando se realizó la última copia de seguridad de volúmenes lógicos.


 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris La copia de seguridad de imagen estática tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen. Utilice la opción `dynamicimage` para realizar una copia de seguridad del volumen tal cual sin volver a montarlo como de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones siguen grabando en el mismo volumen mientras que se está ejecutando la copia de seguridad. Al grabar en un volumen mientras que se está ejecutando una copia de seguridad puede provocar que los datos no sean consistentes y la pérdida de datos después de ejecutar una operación de restauración. La opción `dynamicimage` sustituye el valor de serialización de la copia en la clase de gestión para llevar a cabo una copia de seguridad de una imagen. Después de restaurar una copia de seguridad de una imagen llevada a cabo con la opción `dynamicimage`, siempre debe ejecutar el programa de utilidad `chkdsk`.




 Sistemas operativos Windows La copia de seguridad de imagen desactivada tradicional no permite que otras aplicaciones del sistema tengan acceso de escritura al volumen mientras se realiza la operación. Cuando realiza una copia de seguridad de una imagen mediante un programa de utilidad `snapshotproviderimage=none`, ejecute siempre el programa de utilidad `fsck` después de restaurar los datos.


Para poder restaurar una copia de seguridad de imágenes de un volumen, el cliente de copia de seguridad y archivado debe ser capaz de obtener un bloqueo exclusivo en el volumen que está restaurándose.


 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris Restricción: No utilice copias de seguridad de imágenes dinámicas para sistemas de archivos, ya que el diseño interno del sistema de archivos podría dar lugar a datos incoherentes, incluso cuando no exista actividad de grabación. Asimismo, la copia de seguridad de imágenes dinámicas puede causar una imagen difusa, que podría no ser válida o estar completa al restaurarse.


 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris Si el cliente de copia de seguridad y archivado no consigue montar el sistema de archivos después de restaurar una imagen, ejecute `fsck`. Sin embargo, la ejecución de `fsck` puede afectar a la integridad de grandes cantidades de datos. No utilice la copia de seguridad de imágenes dinámicas con sistemas de archivos JFS2 AIX. El cliente de copia de seguridad y archivado no admite copias de seguridad de imágenes dinámicas con sistemas de archivos JFS2 AIX. Si especifica `dynamicimage=yes` en un sistema de archivos JFS2, el cliente realiza una copia de seguridad de imágenes basada en instantánea. Si por alguna razón no puede crearse la instantánea, el cliente realiza una copia de seguridad de imágenes estática.


 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris Atención: Para evitar perder datos, procure no utilizar la opción `dynamicimage` y asegúrese de que no exista ningún tipo de actividad de grabación en el volumen mientras se está ejecutando la copia de seguridad.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris En los sistemas de archivos AIX JFS2 la cantidad de datos de los que se hace copia de seguridad en el servidor IBM Spectrum Protect durante la copia de seguridad de imágenes estáticas o de instantánea se reduce porque sólo se copian los bloques que utiliza el sistema de archivos o los que tengan un valor menor de la opción imagegapsize. Este método de copia de seguridad de los datos mejora el rendimiento de las copias de seguridad de imágenes. Para obtener más información, consulte Imagegapsize.




 Sistemas operativos AIX Solo para clientes AIX: de manera predeterminada, el cliente realiza una copia de seguridad de imágenes de instantánea en línea de los sistemas de archivos JFS2, durante la cual el volumen queda disponible para otras aplicaciones del sistema.

















 Sistemas operativos Linux Para clientes de Linux solo: de forma predeterminada, el cliente realiza una copia de seguridad de una imagen de instantánea de los sistemas de archivos que hay en un volumen lógico creado por Linux Logical Volume Manager. El volumen está disponible en otras aplicaciones del sistema, mientras que se realiza la copia de seguridad.

 Sistemas operativos Linux En el cliente de Linux: no se admiten las copias de seguridad de imágenes de dispositivos DASD con modalidad de acceso de seguimiento raw en Linux on z Systems.


 Sistemas operativos Windows Si está configurado el soporte de imágenes en línea, el cliente realiza una copia de seguridad de imagen en línea durante la cual el volumen queda disponible para las otras aplicaciones del sistema. El proveedor de instantáneas, tal como se especifica en la opción snapshotproviderimage, mantiene una imagen coherente de un volumen durante la copia de seguridad de imagen activada.




 Sistemas operativos Windows Puede utilizar la opción snapshotproviderimage con el mandato backup image o con la opción include.image para especificar si se va a realizar una copia de seguridad de imágenes en línea o desactivada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Atención: Los sistemas de archivos gestionados por IBM Spectrum Protect for Space Management no se habilitan para la copia de seguridad.


-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Realización de tareas de requisitos previos antes de crear una copia de seguridad de imágenes  
En este tema se indican algunas de las consideraciones que deben tenerse en cuenta al realizar una copia de seguridad de imágenes.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Utilización de las copias de seguridad de imagen para realizar copias de seguridad incrementales del sistema de archivos  
En este tema se enumeran los métodos y los pasos necesarios para utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Realización de una copia de seguridad de imagen mediante la GUI  
Si la característica de copia de seguridad de imágenes está configurada, puede crear una copia de seguridad de imágenes durante la cual el volumen queda disponible para las otras aplicaciones del sistema.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Realización de una copia de seguridad de imagen mediante la línea de mandatos  
Utilice los mandatos backup image y restore image para realizar las operaciones de copia de seguridad de imagen y las operaciones de restauración en un solo volumen.





#### Tareas relacionadas:

 Sistemas operativos Windows Configuración del soporte de copias de seguridad de imagen en línea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea

#### Referencia relacionada:

 Sistemas operativos Windows Snapshotproviderimage

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Realización de tareas de requisitos previos antes de crear una copia de seguridad de imágenes



---


En este tema se indican algunas de las consideraciones que deben tenerse en cuenta al realizar una copia de seguridad de imágenes.

### Acerca de esta tarea

---

A continuación, se indican las consideraciones que deberá tener en cuenta cuando realice una copia de seguridad.

-  Sistemas operativos Windows Para realizar una copia de seguridad desactivada o activada debe tener autorización de administrador del sistema.
-  Sistemas operativos Windows No necesita más de una unidad para realizar una copia de seguridad de imagen.




- 
 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris. Asegúrese de que ninguna otra aplicación utiliza el volumen cuando ejecute una copia de seguridad de imágenes estática. Para garantizar una imagen coherente durante el proceso de copia de seguridad, si se detecta un espacio de archivos en el volumen, el cliente desmonta y vuelve a montar el volumen en modo de sólo lectura, de manera que ninguna otra aplicación pueda acceder a él. Si el volumen se encuentra en uso cuando el cliente intenta desmontarlo, la copia de seguridad da un error. Si el cliente no puede desmontar y volver a montar el volumen en modalidad de sólo lectura porque está utilizándose y no hay disponible una copia de seguridad de instantánea, puede utilizar la opción `dynamicimage` para obligar al cliente a realizar una copia de seguridad de imagen sin desmontar y volver a montar el volumen en modalidad de sólo lectura. Establezca la opción `dynamicimage` en la sentencia `include.image` o desde la línea de mandatos. La copia de seguridad puede resultar dañada si las aplicaciones graban en el volumen mientras la operación de copia de seguridad se encuentra en proceso. Esto puede corregirse ejecutando `fsck` después de una operación de restauración para solucionar los bloques que se hayan dañado.

Si no se detecta ningún sistema de archivos en el volumen del que se está haciendo la copia de seguridad, asegúrese de que todas las aplicaciones que escriben en los volúmenes estén detenidas. El cliente de copia de seguridad/archivado utiliza la tabla del sistema de archivos y la tabla de montaje para detectar los sistemas de archivos soportados.

No incluya archivos del sistema en una copia de seguridad de imagen, ya que los archivos del sistema que se utilizan de forma activa no se pueden desmontar.

Sólo para AIX y Linux: si realiza una copia de seguridad de imágenes de un sistema de archivos que se ha montado en otro punto de montaje y se ha especificado en la tabla de sistemas de archivos, después de llevar a cabo la copia de seguridad de imágenes, se perderán la mayoría de las opciones de montaje de este sistema, salvo el estado de lectura/grabación.

**Importante:** si un sistema de archivos tiene puntos de montaje anidados, desmóntelos antes de intentar realizar una copia de seguridad. De lo contrario, el cliente no puede desmontar el volumen. El sistema de archivos estará *ocupado* si contiene montajes.



- 
 Sistemas operativos Windows. Asegúrese de que ninguna otra aplicación utiliza el volumen mientras ejecuta una copia de seguridad de imágenes fuera de línea. Para garantizar una imagen coherente durante el proceso de copia de seguridad, el cliente bloquea el volumen para que ninguna otra aplicación pueda grabar en él. Si el volumen está siendo utilizado cuando el cliente intenta bloquearlo, la copia de seguridad da un error. Si el cliente no puede bloquear un volumen debido a que está utilizándose, puede realizar una copia de seguridad de imagen activada.
- Utilice la opción `include.image` para asignar una clase de gestión a la imagen del volumen. Si no la asigna, se utilizará la clase de gestión predeterminada para la imagen.
- 
 Sistemas operativos Windows. Nota: Si la opción `snapshotproviderimage` está establecida en *none*, se utilizan los parámetros de serialización de la copia definidos por la clase de gestión.
- Puede excluir un volumen de la copia de seguridad de imagen utilizando la opción `exclude.image`.
- 
 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris. Debe utilizar el punto de montaje para el volumen del sistema de archivos en el que desee realizar una copia de seguridad de imágenes. El cliente no realizará una copia de seguridad del volumen del sistema de archivos sin utilizar un punto de montaje. Realice una copia de seguridad de sistemas de archivos utilizando el nombre montado. Por ejemplo, si `/dev/lv01` se formatea como un sistema de archivos montado en `/home`, escriba este mandato para realizar una copia de seguridad de imagen de este volumen:





```
dsmc backup image /home
```

Realizar una copia de seguridad de volúmenes RAW utilizando el nombre del dispositivo. Por ejemplo, si `/dev/lv02` es un volumen RAW, escriba este mandato para realizar una copia de seguridad de imagen de este volumen:

```
dsmc backup image /dev/lv02
```

Si realiza una copia de seguridad de un volumen RAW formateado como sistema de archivos, asegúrese de que el sistema de archivos no está montado y no tiene ninguna entrada en `/etc/filesystems`.

- 
 Sistemas operativos Windows. Debe utilizar el punto de montaje o la letra de unidad para el volumen en el que desee realizar una copia de seguridad de imágenes. El cliente no realizará una copia de seguridad de un volumen sin utilizar una letra de unidad o un punto de montaje.
  - 
 Sistemas operativos Windows. No incluya la unidad del sistema en una copia de seguridad de imagen porque el cliente no puede tener un bloqueo exclusivo de la unidad del sistema durante la operación de restauración y la imagen de la unidad del sistema no se puede restaurar en la misma ubicación. La copia de seguridad de imágenes no garantiza la coherencia de los objetos del sistema como, por ejemplo, Active Directory. Los objetos del sistema se pueden distribuir en varios volúmenes, y se debe hacer una copia de seguridad de los mismos mediante los mandatos de copia de seguridad correspondientes. Dado que no se puede restaurar una copia de seguridad de imagen en el volumen desde el que el cliente se está ejecutando en ese momento (o en cualquier volumen para el que no se puede obtener un bloqueo exclusivo), debe instalar el programa de cliente en la unidad del sistema.
- Nota: cuando se utiliza WinPE, sí es posible realizar una restauración de imagen de la unidad del sistema. Para obtener más información, consulte IBM Spectrum Protect Técnicas de recuperación mediante Windows Preinstallation Environment (Windows PE).

-  Sistemas operativos Windows Si se detectan sectores de disco con errores en la unidad de origen durante una operación de copia de seguridad de imagen fuera de la LAN o en la LAN, pueden producirse daños en los datos. En este caso, los sectores con errores se pasan por alto al enviar los datos de imagen al servidor de IBM Spectrum Protect. Si se detectan sectores de disco con errores durante la copia de seguridad de imagen, aparece un mensaje de aviso cuando finaliza la copia de seguridad.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Soporte de tipo de dispositivo de volumen para una copia de seguridad de imagen  
En este tema se enumeran los diferentes dispositivos admitidos por el mandato backup image.


**Conceptos relacionados:**





Políticas de gestión de almacenamiento

**Referencia relacionada:**

Opciones exclude

Opciones include

 Sistemas operativos Windows Snapshotproviderimage

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows













## Utilización de las copias de seguridad de imagen para realizar copias de seguridad incrementales del sistema de archivos





---

En este tema se enumeran los métodos y los pasos necesarios para utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos.

Estos métodos de copia de seguridad permiten realizar una restauración a un instante específico de los sistemas de archivos y mejorar el rendimiento de las operaciones de copia de seguridad y restauración. La copia de seguridad sólo la puede realizar en volúmenes con formato y no en volúmenes lógicos RAW.

Puede utilizar uno de los siguientes métodos para realizar copias de seguridad de imagen de volúmenes con sistemas de archivos montados:

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Método 1: Uso de las copias de seguridad de imagen con las copias de seguridad incrementales de sistemas de archivos  
En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad incrementales de sistemas de archivos.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Método 2: Uso de las copias de seguridad de imagen con las copias de seguridad de imagen incremental por fecha  
En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad de imagen incremental por fecha.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Comparación de los métodos 1 y 2  
En este tema se muestra una comparación de los métodos 1 y 2: (1) Uso de la copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos o (2) Uso de la copia de seguridad de imágenes con la copia de seguridad de imágenes incremental por fecha.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Método 1: Uso de las copias de seguridad de imagen con las copias de seguridad incrementales de sistemas de archivos

---

En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad incrementales de sistemas de archivos.

### Acerca de esta tarea

---

### Procedimiento

---

1. Realizar una copia de seguridad de imágenes del sistema de archivos. De este modo se establece una base para las copias de seguridad incrementales futuras.
2. Realice una copia de seguridad de imagen del mismo sistema de archivos para posibilitar la restauración de la imagen.
3. Realice periódicamente copias de seguridad incrementales del sistema de archivos para garantizar que las adiciones y las supresiones se registran de forma precisa en el servidor.
4. Realice una copia de seguridad de imagen periódicamente para garantizar una restauración más rápida.

5. Restaura los datos realizando una restauración incremental. Asegúrese de seleccionar las opciones **Imagen más directorios y archivos incrementales** y **Suprimir archivos inactivos de sistema local** en la ventana Opciones de restauración antes de iniciar el proceso de restauración. Durante la restauración, el cliente realiza lo siguiente:





## Resultados


---

- Restaura la imagen más reciente en el servidor.
- Suprime todos los archivos restaurados en el paso anterior que están desactivados en el servidor. Éstos son los archivos que existían en el momento de realizar la copia de seguridad de imágenes pero que después se suprimieron y grabaron en una copia de seguridad incremental.
- Restaura los archivos nuevos y modificados a partir de las copias de seguridad incrementales.

Nota: Si una copia de seguridad incremental se realiza varias veces después de haberse realizado una copia de seguridad de una imagen, asegúrese de que el grupo de copias de seguridad del servidor de IBM Spectrum Protect dispone de suficientes versiones de los archivos existentes y suprimidos en el servidor para que la posterior restauración de imagen con las opciones incremental y deletefiles pueda suprimir correctamente los archivos.





### Tareas relacionadas:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Copia de seguridad de datos mediante la GUI Java

 Sistemas operativos Windows Copia de seguridad de datos mediante la GUI

Realización de una copia de seguridad de imagen mediante la GUI

Restauración de una imagen mediante la GUI

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Método 2: Uso de las copias de seguridad de imagen con las copias de seguridad de imagen incremental por fecha

---

En este tema figuran los pasos necesarios para realizar copias de seguridad de imágenes con copias de seguridad de imagen incremental por fecha.

## Procedimiento

---

1. Realice una copia de seguridad de imagen del sistema de archivos.
2. Realice una copia de seguridad de imágenes incremental por fecha del sistema de archivos. Con ello solamente se envían al servidor los archivos que se han añadido o modificado desde la copia de seguridad de imágenes más reciente.
3. Periódicamente, realice copias de seguridad completas.
4. Restaura el volumen realizando una restauración incremental. Asegúrese de seleccionar la opción **Imagen más directorios y archivos incrementales** en la ventana Opciones de restauración antes de iniciar el proceso de restauración. Con ello se restaura primero la imagen más reciente y después todas las copias de seguridad incrementales realizadas desde esa fecha.

## Resultados

---

Nota: Debe realizar copias de seguridad de imagen completas periódicamente en los casos siguientes:

- Cuando un sistema de archivos cambie notablemente (más del 40%), tal como se indica en el paso 4 del método 1 y en el paso 3 del método 2. Al realizar la restauración, se proporcionará una imagen del sistema de archivos similar a la que existía en el momento de la última copia de seguridad de imagen incremental por fecha, y además se mejorará el tiempo de restauración.
- Según sea adecuado en su entorno.

De este modo se reduce el tiempo necesario para la restauración, ya que se aplican menos cambios de las copias de seguridad incrementales.





Cuando se utiliza el método 2 se aplican las restricciones siguientes:

- El sistema de archivos no puede tener copias de seguridad incrementales completas anteriores.
- La copia de seguridad de imagen incremental por fecha no desactiva los archivos en el servidor, por lo tanto, cuando restaure una imagen que tenga la opción incremental, los archivos que se hayan suprimido después de la copia de seguridad de imagen original estarán presentes después de la restauración.
- Si se trata de la primera copia de seguridad de imágenes del sistema de archivos, se realiza una copia de seguridad de imágenes completa.
- Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio durante la restauración.

### Tareas relacionadas:

Realización de una copia de seguridad de imagen mediante la GUI

Restauración de una imagen mediante la GUI

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows





## Comparación de los métodos 1 y 2

En este tema se muestra una comparación de los métodos 1 y 2: (1) Uso de la copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos o (2) Uso de la copia de seguridad de imágenes con la copia de seguridad de imágenes incremental por fecha.

Para ayudarle a determinar el método más adecuado para su entorno, en la siguiente tabla se muestra una comparación de los métodos 1 y 2.

Tabla 1. Comparación de métodos de copia de seguridad de imagen incremental

<b>Método 1: Uso de la copia de seguridad de imagen con la copia de seguridad incremental de sistemas de archivos</b>	<b>Método 2: Uso de la copia de seguridad de imagen con la copia de seguridad de imagen incremental por fecha</b>
Los archivos caducan en el servidor cuando se suprimen del sistema de archivos. Al restaurarlos, tiene la opción de suprimir los archivos que caduquen en la imagen del servidor.	Los archivos no caducan en el servidor. Una vez finalizada la restauración de imagen incremental, todos los archivos suprimidos en el sistema de archivos después de la copia de seguridad de imágenes están presentes después de la restauración. Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio.
El tiempo de copia de seguridad incremental es el mismo que en las copias de seguridad incrementales normales.	La copia de seguridad de imagen incremental es más rápida porque el cliente no consulta en el servidor cada archivo copiado.
La restauración es mucho más rápida que una restauración incremental completa del sistema de archivos.	La restauración es mucho más rápida que una restauración incremental completa del sistema de archivos.
Los directorios suprimidos del sistema de archivos después de la última copia de seguridad de imagen no caducan.	Los directorios y archivos suprimidos del sistema de archivos después de la última copia de seguridad de imagen completa no caducan.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows



## Realización de una copia de seguridad de imagen mediante la GUI


Si la característica de copia de seguridad de imágenes está configurada, puede crear una copia de seguridad de imágenes durante la cual el volumen queda disponible para las otras aplicaciones del sistema.

### Acerca de esta tarea

Durante el proceso de copia de seguridad de imágenes, se mantiene una imagen constante del volumen.

 Sistemas operativos Windows Cuando realice una copia de seguridad de imágenes utilizando la opción image backup de la GUI del cliente, la operación de copia de seguridad se ejecuta según el valor snapshotproviderimage del archivo de opciones del cliente (dsm.opt). Si está configurado el soporte de imágenes en línea, el cliente realiza una copia de seguridad de imagen en línea durante la cual el volumen queda disponible para las otras aplicaciones del sistema.

 Sistemas operativos AIX  Sistemas operativos Linux Cuando realice una copia de seguridad de imagen con la opción image backup de la GUI del cliente de archivado y copia de seguridad, la operación de copia de seguridad se ejecuta según el valor de la opción snapshotproviderimage. La opción snapshotproviderimage toma como valor predeterminado una instantánea AIX JFS2 para AIX y una instantánea Linux LVM para Linux. Puede sustituir el valor predeterminado utilizando la pestaña Instantánea del Editor de preferencias y Preferencias de instantánea de imagen.

 Sistemas operativos Oracle Solaris En el caso de clientes Solaris, al seleccionar la opción image backup se ejecuta una copia de seguridad de imágenes estáticas de forma predeterminada. En una copia de seguridad de imagen estática, el cliente desmonta y vuelve a montar el volumen en modo de sólo lectura, de manera que ninguna otra aplicación pueda acceder a él. Puede sustituir el valor predeterminado utilizando la opción include.image y seleccionando dynamicimage yes. En una copia de seguridad de imagen dinámica, el cliente realiza la copia de seguridad de imagen, durante la cual el sistema de archivos no será de sólo lectura.

Para crear una copia de seguridad de imagen del sistema de archivos o del volumen lógico RAW, lleve a cabo los pasos siguientes:



## Procedimiento

1. Pulse el botón **Copia de seguridad** en la ventana principal de IBM Spectrum Protect. Aparecerá la ventana Copia de seguridad.
2. Expanda el árbol de directorios y seleccione los objetos de los que desee hacer una copia de seguridad. Para realizar una copia de seguridad de un volumen lógico RAW, localice y expanda el objeto de árbol de directorios RAW.
3. Pulse en Copia de seguridad. La ventana Lista de tareas de copia de seguridad muestra el estado del proceso de la copia de seguridad. Aparecerá la ventana Informe de copia de seguridad.

## Resultados

- Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Para realizar una copia de seguridad de imagen estática, seleccione **Copia de seguridad de imagen** en la lista desplegable.
- Sistemas operativos Windows Para realizar una copia de seguridad de imagen desactivada, seleccione **Copia de seguridad de instantánea** en la lista desplegable.
- Sistemas operativos Windows Para realizar una copia de seguridad de imagen activada, seleccione **Copia de seguridad de instantánea** en la lista desplegable.
- Sistemas operativos AIX Sistemas operativos Linux *Sólo* en clientes AIX y Linux : para realizar una copia de seguridad de imagen de instantánea, utilice la opción snapshotproviderimage.
- Para realizar una copia de seguridad de imagen incremental por fecha, seleccione **Incremental de imagen (sólo por fecha)** en la lista desplegable.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una copia de seguridad de imagen basada en instantánea:

Sistemas operativos Windows A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una copia de seguridad de imágenes en línea:

- Si desea modificar opciones de copia de seguridad específicas, pulse el botón Opciones. Las opciones que seleccione estarán en vigor únicamente durante la sesión actual.
- Sistemas operativos Windows Puesto que la copia de seguridad de imágenes le permite realizar la copia de seguridad únicamente de los bloques utilizados en un sistema de archivos, el tamaño almacenado de la imagen en el servidor de IBM Spectrum Protect podría ser más pequeño que el tamaño del volumen. Para las copias de seguridad de imágenes activadas, la imagen almacenada puede ser más grande que el sistema de archivos basándose en el tamaño de los archivos de la caché. Para determinar el tamaño real almacenado de la imagen, seleccione Ver > Detalles de archivo. El tamaño real almacenado de la imagen se indica en el campo Tamaño almacenado.
- Si desea modificar opciones de copia de seguridad específicas, pulse el botón Opciones. Las opciones que seleccione estarán en vigor únicamente durante la sesión actual.
- Sistemas operativos Windows Puesto que la copia de seguridad de imágenes le permite realizar la copia de seguridad únicamente de los bloques utilizados en un sistema de archivos, el tamaño almacenado de la imagen en el servidor de IBM Spectrum Protect podría ser más pequeño que el tamaño del volumen. Para las copias de seguridad de imágenes activadas, la imagen almacenada puede ser más grande que el sistema de archivos basándose en el tamaño de los archivos de la caché. Para determinar el tamaño real almacenado de la imagen, seleccione Ver > Detalles de archivo. El tamaño real almacenado de la imagen se indica en el campo Tamaño almacenado.

Sistemas operativos Linux Solo Linux: el cliente IBM Spectrum Protect versión 5.4 (y posteriores) no reconocerá ningún volumen LVM1 para operaciones de imagen. Sin embargo, permite la restauración de las copias de seguridad de imagen anteriores de los volúmenes LVM1 en volúmenes LVM2. En la Tabla 1 se muestran las combinaciones que implican a los niveles de cliente anteriores y nuevos que gestionan volúmenes LVM1 y LVM2 para distintas operaciones de imagen.

Sistemas operativos Linux





Tabla 1. Comparaciones de las operaciones de imagen de LVM1 y LVM2

Versión del cliente IBM Spectrum Protect	Copia de seguridad y restauración de LVM1	Copia de seguridad y restauración de LVM2	Volúmenes combinados	
			Copia de seguridad: LVM1. Restauración: LVM2	Copia de seguridad: LVM2. Restauración: LVM1
V5.3 y anteriores	SÍ	Sólo imagen estática para el sistema de archivos	NO	NO: no se admiten los volúmenes RAW

Versión del cliente IBM Spectrum Protect	Copia de seguridad y restauración de LVM1	Copia de seguridad y restauración de LVM2	Volúmenes combinados	
			Copia de seguridad: LVM1. Restauración: LVM2	Copia de seguridad: LVM2. Restauración: LVM1
V5.4 y posteriores	NO Se visualiza el mensaje de error ANS1090E	Sí	Sí La copia de seguridad del volumen LVM1 debe haberse realizado utilizando el cliente anterior	NO La restauración en el volumen LVM1 falla


**Referencia relacionada:**

Snapshotproviderimage

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Realización de una copia de seguridad de imagen mediante la línea de mandatos

Utilice los mandatos backup image y restore image para realizar las operaciones de copia de seguridad de imagen y las operaciones de restauración en un solo volumen.

 Sistemas operativos Windows Puede utilizar la opción snapshotproviderimage con el mandato backup image o con la opción include.image en el archivo dsm.opt o en la línea de mandatos para especificar si se va a realizar una copia de seguridad de imágenes en línea o desactivada.


Utilice la opción mode con el mandato backup image para realizar una copia de seguridad de imágenes incremental por fecha que únicamente realice una copia de seguridad de los archivos nuevos y de los que se han modificado desde de la copia de seguridad de imágenes completa más reciente. Sin embargo, de este modo solamente realizará una copia de seguridad de los archivos cuya fecha se haya modificado y no de los archivos cuyos permisos se hayan modificado.


**Referencia relacionada:**

Backup Image

Mode

Restore Image

 Sistemas operativos Windows Snapshotproviderimage

 Sistemas operativos AIX

## Copia de seguridad y archivado de archivo basada en instantánea y copia de seguridad de imágenes basada en instantánea

Para clientes de copia de seguridad y archivado que se ejecutan en AIX 5.3 o sistemas de archivos JFS2 posteriores como usuario root, la copia de seguridad de imágenes basada en instantánea se crea mediante las instantáneas predeterminadas.

### Acerca de esta tarea

Opcionalmente puede habilitar las operaciones de copia de seguridad y archivado de nivel de archivo basadas en instantánea; para ello especifique la opción snapshotproviderfs. Si por alguna razón no puede tomarse una instantánea, el cliente intenta realizar una copia de seguridad de imágenes estática o una copia de seguridad de archivos normal.

Si desea especificar una operación de copia de seguridad y archivado de archivo basada en instantánea, defina la opción snapshotproviderfs con el valor JFS2. Este será aplicable a todos los sistemas de archivos JFS2 para ese cliente.

Importante: Utilice una copia de seguridad y archivado basada en instantánea y una copia de seguridad de imágenes basada en instantánea para todos los sistemas de archivos AIX JFS2.

Por ejemplo, para *activar* la copia de seguridad y archivado de archivo basada en instantánea para todos los sistemas de archivos JFS2 del cliente, especifique lo siguiente en la sección del servidor del archivo dsm.sys:

```
snapshotproviderfs JFS2
```

Para *desactivar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea para todos los sistemas de archivos JFS2 del cliente, especifique lo siguiente en la sección del servidor del archivo dsm.sys:

```
snapshotproviderfs NONE
```

Para *activar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para un sistema de archivos JFS2 determinado del cliente, especifique lo siguiente en la sección del servidor del archivo dsm.sys:

```
snapshotproviderfs NONE
include.fs /kalafs1 snapshotproviderfs=JFS2
```

Para *desactivar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para un sistema de archivos JFS2 determinado del cliente, especifique lo siguiente en la sección del servidor del archivo dsm.sys:

```
snapshotproviderfs JFS2
include.fs /kalafs2 snapshotproviderfs=NONE
```

Para *activar* de manera explícita la copia de seguridad y archivado de archivo basada en instantánea sólo para una operación determinada en el cliente, especifique lo siguiente en la línea de mandatos:

```
dsmc incr -snapshotproviderfs=JFS2 /kalafs1
```

Para *desactivar* la copia de seguridad y archivado de archivo basada en instantánea sólo para una operación determinada en el cliente, especifique lo siguiente en la sección del servidor del archivo dsm.sys:


```
snapshotproviderfs JFS2
```

Luego ejecute el mandato backup. Por ejemplo:

```
dsmc incr -snapshotproviderfs=NONE /kalafs2
```

#### Referencia relacionada:

Snapshotproviderfs

 Sistemas operativos Linux

## Protección de los sistemas de archivos Btrfs

---

El sistema de archivos Btrfs debe incluirse como las especificaciones de los archivos para emitir los mandatos de copia de seguridad y restauración, los mandatos de archivado y recuperación y en los mandatos de backup image y restore image. También puede especificar los subvolumenes Btrfs como la especificación del archivo para realizar la copia de seguridad y restauración y las funciones de archivado y recuperación. No puede utilizar la imagen del cliente de archivado y copia de seguridad o los mandatos de restauración de la imagen en un subvolumen Btrfs.

Los sistemas de archivos Btrfs son compatibles en SLES 11 SP2 o posterior, en IBM®System x, System p y System z.

Si desea crear una copia de seguridad de imagen estática del sistema de archivos Btrfs completo, debe desmontar todos los subvolumenes para que el cliente de archivado y copia de seguridad se puede desmontar o montar el sistema de archivos Btrfs durante el proceso de copia de seguridad. Puede evitar los requisitos de montaje y desmontaje si lleva a cabo una copia de seguridad de imagen de instantánea del sistema de archivos Btrfs en vez de una copia de seguridad de una imagen estática.

La función de copia de seguridad y restauración de la imagen no está disponible para los subvolumenes Btrfs. Si intenta realizar la copia de seguridad de un subvolumen utilizando image backup, se muestra el siguiente mensaje:



```
ANS1162E Filesystem could not be mounted
```

Puede montar un subvolumen Btrfs mediante el nombre del subvolumen o el ID del subvolumen.

En sistemas de archivos Btrfs, la copia de seguridad diaria se puede realizar en el sistema de archivos y a nivel del subvolumen. Si lleva a cabo copias de seguridad basadas en diario en un sistema de archivos Btrfs, el diario que se crea es para el sistema de archivos completo; no hay un diario individual para cada subvolumen.

**Restricción:** En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en /etc/fstab, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos

restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo `/etc/fstab` para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.

- 
**Sistemas operativos Linux** Realizar la copia de seguridad y la restauración de los sistemas de archivos Btrfs. Puede realizar la copia de seguridad o restauración o el archivado y la recuperación de los sistemas de archivos Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad incremental, selective, restore, archive, and retrieve.
- 
**Sistemas operativos Linux** Copia de seguridad y restauración de los subvolúmenes Btrfs. Puede realizar una copia de seguridad o restauración o archivar y restaurar volúmenes de Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad incremental, selective, restore, archive y retrieve.

 Sistemas operativos Linux

## Realizar la copia de seguridad y la restauración de los sistemas de archivos Btrfs

Puede realizar la copia de seguridad o restauración o el archivado y la recuperación de los sistemas de archivos Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad incremental, selective, restore, archive, and retrieve.

### Acerca de esta tarea

Si ha utilizado una versión del cliente de archivado y copia de seguridad anterior a la Versión 7.1 para realizar la copia de seguridad del sistema de archivos Btrfs, el tipo de sistema de archivos se ha listado como `Unknown`, en el servidor de GUI de IBM Spectrum Protect y en la salida del mandato. El tipo de archivo del sistema `Unknown` se desplaza antes por IBM Spectrum Protect 7.1, los sistemas de archivos Btrfs no son compatibles formalmente. Si utiliza el cliente de archivado y copia de seguridad V7.1 (o posterior) para realizar la copia de seguridad al mismo sistema de archivos de Btrfs, se vuelve a realizar la copia de seguridad de todos los archivos que tienen listas de control de acceso (ACLs) y atributos extendidos (XATTRs), incluso si su contenido no ha cambiado desde la última copia de seguridad que se creó mediante la versión anterior del cliente. Además, después de realizar la copia de seguridad de un sistema de archivos Btrfs mediante el cliente con V7.1 (o posterior), el tipo de sistema se muestra correctamente como `Btrfs` en la GUI del servidor de IBM Spectrum Protect y en la salida del mandato.

Incluso con un cliente de V7.1 o posterior, copiar un archivo en un sistema de archivos Btrfs podría hacer que el archivo se incluyera en la siguiente operación de copia de seguridad. Por ejemplo, si copia un archivo utilizando el mandato `cp` con las opciones `-p` o `-preserve` (modos "preserve, ownership, and time stamps"), y si se cambian los atributos del archivo, el acceso al atributo ampliado ACL (`system.posix_acl_access`) también cambia. Ya que cambia el atributo ampliado, el cliente realiza la copia de seguridad del archivo completo en vez de solo actualizar los atributos para el archivo.

### Procedimiento

- Monte el sistema de archivos que desea proteger o recuperar. Por ejemplo, utilice la siguiente sintaxis para montar un sistema de archivos: `mount /dev/sdb1 on /btreefs1 type btrfs (rw)`
- Proteja o recupere el sistema de archivos realizando una de las siguientes operaciones:

Operación	Mandato
<b>Copia de seguridad del sistema de archivos</b>	<code>dsmc incr /btreefs1</code>
<b>Restauración del sistema de archivos</b>	<code>dsmc restore /btreefs1/ -subdir=yes -replace=yes</code>
<b>Archivado del sistema de archivos</b>	<code>dsmc archive /btreefs1/ -subdir=yes</code>
<b>Recuperación del sistema de archivos</b>	<code>dsmc retrieve /btreefs1/ -subdir=yes -replace=yes</code>
<b>Copia de seguridad de una instantánea de sistema de archivos</b>	<p>Cree una instantánea del sistema de archivos. Utilice el mandato <code>btrfs subvolume snapshot</code>. El directorio de instantánea que se especifica en este ejemplo es el directorio <code>btreefs1_snap</code> del sistema de archivos denominado <code>/btreefs1</code>.</p> <pre>btrfs subvolume snapshot /btreefs1/ /btreefs1/btreefs1_snap</pre> <p>Emita el mandato del cliente de archivado y copia de seguridad incremental. Especifique la opción <code>snapshotroot</code> y la ubicación de la instantánea Btrfs.</p> <pre>\$DSM_DIR/dsmc incr /btreefs1 -snapshotroot=/btreefs1/btreefs1_snap</pre>

Operación	Mandato
<b>Realización de una copia de seguridad de imagen</b>	<p>Todos los subvolumenes deben estar desmontados antes de crear una copia de seguridad de la imagen.</p> <pre>dsmc backup image /btreefs1 -snapshotproviderimage=none</pre> <p>Para evitar tener que desmontar los subvolumenes, cree una copia de seguridad de imagen basada en instantánea.</p> <pre>dsmc backup image /btreefs1</pre>
<b>Restauración de la copia de seguridad de la imagen</b>	<p>Todos los subvolumenes deben estar desmontados antes de restaurar una copia de seguridad de la imagen.</p> <pre>dsmc restore image /btreefs1</pre>

 Sistemas operativos Linux

## Copia de seguridad y restauración de los subvolumenes Btrfs

Puede realizar una copia de seguridad o restauración o archivar y restaurar volúmenes de Btrfs utilizando los mandatos del cliente de archivado y copia de seguridad incremental, selective, restore, archive y retrieve.

### Procedimiento

1. Liste los subvolumenes y determine sus identificadores.

```
btrfs subvolume list /btreefs1
ID 256 top level 5 path @
ID 262 top level 5 path @/btreefs1_sub1
```

2. Seleccione el directorio que se utilizará como punto de montaje en el subvolumen.

```
mkdir /btreefs1_sub1
```

3. Monte el subvolumen. Por ejemplo, para montar el subvolumen en un dispositivo sdb1 en /btreefs1\_sub1, utilice la siguiente sintaxis: `mount -t btrfs -o subvolid=262 /dev/sdb1 /btreefs1_sub1`

Proteja o recupere el subvolumen utilizando una o más de las siguientes operaciones:

Operación	Mandato
<b>Realizar la copia de seguridad de un subvolumen</b>	<p>Se admiten tanto las copias de seguridad incrementales como las selectivas.</p> <pre>dsmc incr /btreefs1_sub1 dsmc sel /btreefs1_sub1/ -subdir=yes</pre>
<b>Restaurar un subvolumen</b>	<pre>dsmc restore /btreefs1_sub1/ -subdir=yes -replace=yes</pre>
<b>Archivar un subvolumen</b>	<pre>dsmc archive /btreefs1_sub1/ -subdir=yes</pre>
<b>Recuperar un subvolumen</b>	<pre>dsmc retrieve /btreefs1_sub1/ -subdir=yes -replace=yes</pre>
<b>Realizar una instantánea de un subvolumen Btrfs</b>	<p>Cree una instantánea de subvolumen. Utilice el mandato <code>btrfs subvolume snapshot</code>. El directorio de la instantánea que se especifica en este ejemplo es el directorio <code>/btreefs1/btreefs1_sub1_snap</code> para el volumen llamado <code>btreefs1_sub1</code>.</p> <pre>btrfs subvolume snapshot /btreefs1/btreefs1_sub1 /btreefs1/btreefs1_sub1_snap</pre> <p>Emita el cliente de archivado y copia de seguridad del mandato incremental. Especifique la opción raíz de la instantánea y la ubicación de la instantánea Btrfs.</p> <pre>dsmc incr /btreefs1_sub1 -snapshotroot=/btreefs1 /btreefs1_sub1_snap</pre>

## Realice la copia de seguridad de los sistemas de archivos NAS utilizando el Protocolo de gestión de datos de redes

---

Los clientes de archivado y copia de seguridad de Windows, AIX y Solaris pueden utilizar NDMP (Network Data Management Protocol - Protocolo de gestión de datos de redes) para realizar copias de seguridad de imágenes de sistema de archivo de almacenamiento conectado a la red (NAS) y restaurar dichas imágenes de forma eficiente. Las imágenes de sistema de archivo se pueden copiar en, o restaurar desde, bibliotecas o unidades de cinta automatizadas que están conectadas localmente a servidores de archivos NAS de EMC Celerra o de dispositivos de red, o se pueden copiar en, o restaurar desde, unidades de cinta o bibliotecas conectadas de forma local al servidor de IBM Spectrum Protect.

El soporte de NDMP solo está disponible en IBM Spectrum Protect Extended Edition.

Para clientes de Linux x86\_64, se puede utilizar también la copia de seguridad incremental para realizar copias de seguridad de instantáneas de sistemas de archivos de NAS. Consulte el mandato incremental y las opciones snapshotroot, snapdiff, createnewbase y diffsnapshot para obtener más información.

Después de configurar el soporte de NDMP, el servidor se conecta al dispositivo NAS y utiliza NDMP para iniciar, controlar y supervisar cada operación de copia de seguridad y de restauración. El dispositivo NAS realiza la transferencia de datos externos hacia y desde el sistema de archivos NAS a una biblioteca asociada localmente.

La transferencia de datos de archivador a servidor se encuentra disponible para los dispositivos NAS que admitan NDMP versión 4.








Entre las ventajas de realizar copias de seguridad utilizando el soporte de NDMP se incluyen las siguientes:

- La transferencia de datos fuera de la LAN.
- Un alto rendimiento y copias de seguridad y restauraciones escalables.
- La copia de seguridad de dispositivos de cintas locales sin tráfico en la red.

Se proporciona el soporte siguiente:

- Copia de seguridad de imagen del sistema de archivos completa de todos los archivos de un sistema de archivos NAS.
- Copia de seguridad de imagen de archivos diferencial de todos los archivos que se han modificado desde la última copia de seguridad de imagen completa.
- Operaciones de copia de seguridad y restauración paralelas al procesar varios sistemas de archivos NAS.
- Opción de interfaces para iniciar, supervisar o cancelar operaciones de copia de seguridad y de restauración:
  - Cliente web (sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anteriores)
  - Interfaz de mandatos del cliente web de archivado y copia de seguridad (sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0 o V7.1.7 o anteriores)
  - Interfaz de línea de mandatos de cliente administrativo (se pueden programar operaciones de copia de seguridad y restauración utilizando el programador de mandatos administrativos)
  - Cliente web de administración

Las siguientes funciones *no* se admiten:

- Archivar y recuperar
- Planificación de cliente. Utilice los mandatos del servidor para planificar una copia de seguridad NAS.
- Detección de imágenes dañadas.
- Operaciones de transferencia de datos para datos NAS almacenados por IBM Spectrum Protect:
  - Migración
  - Reclamación
  - Exportación
  - Generación de juegos de copias de seguridad
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Copia de seguridad de los sistemas de archivos NAS con la GUI del cliente web utilizando el Protocolo de gestión de datos de redes NDMP. Para tanto la GUI del cliente web como la interfaz de línea de mandatos del cliente, debe especificar `passwordaccess=generate` (que es una restricción del cliente web actual para el nodo de cliente) y `set authentication=on` en el servidor.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Copia de seguridad de sistemas de archivos NAS mediante la línea de mandatos. La copia de seguridad incremental también puede utilizarse para realizar copias de seguridad de instantáneas de sistemas de archivos de NAS.
-  Sistemas operativos Windows Métodos para realizar la copia de seguridad y recuperar los datos en servidores de archivos NAS a los que se accede mediante el protocolo CIFS

El cliente de copia de seguridad y archivado puede procesar los datos del servidor de archivos del almacenamiento adjunto de red (NAS) al que se accede mediante el protocolo Common Internet File System (CIFS).

**Conceptos relacionados:**

Requisitos de soporte para NDMP (sólo Extended Edition)




**Referencia relacionada:**

Diffsnapshot

Incremental

Snapdiff

Snapshotroot

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Copia de seguridad de los sistemas de archivos NAS con la GUI del cliente web utilizando el Protocolo de gestión de datos de redes NDMP

---

Para tanto la GUI del cliente web como la interfaz de línea de mandatos del cliente, debe especificar `passwordaccess=generate` (que es una restricción del cliente web actual para el nodo de cliente) y `set authentication=on` en el servidor.

Siempre se le solicitará un identificador de usuario y una contraseña. Para visualizar nodos NAS y llevar a cabo funciones NAS, debe entrar un identificador de usuario y una contraseña de administración autorizados. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando tanto desde la línea de mandatos como desde la Web.

Puede utilizar la opción `toc` con la opción `include.fs.nas` en el archivo de opciones del cliente para especificar si el cliente guarda la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, puede utilizar el cliente web de Windows para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que deben restaurarse. Para crear una tabla de contenido, debe definir el atributo `TOCDESTINATION` en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Tenga en cuenta que, para crear una tabla de contenido, se necesitan un proceso adicional, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.

El interfaz de cliente web está disponible sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.

Para realizar una copia de seguridad de sistemas de archivos NAS utilizando la GUI del cliente web:

1. Pulse Copia de seguridad en la ventana principal. Se muestra la ventana Backup.
2. Expanda el árbol de directorios si es preciso.

Nota:

- a. El nodo raíz denominado Nodos no se puede seleccionar. Este nodo sólo aparece si hay un complemento NAS presente en la estación de trabajo cliente.
  - b. Los nodos NAS se muestran en el mismo nivel que el del nodo de la estación de trabajo cliente. Sólo aparecen los nodos para los que tiene autorización el administrador.
  - c. Puede expandir los nodos NAS hasta mostrar los espacios de archivos, aunque es la expansión máxima (no muestra nombres de archivo).
3. Pulse las casillas situadas junto a los nodos o los sistemas de archivos de los que desea realizar la copia de seguridad.
  4. Pulse el tipo de copia de seguridad que desee realizar en el menú desplegable de tipo de copia de seguridad. La lista de tipos de copia de seguridad NAS está activa sólo cuando se selecciona por primera vez los objetos de copia de seguridad NAS. Copia de seguridad completa realiza una copia de seguridad de todo el sistema de archivos. Diferencial realiza una copia de seguridad de los cambios realizados desde la copia de seguridad completa más reciente.
  5. Pulse en Copia de seguridad. La ventana Lista de tareas de copia de seguridad NAS muestra el estado del proceso y la barra de progreso de la copia de seguridad. El número que aparece junto a la barra de progreso indica la cantidad de bytes de los que se ha realizado copia de seguridad hasta ese momento. Cuando la copia de seguridad finaliza, la ventana NAS Backup Report muestra los detalles de proceso, incluido el tamaño actual de la copia de seguridad, incluidos los bytes totales de los que se ha realizado la copia de seguridad.

Nota: Si es necesario cerrar la sesión del navegador web, las operaciones NAS continúan después de la desconexión. Puede utilizar el botón Descartar situado en la ventana Lista de tareas de la copia de seguridad NAS para salir del proceso de supervisión sin finalizar la operación actual.

6. (Opcional) Para procesar la supervisión de una operación desde la ventana principal de la GUI, abra el menú Actions y seleccione IBM Spectrum Protect Activities. Durante una copia de seguridad, la barra de estado indica el estado del proceso. No aparece ningún porcentaje de aproximación para las copias de seguridad diferencial.

A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una copia de seguridad de los sistemas de archivo NAS mediante la GUI del cliente web.

- Las copias de seguridad de estaciones de trabajo y remotas (NAS) se excluyen mutuamente en una ventana Copia de seguridad. Tras haber seleccionado un elemento para realizar una copia de seguridad, el siguiente elemento que seleccione deberá ser del mismo tipo (NAS o no NAS).
- No se mostrarán detalles en el marco derecho de la ventana Copia de seguridad correspondientes a los nodos o sistemas de archivos NAS. Para ver información sobre los objetos en el nodo de NAS, resalte el objeto y seleccione View > File Details en el menú.
- Para suprimir espacios de archivo NAS, seleccione Utilities > Delete Filespaces.
- Las opciones de copia de seguridad no son válidas para los espacios de archivos NAS y se pasan por alto durante una operación de copia de seguridad de NAS.

**Conceptos relacionados:**

Descripción general de la configuración del cliente web

Restaurar sistemas de archivos NAS

**Referencia relacionada:**

Toc

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows







## Copia de seguridad de sistemas de archivos NAS mediante la línea de mandatos

La copia de seguridad incremental también puede utilizarse para realizar copias de seguridad de instantáneas de sistemas de archivos de NAS.
















Puede utilizar el cliente de línea de mandatos sólo si se conecta al servidor de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior. Para los servidores de IBM Spectrum Protect V8.1.2 o anteriores, utilice los mandatos del servidor en el cliente de línea de mandatos administrativo (dsmadm).


Tabla 1 enumera los mandatos y opciones que puede utilizar para realizar una copia de seguridad de las imágenes del sistema de archivos NAS desde la línea de mandatos.


Tabla 1. Opciones y mandatos NAS

Opción o mandato	Definición	Página
domain.nas	Utilice la opción domain.nas para especificar los volúmenes que se incluirán en el dominio predeterminado para las copias de seguridad NAS.	Domain.nas
exclude.fs.nas	Utilice la opción exclude.fs.nas para excluir sistemas de archivos del servidor de archivos NAS del proceso de copia de seguridad de imágenes cuando se utiliza con el mandato backup nas.   Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción <i>sólo</i> es válida para clientes AIX y Solaris.   Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.	Opciones exclude
include.fs.nas	Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si se debe guardar la información de la tabla de contenidos (TOC) durante una copia de seguridad de imagen del sistema de archivos NAS mediante la opción <b>toc</b> con la opción include.fs.nas en el archivo de opciones del cliente.   Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción <i>sólo</i> es válida para clientes AIX y Solaris.   Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.	Opciones include



Opción o mandato	Definición	Página
query node	Utilice el mandato query node para mostrar todos los nodos en los que un identificador de usuario de administración determinado dispone de autorización para realizar operaciones. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando.	Query Node
backup nas	Utilice el mandato backup nas para crear una copia de seguridad de imagen de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (almacenamiento conectado a red).	Backup NAS
toc	Utilice la opción toc con el mandato backup nas o la opción include.fs.nas para especificar si se debe guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.	Toc
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows monitor process	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Utilice el mandato monitor process para mostrar los procesos actuales de copia de seguridad y restauración de todos los nodos NAS sobre los que un usuario de administración tiene autorización. El usuario de administración puede seleccionar el proceso que desea supervisar.	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Monitor Process
cancel process	Utilice el mandato cancel process para mostrar los procesos actuales de copia de seguridad y restauración de todos los nodos NAS sobre los que un usuario de administración tiene autorización. Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar.	Cancel Process
query backup	Utilice el mandato query backup con la opción class para mostrar información sobre las imágenes de sistema de archivos de las que se ha realizado una copia de seguridad para un servidor de archivos NAS.	Query Backup
query filespace	Utilice el mandato query filespace con la opción class para visualizar una lista de espacios de archivos pertenecientes a nodo NAS.	Query Filespace
delete filespace	Utilice el mandato delete filespace con la opción class para que se visualice una lista de los espacios de archivos que pertenecen a un nodo NAS y para seleccionar el que desea suprimir.	Delete Filespace

 Sistemas operativos Windows Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Los nodos NAS representan un nuevo tipo de nodo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en IBM Spectrum Protect. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos que especifique se aplica a todos los servidores de archivos NAS.
- Independientemente de la plataforma del cliente, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol10.
-  Sistemas operativos Windows En el sistema de archivos NAS es necesario utilizar llaves { } como delimitadores de los nombres de sistemas de archivos cuando se utiliza la línea de mandatos, por ejemplo: {/vol/vol10}. No utilice llaves como delimitadores en el archivo de opciones.

Nota: Cuando se inicia una copia de seguridad de NAS utilizando la interfaz de línea de mandatos, la GUI de cliente o el cliente web, el servidor empieza un proceso para iniciar, controlar y supervisar la operación. Es posible que tarde unos cuantos minutos en observar el progreso en la interfaz de línea de mandatos porque el servidor debe realizar el montaje, y otras tareas necesarias, antes de que se produzca el traspaso de datos.

**Referencia relacionada:**

Toc

 Sistemas operativos Windows

# Métodos para realizar la copia de seguridad y recuperar los datos en servidores de archivos NAS a los que se accede mediante el protocolo CIFS

El cliente de copia de seguridad y archivado puede procesar los datos del servidor de archivos del almacenamiento adjunto de red (NAS) al que se accede mediante el protocolo Common Internet File System (CIFS).

Utilice los siguientes métodos para realizar una copia de seguridad y recuperar datos en dispositivos NAS:

- Utilice un cliente de archivado y copia de seguridad para hacer una copia de seguridad y restaurar datos utilizando CIFS para acceder a los archivos desde el cliente de archivado y copia de seguridad. Los datos pueden almacenarse en el servidor de IBM Spectrum Protect con granularidad a nivel de archivo utilizando el método de copia de seguridad incremental-progresiva. Los datos se almacenan en la jerarquía de almacenamiento de IBM Spectrum Protect y puede migrarse, reclamarse y realizarse una copia de seguridad de la misma en una agrupación de almacenamiento de copia.

Este método aumenta el uso del procesador cuando el cliente accede a los archivos individuales. Este método requiere que los datos fluyan a través del cliente. Este método también requiere que los datos fluyan a través del servidor de IBM Spectrum Protect, salvo que se utilice una configuración fuera de la red de área local.

- Utilice la opción `snapdiff` para reducir los problemas de rendimiento de la copia de seguridad CIFS. Esta opción almacena los datos con la granularidad a nivel de archivo mediante la copia de seguridad incremental para CIFS.
- Utilice un cliente de copia de seguridad y archivado que se está ejecutando en el dispositivo de NAS, si puede utilizar los programas externos con el sistema operativo NAS.

Este método reduce el uso del procesador de CIFS. Los datos se pueden guardar en el servidor de IBM Spectrum Protect con la granularidad a nivel de archivo mediante la utilización de una copia de seguridad incremental progresiva. Los datos se almacenan en la jerarquía de almacenamiento de IBM Spectrum Protect y puede migrarse, reclamarse y realizarse una copia de seguridad de la misma en una agrupación de almacenamiento de copia. Este método requiere que los datos fluyan a través del cliente de copia de seguridad y archivado. Este método también requiere que los datos fluyan por una red y a través de un servidor de IBM Spectrum Protect, salvo que se utilice una configuración fuera de la LAN.

- Utilice NDMP con el cliente de copia de seguridad y archivado. Se hace una copia de seguridad de los sistemas de archivos como imágenes completas (todos los archivos) o imágenes diferenciales (todos los archivos modificados desde la última copia de seguridad completa). Las imágenes objeto de copia de seguridad se almacenan en un dispositivo de cintas al que accede el servidor de archivos NAS. Este método proporciona un gran rendimiento porque no hay datos fluyendo a través de un cliente de archivado y copia de seguridad o un servidor de IBM Spectrum Protect. Los datos con copia de seguridad en el servidor que se han copiado mediante NDMP no se pueden migrar, reclamar o copiar a una agrupación de almacenamiento de copia.

Existen las siguientes limitaciones para los datos de servidor de archivos NAS cuando se accede a él mediante CIFS:

- La información sobre seguridad del directorio y archivos podría no estar accesible cuando la cuenta de Windows que realiza la copia de seguridad no es miembro del grupo de administradores del dominio del que el servidor de archivos NAS es miembro de confianza. También es posible que estos errores de acceso de seguridad impidan realizar una copia de seguridad total del archivo o directorio.
- La disminución del rendimiento se produce a causa del acceso remoto a los datos.
- Las unidades correlacionadas aparecen en el cliente como sistemas de archivos NTFS, pero es posible que no tengan la funcionalidad NTFS completa. Por ejemplo, se ha establecido el atributo de cifrado de un archivo pero, cuando el cliente realiza una copia de seguridad del archivo, esta no puede realizarse correctamente porque la configuración del cifrado a nivel de volumen indica que el volumen no admite el cifrado. Los sistemas de archivos ReFS también aparecen ante el cliente como sistemas de archivos NTFS.

Consejo: Utilice NDMP con el cliente de copia de seguridad y archivado en un servidor de archivos NAS para realizar la copia de seguridad y restauración de los volúmenes en vez de realizar la copia de seguridad y restauración de los volúmenes mediante las unidades correlacionadas remotas.

## Referencia relacionada:

Snapdiff

 Sistemas operativos Windows

## Soporte para Persistent Storage Manager de CDP

Persistent Storage Manager (PSM) es la tecnología de instantánea que se incluye con un número de cajas de sistemas NAS basados en el Microsoft Server Appliance Kit, que incluye IBM® TotalStorage NAS 200, 300 y 300G.





Puede utilizar el cliente de archivado y copia de seguridad para realizar la copia de seguridad de las imágenes persistentes (PI) de un volumen producido por PSM. Primero debe asegurarse de que el volumen tiene una etiqueta. Luego podrá utilizar PSM para planificar o crear una imagen persistente con un nombre de imagen concreto, como `snapshot.daily`, y establecer el número de imágenes que

deben guardarse en 1. PSM grabará encima de la PI cuando sea necesario y puede utilizar el cliente para hacer una copia de seguridad incremental de la PI. En este caso, el cliente realiza la copia de seguridad solo de los archivos que se han cambiado entre instantáneas. Una ventaja de hacer una copia de seguridad de una PI de PSM en lugar de hacerla del volumen real es que en la PI no hay archivos abiertos.

Tenga en cuenta los siguientes artículos antes de utilizar Persistent Storage Manager:

- De forma predeterminada, PSM utiliza un nombre de variable (*snapshot.%i*) y mantiene determinada cantidad de imágenes. Importante: No utilice el cliente con PSM de esta forma. El cliente ve cada imagen como exclusiva y realiza una copia completa de cada una de ellas.
- El cliente requiere que el volumen utilizado para realizar la PI tenga una etiqueta. Si el volumen no tiene etiqueta, el cliente no hace una copia de seguridad de su PI.
- Utilice la función de copia de seguridad de imagen para realizar la copia de seguridad del volumen original que se utiliza para crear la PI. Sin embargo, no puede utilizar la función de imagen de copia de seguridad para realizar la copia de seguridad de la PI.
- Para evitar realizar la copia de seguridad de archivos innecesarios cuando realiza la copia de seguridad de PSM, incluya las siguientes entradas en su archivo de opciones del cliente (dsm.opt):

```
exclude.dir "Persistent Storage Manager State"
exclude.file "*.psm"
exclude.file "*.otm"
```

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Copia de seguridad de sistemas de archivos de red





---


Puede configurar el cliente de archivado y copia de seguridad para proteger archivos a los que se accede con el protocolo NFS (Network File System) o con el protocolo CIFS (Common Internet File System).

Si bien es posible conseguir un mejor rendimiento de copia de seguridad gracias a la instalación del cliente de archivado y copia de seguridad donde existe físicamente el sistema de archivos. Pero a veces es necesario acceder a los sistemas de archivos utilizando NFS o CIFS para hacer copias de seguridad o recuperar datos en unidades compartidas remotas. El cliente de archivado y copia de seguridad en sistemas operativos AIX, Linux, Mac OS X y Solaris puede realizar copias de seguridad, archivar, restaurar y recuperar datos de archivos en una unidad compartida montada en NFS o CIFS. Estas operaciones son válidas en todas las versiones del protocolo NFS, incluyendo NFS versión 2, NFS versión 3 y NFS versión 4.

El cliente de copia de seguridad y archivado puede hacer copia de seguridad y restaurar listas de control de acceso cuando está configurado para utilizar NFS versión 4.

Se aplican las siguientes restricciones cuando el cliente de archivado y copia de seguridad protege datos en volúmenes de sistemas de archivos de red:

- Los clientes de archivado y copia de seguridad no pueden completar copias de seguridad de imagen de volúmenes de sistemas de archivos de red.
- Los clientes de copia de seguridad y archivado de AIX no pueden completar copias de seguridad de archivos basadas en instantáneas ni archivar archivos en volúmenes del sistema de archivos de la red.
- Los clientes de archivado y copia de seguridad no pueden completar copias de seguridad basadas en registro diario de volúmenes de sistemas de archivos de red.
- Es posible que los clientes de archivado y copia de seguridad no puedan realizar copias de seguridad de instantáneas de volúmenes de NetApp si se accede a ellas utilizando el protocolo NFS. Si el archivador NetApp proporciona identificadores de dispositivos distintos para sus instantáneas de volúmenes, dichas instantáneas se pueden excluir de las copias de seguridad. El comportamiento depende de la versión del SO, de la versión del archivador NetApp y de su configuración.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copia de seguridad de sistemas de archivos NFS con la función de espacio de nombres global  
Los clientes de NFS V4 pueden realizar una copia de seguridad de los sistemas de archivos NFS se montan mediante la función del espacio de nombres global, llamado *referencia*. La copia de seguridad de todos los sistemas de archivos del espacio de nombres global se realiza en un único espacio de archivos.

 Sistemas operativos AIX

## Copia de seguridad de los sistemas de archivos con partición de carga de trabajo de AIX

---

Mediante la utilización del cliente de archivado y copia de seguridad en AIX, puede realizar la copia de seguridad y restaurar los datos del archivo de partición local dentro de la partición global utilizando el espacio de nombres disponible dentro de la partición global.

Cada partición de carga de trabajo (WPAR) tiene su propio dominio de seguridad, por lo que el usuario raíz global tiene garantizado el acceso a todos los datos.

Las WPAR son particiones que se crean por completo en el software de una sola imagen del sistema AIX, con los atributos siguientes:

- Normalmente la WPAR parece un sistema AIX autónomo completo
- No hay asistencia ni configuración de hardware de ningún tipo

Las particiones de carga de trabajo proporcionan un entorno seguro y aislado para aplicaciones de empresa en términos de proceso, señal y espacio de sistemas de archivos. El software que se ejecuta en el contexto de una partición de carga de trabajo tiene su propia instancia de AIX.

El ejemplo siguiente muestra una configuración de WPAR a partir de la WPAR global:

Global partition:

Nombre del sistema: shimla  
Nombre del archivo: /home /opt

WPAR #1 configuration:

Nombre: wpar1  
Sistema de archivos: /home; name in global WPAR: /wpars/wpar1/home

WPAR #2 configuration:

Nombre: wpar2  
Sistema de archivos: /data; name in global WPAR: /wpars/wpar2/data

Hay dos formas de realizar copia de seguridad de los datos de la WPAR. Estos son:

- Realice una copia de seguridad de todos los sistemas de archivos WPAR como espacios de archivo en la partición global. El nombre de espacio de archivos se debe utilizar para identificar el WPAR al cual pertenece. Todos los datos se gestionan en un nodo mediante una planificación. Si utiliza la configuración de ejemplo, aquí encontrará un archivo de ejemplo dsm.sys con una stanza del servidor para todos los archivos, tanto global como local:

```
SERvername shimla
TCPPort      1500
TCPServeraddress servidor.ejemplo.com
nodename     shimla
PasswordAccess generate
Domain       /wpars/wpar1/home /wpars/wpar2/data /home /opt
```

- Realice una copia de seguridad de cada sistema de archivos de la WPAR bajo un nombre de nodo distinto. De esta forma se proporciona la segregación del nombre de espacios de archivos para cada WPAR. Cada WPAR debe tener un nombre de nodo independiente y un planificador en ejecución en la partición global. Además, se han de configurar los tres servicios del planificador, utilizando para cada uno de ellos un archivo dsm.opt distinto correspondiente al nombre de la stanza del servidor. Este método permite que cada operación de copia de seguridad de WPAR se pueda gestionar de forma independiente de las demás. Aquí encontrará un archivo de ejemplo, dsm.sys, que utiliza la configuración de ejemplo, con tres secciones de servidor: una para wpar1, otra para wpar2 y otra para la partición global shimla:

```
SERvername shimla_wpar1
TCPPort      1500
TCPServeraddress servidor.ejemplo.com
nodename     wpar1
PasswordAccess generate
Domain       /wpars/wpar1/home
```

```
SERvername shimla_wpar2
TCPPort      1500
TCPServeraddress servidor.ejemplo.com
nodename     wpar2
PasswordAccess generate
Domain       /wpars/wpar2/data
```

```
SERvername shimla
TCPPort      1500
TCPServeraddress servidor.ejemplo.com
nodename     shimla
PasswordAccess generate
Domain       /home /opt
```

 Sistemas operativos Oracle Solaris

## Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte

En los sistemas Solaris SPARC y Solaris x86, puede hacer copia de seguridad de los sistemas de archivos Zettabyte (ZFS -Zettabyte file systems), utilizando instantáneas ZFS. La ventaja de este método frente a una copia de seguridad incremental o selectiva ordinaria es que los archivos y carpetas de una instantánea siempre están en estado de sólo lectura, de forma que no se pueden modificar durante una copia de seguridad.

## Acerca de esta tarea

---

Puede crear una instantánea ZFS con mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs snapshot tank/myZFS@mySnapshot
```

En este ejemplo, el nombre de la agrupación ZFS es tank y el nombre del sistema de archivos ZFS es myZFS. Los archivos que pertenecen a esta instantánea ZFS se encuentran en el subdirectorio denominado tank/myZFS/.zfs/snapshot/mySnapshot/.

## Procedimiento

---

Utilice uno de los dos métodos siguientes para hacer copia de seguridad de una instantánea ZFS.

- Realizar una copia de seguridad de cada archivo de la instantánea con la opción snapshotroot. Por ejemplo:

```
dsmc inc -snapshotroot=/tank/myZFS/.zfs/snapshot/mySnapshot /tank/myZFS
```

Esta opción permite al administrador sustituir la vía de acceso de instantánea actual por la vía de acceso del sistema de archivos ZFS de forma que se hace la copia de seguridad de los archivos y carpetas bajo el sistema de archivos original.

- Hacer una copia de seguridad de la instantánea completa con mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs send tank/myZFS@mySnapshot > /tmpdir/mySnapshotFile
```


La ventaja de realizar una copia de seguridad de la instantánea completa es que se puede realizar una restauración de todo el sistema de archivos en un escenario de recuperación tras desastre.

### Conceptos relacionados:

Restauración de sistemas de archivos ZFS de Solaris

### Referencia relacionada:

Snapshotroot

 Sistemas operativos AIX

## Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX

---

Utilice el sistema de archivos cifrados (EFS) de JFS2 de AIX para realizar una copia de seguridad de los archivos en formato de texto legible o sin formato (RAW). Con el formato de texto legible, el archivo se descifra mediante EFS a medida que se va leyendo. Si no se aplica formato, los datos no se descifran. El valor predeterminado es no aplicar formato, pero cuando establece la opción efsdecrypt en yes, obtiene copias de seguridad de texto legible.

## Acerca de esta tarea

---

**Importante:** siempre que ejecute una copia de seguridad que incluya archivos cifrados en un EFS, debe asegurarse de que utiliza la especificación correcta de la opción efsdecrypt . Si el valor de la opción efsdecrypt cambia entre las dos copias de seguridad incrementales, se volverá a realizar una copia de seguridad de todos los archivos cifrados de los sistemas de archivos EFS, incluso si no se han modificado desde la última copia de seguridad. Por ejemplo, si ejecuta una copia de seguridad incremental de archivos cifrados de los que anteriormente había hecho una copia de seguridad como raw, debe asegurarse de que efsdecrypt se ha especificado como no. Si cambia el valor de efsdecrypt a yes, se volverá a realizar una copia de seguridad de todos los archivos en texto legible incluso si no se han modificado; por lo tanto, asegúrese de utilizar esta opción cuidadosamente.

Si intenta restaurar un archivo cifrado en una estación de trabajo que no admite EFS o en un sistema de archivos en el que EFS no esté activo, se escribirá un mensaje de error y el archivo se pasará por alto.

Estos son algunos de los motivos para realizar una copia de seguridad de EFS utilizando el cifrado de texto legible:

- Este tipo de descifrado es útil si desea utilizar el cifrado del cliente de archivado y copia de seguridad de IBM Spectrum Protect u otro tipo de cifrado de hardware (para los sistemas de cintas, por ejemplo).
- Puede utilizar el texto en formato legible para el archivado de datos a largo plazo, debido a que los datos se almacenan independientemente de la plataforma o del esquema de cifrado.

Estos son algunos de los puntos a tener en cuenta cuando se realiza una copia de seguridad de un archivo en texto legible:

- El usuario que ha invocado el cliente de copia de seguridad y archivado debe poder descifrarlo.

- El usuario puede tener acceso de lectura a un archivo, pero puede no tener acceso a la clave.

En los casos siguientes se emite un mensaje de error:

## Procedimiento

1. El usuario está en modalidad de salvaguarda root y EFS reconoce el concepto de dos tipos de usuario root. El administrador root es la modalidad tradicional. Con una modalidad de salvaguarda root no se tendrá acceso a los datos no cifrados, a menos que el usuario sea el propietario o un miembro del grupo de archivos.
2. El usuario trabaja con un ID de usuario no root y está intentando archivar un archivo para el que tiene acceso de lectura, pero el usuario no es propietario o miembro del grupo de archivos. EFS no permitirá que los datos se descifren.


## Resultados

Estos son algunos de los puntos que se han de tener en cuenta cuando se realiza una copia de seguridad de los datos sin formato de EFS:

- El cliente de copia de seguridad y archivado no respetará la configuración de cifrado del cliente, que impide el doble cifrado, sino sólo en el cliente. El servidor no sabe que los datos están cifrados, por lo que el cifrado que realice una unidad de cinta, por ejemplo, seguirá teniendo lugar.
- El cliente no respetará la configuración de compresión, por lo que el cliente ni intentará comprimir los datos.
- El cliente no hace copia de seguridad ni restaura de forma automática los archivos del almacén de claves. Cuando restaure archivos cifrados, puede que tenga que restaurar los almacenes de claves para poder descifrar los datos.

### Sugerencias:

1. Para proteger el almacén de claves, asegúrese de que el contenido de /var/efs se incluya en las copias de seguridad periódicas.
  2. Para los datos del almacén de claves, utilice la política de almacenamiento de IBM Spectrum Protect con un número de versiones ilimitado.
- La copia de seguridad de los archivos EFS (sistema de archivos cifrado) que se ha realizado en modalidad sin formato (valor predeterminado) no se puede restaurar mediante un cliente de copia de seguridad y archivado anterior a la versión 5.5 o mediante un cliente de otra plataforma UNIX.

 Sistemas operativos AIX

## Copia de seguridad de los atributos ampliados de AIX JFS2

El sistema de archivos de AIX JFS2 (Enhanced Journal File System) proporciona el proceso de copia de seguridad de los atributos ampliados para todos los sistemas de archivos que admiten atributos ampliados con nombre.


Se hace copia de seguridad de estos atributos ampliados de forma automática con cada objeto que dispone de datos de atributos ampliados y no se exige ninguna otra acción.

Cuando el sistema de archivos se define con el formato v2, el único sistema de archivos que admite atributos ampliados con nombre es JFS2. Puede utilizar JFS2 para los atributos ampliados de archivos y directorios, pero no para los atributos ampliados de enlaces simbólicos.

 Sistemas operativos Linux  Sistemas operativos Windows

## Realización de copia de seguridad de máquinas virtuales VMware

Puede utilizar el cliente de archivado y copia de seguridad para realizar copias de seguridad y restaurar una máquina virtual (VM) a VMware. Las copias de seguridad completas de la máquina virtual operan a nivel de una imagen de disco. Las copias de seguridad incrementales solo copian los datos modificados desde la última copia de seguridad completa.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.



 Sistemas operativos Linux La Tabla 1 lista las prestaciones de copia de seguridad y restauración para máquinas virtuales VMware que el cliente de archivado y copia de seguridad puede realizar modificaciones en las plataformas Linux.

Tabla 1. Prestaciones de copia de seguridad y restauración para máquinas virtuales VMware en plataformas Linux

Prestación	Observación
------------	-------------

Prestación	Observación
Copia de seguridad de máquina virtual incremental-constante completa:	<p>Una copia de seguridad de máquina virtual completa es necesaria antes de poder crear copias de seguridad incrementales. Si planifica copias de seguridad incrementales, constantes, este tipo de copia de seguridad se selecciona automáticamente para la primera copia de seguridad si una copia de seguridad completa no se hubiera creado todavía. Los datos de copias de seguridad incrementales se combinan con datos de la copia de seguridad completa para crear una imagen sintética de la copia de seguridad completa. Las copias de seguridad incrementales, constantes subsiguientes leen todos los bloques utilizados y los copian en el servidor IBM Spectrum Protect. Cada copia de seguridad completa, incremental, constante, de máquina virtual lee y copia todos los bloques utilizados, tanto si han cambiado los bloques o no, desde la copia de seguridad anterior. Aún puede planificar una copia de seguridad completa de la máquina virtual, aunque una copia de seguridad completa ya no sea necesaria. Por ejemplo, puede ejecutar una copia de seguridad completa de máquina virtual para crear una copia de seguridad a un nodo con otro nombre, con los valores de retención diferentes.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>
Copia de seguridad de máquina virtual incremental-constante-incremental:	<p>Requiere que cree una copia de seguridad completa de la máquina virtual una única vez. La copia de seguridad completa de la máquina virtual copia todos los bloques de disco utilizados propiedad de una máquina virtual en el servidor de IBM Spectrum Protect. Después de completarse la copia de seguridad completa inicial, todas las copias de seguridad posteriores de la máquina virtual son copias incrementales, constantes, incrementales. Cada copia de seguridad incremental, constante, incremental copia únicamente los bloques que se han modificado desde la copia de seguridad anterior, independientemente del tipo de la copia de seguridad anterior. El servidor utiliza una tecnología de agrupación que asocia los bloques cambiados a partir de la copia de seguridad más reciente con datos ya almacenados en el servidor de copias de seguridad anteriores. Una copia de seguridad completa nueva se crea, entonces, cada vez que los bloques cambiados se copian en el servidor mediante una copia de seguridad incremental, constante, incremental.</p> <p>La modalidad de copia de seguridad incremental, constante, incremental proporciona las ventajas siguientes:</p> <ul style="list-style-type: none"> <li>• Mejora la eficacia de la realización de copias de seguridad de máquinas virtuales.</li> <li>• Simplifica las operaciones de restauración de datos.</li> <li>• Optimiza las operaciones de restauración de datos.</li> </ul> <p>Durante una operación de restauración, puede especificar opciones para la hora de instante específico y la fecha de instante específico para recuperar los datos. Los datos se restauran a partir de la copia de seguridad completa original y todos los bloques cambiados asociadas con los datos.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>
Elemento de recuperación para archivos y carpetas a partir de una copia de seguridad completa de la máquina virtual:	Ofrece la posibilidad de recuperar archivos y carpetas a partir de una copia de seguridad completa de una máquina virtual. La recuperación de elementos solo está disponible con el IBM Spectrum Protect Recovery Agent.
Restauración completa de la máquina virtual:	Restaura todos los sistemas de archivos, discos virtuales y la configuración de la máquina virtual.

 Sistemas operativos Windows La Tabla 2 lista las operaciones de copia de seguridad y restauración para máquinas virtuales VMware que el cliente de archivado y copia de seguridad puede realizar modificaciones en las plataformas Windows.

Restricción: Puede completar las operaciones de copia de seguridad y restauración de VMware con el cliente de copia de seguridad y archivado sólo en sistemas operativos Windows de 64 bits.







Tabla 2. Prestaciones de copia de seguridad y restauración para máquinas virtuales VMware en plataformas Windows

Prestación	Observación
------------	-------------

Prestación	Observación
Copia de seguridad de máquina virtual incremental-constante completa:	<p>Requiere el producto bajo licencia de IBM Spectrum Protect for Virtual Environments.</p> <p>Una copia de seguridad de máquina virtual completa es necesaria antes de poder crear copias de seguridad incrementales. Si planifica copias de seguridad incrementales, constantes, este tipo de copia de seguridad se selecciona automáticamente para la primera copia de seguridad si una copia de seguridad completa no se hubiera creado todavía. Los datos de copias de seguridad incrementales se combinan con datos de la copia de seguridad completa para crear una imagen sintética de la copia de seguridad completa. Las copias de seguridad incrementales, constantes subsiguientes leen todos los bloques utilizados y los copian en el servidor IBM Spectrum Protect. Cada copia de seguridad completa, incremental, constante, de máquina virtual lee y copia todos los bloques utilizados, tanto si han cambiado los bloques o no, desde la copia de seguridad anterior. Aún puede planificar una copia de seguridad completa de la máquina virtual, aunque una copia de seguridad completa ya no sea necesaria. Por ejemplo, puede ejecutar una copia de seguridad completa de máquina virtual para crear una copia de seguridad a un nodo con otro nombre, con los valores de retención diferentes.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>
Copia de seguridad de máquina virtual incremental-constante-incremental:	<p>Requiere el producto bajo licencia de IBM Spectrum Protect for Virtual Environments.</p> <p>Requiere que cree una copia de seguridad completa de la máquina virtual una única vez. La copia de seguridad completa de la máquina virtual copia todos los bloques de disco utilizados propiedad de una máquina virtual en el servidor de IBM Spectrum Protect. Después de completarse la copia de seguridad completa inicial, todas las copias de seguridad posteriores de la máquina virtual son copias incrementales, constantes, incrementales. Cada copia de seguridad incremental, contante, incremental copia únicamente los bloques que se han modificado desde la copia de seguridad anterior, independientemente del tipo de la copia de seguridad anterior. El servidor utiliza una tecnología de agrupación que asocia los bloques cambiados a partir de la copia de seguridad más reciente con datos ya almacenados en el servidor de copias de seguridad anteriores. Una copia de seguridad completa nueva se crea, entonces, cada vez que los bloques cambiados se copian en el servidor mediante una copia de seguridad incremental, constante, incremental.</p> <p>La modalidad de copia de seguridad incremental, constante, incremental proporciona las ventajas siguientes:</p> <ul style="list-style-type: none"> <li>• Mejora la eficacia de la realización de copias de seguridad de máquinas virtuales.</li> <li>• Simplifica las operaciones de restauración de datos.</li> <li>• Optimiza las operaciones de restauración de datos.</li> </ul> <p>Durante una operación de restauración, puede especificar opciones para la hora de instante específico y la fecha de instante específico para recuperar los datos. Los datos se restauran a partir de la copia de seguridad completa original y todos los bloques cambiados asociadas con los datos.</p> <p>No puede utilizar esta modalidad de copia de seguridad para realizar la copia de seguridad de la máquina virtual de VMware si el cliente se configura para cifrar los datos de copia de seguridad.</p>
Elemento de recuperación para archivos y carpetas a partir de una copia de seguridad completa de la máquina virtual:	<p>Requiere el producto bajo licencia de IBM Spectrum Protect for Virtual Environments.</p> <p>Ofrece la posibilidad de recuperar archivos y carpetas a partir de una copia de seguridad completa de una máquina virtual. La recuperación de elementos solo está disponible con el IBM Spectrum Protect Recovery Agent.</p>
Restauración completa de la máquina virtual:	<p>Restaura todos los sistemas de archivos, discos virtuales y la configuración de la máquina virtual.</p>



Prestación	Observación
Restauración a nivel de archivos de la máquina virtual:	<p>El acercamiento de restauración depende del tipo de copia de seguridad de la máquina virtual:</p> <ul style="list-style-type: none"> <li>• Si tiene licencia para IBM Spectrum Protect for Virtual Environments, puede restaurar los archivos y directorios a partir de una copia de seguridad de imagen de máquina virtual completa.</li> <li>• Los usuarios del cliente de archivado y copia de seguridad pueden restaurar los archivos y directorios creados por las copias de seguridad a nivel de archivos de una máquina virtual. Utilice el mandato restore para restaurar archivos individuales desde una copia de seguridad a nivel de archivos de una máquina virtual, nunca el mandato restore vm.</li> </ul> <p>Nota: Las operaciones de copia de seguridad a nivel de archivo se han creado con clientes de copia de seguridad y archivado de la versión 7.1 o anterior.</p>


-  Sistemas operativos Linux  Sistemas operativos Windows Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware  
 Utilice los siguientes pasos para preparar el entorno VMware para realizar copias de seguridad de máquinas virtuales VMware completas. El servidor de seguridad de vStorage puede ejecutar un cliente de Windows o de Linux.
-  Sistemas operativos Linux  Sistemas operativos Windows Creación de copias de seguridad completas de máquinas virtuales VMware  
 Una copia de seguridad completa de una máquina virtual VMware es una copia de la totalidad de la máquina virtual, incluidos los discos virtuales y el archivo de configuración de la máquina virtual. Este tipo de copia de seguridad es parecido a una copia de seguridad de imágenes de imagen. Para crear una copia de seguridad completa, configure el cliente de archivado y copia de seguridad en el servidor de seguridad vStorage. El servidor de seguridad vStorage debe ejecutarse en un cliente Windows o Linux.
-  Sistemas operativos Linux  Sistemas operativos Windows Copias de seguridad paralelas de máquinas virtuales  
 Con un proceso de copia de seguridad paralela, puede utilizar un único nodo de transportador de datos para realizar la copia de seguridad de varias máquinas virtuales (VM) al mismo tiempo y así optimizar el rendimiento de las copias de seguridad.

 Sistemas operativos Linux  Sistemas operativos Windows


## Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware


Utilice los siguientes pasos para preparar el entorno VMware para realizar copias de seguridad de máquinas virtuales VMware completas. El servidor de seguridad de vStorage puede ejecutar un cliente de Windows o de Linux.

### Antes de empezar


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

### Procedimiento

- Para configurar el entorno de almacenamiento para copias de seguridad, complete los pasos siguientes:
  - Configure el entorno de almacenamiento para que el servidor de copias de seguridad de vStorage pueda acceder a los volúmenes de almacenamiento que están en el conjunto de servidores ESX.
  - Si utiliza almacenamiento conectado a red (NAS) o almacenamiento conectado de forma directa, asegúrese de que el servidor de seguridad vStorage accede a los volúmenes con transporte basado en red.
  - Opcional: Para el acceso a datos, haga lo siguiente:
    - Cree zonas de red de área de almacenamiento (SAN) que su servidor de seguridad vStorage pueda utilizar para acceder a las unidades lógicas de almacenamiento (LUN) en las que se encuentran sus almacenes de datos VMware.
    - Configure sus correlaciones de host de subsistema de discos para que todos los servidores ESX y el proxy de copia de seguridad puedan acceder a los mismos volúmenes de disco.
- Para configurar el servidor de seguridad vStorage, complete los pasos siguientes:
  -  Sistemas operativos Linux Configure y exporte la variable de entorno LD\_LIBRARY\_PATH para que apunte al directorio de instalación del cliente. Por ejemplo:
 

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```
  -  Sistemas operativos Linux Añada el directorio de instalación del cliente a la vía de acceso de cada cuenta que utiliza los mandatos del cliente de archivado y copia de seguridad, por ejemplo, dsmc, dsmcad o dsmj.
 

```
export LD_LIBRARY_PATH=/opt/tivoli/tsm/client/ba/bin
```

- c.  Sistemas operativos Windows Cuando el cliente de archivado y copia de seguridad se ejecute en un servidor de seguridad vStorage, se hará referencia a esta configuración de cliente como el IBM Spectrum Protect *nodo transportador de datos*. Un sistema de Windows que es un transportador de datos debe tener un cliente de Windows de 64 bits instalado. Un nodo transportador de datos utiliza normalmente el SAN para realizar copias de seguridad y restaurar datos. Si configura el nodo transportador de datos para acceder directamente a los volúmenes de almacenamiento, desactive la asignación de letra de unidad automática. Si no se desactiva, el cliente del nodo transportador de datos podría dañar la correlación de datos sin procesar (RDM) de los discos virtuales. Si la RDM de los discos virtuales está dañada, la copia de seguridad fallará. Al restaurar configuraciones, tenga en cuenta las siguientes condiciones:

El nodo de transportador de datos se encuentra en un sistema Windows Server 2012 o Windows Server 2012 R2:

Si prevé el uso de la SAN para restaurar datos, debe definir la política de SAN de Windows como OnlineAll. Ejecute diskpart.exe y escriba los mandatos siguientes para desactivar la asignación automática de letra de unidad y establezca la política de SAN en OnlineAll:

```
diskpart
  automount disable
  automount scrub
  san policy OnlineAll
  exit
```



El cliente de archivado y copia de seguridad está instalado en una máquina virtual en un sistema Windows Server 2012 o Windows Server 2012 R2:


Si prevé el uso del transporte hotadd para restaurar datos desde discos añadidos dinámicamente, la política de SAN de ese sistema debe estar definida como OnlineAll.

Si el cliente utiliza la SAN o el transporte hotadd, la política de SAN de Windows debe estar definida como OnlineAll. Si la política de SAN no está definida como OnlineAll, las operaciones de restauración fallarán y se devolverá el siguiente mensaje:

```
ANS9365E VMware vStorage API error.
IBM Spectrum Protect function name: vddksdk Write
IBM Spectrum Protect file : vmvddksdk.cpp (2271)
API return code : 1
API error message : Unknown error
ANS0361I DIAG: ANS1111I VmRestoreExtent(): VixDiskLib Write
FAILURE startSector=512 sectorSize=512 byteOffset=262144,
rc=-1
```

Para ver una descripción de los valores de transporte de vStorage y saber cómo puede sustituir los valores predeterminados, consulte el tema siguiente:

 Sistemas operativos Linux  Sistemas operativos Windows Vmstortransport

- d.  Sistemas operativos Windows Instale el cliente de copia de seguridad y archivado en el servidor de seguridad vStorage. En la página de configuración personalizada del asistente de instalación, seleccione Archivos de tiempo de ejecución de API de vStorage VMware.


Importante: Si va a mover los datos de copia de seguridad mediante una copia de seguridad fuera de la LAN, la SAN debe tener conexiones independientes para la cinta y el disco.


3. Para modificar IBM Spectrum Protect, complete los pasos siguientes:

- a. Acceda a la línea de mandatos de administración del cliente de copia de seguridad y archivado.  
b. Desde el cliente de copia de seguridad y archivado del servidor de seguridad vStorage, escriba el siguiente mandato para registrar el nodo:

```
register node my_server_name my_password
```


Donde *my\_server\_name* es el nombre completo del sistema del servidor de seguridad vStorage y *my\_password* es la contraseña para acceder a él.

 Sistemas operativos Windows Consejo: En los sistemas Windows, puede obtener el nombre del sistema completo del servidor pulsando con el botón derecho del ratón en Mi PC. Pulse en la pestaña de nombre de sistema y consulte la lista que aparece al lado de Nombre completo del sistema.

- c.  Sistemas operativos Windows Desde el cliente de copia de seguridad y archivado del servidor de seguridad vStorage, escriba el siguiente mandato para registrar el nodo:

```
register node my_vm_name my_password
```

donde *my\_vm\_name* es el nombre completo de la máquina virtual de la que se va a realizar una copia de seguridad.

4.  Sistemas operativos Windows Si realiza una copia de seguridad de una máquina virtual en la que hay volúmenes montados en directorios en vez de en letras de unidad, los archivos podrían no almacenarse en la ubicación correcta. Los errores podrían deberse a que el punto de montaje no se corresponde con los puntos de montaje reales de los archivos copiados. Los errores se deben a que los puntos de montaje de una máquina virtual que se ejecuta en Windows no tienen ninguna asignación de letra de unidad. Cuando utilice vStorage APIs de VMware para Data Protection, se crea un nombre de espacio de archivo que incluye



una asignación de número. Los nombres de `espacio de archivo` que se han creado para el punto de montaje no se corresponden con los puntos de montaje reales del archivo del que se ha realizado una copia de seguridad.

Para realizar una copia de seguridad o restaurar los archivos en su ubicación original, siga estos pasos:

















- Para restaurar los archivos a su ubicación original, correlacione la unidad o asigne una letra de unidad al punto de montaje desde la máquina virtual.
- Si restaura un archivo que renombró la vStorage API, seleccione una ubicación de restauración diferente.
- Cuando utilice los puntos de montaje sin las asignaciones de la letra de unidad, utilice una sentencia de inclusión o exclusión para ese volumen. Consulte el siguiente ejemplo de una sentencia de exclusión:

```
exclude \\machine\3$\dir1\...\*.doc
```

#### Tareas relacionadas:

 Sistemas operativos Linux  Sistemas operativos Windows Creación de copias de seguridad completas de máquinas virtuales VMware


#### Referencia relacionada:

 Sistemas operativos Linux  Sistemas operativos Windows Backup VM  
 Sistemas operativos Linux  Sistemas operativos Windows Query VM  
 Sistemas operativos Linux  Sistemas operativos Windows Restore VM  
 Sistemas operativos Linux  Sistemas operativos Windows Vmchost  
 Sistemas operativos Linux  Sistemas operativos Windows Vmcpw  
 Sistemas operativos Linux  Sistemas operativos Windows Vmcuser  
 Sistemas operativos Linux  Sistemas operativos Windows Vmvtortransport  
 Sistemas operativos Linux  Sistemas operativos Windows

## Creación de copias de seguridad completas de máquinas virtuales VMware

Una copia de seguridad completa de una máquina virtual VMware es una copia de la totalidad de la máquina virtual, incluidos los discos virtuales y el archivo de configuración de la máquina virtual. Este tipo de copia de seguridad es parecido a una copia de seguridad de imágenes de imagen. Para crear una copia de seguridad completa, configure el cliente de archivado y copia de seguridad en el servidor de seguridad vStorage. El servidor de seguridad vStorage debe ejecutarse en un cliente Windows o Linux.

### Antes de empezar

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

### Procedimiento

- Para preparar el entorno, complete los pasos del siguiente tema:

Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware


- Para configurar el cliente de archivado y copia de seguridad en un servidor de seguridad vStorage, complete los pasos siguientes:
  - Desde la página de bienvenida de la GUI del cliente de copia de seguridad y archivado, pulse Editar > Preferencias del cliente.
  - Seleccione la ficha Copia de seguridad de máquina virtual.
  - Seleccione Máquina virtual completa de VMWare.
  - En la lista de Tipos de copia de seguridad de dominio, seleccione Máquina virtual de dominio.
  - En el campo Host, especifique un nombre de host para cada servidor ESX o el nombre de host del centro virtual. Si especifica el centro virtual, puede realizar la copia de seguridad de las máquinas virtuales desde cualquier servidor VMware gestionado por dicho centro virtual.
  - Escriba la información de contraseña y de ID de usuario para el host que ha especificado en el campo Host.
  - Opcional: Si desea sobrescribir la clase de gestión predeterminada para las copias de seguridad de la máquina virtual completa, especifique la clase de gestión que desee utilizar.
  - En el campo Ubicación del almacén de datos, especifique la vía de acceso al directorio donde se almacenarán los archivos.
  - Pulse Aceptar para guardar los cambios.
- Para crear una copia de seguridad de las máquinas virtuales, complete los pasos siguientes:
  - En la línea de mandatos del servidor de seguridad vStorage, ejecute el siguiente mandato:

```
dsmc backup vm my_vm_name -mode=ifull -vmbackuptype=fullvm
```

Donde `my_vm_name` es el nombre de su máquina virtual.

- Compruebe que el mandato se completa sin errores. El siguiente mensaje indicará una terminación correcta:


```
Mandato de copia de seguridad de la máquina virtual completo
Número total de máquinas virtuales que se han copiado con éxito: 1
máquina virtual vmname copiada a nodename NODE
Número total de máquinas virtuales que han fallado: 0
Número total de máquinas virtuales procesadas: 1
```

4.  **Sistemas operativos Linux** Para verificar si puede restaurar los archivos para la máquina virtual, complete los pasos siguientes:
  - a. En la interfaz de línea de mandatos del servidor de seguridad vStorage, ejecute el mandato siguiente:

```
dsmc restore vm my_vm_name
```


- b. Si se produce algún error en el proceso de restauración, consulte el archivo de registro de errores para obtener más información.

Consejo: El archivo de registro se guarda en /opt/ibm/Tivoli/TSM/baclient/dsmerror.log

5.  **Sistemas operativos Windows** Para verificar si puede restaurar los archivos para la máquina virtual, complete los pasos siguientes:

- a. En la interfaz de línea de mandatos del servidor de seguridad vStorage, ejecute el mandato siguiente:

```
dsmc restore vm my_vm_name
```



 **Sistemas operativos Windows** La ubicación predeterminada de la restauración está en el siguiente directorio:  
c:\mnt\tsmvmbackup\my\_vm\_name\fullvm\RESTORE\_DATE\_yyyy\_mm\_dd[hh\_mm\_ss].

- b. Si se produce algún error en el proceso de restauración, consulte el archivo de registro de errores para obtener más información.



Consejo: El registro de errores se guarda en el siguiente archivo:

```
c:\Archivos de Programa\Tivoli\TSM\baclient\dsmerror.log
```

























#### Conceptos relacionados:

 **Sistemas operativos Linux**  **Sistemas operativos Windows** Copias de seguridad paralelas de máquinas virtuales

#### Tareas relacionadas:


 **Sistemas operativos Linux**  **Sistemas operativos Windows** Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware

#### Referencia relacionada:

 **Sistemas operativos Linux**  **Sistemas operativos Windows** Backup VM  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Domain.vmfull  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Query VM  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Restore VM  
 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Windows** Mode  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Vmchost  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Vmcpw  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Vmcuser  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Vmmc  
 **Sistemas operativos Linux**  **Sistemas operativos Windows** Vmvstortransport  
 **Sistemas operativos Linux**  **Sistemas operativos Windows**

## Copias de seguridad paralelas de máquinas virtuales

Con un proceso de copia de seguridad paralela, puede utilizar un único nodo de transportador de datos para realizar la copia de seguridad de varias máquinas virtuales (VM) al mismo tiempo y así optimizar el rendimiento de las copias de seguridad.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.


Para obtener información sobre las operaciones de copia de seguridad paralela, consulte el apartado Realización de copias de seguridad de varias máquinas virtuales en paralelo.

 **Sistemas operativos Windows**

## Realización de copias de seguridad de máquinas virtuales en un sistema Hyper-V

Puede utilizar el cliente de archivado y copia de seguridad para realizar copias de seguridad de máquinas virtuales gestionadas por un servidor de Microsoft Hyper-V.

Para obtener información sobre cómo proteger las máquinas virtuales de Hyper-V, consulte el apartado IBM Spectrum Protect for Virtual Environments, Data Protection for Microsoft Hyper-V .

-  Sistemas operativos Windows Limitaciones de soporte de copia de seguridad de Hyper-V  
Debido a la integración estrecha la Agrupación en clúster de migración tras error de Microsoft con los volúmenes compartidos e Hyper-V, las siguientes limitaciones se aplican cuando utiliza el cliente de copia de seguridad y archivado.

 Sistemas operativos Linux  Sistemas operativos Windows

## Copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

---

Utilice Tivoli Storage Manager FastBack para realizar copias de seguridad y archivado de las instantáneas más recientes para retención a corto plazo.

Utilice los mandatos `archive fastback` y `backup fastback` para archivar y realizar una copia de seguridad de volúmenes especificados mediante las opciones `fbpolicyname`, `fbclientname` y `fbvolumename` para retención a largo plazo.

### Conceptos relacionados:

Requisitos de instalación de copia de seguridad y archivado de datos de cliente de Tivoli Storage Manager FastBack

Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

### Referencia relacionada:

`Fbclientname`

`Fbpolicyname`

`Fbvolumename`

 Sistemas operativos Windows

## Copia de seguridad de las definiciones de compartición de Net Appliance CIFS

---

Las definiciones de compartición de Network Appliance (NetApp) CIFS incluyen los permisos de compartición que se han establecido en el servidor de archivos.

### Acerca de esta tarea

---

El cliente de Windows realiza la copia de seguridad de la definición de compartición de CIFS en el directorio raíz, la compartición de CIFS correlacionado o en el nombre UNC. Este soporte necesita que el servidor de archivos de Net Appliance ejecute software DATA ONTAP que presente los compartimientos de CIFS a los clientes remotos como si se trataran de compartimientos de NTFS remotos normales.

La copia de seguridad del directorio raíz de una compartición de CIFS se realiza con una copia de seguridad incremental progresiva completa del nombre de unidad/UNC correlacionado. Consulte los dos ejemplos siguientes:

```
net use x: \\NetAppFiler\CifsShareName
dsmc incr x:
```

```
dsmc incr \\NetAppFiler\CifsShareName
```

Se muestra la siguiente salida cuando se realiza la copia de seguridad del directorio raíz (y la definición de compartición):

```
Directory-->                0 \\NetAppFiler\CifsShare\ [Sent]
```

### Conceptos relacionados:

Restaurar compartimientos de Net Appliance CIFS

### Referencia relacionada:

`Snapdiff`





## Visualización del estado del proceso de copia de seguridad


---

Durante una copia de seguridad, de forma predeterminada, el cliente de copia de seguridad y archivado muestra el estado de cada archivo del que intenta realizar una copia de seguridad.

El cliente informa del tamaño, la vía de acceso, el nombre del archivo, el número total de bytes transferidos y de si el intento de copia de seguridad se ha realizado correctamente. Estos datos también se registran en el archivo `dsmsched.log` para los mandatos

planificados.

























 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El cliente web y la GUI de Java™ del cliente de copia de seguridad/archivado proporcionan una ventana denominada Lista de tareas en la que se visualiza información acerca de los archivos durante el proceso. Cuando finaliza una tarea, la ventana Informe de copia de seguridad muestra los detalles del proceso. Pulse el botón Ayuda en la ventana Informe de copia de seguridad para obtener la ayuda contextual.

















 Sistemas operativos Windows El cliente web y la GUI del cliente de copia de seguridad/archivado proporcionan una ventana denominada Lista de tareas en la que se visualiza información acerca de los archivos durante el proceso. Cuando finaliza una tarea, la ventana Informe de copia de seguridad muestra los detalles del proceso. Pulse el botón Ayuda en la ventana Informe de copia de seguridad para obtener la ayuda contextual.














En la línea de mandatos de copia de seguridad y archivado, el nombre de cada archivo se visualiza después de enviarlo al servidor. En el indicador de progreso se muestra el progreso general.

Tabla 1 enumera algunos mensajes informativos y significados.

Tabla 1. Mensajes informativos de la línea de mandatos del cliente


Mensaje informativo	Significado
Directory-->	Indica el directorio del que se debe hacer una copia de seguridad.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Normal File-->.	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Cualquier archivo que no sea un directorio, un vínculo simbólico o un archivo especial.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Special File-->	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Los archivos especiales definen dispositivos para el sistema o archivos temporales creados por procesos. Existen tres tipos básicos de archivos especiales: FIFO (el primero en entrar es el primero en salir), de bloques y de caracteres. Los archivos FIFO también se denominan conductos. Los pipes los crea un proceso para permitir temporalmente la comunicación con otro proceso. Estos archivos dejan de existir cuando finaliza el primer proceso. Los archivos de bloques y de caracteres definen dispositivos. El cliente sólo procesa archivos especiales de dispositivos y conductos con nombre. Los archivos especiales de socket no se procesan.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Symbolic Link-->	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Indica que el cliente realiza una copia de seguridad de un enlace simbólico.
Updating-->	Indica que solamente se envían metadatos del archivo, no el propio archivo.
Expiring-->	Indica que un objeto (archivo o directorio) del servidor que ya no existe en el cliente pasa a estar caducado e inactivo en el servidor.
Total objetos inspeccionados:	Según se indica. Cuando se utiliza la copia de seguridad con registro por diario, el número de objetos inspeccionados podría ser menor que el número de objetos cuya copia de seguridad se ha realizado.  Cuando se utiliza la copia de seguridad incremental de diferencias de instantáneas, el número de objetos que se inspeccionan es cero. El número es cero porque el cliente realiza una copia de seguridad incremental de los archivos que NetApp marca como un cambio. El cliente no explora el volumen en busca de archivos que han cambiado.
Total objetos con copia de seguridad:	Según se indica.
Número total de objetos cifrados:	Se trata de un recuento de los objetos que se han cifrado durante el proceso de copia de seguridad o de archivo.
Tipo de cifrado de datos:	Especifica el tipo de algoritmo de cifrado (por ejemplo, AES de 256 bits), si se han cifrado uno o varios objetos durante el proceso de copia de seguridad o de archivo.
Total objetos actualizados:	Son los archivos cuyos atributos como, por ejemplo, el propietario o los permisos del archivo, han cambiado.

Mensaje informativo	Significado
Total objetos vueltos a vincular:	Para obtener más información, consulte el apartado Vincular clases de gestión a archivos.
Total objetos suprimidos:	Es un recuento de los objetos que se suprimen de la estación de trabajo cliente después de haberse archivado correctamente en el servidor. El recuento es cero para todos los mandatos de copia de seguridad.
Total objetos caducados:	Para obtener más información, consulte la sección acerca de las copias de seguridad incrementales completas y parciales.
Total objetos no restaurados:	Los objetos pueden fallar por diversas razones. Consulte el archivo dsmerror.log para obtener más detalles.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Número total de objetos de diferencia de instantánea:	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Para copias de seguridad incrementales de diferencia de instantánea, ello representa el número total de objetos a los que se ha realizado una copia de seguridad y el número total de objetos caducados.
Total de objetos con optimización de almacenamiento:	Especifica el número de archivos cuyas duplicaciones se han eliminado.
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Número total de bytes inspeccionados:	 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Especifica el tamaño total de los archivos que se han seleccionado para la operación. Por ejemplo, el número total de bytes inspeccionados para este mandato es el número de bytes que se utilizan en el volumen /Volumes/BUILD:  <code>dsmc INCREMENTAL /Volumes/BUILD/* -SU=Yes</code>
Bytes totales antes de la optimización de almacenamiento:	Especifica el número de bytes que se enviarán al servidor de IBM Spectrum Protect y si el cliente no elimina datos redundantes. Compare esta cantidad con Total de bytes después de la optimización de almacenamiento. Incluye el tamaño de metadatos y puede ser superior a los bytes inspeccionados.
Total de bytes después de la optimización de almacenamiento	Especifica el número de bytes que se envían al servidor de IBM Spectrum Protect después de la deduplicación de los archivos en el sistema cliente. Incluye el tamaño de metadatos y puede ser superior a los bytes procesados.
 Sistemas operativos Windows Número total de bytes inspeccionados:	 Sistemas operativos Windows Especifica el tamaño total de los archivos que se han seleccionado para la operación. Por ejemplo, el número total de bytes inspeccionados para este mandato es el número de bytes utilizados en el directorio C:\Users  <code>dsmc.exe INCREMENTAL C:\Users\* -su=yes</code>
Número total de bytes procesados:	Especifica el tamaño total de los archivos que se han procesado para la operación.
Tiempo de transferencia de datos:	El tiempo total para transferir datos a través de la red. Las estadísticas de la transferencia podrían no coincidir con las estadísticas del archivo si ha vuelto a intentarse ejecutar la operación debido a una anomalía en las comunicaciones o a la pérdida de la sesión. Las estadísticas de transferencia muestran el número de bytes que se intentó transferir durante todos los intentos realizados con el mandato.
Velocidad de transferencia de datos en red:	La velocidad media a la que la red transfiere datos entre el cliente y el servidor. La velocidad se calcula dividiendo el número total de bytes transferidos por el tiempo que ha sido preciso para transferir los datos por la red. El tiempo que el cliente necesita para procesar los objetos no se incluye en la velocidad de transferencia de la red. Por lo tanto, la velocidad de red es superior a la velocidad compuesta.

Mensaje informativo	Significado
Velocidad de transferencia de datos compuesta:	<p>La velocidad media a la que IBM Spectrum Protect y la red transfieren datos entre el cliente y el servidor. La velocidad se calcula dividiendo el número total de bytes transferidos por el tiempo que transcurre desde el principio hasta el final del proceso. En la velocidad de transferencia compuesta se incluyen el tiempo de proceso de IBM Spectrum Protect y el tiempo de la red. Por lo tanto, la velocidad de transferencia compuesta es inferior a la velocidad de transferencia de red.</p> <p> Sistemas operativos Windows <b>Nota:</b> de vez en cuando, la velocidad de transferencia de datos compuesta podría ser superior a la velocidad de transferencia de datos de la red. Esto es debido a que el cliente de copia de seguridad/archivado puede tener varias sesiones simultáneas con el servidor de copia de seguridad. Si establece la opción resourceutilization, el cliente intenta mejorar el rendimiento y el equilibrio de carga utilizando varias sesiones cuando realiza una copia de seguridad de un volumen u otros juegos de archivos. Si hay varias sesiones abiertas durante la operación de copia de seguridad, el tiempo de transferencia de datos representa la suma de los tiempos de todas las sesiones. En este caso, el tiempo de transferencia de datos compuesta se visualizará incorrectamente con un valor mayor. Sin embargo, si se ejecuta una sola sesión, la velocidad de transferencia de datos compuesta siempre se visualizará con un valor menor que la velocidad de transferencia de datos en red.</p> <p> sistemas operativos Mac OS X  Sistemas operativos AIX   Sistemas operativos Linux  Sistemas operativos Oracle Solaris</p> <p>Nota: A veces, la velocidad de transferencia de datos agregados puede ser más alta que la velocidad de transferencia de datos de red. Esto es debido a que el cliente de copia de seguridad/archivado puede tener varias sesiones simultáneas con el servidor de copia de seguridad. Si establece la opción resourceutilization, el cliente intenta mejorar el rendimiento y el equilibrio de carga utilizando varias sesiones cuando realiza una copia de seguridad de un espacio de archivos u otros juegos de archivos. Si hay varias sesiones abiertas durante la operación de copia de seguridad, el tiempo de transferencia de datos representa la suma de los tiempos de todas las sesiones. En este caso, el tiempo de transferencia de datos compuesta se visualizará incorrectamente con un valor mayor. Sin embargo, si se ejecuta una sola sesión, la velocidad de transferencia de datos compuesta siempre se visualizará con un valor menor que la velocidad de transferencia de datos en red.</p>
Comprimido:	Especifica el porcentaje de datos enviados por la red dividido por el tamaño original del archivo en el disco. Por ejemplo, si los bytes de datos enviados por la red son 10 K y el archivo tiene 100 K, el valor de compresión será: $== (1 - (10240/102400)) \times 100 == 90\%$ .
Total number of objects grew:	El número total de archivos que han aumentado como resultado de la compresión.
Reducción de optimización de almacenamiento:	Especifica el tamaño de las extensiones duplicadas que se han encontrado, dividido por el tamaño inicial de los datos o del archivo. Por ejemplo, si el tamaño de objeto inicial es de 100 MB, tras la optimización de almacenamiento, será de 25 MB. La reducción sería: $(1 - 25/100) \times 100 = 75\%$ .
Proporción de reducción de datos en total:	Añade efectos de compresión e incrementales. Por ejemplo, si los bytes inspeccionados son 100 MB y los bytes enviados son 10 MB, la reducción sería: $(1 - 10/100) \times 100 = 90\%$
Tiempo del proceso:	El tiempo de proceso activo que requiere completar un mandato. Esto se calcula restando la hora de inicio del proceso de un mandato a la hora final de la finalización del proceso del mandato.
Total bytes transferidos:	Según se indica.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Número total de bytes transferidos fuera de la LAN:	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Número total de bytes de datos transferidos durante una operación fuera de la LAN. Si la opción enablelanfree se establece en no, esta línea no aparecerá.
Número total de bytes inspeccionados:	El tamaño total de los archivos seleccionados para la operación.












Mensaje informativo	Significado
Número total de reintentos:	El número total de reintentos durante una operación de copia de seguridad. Según los valores del atributo de serialización y la opción <code>changingretries</code> , es posible que no se haga copia de seguridad de un archivo abierto por otro proceso durante el primer intento de copia de seguridad. Es posible que el cliente de copia de seguridad intente hacer copia de seguridad de un archivo varias veces durante una operación de copia de seguridad. Este mensaje indica el número total de reintentos para todos los archivos incluidos en la operación de copia de seguridad.

 Sistemas operativos Windows

## Copia de seguridad(Windows): Consideraciones adicionales

En este apartado trata sobre la información adicional que debe tenerse en cuenta al realizar una copia de seguridad de los datos.

-  **Sistemas operativos WindowsArchivos abiertos**  
Es posible que algunos archivos de su sistema se estén utilizando cuando intente realizar la copia de seguridad de los mismos. Estos se denominan *archivos abiertos* debido a que una aplicación los ha bloqueado para su utilización exclusiva.
-  **Sistemas operativos WindowsNombre de espacio de archivo antiguos en especificaciones de archivos**  
Si tiene dos o más espacios de archivos de modo que el nombre de un espacio de archivo es el mismo que el inicio de otro nombre de espacio de archivo, existirá una ambigüedad cuando intente restaurar, recuperar, consultar o realizar cualquier otra operación en la que sea necesario el nombre de espacio de archivo como parte de la especificación del mismo.
-  **Sistemas operativos WindowsClases de gestión**  
IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor.
-  **Sistemas operativos WindowsSistemas de archivos suprimidos**  
Cuando se ha suprimido un sistema de archivos o una unidad, o dejan de hacerse copias de seguridad de estos mediante el cliente, las versiones de copia de seguridad existentes de cada archivo se gestionan según los siguientes atributos de política: Número de días que se deben mantener inactivas las versiones de copia de seguridad y número de días que se debe mantener la última versión de copia de seguridad (si no hay ninguna versión activa).
-  **Sistemas operativos WindowsCopia de seguridad de soportes de almacenamiento extraíbles**  
El cliente de copia de seguridad y archivado realiza copias de seguridad de los medios extraíbles (tales como cintas, cartuchos o disquetes) según la etiqueta de la unidad, no la letra de la misma.
-  **Sistemas operativos WindowsUnidades fijas**  
El cliente de copia de seguridad y archivado puede realizar una copia de seguridad de las unidades fijas aunque no tengan una etiqueta, incluidos los alias de unidad creados con el mandato **subst** de DOS. Esto se aplica tanto al alias de la unidad como a la unidad física subyacente, ya que el nombre del alias y la etiqueta de la unidad física son lo mismo.
-  **Sistemas operativos WindowsEspacios de archivos NTFS y ReFS**  
Cuando se realiza copia de seguridad de archivos en particiones NTFS o ReFS, el cliente también realiza copia de seguridad de la información de seguridad del archivo y de los siguientes descriptores del archivo.
-  **Sistemas operativos WindowsNombres del convenio de denominación universal**  
Un nombre del convenio de denominación universal (UNC) es un nombre de recurso de red para un recurso compartido en una estación de trabajo.
-  **Sistemas operativos WindowsMétodos de protección de archivo Microsoft Dfs**  
Hay algunos métodos que se pueden utilizar para proteger los datos del entorno Dfs de Microsoft.

 Sistemas operativos Windows

## Archivos abiertos

Es posible que algunos archivos de su sistema se estén utilizando cuando intente realizar la copia de seguridad de los mismos. Estos se denominan *archivos abiertos* debido a que una aplicación los ha bloqueado para su utilización exclusiva.

No es muy habitual que los archivos estén abiertos en el modo 'bloqueado'. Una aplicación puede abrir un archivo de esta forma para impedir que otras aplicaciones o usuarios lean el archivo o accedan a éste pero puede impedir que los programas de copia de seguridad lean el archivo para realizar la copia de seguridad.

La mejor opción no siempre es utilizar la función de archivos abiertos para realizar una copia de seguridad de los archivos abiertos o bloqueados. Podrían existir casos en los que una aplicación abriera un archivo o un grupo de archivos en modalidad 'bloqueada' para impedir el acceso de estos archivos en un estado incoherente.

Para evitar el incremento del uso del procesador al crear una instantánea de volumen para cada copia de seguridad, y en las plataformas en las que la función de archivos abiertos no esté disponible o no esté en uso, tenga en cuenta los siguientes puntos:

- Si el archivo no es importante o puede volver a crearse fácilmente (por ejemplo, un archivo temporal), puede pasar por alto el hecho de que no se haya hecho copia de seguridad del mismo y optar por excluirlo.
- Si el archivo es importante:
  - Asegúrese de que esté cerrado antes de intentar realizar copia de seguridad de él. Si las copias de seguridad se ejecutan de acuerdo a una planificación, utilice la opción `preschedulecmd` para escribir un mandato que cierre el archivo. Por ejemplo, si el archivo abierto es una base de datos, emita un mandato para cerrar la base de datos. Puede utilizar la opción `postschedulecmd` para reiniciar la aplicación que utiliza el archivo después de que la copia de seguridad esté completada. Si no está utilizando una planificación para la copia de seguridad, cierre la aplicación que utiliza el archivo antes de arrancar la operación de copia de seguridad.
  - El cliente puede realizar copia de seguridad de un archivo incluso si está abierto y se modifica durante la operación de copia de seguridad. Esto es útil sólo si el archivo está utilizable incluso aunque cambie durante la operación de copia de seguridad. Para efectuar copia de seguridad de estos archivos, asigne una clase de gestión con una serialización *dinámica* o *dinámica compartida*.

Nota: Si el soporte de archivos abiertos no está configurado: esto no siempre es posible mientras el cliente intenta realizar copias de seguridad de los archivos abiertos. Algunos archivos se abren exclusivamente para la aplicación que los abrió. Si el cliente encuentra uno de estos archivos, no podrá leerlo para realizar una copia de seguridad. Si sabe que existe este tipo de archivos en su entorno, debe excluirlos de la copia de seguridad para evitar que aparezcan mensajes de error en el archivo de anotaciones.

**Conceptos relacionados:**

Visualizar información sobre clases de gestión y grupos de copia

Seleccionar una clase de gestión para los archivos

 Sistemas operativos Windows

## Nombre de espacio de archivo antiguos en especificaciones de archivos

Si tiene dos o más espacios de archivos de modo que el nombre de un espacio de archivo es el mismo que el inicio de otro nombre de espacio de archivo, existirá una ambigüedad cuando intente restaurar, recuperar, consultar o realizar cualquier otra operación en la que sea necesario el nombre de espacio de archivo como parte de la especificación del mismo.

Tome como ejemplo los siguientes espacios de archivo y las copias de seguridad que contienen:

Nombre de espacio de archivo	Nombre de archivo
\\storman\home	amr\project1.doc
\\storman\home\amr	project2.doc

Tenga que cuenta que el nombre del primer espacio de archivo, `\\storman\home`, coincide con el comienzo del nombre del segundo espacio de archivo, `\\storman\home\amr`. Cuando utilice la interfaz del cliente de línea de mandatos de copia de seguridad y archivado para restaurar o consultar un archivo desde cualquier de estos espacios de archivo, de forma predeterminada el cliente hace coincidir el nombre de espacio de archivo más largo en la especificación de archivo, `\\storman\home\amr`. Para trabajar con archivos en el espacio de archivos con el nombre más corto `\\storman\home`, utilice llaves `{ }` alrededor de la parte del nombre de espacio de archivo de la especificación de archivo.

Esto significa que el siguiente mandato de consulta encuentra `project2.doc` pero no encuentra `project1.doc`:

```
dsmc query backup "\\storman\home\amr\*"
```


Esto se produce porque el nombre más largo de los dos espacios de archivo es `\\storman\home\amr` y ese espacio de archivo contiene la copia de seguridad de `project2.doc`.

Para encontrar `project1.doc`, meta el nombre del espacio de archivo entre llaves. El siguiente mandato encuentra `project1.doc` pero no encuentra `project2.doc`:

```
dsmc query backup "{\\storman\home}\amr\*"
```

De forma similar, el siguiente mandato restaura `command restores project1.doc` pero no restaura `project2.doc`:

```
dsmc restore {\\storman\home}\amr\project1.doc
```

 Sistemas operativos Windows

## Clases de gestión

IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor.

Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión utilizada es una clase de gestión predeterminada seleccionada o la que el usuario asigne al archivo con la opción `include` en la lista de opciones de

inclusión/exclusión. La clase de gestión seleccionada debe contener un grupo de copia de seguridad para que se realice la copia de seguridad del archivo.

Seleccione **Herramientas** → **Ver información de políticas** en la GUI del cliente de copia de seguridad/archivado o del cliente web para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para su nodo cliente.

**Conceptos relacionados:**

Políticas de gestión de almacenamiento

**Tareas relacionadas:**

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

 Sistemas operativos Windows

## Sistemas de archivos suprimidos

---

Cuando se ha suprimido un sistema de archivos o una unidad, o dejan de hacerse copias de seguridad de estos mediante el cliente, las versiones de copia de seguridad existentes de cada archivo se gestionan según los siguientes atributos de política: Número de días que se deben mantener inactivas las versiones de copia de seguridad y número de días que se debe mantener la última versión de copia de seguridad (si no hay ninguna versión activa).

Si no lleva a cabo ninguna otra acción, las versiones de copia de seguridad activas se conservan indefinidamente. Si no necesita guardar de manera indefinida las versiones activas, utilice el mandato expire para desactivar las versiones activas.

También puede utilizar el mandato delete backup para suprimir versiones de copia de seguridad individuales, o bien el mandato delete filespace para suprimir el espacio de archivos completo. El administrador del servidor de IBM Spectrum Protect deberá otorgarle autorización para suprimir copias de seguridad para que pueda utilizar estos mandatos. Si el espacio de archivos también contiene versiones de archivado, también deberá tener autorización de supresión de archivado para utilizar el mandato delete filespace.

Utilice el mandato query session para determinar si tiene autorización de supresión de archivado y de supresión de copia de seguridad. Como alternativa, solicite al administrador del servidor IBM Spectrum Protect que suprima por usted el espacio de archivos.

Cuando elimina un sistema de archivos, no tiene ningún efecto sobre las versiones de archivado existentes. Sin embargo, si ya no necesita versiones de archivado, puede utilizar los mandatos delete archive o delete filespace para suprimir los archivados.

**Conceptos relacionados:**

Políticas de gestión de almacenamiento

 Sistemas operativos Windows

## Copia de seguridad de soportes de almacenamiento extraíbles

---

El cliente de copia de seguridad y archivado realiza copias de seguridad de los medios extraíbles (tales como cintas, cartuchos o disquetes) según la etiqueta de la unidad, no la letra de la misma.

Si una unidad no tiene etiqueta, no se realiza la copia de seguridad. Utilizar etiquetas de unidad permite realizar tareas tales como realizar copias de seguridad de disquetes diferentes de la unidad a:.

Para una restauración o recuperación, se mantiene un espacio de archivos separado para cada etiqueta de unidad. Estas etiquetas se convierten en los nombres de los espacios de archivos en el servidor de IBM Spectrum Protect. Si se cambia la etiqueta de una unidad de la que ya se ha efectuado copia de seguridad, el cliente la considera una unidad nueva y no la relaciona con la unidad anterior.

Puesto que el cliente utiliza las etiquetas para gestionar copias de seguridad y copias archivadas de los medios extraíbles, el usuario tendrá que usar ocasionalmente estas etiquetas para localizar datos al utilizar mandatos. Por ejemplo, si intenta restaurar un archivo de un disquete o un DVD-ROM con d:\projx\file.exe como nombre de archivo, IBM Spectrum Protect sustituye la etiqueta actual de la unidad d: por la d: . Si la etiqueta de la unidad d: es d-disk, d:\projx\file.exe pasa a ser {d-disk}\projx\file.exe, y la etiqueta se coloca entre llaves.

Si la etiqueta de la unidad d: no coincide con un nombre de espacio de archivos del servidor, IBM Spectrum Protect no podrá localizar los archivos mediante la etiqueta actual de la unidad d: . Sin embargo, el cliente puede localizar los archivos si utiliza el nombre de espacio de archivos de acuerdo con la etiqueta de unidad original. Se puede producir una discrepancia entre una etiqueta y un nombre de espacio de archivos si se etiquetan de nuevo las unidades o si se accede a IBM Spectrum Protect desde una estación de trabajo distinta de la utilizada para realizar la copia de seguridad de los archivos. Si no ha asignado otra etiqueta a la unidad y está en la misma estación de trabajo desde donde realizó la copia de seguridad del archivo, puede utilizar la letra de la unidad como versión abreviada del nombre del espacio de archivos (etiqueta de unidad).

 Sistemas operativos Windows

## Unidades fijas

---

El cliente de copia de seguridad y archivado puede realizar una copia de seguridad de las unidades fijas aunque no tengan una etiqueta, incluidos los alias de unidad creados con el mandato **subst** de DOS. Esto se aplica tanto al alias de la unidad como a la unidad física subyacente, ya que el nombre del alias y la etiqueta de la unidad física son lo mismo.

 Sistemas operativos Windows

## Espacios de archivos NTFS y ReFS

---

Cuando se realiza copia de seguridad de archivos en particiones NTFS o ReFS, el cliente también realiza copia de seguridad de la información de seguridad del archivo y de los siguientes descriptores del archivo.

Se realiza una copia de seguridad de los siguientes descriptores de archivo:

- Información de seguridad de propietario (SID)
- SID de grupo primario
- Lista de control de accesos discrecional
- Lista de control de accesos de sistema

Debe especificar un nombre de espacio de archivos que contenga tanto texto en mayúsculas y minúsculas como texto en minúsculas, y entre comillas y paréntesis. Por ejemplo, {"NTFSDrive"}. En la modalidad de bucle se pueden utilizar indistintamente comillas dobles o comillas simples. Por ejemplo: {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.



 Sistemas operativos Windows

## Nombres del convenio de denominación universal

---

Un nombre del convenio de denominación universal (UNC) es un nombre de recurso de red para un recurso compartido en una estación de trabajo.

El nombre de recurso incluye el nombre asignado a la estación de trabajo y un nombre que el usuario asigna a una unidad o directorio para que pueda compartirse. El nombre que se asigna se conoce también como *nombre de punto compartido*.

-  Sistemas operativos Windows Ejemplos: nombres UNC en las listas de dominios  
En este tema se muestran algunos ejemplos de utilización de nombres UNC para especificar una lista de dominios.
-  Sistemas operativos Windows Ejemplos: copia de seguridad de nombres UNC  
Puede realizar copia de seguridad de archivos compartidos en una red, mediante el uso de un nombre UNC. Se muestran algunos ejemplos de copia de seguridad de archivos de nombre UNC.

 Sistemas operativos Windows

## Ejemplos: nombres UNC en las listas de dominios

---

En este tema se muestran algunos ejemplos de utilización de nombres UNC para especificar una lista de dominios.

### Acerca de esta tarea

---

Debe especificar la siguiente información:

- Una letra de unidad para un medio extraíble
- Letras de unidad o nombres UNC para las unidades fijas locales
- Letras de unidad o nombres UNC para las unidades correlacionadas remotas
- nombres UNC para las unidades remotas no correlacionadas

Ejemplo 1: para especificar una unidad a: que contenga medios extraíbles, escriba:

```
domain a: \\local\c$
```

Ejemplo 2: para especificar la unidad fija c:, escriba:

```
domain c: \\remote\share1 \\remote\c$
```

 Sistemas operativos Windows

## Ejemplos: copia de seguridad de nombres UNC

Puede realizar copia de seguridad de archivos compartidos en una red, mediante el uso de un nombre UNC. Se muestran algunos ejemplos de copia de seguridad de archivos de nombre UNC.

Un nombre UNC es un nombre de recurso de red para un punto compartido de una estación de trabajo. El nombre de recurso incluye el nombre asignado a la estación de trabajo y un nombre que el usuario asigna a una unidad o directorio para que pueda compartirse. El nombre que se asigna se conoce también como nombre de punto compartido.

La utilización de un nombre UNC le permite realizar una copia de seguridad de directorios compartidos específicos en un espacio de archivos separado. Esto le resultará útil si, por ejemplo, usted o el administrador desean realizar una copia de seguridad de una parte pequeña de datos a la que de otra forma no podría acceder. No se realiza copia de seguridad de las unidades en un espacio de archivos separado.

Se puede acceder a las unidades locales mediante un nombre UNC, excepto en el caso de las unidades que contienen medios extraíbles (como cintas, cartuchos o disquetes). Puede acceder a estas unidades utilizando un nombre compartido de administración predefinido, que consiste en la letra de la unidad local seguida del símbolo \$. Por ejemplo, para especificar un nombre UNC en la unidad c: para la estación de trabajo *ocean*, escriba:

```
\\ocean\c$
```

El símbolo \$ *debe* incluirse en la letra de unidad.

Para especificar un nombre UNC para la estación de trabajo *ocean* y el punto compartido *wave*, escriba:

```
\\ocean\wave
```

Cuando acceda a archivos, no es necesario especificar la letra de la unidad, salvo en unidades que contengan medios extraíbles.

Consulte la tabla siguiente para obtener ejemplos sobre la copia de seguridad selectiva de archivos que utilizan nombres UNC. En estos ejemplos se supone lo siguiente:

- La estación de trabajo en la que se ejecuta **dsmc** es *major*.
- Los nombres compartidos *betarc* y *testdir* de la estación de trabajo *alpha1* se correlacionan con las unidades *r* y *t*, respectivamente.

Tabla 1. Ejemplos de UNC

Ejemplo	Observación
dsmc sel \\alpha1\c\$\	el nombre del espacio de archivos remoto es \\alpha1\c\$
dsmc sel \\major\c\$\	el nombre del espacio de archivos fijo local es \\major\c\$
dsmc sel a:\	el nombre del espacio de archivos extraíble local es la etiqueta de volumen de a:
dsmc sel \\alpha1\betarc\	el nombre del espacio de archivos remoto es \\alpha1\betarc
dsmc sel \\alpha1\testdir\	el nombre del espacio de archivos remoto es \\alpha1\testdir
dsmc sel d:\	el nombre del espacio de archivos fijo local es \\major\d\$
dsmc sel c:\	el nombre del espacio de archivos es \\major\c\$
dsmc sel r:\	el nombre del espacio de archivos es \\alpha1\betarc

También puede especificar nombres UNC para las listas de dominios y de inclusión/exclusión.

### Tareas relacionadas:

Creación de una lista de inclusión/exclusión

### Referencia relacionada:

Domain

 Sistemas operativos Windows

## Métodos de protección de archivo Microsoft Dfs

Hay algunos métodos que se pueden utilizar para proteger los datos del entorno Dfs de Microsoft.

### Acerca de esta tarea

A continuación, se muestran los métodos para proteger datos Dfs de Microsoft:

## Procedimiento

---

1. Realice una copia de seguridad de los metadatos de los vínculos Dfs y de los datos reales del destino del recurso compartido de cada vínculo desde la estación de trabajo que contenga la raíz Dfs. Este método simplifica la copia de seguridad y la restauración, ya que consolida todas las actividades de IBM Spectrum Protect en una sola estación de trabajo. La desventaja de este método es que requiere una transferencia adicional a través de la red durante la copia de seguridad para acceder a los datos almacenados en los destinos de los vínculos.
2. Realice una copia de seguridad únicamente de los metadatos de los vínculos Dfs que residan localmente en la estación de trabajo que contenga la raíz Dfs. Realice una copia de seguridad de los datos que hay en el destino de cada vínculo desde la estación de trabajo o las estaciones de trabajo en las que los datos sean también locales. Este método aumenta el rendimiento de las operaciones de copia de seguridad y restauración, ya que elimina la transferencia adicional a través de la red, pero requiere que las operaciones de copia de seguridad y restauración se coordinen entre varias estaciones de trabajo.

## Resultados

---

Nota:

1. Consulte el archivo README del producto para obtener información acerca de las limitaciones actuales de esta función.

Se accede a los archivos contenidos en el componente Servidor Dfs utilizando un nombre UNC estándar, como por ejemplo:

```
\\nombreservidor\raízdfs\
```

siendo nombreservidor el nombre del host y raízdfs el nombre de la raíz Dfs.

Si establece la opción `dfsbackupmntpnt` a `yes` (que es el valor predeterminado), una copia de seguridad incremental de una raíz Dfs no recorre los puntos de unión Dfs. Sólo se efectúa copia de seguridad de los metadatos de punto de unión. Esta es la configuración que debe usar para que el cliente se pueda utilizar para restaurar vínculos Dfs.

Puede utilizar la opción `dfsbackupmntpnt` para especificar si el cliente ve un punto de montaje Dfs como una unión Dfs de Microsoft o como un directorio.

Importante: Restablezca primero los metadatos del punto de unión de Dfs. De este modo, se vuelven a crear los vínculos. A continuación, se debe restaurar cada punto de unión y los datos de cada uno de ellos por separado. Si primero no se restauran los metadatos de los puntos de unión, el cliente creará un directorio en la raíz Dfs utilizando el mismo nombre que el del punto de unión y restaurará los datos en ese directorio.

El ejemplo siguiente se refiere al método 1 expuesto anteriormente y muestra cómo utilizar el cliente para realizar copias de seguridad y restaurar un entorno Microsoft Dfs. Se presupone que existe un entorno Dfs de dominio en la estación de trabajo `wkst1`:

Raíz Dfs

```
\\wkst1\abc64test
```

Vínculo Dfs 1

```
\\wkst1\abc64test\tools
```

Vínculo Dfs 2

```
\\wkst1\abc64test\trees
```

Procedimiento de copia de seguridad:

1. Establezca la opción `dfsbackupmntpnt` en `yes` en el archivo de opciones del cliente (`dsm.opt`).
2. Escriba el mandato siguiente para realizar una copia de seguridad de la información sobre puntos de unión de los vínculos:

```
dsmc inc \\wkst1\abc64test
```

3. Escriba el mandato siguiente para realizar una copia de seguridad de los datos del vínculo `tools`:

```
dsmc inc \\wkst1\abc64test\tools
```

4. Escriba el mandato siguiente para realizar una copia de seguridad de los datos del vínculo `trees`:

```
dsmc inc \\wkst1\abc64test\trees
```

Nota: DFS Replication utiliza carpetas de transición que actúan como cachés para los archivos nuevos y modificados que se van a replicar desde los miembros remitentes a miembros destinatarios. Si no desea realizar una copia de seguridad de estos archivos, puede excluirlos de la copia mediante la opción `exclude.dir`.

```
exclude.dir x:\...\Dfsrprivate
```

Procedimiento de restauración:

1. Vuelva a crear manualmente los recursos compartidos en las estaciones de trabajo de destino en el caso de que no existan.
2. Vuelva a crear la raíz Dfs utilizando el nombre exacto que tenía en el momento de realizar la copia de seguridad.
3. Escriba el mandato siguiente para recuperar los datos del vínculo tools. Este paso no es necesario si los datos siguen existiendo en el destino del vínculo.

```
dsmc restore \\wkst1\abc64test\tools\* -sub=yes
```

4. Escriba el mandato siguiente para recuperar los datos del vínculo trees. Este paso no es necesario si los datos siguen existiendo en el destino del vínculo.

```
dsmc restore \\wkst1\abc64test\trees\* -sub=yes
```

5. Utilice el snap-in de la consola de gestión de DFS para volver a establecer la replicación para cada vínculo, si es necesario.

























Se aplican las siguientes limitaciones a la restauración de datos Dfs de Microsoft:






- El cliente no restaura la raíz de Dfs. Para volver a crear el árbol Dfs, primero debe crear manualmente la raíz Dfs y, a continuación, iniciar la restauración para volver a crear los vínculos.
- El cliente sólo puede realizar una copia de seguridad del árbol Dfs (tanto el Dfs basado en dominio como el Dfs autónomo) situado en la estación de trabajo local. No puede realizar copia de seguridad de Dfs si el servidor host Dfs no es la estación de trabajo local.
- El cliente no puede volver a crear las carpetas compartidas al restaurar. Por ejemplo, si elimina el punto de unión y la carpeta compartida a la que el punto de unión hace referencia, la restauración de la raíz Dfs vuelve a crear el punto de unión Dfs, pero la restauración de un punto de unión crea una carpeta local en lugar de crear la carpeta de red compartida original de la que se realizó copia de seguridad.
- Si se crea un vínculo Dfs con una réplica y el recurso compartido de la réplica se encuentra en un servidor distinto, el cliente no mostrará los datos de la réplica.
- Si se agrega o modifica una raíz de DFS, el cliente no realizará la copia de seguridad de la misma. Debe especificar la raíz de DFS en la opción domain del archivo de opciones del cliente (dsm.opt) independientemente de si se ha especificado DOMAIN ALL-LOCAL.

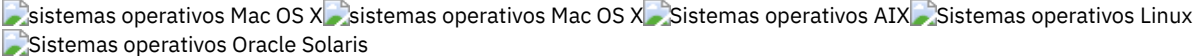
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad(UNIX y Linux): Consideraciones adicionales

Hay algunas situaciones especiales que debe tener en cuenta antes de realizar una copia de seguridad de los datos.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Archivos almacenados  
Al realizar copias de seguridad y copias archivadas de archivos, IBM Spectrum Protect almacena estas copias en un espacio de archivos del almacenamiento que tiene el mismo nombre que el sistema de archivos o el punto de montaje virtual en el que se crearon los archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Sistemas de archivos especiales  
Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. El cliente de copia de seguridad y archivado pasa por alto los sistemas de archivos especiales y su contenido.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
NFS o puntos de montaje virtuales  
Cuando se realiza una copia de seguridad de los archivos y se archivan desde un sistema de archivos o punto de montaje virtual, el cliente no sigue los puntos de montaje NFS o virtuales anidados (si se ha definido alguno en un sistema de archivos). No se realizará copia de seguridad ni se archivarán los puntos de montaje de NFS o virtuales anidados.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Clases de gestión  
IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copias de seguridad de enlaces simbólicos  
El cliente de copia de seguridad y archivado realiza una copia de seguridad de los enlaces simbólicos de manera diferente a los archivos y directorios normales.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Enlaces fijos  
Cuando hace copia de seguridad de archivos que tienen un enlace fijo, el cliente de copia de seguridad y archivado hará una copia de seguridad de cada instancia del archivo enlazado.

- 
**Sistemas operativos AIX** **Sistemas operativos Linux** **Sistemas operativos Oracle Solaris** **Archivos esparcidos**  
 Los archivos esparcidos no tienen espacio de disco asignado para cada bloque en todo el espacio de direcciones, lo que provoca la aparición de espacios vacíos en los archivos. Los espacios vacíos se detectan por su contenido, que siempre está formado por ceros, y estos ceros ocupan espacio.
- 
**sistemas operativos Mac OS X** **Sistemas operativos AIX** **Sistemas operativos Linux** **Sistemas operativos Oracle Solaris**  
**Montajes de hard y soft de NFS**  
 Cuando el cliente de copia de seguridad y archivado se conecta a un sistema de archivos NFS, puede utilizar un montaje por hardware o un montaje por software.
- 
**sistemas operativos Mac OS X** **Sistemas operativos AIX** **Sistemas operativos Linux** **Sistemas operativos Oracle Solaris**  
**Sistemas de archivos suprimidos**  
 Cuando se ha suprimido un sistema de archivos o una unidad, o dejan de hacerse copias de seguridad de los mismos mediante el cliente de copia de seguridad y archivado, las versiones de copia de seguridad existentes de cada archivo se gestionan según los siguientes atributos de política: Número de días que se deben mantener inactivas las versiones de copia de seguridad y número de días que se debe mantener la última versión de copia de seguridad (si no hay ninguna versión activa)
- 
**sistemas operativos Mac OS X** **Sistemas operativos AIX** **Sistemas operativos Linux** **Sistemas operativos Oracle Solaris**  
**Archivos abiertos**  
 El cliente de copia de seguridad y archivado busca archivos que se han modificado entre el inicio y la finalización de la copia de seguridad del archivo.
- 
**sistemas operativos Mac OS X** **Sistemas operativos AIX** **Sistemas operativos Linux** **Sistemas operativos Oracle Solaris**  
**Caracteres comodín**  
 Puede utilizar los caracteres comodín del sistema operativo en las especificaciones de archivo con el cliente de copia de seguridad y archivado. Estos caracteres permiten seleccionar grupos de archivos que tienen nombres similares.


**sistemas operativos Mac OS X** **sistemas operativos Mac OS X** **Sistemas operativos AIX** **Sistemas operativos Linux**  
**Sistemas operativos Oracle Solaris**

## Archivos almacenados

Al realizar copias de seguridad y copias archivadas de archivos, IBM Spectrum Protect almacena estas copias en un espacio de archivos del almacenamiento que tiene el mismo nombre que el sistema de archivos o el punto de montaje virtual en el que se crearon los archivos.

Por ejemplo, si tiene un sistema de archivos denominado `/home` y ha realizado una copia de seguridad de un archivo llamado `doc1` en el directorio `/home/monnett`, IBM Spectrum Protect almacena el archivo en un espacio de archivos llamado `/home`. Si posteriormente define `/home/monnett` como un punto de montaje virtual, cualquier archivo del que realice una copia de seguridad del directorio `/home/monnett`, como por ejemplo `doc2`, se almacena en un espacio de archivos denominado `/home/monnett`. Si especifica este mandato:

```
dsmc query backup "/home/monnett/*"
```

IBM Spectrum Protect busca archivos en el espacio de archivos `/home/monnett`. Siempre busca un archivo en el espacio de archivos con el nombre más largo que coincida con la especificación de archivo que incluya en el mandato. Encuentra el archivo denominado `doc2` cuya copia de seguridad es posterior a la definición del punto de montaje virtual. Sin embargo, no encuentra el archivo denominado `doc1` porque la copia de seguridad de dicho archivo se realizó antes de definir el punto de montaje virtual y la copia de seguridad se almacenó en el espacio de archivos `/home`.

Para listar o restaurar el archivo `doc1` mediante un mandato, debe especificar explícitamente el nombre de espacio de archivos delimitándolo entre llaves. Por ejemplo:

```
dsmc query backup "{/home}/monnett/*"
dsmc restore {/home}/monnett/doc1
```

Si elimina posteriormente el punto de montaje virtual `/home/monnett` y realiza copias de seguridad de más archivos del directorio `/home/monnett`, las copias de seguridad se volverán a almacenar en el espacio de archivos `/home`. Por ejemplo, si realiza una copia de seguridad de un archivo denominado `doc3` del directorio `/home/monnett`, se almacena en el espacio de archivos `/home`. No se almacena en el espacio de archivos `/home/monnett`.

Sin embargo, puesto que el espacio de archivos `/home/monnett` ya existe, cuando intente consultar o restaurar el archivo `doc3`, IBM Spectrum Protect buscará este archivo en el espacio de archivos `/home/monnett` a menos que especifique el nombre del espacio de archivos correcto. Por ejemplo:

```
dsmc query backup "{/home}/monnett/*"
dsmc restore {/home}/monnett/doc2
```

**Nota:** Debe especificar explícitamente el nombre del espacio de archivos sólo cuando puede haber más de una resolución de la especificación del archivo.



Por ejemplo, si existen los espacios de archivos siguientes en el almacenamiento:

```
/home
/home/monnett
/home/monnett/project1
/home/monnett/project1/planning
```

y, a continuación, especifique:

```
dsmc query backup "/home/monnett/project1/planning/*"
```

IBM Spectrum Protect busca archivos sólo en el espacio de archivos `/home/monnett/project1/planning`, aunque uno o varios espacios de archivos contengan una vía de acceso con el mismo nombre. Sin embargo, si especifica una de estas opciones:

```
dsmc query backup "{/home}/monnett/project1/planning/*"
dsmc query backup "{/home/monnett}/project1/planning/*"
dsmc query backup "{/home/monnett/project1}/planning/*"
```

IBM Spectrum Protect busca archivos sólo en el espacio de archivos `/home`, el espacio de archivos `/home/monnett` o el espacio de archivos `/home/monnett/project1`, dependiendo del formato que utilice.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Sistemas de archivos especiales

---

Los sistemas de archivos especiales contienen información dinámica generada por el sistema operativo; no contienen datos ni archivos. El cliente de copia de seguridad y archivado pasa por alto los sistemas de archivos especiales y su contenido.

Los sistemas de archivos especiales son los siguientes:

- el sistema de archivos `/proc` en la mayoría de las plataformas UNIX
- el sistema de archivos `/dev/fd` en Solaris
- el sistema de archivos `/dev/pts` en Linux

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## NFS o puntos de montaje virtuales

---

Cuando se realiza una copia de seguridad de los archivos y se archivan desde un sistema de archivos o punto de montaje virtual, el cliente no sigue los puntos de montaje NFS o virtuales anidados (si se ha definido alguno en un sistema de archivos). No se realizará copia de seguridad ni se archivarán los puntos de montaje de NFS o virtuales anidados .

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Clases de gestión

---

IBM Spectrum Protect utiliza clases de gestión para determinar cómo se deben gestionar las copias de seguridad en el servidor.

Cada vez que efectúe una copia de seguridad de un archivo, se asignará al archivo una clase de gestión. La clase de gestión utilizada es una clase de gestión predeterminada seleccionada o la asignada al archivo con la opción `include` en la lista de opciones de inclusión/exclusión. La clase de gestión seleccionada debe contener un grupo de copia de seguridad para que se realice la copia de seguridad del archivo.

Seleccione **Programas de utilidad** → **Ver información de políticas** en la GUI Java™ o en el cliente web para ver las políticas de copia de seguridad definidas por el servidor de IBM Spectrum Protect para su nodo cliente.

### Conceptos relacionados:

Políticas de gestión de almacenamiento

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copias de seguridad de enlaces simbólicos

---









El cliente de copia de seguridad y archivado realiza una copia de seguridad de los enlaces simbólicos de manera diferente a los archivos y directorios normales.

La manera en la que el cliente realiza una copia de seguridad de los enlaces simbólicos depende de la configuración de las opciones, de la posibilidad de acceder o no al directorio de destino y de la forma de especificación de los objetos.

Un *enlace simbólico UNIX* es un archivo que contiene un puntero a otro archivo o directorio. El objeto al que señala el enlace simbólico se denomina objeto de destino.

Se puede realizar una copia de seguridad de un enlace simbólico como información de la vía de acceso a un directorio de destino o como un directorio. Si se realiza una copia de seguridad del enlace simbólico como un directorio, también se podrá hacer una copia de seguridad de los archivos y carpetas de ese directorio de destino.

Nota: el proceso de los vínculos simbólicos que se describe en este apartado no es aplicable a Mac OS X. La copia de seguridad de los vínculos simbólicos se hace siempre como archivos y nunca se siguen.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Ejemplos: copia de seguridad incremental o selectiva de enlaces simbólicos  
El modo en el que el cliente realiza copias de seguridad de un enlace simbólico depende de si su destino es un archivo o un directorio, y de cómo se especifique en el mandato de copia de seguridad incremental o selectiva.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copia de seguridad incremental de un dominio solamente  
El cliente hace copias de seguridad de un enlace simbólico durante una copia de seguridad incremental del dominio, si el enlace simbólico está definido como punto de montaje virtual y la opción `followsymbolic` está configurada como `yes`.

#### Referencia relacionada:

Archsymlinkasfile

Followsymbolic

Virtualmountpoint

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Ejemplos: copia de seguridad incremental o selectiva de enlaces simbólicos

El modo en el que el cliente realiza copias de seguridad de un enlace simbólico depende de si su destino es un archivo o un directorio, y de cómo se especifique en el mandato de copia de seguridad incremental o selectiva.

Si un enlace simbólico dirige a un archivo, el cliente solamente realiza una copia de seguridad de la información de la vía de acceso. El cliente no realiza copias de seguridad del archivo de destino del enlace simbólico.

Si un enlace simbólico dirige a un directorio, la copia de seguridad depende de cómo se especifique el directorio en el mandato.

Si se especifica con una barra inclinada final en un mandato de copia de seguridad selectiva o incremental, el cliente guarda el enlace simbólico como directorio y realiza una copia de seguridad del contenido del directorio de destino.

Si el enlace simbólico se especifica sin barra inclinada final, o si no se indica ningún enlace simbólico explícitamente en una especificación de archivo de la copia de seguridad, el cliente solamente realiza una copia de seguridad de la información de la vía de acceso del directorio de destino. No se realiza ninguna copia de seguridad del contenido del directorio de destino.

En el siguiente ejemplo, suponga que `symdir` es un enlace simbólico al directorio de destino `/fs1/guest/`. `/fs1/guest/` contiene estos objetos:

- `/fs1/guest/file` (un archivo)
- `/fs1/guest/dir1` (un directorio)
- `/fs1/guest/dir1/file1` (un archivo)

#### Ejemplo 1

```
dsmc incr /home/gillis/symdir/
```

En este ejemplo, el cliente realiza una copia de seguridad del enlace simbólico como directorio y del contenido del directorio de destino `/fs1/guest/`. Si especifica la opción `subdir=yes`, el cliente realiza una copia de seguridad de los subdirectorios de `/fs1/guest/`.

#### Ejemplo 2

```
dsmc incr /home/gillis/symdir/dir1
```

#### Ejemplo 3

```
dsmc incr /home/gillis/symdir/dir1/
```

En Ejemplo 2 y Ejemplo 3, el cliente realiza una copia de seguridad del enlace simbólico como directorio y del subdirectorio `/dir1/` del directorio de destino. La barra inclinada final solamente es relevante en el enlace simbólico y es irrelevante en subdirectorios del enlace simbólico. Si especifica la opción `subdir=yes`, el cliente realiza una copia de seguridad de los subdirectorios del directorio `/fs1/guest/dir1`. Las copias de seguridad almacenadas en el servidor de IBM Spectrum Protect tienen la vía de acceso `/home/gillis/symdir/dir1/file1`.

#### Ejemplo 4

```
dsmc incr /home/gillis/symdir
```

En Ejemplo 4, dado que no hay barra inclinada final tras el enlace simbólico, el cliente solamente realiza una copia de seguridad de la vía de acceso del directorio de destino. El cliente no realiza copias de seguridad del enlace simbólico como directorio ni de los archivos o carpetas del directorio de destino.

#### Ejemplo 5

```
dsmc incr /home/gillis/
```

En Ejemplo 5, dado que no se ha indicado explícitamente el enlace simbólico en la especificación de archivo de la copia de seguridad, el cliente solamente realiza una copia de seguridad de la vía de acceso del directorio de destino. Al igual que en el ejemplo 3, el cliente no realiza copias de seguridad del enlace simbólico como directorio ni de los archivos o carpetas del directorio de destino.

**Restricción:** Si realiza una copia de seguridad de un enlace simbólico como directorio y después lleva a cabo una copia de seguridad incremental que no lo copie también como directorio, el enlace simbólico caduca como directorio, así como los archivos y directorios dentro de él.

Por ejemplo, suponga que primero realiza una copia de seguridad del enlace simbólico `symdir` como directorio, y realiza una copia de seguridad del contenido del directorio de destino. El mandato del ejemplo 1 anterior hace esto. El cliente crea copias de seguridad con una vía de acceso de alto nivel `/home/gillis/symdir/`. En el siguiente ejemplo, el cliente crea copias de seguridad con estas vías de accesos:

- `/home/gillis/symdir/`
- `/home/gillis/symdir/file`
- `/home/gillis/symdir/dir1`
- `/home/gillis/symdir/dir1/file1`

Se hace una copia de seguridad del contenido de `/home/gillis` mediante el siguiente mandato:

```
dsmc inc /home/gillis/ -subdir=yes
```




Este mandato procesa `symdir` como un enlace simbólico y no procesa ninguno de los objetos a los que apunta el enlace simbólico. Por lo tanto, el cliente hace que caduquen las copias de seguridad del directorio `/home/gillis/symdir/` que se crearon en Ejemplo 1.




 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copia de seguridad incremental de un dominio solamente

El cliente hace copias de seguridad de un enlace simbólico durante una copia de seguridad incremental del dominio, si el enlace simbólico está definido como punto de montaje virtual y la opción `followsymbolic` está configurada como `yes`.

El cliente hará copias de seguridad de un enlace simbólico y de un directorio de destino cuando todo lo que viene a continuación sea verdad:

- El cliente realiza una copia de seguridad incremental del dominio.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El enlace simbólico se define como punto de montaje virtual por medio de la opción `virtualmountpoint`.
- `followsymbolic=yes`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Las opciones `virtualmountpoint` y `followsymbolic` añaden el enlace simbólico al dominio. El mandato Incremental hace una copia de seguridad del dominio, que incluye el destino del enlace simbólico.

#### Referencia relacionada:

`Followsymbolic`  
`Virtualmountpoint`

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Enlaces fijos




Cuando hace copia de seguridad de archivos que tienen un enlace fijo, el cliente de copia de seguridad y archivado hará una copia de seguridad de cada instancia del archivo enlazado.

Por ejemplo, si hace una copia de seguridad de dos archivos que tienen un enlace fijo, el cliente hace dos copias de seguridad de los datos de los archivos.

Cuando se restauren archivos con enlace fijo, el cliente intentará restablecer los vínculos. Por ejemplo, si se había establecido un enlace fijo entre dos archivos y solo se encuentra uno en su estación de trabajo, al restaurar ambos archivos habrá un enlace fijo entre los dos. También se aplicarán enlaces fijos a los archivos aunque ninguno de los archivos exista en el momento de la restauración si ambos

archivos se restauran conjuntamente mediante la ejecución de un único mandato. La única excepción de este procedimiento se da cuando se realizan copias de seguridad dos archivos entre los que hay un enlace fijo y se interrumpe la conexión entre éstos en la estación de trabajo. Si restaura los dos archivos desde el servidor con el proceso de restauración estándar (o clásico), el cliente respeta el sistema de archivos actual y no vuelve a establecer el enlace fijo.

Importante: Si no realiza la copia de seguridad y la restauración al mismo tiempo de todos los archivos que tienen enlaces fijos, se producirán problemas. Para garantizar que los archivos unidos mediante enlaces fijos permanecen sincronizados, realice una copia de seguridad de todos los archivos que están conectados entre sí mediante enlaces fijos al mismo tiempo y, a continuación, restaure estos mismos archivos juntos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archivos esparcidos

---

Los archivos esparcidos no tienen espacio de disco asignado para cada bloque en todo el espacio de direcciones, lo que provoca la aparición de espacios vacíos en los archivos. Los espacios vacíos se detectan por su contenido, que siempre está formado por ceros, y estos ceros ocupan espacio.

El valor predeterminado consiste en restaurar el archivo esparcido sin los espacios vacíos, con lo que se obtiene más espacio de disco libre. El cliente de copia de seguridad y archivado detecta los archivos esparcidos durante una operación de copia de seguridad y los marca como esparcidos en el servidor de IBM Spectrum Protect.





Nota: Los archivos esparcidos no se aplican a Mac OS X.


El cliente de copia de seguridad y archivado hace copia de seguridad de un archivo esparcido si la compresión del cliente está desactivada.

### Referencia relacionada:

Compression

Makesparsefile

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux

 Sistemas operativos Oracle Solaris

## Montajes de hard y soft de NFS

---

Cuando el cliente de copia de seguridad y archivado se conecta a un sistema de archivos NFS, puede utilizar un montaje por hardware o un montaje por software.

El cliente utiliza el valor de la opción `nfstimeout` para determinar el tiempo de espera de una llamada de un sistema NFS para responder antes de que exceda el tiempo de espera; este valor se aplica a montajes por hardware y software. El valor predeterminado es 0 segundos. Esto significa que el cliente utiliza el comportamiento predeterminado de llamadas de sistema NFS.

Tenga en cuenta las consecuencias de los montajes por hardware y software si el montaje queda obsoleto (por ejemplo, si el servidor del sistema de archivos no está disponible).

### Montaje por hardware

Si el sistema de archivos NFS está montado por hardware, los daemons NFS intentan repetidamente establecer contacto con el servidor. Los reintentos de los daemons de NFS no excederán el tiempo de espera, afectan al rendimiento del sistema y no pueden interrumpirse. Sin embargo, el control vuelve al cliente cuando se alcanza el valor `nfstimeout`.

### Montaje por software

Si el sistema de archivos NFS está montado por software, NFS intenta repetidamente establecer contacto con el servidor hasta que:

- Se establezca una conexión
- Se alcance el umbral de reintentos de NFS
- Se alcance el valor `nfstimeout`

Cuando se produce uno de estos sucesos, el control vuelve al programa que ha efectuado la llamada.

Nota: En sistemas de UNIX y Linux, la opción `nfstimeout` puede fallar si el montaje de NFS es duro. Si se cuelga el proceso, desactive la opción `nfstimeout` y monte el sistema de archivos NFS montado por software de este modo:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Los parámetros son los siguientes:

`soft`

Genera un montaje por software del sistema de archivos NFS. Si se produce un error, la función `stat()` devuelve un error. Si ha utilizado la opción `hard stat()`, nunca vuelve hasta que el sistema de archivos está disponible.

`timeo=n`

Establece el tiempo de espera para un error de montaje de tipo `soft` en  $n$  décimas de segundo.

`retry=n`

Establece el número de veces que se puede intentar el montaje, donde  $n$  es un entero; la opción predeterminada es 10000.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Sistemas de archivos suprimidos

---

Cuando se ha suprimido un sistema de archivos o una unidad, o dejan de hacerse copias de seguridad de los mismos mediante el cliente de copia de seguridad y archivado, las versiones de copia de seguridad existentes de cada archivo se gestionan según los siguientes atributos de política: Número de días que se deben mantener inactivas las versiones de copia de seguridad y número de días que se debe mantener la última versión de copia de seguridad (si no hay ninguna versión activa)

Si no lleva a cabo ninguna otra acción, las versiones de copia de seguridad activas se conservan indefinidamente. Si no necesita guardar de manera indefinida las versiones activas, utilice el mandato `expire` para desactivar las versiones activas.

Si no necesita guardar ninguna de las versiones de copia de seguridad, utilice el mandato `delete backup` para suprimir todas las versiones de copia de seguridad del espacio de archivos. El administrador del servidor de IBM Spectrum Protect deberá otorgarle autorización para suprimir copias de seguridad antes de utilizar estos mandatos. Utilice el mandato `query session` para determinar si tiene autorización de supresión de copia de seguridad. Como alternativa, solicite al administrador del servidor IBM Spectrum Protect que suprima por usted el espacio de archivos.

### Conceptos relacionados:

Políticas de gestión de almacenamiento

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archivos abiertos

---

El cliente de copia de seguridad y archivado busca archivos que se han modificado entre el inicio y la finalización de la copia de seguridad del archivo.

Puede que algunos archivos del sistema estén utilizándose o estén abiertos mientras intenta realizar la copia de seguridad de éstos. Puesto que un archivo abierto puede cambiar, puede que una acción de copia de seguridad no refleje el contenido correcto del archivo en un momento determinado.

Plantéese si el archivo es importante y si puede volver a crearlo. Si no es importante, puede que no desee realizar una copia de seguridad de él. Si el archivo es importante, un usuario `root` en la estación de trabajo puede garantizar que el archivo esté cerrado antes de realizar la copia de seguridad.

Si las copias de seguridad se ejecutan según una planificación, un usuario `root` puede utilizar la opción `preschedulecmd` para especificar un mandato que cierre el archivo. Por ejemplo, si el archivo abierto es una base de datos, utilice el mandato `quiesce` de la base de datos para cerrarla. Un usuario `root` puede utilizar la opción `postschedulecmd` para reiniciar la aplicación que utiliza el archivo una vez finalizada la copia de seguridad. Si no sigue ninguna planificación para la copia de seguridad, asegúrese de cerrar la aplicación que utiliza el archivo antes de iniciar la copia de seguridad.

El cliente puede realizar una copia de seguridad de un archivo aunque esté abierto y se modifique durante la operación de copia de seguridad. Esto es útil sólo si el archivo está utilizable incluso aunque cambie durante la operación de copia de seguridad. Para efectuar copias de seguridad de estos archivos, asigne a los archivos una clase de gestión con serialización *dinámica* o *dinámica compartida*.

### Conceptos relacionados:

Visualizar información sobre clases de gestión y grupos de copia

Seleccionar una clase de gestión para los archivos

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Caracteres comodín

---

Puede utilizar los caracteres comodín del sistema operativo en las especificaciones de archivo con el cliente de copia de seguridad y archivado. Estos caracteres permiten seleccionar grupos de archivos que tienen nombres similares.

En un mandato, los caracteres comodín sólo pueden utilizarse en el nombre o la extensión del archivo. No pueden utilizarse para especificar archivos, sistemas de archivos ni directorios de destino. Cuando utilice caracteres comodín en la modalidad de no bucles,

como en `dsmc sel "/home/ledger.*"`, incluya entre comillas el parámetro que contiene el asterisco para asegurarse de que el sistema no interpreta el carácter comodín y genera resultados inesperados. En la tabla siguiente se incluye información sobre el carácter comodín.

Importante: Utilice un asterisco (\*) en lugar de una interrogación (?) como carácter comodín cuando intente buscar la coincidencia de un patrón en una página de códigos de varios bytes con el fin de evitar que se produzcan resultados no esperados.

En esta tabla se muestran algunos patrones comodín y cómo especificarlos.


<b>* (Asterisco)</b>	<b>Ninguno o varios caracteres que coinciden con todos los archivos:</b>	
<b>*.cpp</b>	Con la extensión cpp	
<b>hm**</b>	Empieza por hm, independientemente de la extensión, pero debe tener el carácter !	
<b>hm*</b>	Empieza por hm, independientemente de si existe una extensión	
<b>*h**</b>	Con una h en algún lugar del nombre de archivo, independientemente de la extensión, pero debe tener un .	
<b>? (Signo de interrogación)</b>	<b>Un carácter que coincide con todos los archivos con:</b>	
<b>?cpp</b>	La extensión cpp con un único carácter en el nombre del archivo	
<b>hm?cpp</b>	Nombres de tres caracteres que empiezan por hm y que tienen la extensión cpp	
<b>* ? (Asterisco y signo de interrogación)</b>	<b>Combinaciones de asterisco y signos de interrogación que coinciden con:</b>	
<b>??hm.*</b>	Todos los nombres de archivo de cuatro caracteres que acaban en hm., independientemente de su extensión	

En un nombre de vía de acceso de una especificación de archivo, no se puede especificar un directorio cuyo nombre contenga un asterisco (\*) o un signo de interrogación (?). El cliente únicamente reconoce estos caracteres como caracteres comodín.





## Restauración de los datos

Utilice IBM Spectrum Protect para restaurar versiones de copia de seguridad de archivos específicos, de un grupo de archivos con nombres similares o de directorios completos.



















Estas versiones de copia de seguridad se pueden restaurar en caso de que los archivos originales se pierdan o resulten dañados. Seleccione los archivos que desea restaurar utilizando una especificación de archivo (vía de acceso, nombre y extensión de archivo), una lista de directorios o una vía de acceso de subdirectorios en un directorio y sus subdirectorios.


































 Sistemas operativos Windows Nota: Cuando se restaura un directorio, su fecha y hora de modificación se establecen según la fecha y la hora de la operación de restauración, no según la fecha y la hora que tenía el directorio en el momento de realizar la copia de seguridad. Esto se debe a que IBM Spectrum Protect restaura primero los directorios y, a continuación, añade los archivos a los directorios.





Todos los procedimientos de copia de seguridad y restauración de cliente que aparecen en este tema también se aplican al cliente web. Sin embargo, el cliente web no dispone de un Editor de preferencias para configurar las opciones del cliente.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Atención: No restaure archivos del sistema operativo como directorios base del sistema, módulos de kernel o parches a su ubicación original mientras el sistema de archivos esté en ejecución. El sistema operativo se podría colgar o bloquear.

































Estas son las principales tareas de restauración:

-  Sistemas operativos Windows Restauración de archivos y directorios
-  Sistemas operativos Windows Restauración del estado del sistema de Windows
-  Sistemas operativos Windows Restauración de los archivos de Recuperación automática del sistema
-  Sistemas operativos Windows Restauración de archivos y árboles Dfs de Microsoft
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Restauración de una imagen
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Restauración de datos mediante la GUI
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Ejemplos de restauración desde la línea de mandatos
- Restauración de datos desde un conjunto de copias de seguridad
- Restauración de datos a un instante específico

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Restaurar sistemas de archivos NAS
-  Sistemas operativos Windows Cómo autorizar a otro usuario para que restaure o recupere archivos
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Cómo autorizar a otro usuario para que restaure o recupere archivos
-  Sistemas operativos Windows Restauración o recuperación de archivos de otro nodo cliente
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Restauración o recuperación de archivos de otro nodo cliente
-  Sistemas operativos Windows Restauración o recuperación de archivos en otra estación de trabajo
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Restaurar o recuperar archivos en otra estación de trabajo
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Restauración de un disco en caso de pérdida del mismo
-  Sistemas operativos Windows Supresión de espacios de archivos
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Supresión de espacios de archivos
-  Sistemas operativos Windows Restauración de datos desde la copia de seguridad de VMware


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Consulte *IBM Spectrum Protect para Space Management para UNIX y Linux* para obtener detalles sobre la restauración de archivos migrados y sobre la opción `restoremigstate`.

-  Sistemas operativos Windows Nombres de archivos duplicados  
Si intenta restaurar un archivo cuyo nombre es el mismo que el nombre abreviado de un archivo ya existente, se producirá un error de colisión de nombres de archivos (existencia de nombres duplicados de archivo).
-  Sistemas operativos Windows Restauración de nombres del convenio de denominación universal  
La utilización de un nombre UNC permite restaurar archivos compartidos específicos en un espacio de archivos aparte. Esto le resultará útil si, por ejemplo, usted o el administrador desean restaurar una parte de datos a la que de otra forma no podría acceder.
-  Sistemas operativos Windows Restaurar copias de seguridad activas o inactivas  
El administrador determina cuántas versiones de copia de seguridad mantiene IBM Spectrum Protect para cada archivo de la estación de trabajo. Tener varias versiones de un archivo le permite restaurar versiones anteriores en el caso de que la copia de seguridad más reciente esté dañada.
-  Sistemas operativos Windows Restauración de archivos y directorios  
Puede localizar los archivos que desea restaurar mediante las operaciones de búsqueda y filtrado.
-  Sistemas operativos Windows Restauración del estado del sistema de Windows  
Microsoft Volume Shadowcopy Service (VSS) se admite en los clientes de copia de seguridad y archivado de Windows. El cliente utiliza VSS para restaurar el estado del sistema. La función de restauración de estado del sistema está en desuso para las operaciones de restauración de estado del sistema en línea.
-  Sistemas operativos Windows Restauración de los archivos de Recuperación automática del sistema  
Puede restaurar los archivos de Recuperación automática del sistema (ASR) para recuperar la información de configuración del estado del sistema Windows y el estado del sistema si se produce un error muy grave del sistema o de hardware.
-  Sistemas operativos Windows Restaurar el sistema operativo cuando está funcionando el sistema  
Si su sistema está funcionando, puede restaurar el sistema operativo desde los archivos de la copia de seguridad.
- Recuperación de un equipo cuando el sistema operativo de Windows no funciona  
Si el sistema tiene un error de hardware o software catastrófico, puede recuperar un sistema operativo de Windows con Automated System Recovery (ASR).
-  Sistemas operativos Windows Restauración de archivos y árboles Dfs de Microsoft  
Para restaurar los puntos de unión Dfs y los datos de cada punto de unión, primero restaure los metadatos de punto de unión Dfs y después restaure separadamente cada punto de unión.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Restauración de una imagen  
Existen algunos puntos que debe tener en cuenta antes de comenzar a restaurar imágenes en el sistema.
- Restauración de datos desde un conjunto de copias de seguridad  
El administrador de IBM Spectrum Protect puede generar un conjunto de copias de seguridad, que es una colección de los archivos que residen en el servidor, en soportes portables creados en un dispositivo utilizando un formato compatible con el dispositivo de cliente.
-  Sistemas operativos Windows Restaurar compartimientos de Net Appliance CIFS  
La restauración de la definición de compartición implica la restauración del directorio raíz del espacio de archivos de compartición que, en la mayoría de las circunstancias, puede realizarse como se indica a continuación: `dsmc rest \\NetAppFiler\CifsShareName\ -dirsonly`
-  Sistemas operativos Windows Restauración de datos desde la copia de seguridad de VMware  
Puede utilizar diversos métodos para restaurar datos de copias de seguridad en máquinas virtuales VMware. El método de restauración depende del tipo de copia de seguridad y versión del software del cliente de copia de seguridad y archivado que utilice para ejecutar la restauración.

-  **Sistemas operativos Windows** Restaurar objetos individuales de Active Directory en Windows  
 Puede restaurar objetos individuales de Active Directory para realizar la recuperación después de la supresión o daños accidentales de objetos de Active Directory sin que requieran la conclusión o el reinicio del servidor de Active Directory.
- Restaurar o recuperar datos durante una migración tras error  
 Cuando el cliente se migra a servidor secundario, puede restaurar o recuperar los datos replicados desde servidor secundario.
-  **Sistemas operativos Windows** Cómo autorizar a otro usuario para que restaure o recupere archivos  
 Puede autorizar a otro usuario de otro nodo para restaurar las versiones de copia de seguridad o para recuperar las copias archivadas. De esta forma, podrá compartir archivos con otras personas o con otras estaciones de trabajo que utilice con un nombre de nodo distinto.
-  **Sistemas operativos Windows** Restauración o recuperación de archivos de otro nodo cliente  
 Después de que los usuarios concedan acceso a los archivos del servidor, puede restaurar o recuperar dichos archivos en el sistema local.
-  **Sistemas operativos Windows** Restauración o recuperación de archivos en otra estación de trabajo  
 Si utiliza una estación de trabajo diferente, puede restaurar o recuperar archivos de los que ha efectuado copia de seguridad en su propia estación de trabajo.
-  **Sistemas operativos Windows** Supresión de espacios de archivos  
 Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris** Restaurar una imagen en archivo  
 Al realizar una copia de seguridad de una imagen, el cliente de archivado y copia de seguridad realiza una copia de seguridad del primer sector del volumen, pero, al restaurar los datos, omite el primer sector para mantener el bloque de control del volumen lógico original del volumen de destino.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux** Gestión de datos del sistema de archivos GPFS con agrupaciones de almacenamiento  
 Con la tecnología Global Parallel File Systems (GPFS), puede gestionar los datos utilizando agrupaciones de almacenamiento. Una agrupación de almacenamiento es una colección de discos o RAID que tienen propiedades similares y que se gestionan conjuntamente como un grupo.
- Restauración de datos a un instante específico  
 Utilice una restauración a un *instante específico* para restaurar archivos al estado que tenían en una fecha y hora específicos.
-  **Sistemas operativos AIX** Restauración de archivos cifrados AIX  
 Cuando se realiza una copia de seguridad de archivos en formato en bruto a partir de un Sistema de archivos de cifrado (EFS) de JFS2 de AIX, solamente podrá restaurarla en el mismo EFS de JFS2 o en otro. No se pueden restaurar en ningún otro sistema de archivos distinto, ni en ninguna otra plataforma.
-  **Sistemas operativos AIX** Restaurar sistemas de archivos con partición de carga de trabajo de AIX  
 Todos los archivos que se crean mediante la partición de carga de trabajo local (WPAR) y que se copian mediante un cliente de copia de seguridad y archivado que está instalado en la WPAR global se pueden restaurar mediante el cliente instalado en la WPAR global.
-  **Sistemas operativos AIX**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos Windows** Restaurar sistemas de archivos NAS  
 Las imágenes del sistema de archivos NAS se restauran mediante el cliente web o la interfaz de línea de mandatos. El interfaz de cliente web está disponible sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris** Restaurar copias de seguridad activas o inactivas  
 El administrador determina cuántas versiones de copia de seguridad mantiene IBM Spectrum Protect para cada archivo de la estación de trabajo.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris** Restauración de datos mediante la GUI  
 En esta sección figuran los pasos que es necesario seguir para restaurar versiones de copias de seguridad de archivos o subdirectorios individuales.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris** Ejemplos de restauración desde la línea de mandatos  
 Este tema enumera algunos ejemplos de los mandatos restore para su uso en tareas específicas.
-  **Sistemas operativos Oracle Solaris** Restauración de sistemas de archivos ZFS de Solaris  
 Zettabyte File Systems (ZFS) utiliza las agrupaciones de almacenamiento para gestionar el almacenamiento físico.
-  **Sistemas operativos Mac OS X**  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris** Tareas de restauración adicionales  
 En este apartado se indican algunas consideraciones avanzadas para la restauración de datos.

**Tareas relacionadas:**

Inicio de una sesión de cliente web

 **Sistemas operativos Windows**

## Nombres de archivos duplicados

---



Si intenta restaurar un archivo cuyo nombre es el mismo que el nombre abreviado de un archivo ya existente, se producirá un error de colisión de nombres de archivos (existencia de nombres duplicados de archivo).

Un ejemplo de esto es cuando el archivo *abcdefghijkl.doc* tiene el nombre corto *abcdef~1.doc* y desea restaurar o recuperar un archivo denominado explícitamente *abcdef~1.doc* en el mismo directorio. En este caso, se produce un conflicto, porque el nombre del archivo que está restaurando entra en disputa con el nombre corto de *abcdefghijkl.doc*.

Puede darse un conflicto de nombres incluso en caso de que los archivos se restauren o recuperen en un directorio vacío. Por ejemplo, los archivos *abcdef~1.doc* y *abcdefghijkl.doc* podrían haber existido originalmente en el directorio como *abcdefghijkl.doc* y *abcdef~2.doc*. Durante la restauración, si se restaura primero *abcdefghijkl.doc*, el sistema operativo Windows le asigna el nombre abreviado *abcdef~1.doc*. Cuando se restaura *abcdef~1.doc*, se produce la situación de nombres de archivos duplicados.

IBM Spectrum Protect trata estas situaciones de acuerdo con el valor de la opción *replace*. Utilice la opción *replace* para especificar si se debe grabar encima de un archivo existente o si se le debe solicitar su elección al restaurar o recuperar archivos.

Con el fin de corregir una situación en que se ha producido una colisión de nombre de archivos, puede efectuarse lo siguiente:

- Restaurar o recuperar el archivo con el nombre de archivo corto en una ubicación diferente.
- Detener la operación de restauración o recuperación y cambiar el nombre del archivo ya existente.
- Desactivar el soporte de nombres de archivos abreviados en Windows.
- No utilizar nombres de archivos como *abcdef~1.doc*, que pueden entrar en conflicto con el convenio de denominación de nombres abreviados.

#### Referencia relacionada:

Replace

 Sistemas operativos Windows

## Restauración de nombres del convenio de denominación universal

---

La utilización de un nombre UNC permite restaurar archivos compartidos específicos en un espacio de archivos aparte. Esto le resultará útil si, por ejemplo, usted o el administrador desean restaurar una parte de datos a la que de otra forma no podría acceder.

Excepto en el caso de las unidades con medio extraíble, las letras de unidades locales son accesibles utilizando un nombre UNC local, que incluye el nombre de estación de trabajo y una designación para la letra de unidad. Por ejemplo, para especificar un nombre UNC en la unidad *c*: para la estación de trabajo *ocean*, escriba:

```
\\ocean\c$
```

El símbolo *\$* *debe* incluirse en la letra de unidad.

Para especificar un nombre UNC para la estación de trabajo *ocean* y el punto compartido *wave*, escriba:

```
\\ocean\wave
```

Cuando acceda a los archivos, no es necesario especificar la letra de la unidad *salvo* para dispositivos con medios extraíbles.

 Sistemas operativos Windows

## Restaurar copias de seguridad activas o inactivas

---

El administrador determina cuántas versiones de copia de seguridad mantiene IBM Spectrum Protect para cada archivo de la estación de trabajo. Tener varias versiones de un archivo le permite restaurar versiones anteriores en el caso de que la copia de seguridad más reciente esté dañada.

La versión de copia de seguridad más reciente es la versión *activa*. Cualquier otra versión de copia de seguridad es una versión *inactiva*. Cada vez que IBM Spectrum Protect hace copias de seguridad de archivos, marca la nueva versión de copia de seguridad como copia de seguridad activa y la copia de seguridad activa anterior pasa a ser inactiva. Cuando se alcanza el número máximo de versiones inactivas, IBM Spectrum Protect suprime la versión inactiva más antigua.

Para restaurar una versión de copia de seguridad inactiva, debe visualizar ambas versiones, la activa y la inactiva, pulsando la opción **Visualizar archivos activos/inactivos** del menú **Ver**. Para ver sólo las versiones activas (opción predeterminada), pulse la opción **Visualizar sólo archivos activos** del menú **Ver**. Si intenta restaurar a la vez las versiones activa e inactiva de un archivo, sólo se restaurará la versión activa.

En la línea de mandatos de IBM Spectrum Protect, utilice la opción *inactive* para visualizar los objetos activos e inactivos.

#### Referencia relacionada:



Inactive


## Restauración de archivos y directorios

---

Puede localizar los archivos que desea restaurar mediante las operaciones de búsqueda y filtrado.

El filtrado muestra sólo los archivos que coinciden con los criterios de filtrado de la operación de restauración. Los archivos que no coinciden con los criterios de filtrado no se visualizan. El proceso de filtrado busca los archivos en el directorio especificado pero no incluye los subdirectorios.

-  Sistemas operativos Windows Restauración de datos mediante la GUI  
Puede utilizar el cliente GUI para restaurar archivos y directorios.
-  Sistemas operativos Windows Ejemplos de restauración de datos mediante la línea de mandatos  
Puede utilizar los ejemplos incluidos en este tema cuando necesite restaurar objetos desde el almacenamiento del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows

## Restauración de datos mediante la GUI

---

Puede utilizar el cliente GUI para restaurar archivos y directorios.

### Acerca de esta tarea

---

Restricción: La GUI de cliente web no puede examinar los recursos de la red para realizar una operación de restauración. No se listan unidades compartidas si se expande la rama de Red. Puede restaurar un recurso de red desde el cliente web a condición de que se procese el archivo entero. Especifique el sistema de archivos compartidos en la opción domain del archivo de opciones `dsm.opt`. Por ejemplo, `domain all-local \\server\share`. Para completar la operación de restauración, especifique Compartición de red en el diálogo Destino de la restauración. Este procesa todos los sistemas de archivos especificados por la opción domain. Como alternativa, puede utilizar el cliente de GUI para realizar la operación de restauración.

### Procedimiento

---

1. Pulse Restaurar en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios pulsando en el signo más (+) o en el icono de carpeta situado junto a un objeto del árbol. Seleccione el objeto que desea restaurar. Para buscar o filtrar los archivos, pulse en el icono Buscar desde la barra de herramientas.
3. Pulse en las casillas de selección que se encuentran junto a los objetos que desea restaurar.
4. Si desea modificar opciones de restauración específicas, pulse el botón Opciones. Cualquier opción que cambie será eficaz solo durante la sesión actual.
5. Pulse Restaurar. Aparecerá la ventana Destino de restauración. Entre la información pertinente.
6. Pulse Restaurar. La ventana Lista de tareas de restauración muestra el estado del proceso.

#### Tareas relacionadas:

Copia de seguridad de datos mediante la GUI

 Sistemas operativos Windows

## Ejemplos de restauración de datos mediante la línea de mandatos

---

Puede utilizar los ejemplos incluidos en este tema cuando necesite restaurar objetos desde el almacenamiento del servidor de IBM Spectrum Protect.



En la tabla siguiente se muestran ejemplos de cómo utilizar los mandatos de restauración para restaurar objetos desde el almacenamiento del servidor de IBM Spectrum Protect.

Tabla 1. Ejemplos de restauración desde la línea de mandatos

Tarea	Mandato	Consideraciones
-------	---------	-----------------

Tarea	Mandato	Consideraciones
Restaurar la versión más reciente de copia de seguridad del archivo <code>c:\doc\h1.doc</code> , aunque la copia de seguridad esté inactiva.	<code>dsmc restore c:\doc\h1.doc -latest</code>	Si el archivo que está restaurando ya no reside en la estación de trabajo y ha realizado una copia de seguridad incremental después de suprimir el archivo, no habrá ninguna copia de seguridad activa del archivo en el servidor. En este caso, utilice la opción <code>latest</code> para restaurar la versión de copia de seguridad más reciente. IBM Spectrum Protect restaura la versión de copia de seguridad más reciente, ya sea activa o inactiva. Consulte el apartado <code>Latest</code> para obtener más información.
Visualizar una lista de versiones de copia de seguridad activas e inactivas para seleccionar las versiones que se restaurarán.	<code>dsmc restore c:\project\* -pick -inactive</code>	Si intenta restaurar a la vez las versiones activa e inactiva de un archivo, sólo se restaurará la versión activa. Consulte los apartados <code>Pick</code> y <code>Inactive</code> para obtener más información.
Restaurar todos los archivos que tienen la extensión de archivo <code>.c</code> del directorio <code>c:\devel\projecta</code> .	<code>dsmc restore c:\devel\projecta\*.c</code>	Si no especifica ningún destino, los archivos se restaurarán en su ubicación original.
Restaurar el archivo <code>c:\project\doc\h1.doc</code> a su directorio original.	<code>dsmc restore c:\project\doc\h1.doc</code>	Si no especifica ningún destino, los archivos se restaurarán en su ubicación original.
Restaurar el archivo <code>c:\project\doc\h1.doc</code> con un nuevo nombre y en otro directorio.	<code>dsmc restore c:\project\doc\h1.doc c:\project\newdoc\h2.doc</code>	Ninguna
Restaurar los archivos de la unidad <code>e:</code> y todos sus subdirectorios.	<code>dsmc restore e:\ -subdir=yes</code>	Se debe utilizar la opción <code>subdir</code> para restaurar los atributos/permisos de directorio. Consulte el apartado <code>Subdir</code> para obtener más información sobre la opción <code>subdir</code> .
Restaurar todos los archivos del directorio <code>c:\mydir</code> en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.	<code>dsmc restore -pitd=8/17/2002 -pitt=13:00:00 c:\mydir\</code>	Consulte los apartados <code>Pitdate</code> y <code>Pittime</code> para obtener más información sobre las opciones <code>pitdate</code> y <code>pittime</code> .
Restaurar el archivo <code>c:\doc\h2.doc</code> a su directorio original en la estación de trabajo, llamada <code>star</code> .	<p><code>dsmc restore c:\doc\h2.doc \\star\c\$\</code></p> <p>Para restaurar el archivo en "star", cuyo nombre se ha cambiado por "meteor", escriba:</p> <p><code>dsmc restore \\star\c\$\doc\h2.doc \\meteor\c\$\</code></p> <p>También puede entrarse:</p> <p><code>dsmc restore \\star\c\$\doc\h2.doc c:\</code></p> <p>Este ejemplo resulta válido, ya que si el nombre de la estación de trabajo no está incluido en la especificación, se presupone el nombre de la estación de trabajo local ("meteor", en este caso).</p>	En este manual, el nombre de la estación de trabajo forma parte del nombre de archivo. Por lo tanto, si se realizan copias de seguridad de archivos en una estación de trabajo y se desea restaurarlos en otra, debe especificarse un destino. Ello sucede incluso en el caso de que se restauren los archivos en la misma estación de trabajo física, pero ésta tiene un nuevo nombre.

Tarea	Mandato	Consideraciones
Restaurar un archivo del que originalmente se ha hecho copia de seguridad desde el disquete "workathome" en la unidad a: y restaurarlo en un disquete en la unidad a: con la etiqueta "extra".	<pre>dsmc restore {workathome}\doc\h2.d oc a:\doc\h2.doc</pre>	Si está restaurando un archivo en un disco con una etiqueta distinta a la del disco desde el que se realizó copia de seguridad, debe utilizar el nombre del espacio de archivos (etiqueta) del disco de copia de seguridad en lugar de la letra de la unidad.
Restaurar los archivos especificados en el archivo c:\filelist.txt en el directorio d:\dir.	<pre>dsmc restore - filelist=c:\filelist. txt d:\dir\</pre>	Consulte el apartado Filelist para obtener más información sobre la restauración de una lista de archivos.
Restaurar todos los miembros de la copia de seguridad de grupo virtfs\group1 almacenada en el servidor de IBM Spectrum Protect.	<pre>dsmc restore group {virtfs}\group1</pre>	Consulte el apartado Restore Group para obtener más información.

-  Sistemas operativos Windows Ejemplos: restauración de grandes cantidades de datos  
Si debe restaurar un gran número de archivos, obtendrá un mejor rendimiento con la interfaz de línea de mandatos que con la interfaz de la GUI. Además, mejorará el rendimiento si especifica varios mandatos restore a la vez.
-  Sistemas operativos Windows Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicializable  
En este tema se describen los procesos de restauración estándar (o clásica), de restauración sin consulta y de restauración reinicializable.

#### Conceptos relacionados:

Utilización de los mandatos

#### Referencia relacionada:

Restore

 Sistemas operativos Windows

## Ejemplos: restauración de grandes cantidades de datos

Si debe restaurar un gran número de archivos, obtendrá un mejor rendimiento con la interfaz de línea de mandatos que con la interfaz de la GUI. Además, mejorará el rendimiento si especifica varios mandatos restore a la vez.

### Acerca de esta tarea

Por ejemplo, para restaurar todos los archivos en el espacio de archivos c:, escriba:

```
dsmc restore c:\* -subdir=yes -replace=all -tapeprompt=no
```

Sin embargo, si entra más de un mandato para los directorios raíz del espacio de archivos c:, puede restaurar los archivos más rápidamente. Por ejemplo, escriba estos mandatos:

```
dsmc restore c:\users\ -subdir=yes -replace=all -tapeprompt=no  
dsmc restore c:\data1\ -subdir=yes -replace=all -tapeprompt=no  
dsmc restore c:\data2\ -subdir=yes -replace=all -tapeprompt=no
```

O bien, si necesita restaurar archivos de varias unidades, escriba estos mandatos:

```
dsmc restore c:\* -subdir=yes -replace=all -tapeprompt=no  
dsmc restore d:\* -subdir=yes -replace=all -tapeprompt=no  
dsmc restore e:\* -subdir=yes -replace=all -tapeprompt=no
```

También puede utilizar la opción quiet con el mandato restore para ahorrar tiempo de proceso. Sin embargo, no recibirá mensajes informativos para archivos individuales.

Nota: Si ya tiene los valores adecuados establecidos para las opciones subdir, replace, tapeprompt y quiet en el archivo de opciones del cliente, no es necesario incluirlas en los mandatos.

Cuando escriba múltiples mandatos para restaurar los archivos, debe especificar una parte exclusiva del espacio de archivos en cada mandato restore. No utilice en los mandatos ninguna especificación de archivo que se solape.

Para visualizar una lista de los directorios raíz de un espacio de archivos, utilice el mandato query backup. Por ejemplo:

```
dsmc query backup -dirsonly -subdir=no c:\
```




Como norma general, puede escribir de dos a cuatro mandatos restore a la vez. El número máximo que puede ejecutar a la vez sin degradar el rendimiento depende de factores tales como la utilización de la red y la cantidad de memoria disponible. Por ejemplo, si \users y \data1 se encuentran en la misma cinta, el proceso de restauración de \data1 debe esperar hasta que haya finalizado la restauración de \users. Sin embargo, si \data2 está en una cinta diferente y hay al menos dos unidades de cintas disponibles, la restauración de \data2 puede empezar al mismo tiempo que la de \users.

La velocidad a la cual se pueden restaurar los archivos también depende del número de unidades de cintas disponible y de si el administrador está utilizando la función de proximidad para mantener los espacios de archivos asignados en la menor cantidad de volúmenes posible. Si el administrador está utilizando la función de proximidad, también se reduce el número de montajes de medios de acceso secuencial necesarios para las operaciones de restauración.

## Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicializable

---

En este tema se describen los procesos de restauración estándar (o clásica), de restauración sin consulta y de restauración reinicializable.

-  Sistemas operativos Windows Proceso de restauración de consulta estándar  
El proceso de restauración de consulta estándar también se denomina restauración clásica. En este tema se explica cómo instalar los trabajos de restauración de consulta estándar.
-  Sistemas operativos Windows Sin consulta de proceso de restauración  
En el proceso de restauración sin consulta, se envía una sola solicitud de restauración al servidor en lugar de consultar al servidor para cada objeto que se debe restaurar.
-  Sistemas operativos Windows Proceso de restauración reinicializable  
Si el proceso de restauración se detiene debido a un corte de la alimentación o a una anomalía de la red, el servidor registra el punto en que se ha interrumpido la restauración.

## Proceso de restauración de consulta estándar

---

El proceso de restauración de consulta estándar también se denomina restauración clásica. En este tema se explica cómo instalar los trabajos de restauración de consulta estándar.

Los trabajos de restauración de consulta estándar funcionan de la siguiente manera:


- El cliente realiza una consulta al servidor para obtener una lista de los archivos de los que se ha hecho copia de seguridad correspondientes al espacio de archivos de cliente que desea restaurar.
- El servidor envía una lista de los archivos de los que se ha hecho copia de seguridad que coinciden con los criterios de la restauración. Si desea restaurar archivos activos e inactivos, el servidor envía información sobre todos los archivos de los que se ha hecho copia de seguridad al cliente.
- La lista de los archivos devuelta desde el servidor se clasifica en la memoria del cliente con el fin de determinar el orden de restauración de los archivos y minimizar el número de montajes de cintas necesarios para ejecutar la restauración.
- El cliente indica al servidor que restaure datos de archivo y objetos de directorio.
- Los directorios y archivos por restaurar se envían del servidor al cliente.

## Sin consulta de proceso de restauración





---


En el proceso de restauración sin consulta, se envía una sola solicitud de restauración al servidor en lugar de consultar al servidor para cada objeto que se debe restaurar.

1. El cliente indica al servidor que va a realizar una restauración sin consulta y le facilita los detalles sobre directorios, archivos y espacios de archivos.
2. El servidor utiliza una tabla independiente para realizar el seguimiento de entradas que guían la restauración.
3. Los datos por restaurar se envían al cliente. Los objetos de archivo y de directorio que se almacenan en el disco se envían inmediatamente, puesto que no es necesario clasificar dichos datos antes de restaurar el objeto.
4. Puede utilizar varias sesiones para restaurar los datos. Si los datos se encuentran en varias cintas, hay diversos puntos de montaje disponibles en el servidor. La combinación de la opción resourceutilization y MAXNUMMP permite el uso de varias sesiones.


 Sistemas operativos Windows Cuando proporcione una especificación de archivo de origen en el mandato restore y no especifique ninguna de las opciones: inactive, latest, pick, fromdate o todate, el cliente utiliza un método de *restauración sin consulta* para restaurar los archivos y los directorios desde el servidor. Este método se denomina restauración sin consulta ya que en lugar de realizar una

consulta al servidor para cada objeto que se debe restaurar, se le envía una única solicitud de restauración. En este caso, el servidor devuelve los archivos y directorios al cliente sin que el cliente tenga que realizar ninguna acción adicional. Éste simplemente acepta los datos procedentes del servidor y los restaura en el destino especificado en el mandato restore.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Cuando proporcione una especificación de archivo de origen en el mandato restore y no especifique ninguna de las opciones: inactive, latest, pick, fromdate, todate, el cliente utiliza un método de *restauración sin consulta* para restaurar los archivos y los directorios desde el servidor. Este método se denomina restauración sin consulta ya que en lugar de realizar una consulta al servidor para cada objeto que se debe restaurar, se le envía una única solicitud de restauración. En este caso, el servidor devuelve los archivos y directorios al cliente sin que el cliente tenga que realizar ninguna acción adicional. Éste simplemente acepta los datos procedentes del servidor y los restaura en el destino especificado en el mandato restore.

 sistemas operativos Mac OS X Utilizando el cliente GUI de IBM Spectrum Protect, un ejemplo de un mandato con carácter comodín sin restricciones sería seleccionar una carpeta de la ventana del árbol de restauración. Un ejemplo de un mandato con carácter comodín con restricciones sería seleccionar archivos individuales de una carpeta.


Utilizando el cliente de línea de mandatos, un ejemplo de un mandato con carácter comodín sin restricciones:

 sistemas operativos Mac OS X

```
"/Users/user1/Documents/2004/*"
```

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
/home/mydocs/2004/*
```

 Sistemas operativos Windows

```
c:\mydocs\2004\*
```

Un ejemplo de una especificación de archivo con carácter comodín con restricciones sería:

 sistemas operativos Mac OS X

```
/Users/user1/Documents/2004/sales.*
```

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
/home/mydocs/2004/sales.*
```

 Sistemas operativos Windows


```
c:\mydocs\2004\sales.*
```





## Proceso de restauración reiniciable

---

Si el proceso de restauración se detiene debido a un corte de la alimentación o a una anomalía de la red, el servidor registra el punto en que se ha interrumpido la restauración.






El cliente conoce este registro como *restauración reiniciable*. Se puede disponer de varias sesiones de restauración reiniciables. Utilice el mandato query restore o seleccione **restartable restores** en el menú Acciones para averiguar si su cliente tiene alguna sesión de restauración reiniciable en la base de datos del servidor.

 Sistemas operativos Windows Debe completar una restauración reiniciable antes de intentar llevar a cabo más copias de seguridad del sistema de archivos. Si intenta repetir la restauración interrumpida o realizar una copia de seguridad del espacio de archivos de destino, no lo logrará porque no ha concluido la restauración original. Para reiniciar la restauración en el punto en que se interrumpió, utilice el mandato restart restore; para suprimir la restauración reiniciable, utilice el mandato cancel restore. Si reinicia la restauración interrumpida, ésta se reinicia desde la primera transacción, que podría constar de uno o varios archivos, que no se había restaurado por completo en el momento de producirse la interrupción. Por este motivo, puede que reciba algunos mensajes que le preguntarán si han de sustituirse archivos de la transacción interrumpida cuya restauración ya se ha realizado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Debe completar una restauración reiniciable antes de intentar llevar a cabo más copias de seguridad del sistema de archivos. Si intenta repetir la restauración interrumpida o realizar una copia de seguridad del espacio de archivos de destino, no lo logrará porque no ha concluido la restauración original. Para reiniciar la restauración en el punto en que se interrumpió, utilice el mandato restart restore; para suprimir la restauración reiniciable, utilice el mandato cancel restore.

En el cuadro de diálogo **Restauraciones reiniciables** de la GUI de IBM Spectrum Protect, puede seleccionar y suprimir la restauración interrumpida o bien puede reiniciarla. Si reinicia la restauración interrumpida, ésta se reinicia desde la primera transacción, que podría constar de uno o varios archivos, que no se había restaurado por completo en el momento de producirse la interrupción. Por este

motivo, puede que reciba algunos mensajes que le preguntarán si han de sustituirse archivos de la transacción interrumpida cuya restauración ya se ha realizado.


 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Para llevar a cabo restauraciones reiniciables mediante la GUI del cliente Web, siga los pasos siguientes:

1. Seleccione **Acciones** → **Restauraciones reiniciables** en el panel inicial.
2. Seleccione la sesión de restauración reiniciable que desee llevar a cabo.
3. Pulse el botón **Reiniciar** de la parte superior del panel.

**Referencia relacionada:**

Resourceutilization

Restore

 Sistemas operativos Windows

## Restauración del estado del sistema de Windows

---

Microsoft Volume Shadowcopy Service (VSS) se admite en los clientes de copia de seguridad y archivado de Windows. El cliente utiliza VSS para restaurar el estado del sistema. La función de restauración de estado del sistema está en desuso para las operaciones de restauración de estado del sistema en línea.

### Acerca de esta tarea

---

Ya no puede restaurar el estado del sistema en un sistema que sigue en línea. En lugar de ello, utilice el método de recuperación basado en ASR para restaurar el estado del sistema en modo Windows PE fuera de línea. Para obtener más información, consulte los siguientes artículos de la wiki de IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Si intenta restaurar el estado del sistema con el mandato `dsmc restore systemstate`, desde la GUI del cliente de archivado y copia de seguridad, o desde el cliente web, aparecerá el siguiente mensaje:

```
ANS5189E Online SystemState restore has been deprecated. Please use offline  
WinPE method for performing system state restore.
```

**Conceptos relacionados:**

Recuperación de un equipo cuando el sistema operativo de Windows no funciona

**Referencia relacionada:**

Restore Systemstate

 Sistemas operativos Windows

## Restauración de los archivos de Recuperación automática del sistema

---

Puede restaurar los archivos de Recuperación automática del sistema (ASR) para recuperar la información de configuración del estado del sistema Windows y el estado del sistema si se produce un error muy grave del sistema o de hardware.

### Antes de empezar

---

Debe ser miembro del grupo de Administradores u Operadores de copia de seguridad para realizar la copia de seguridad y restaurar archivos ASR.

### Acerca de esta tarea

---

El cliente de archivado y copia de seguridad restaura los datos ASR cuando el cliente de archivado y copia de seguridad restaura el estado del sistema de Windows.


### Procedimiento

---

Para restaurar los archivos ASR en sistemas operativos de Windows, utilice el mandato `restore systemstate`.

**Conceptos relacionados:**

Recuperación de un equipo cuando el sistema operativo de Windows no funciona

 Sistemas operativos Windows

## Restaurar el sistema operativo cuando está funcionando el sistema

---

Si su sistema está funcionando, puede restaurar el sistema operativo desde los archivos de la copia de seguridad.

### Acerca de esta tarea

---

Si Active Directory está instalado, debe estar en modalidad de restauración de Active Directory. Cuando se realiza una recuperación del sistema operativo incluyendo el estado del sistema, utilice el siguiente orden de restauración. No reinicie el sistema entre cada paso, aunque se le solicite que lo haga.

### Procedimiento

---

1. Restablezca la unidad del sistema. Por ejemplo: `dsmc restore c:\* -sub=yes -rep=all`.
2. Restablezca el estado del sistema. Por ejemplo: `dsmc restore systemstate`.

 Sistemas operativos Windows

## Recuperación de un equipo cuando el sistema operativo de Windows no funciona


---

Si el sistema tiene un error de hardware o software catastrófico, puede recuperar un sistema operativo de Windows con Automated System Recovery (ASR).

- Crear un CD arrancable WinPE  
Antes de poder recuperar un sistema Windows mediante Automated System Recovery (ASR), debe crear un CD o DVD arrancable de Windows Preinstallation Environment (WinPE).
- Restaurar el sistema operativo de Windows con Automated System Recovery  
Puede restaurar el sistema operativo de Windows de un equipo con Automated System Recovery (ASR).

#### Tareas relacionadas:

Restaurar el sistema operativo cuando está funcionando el sistema

 Sistemas operativos Windows

## Crear un CD arrancable WinPE

---

Antes de poder recuperar un sistema Windows mediante Automated System Recovery (ASR), debe crear un CD o DVD arrancable de Windows Preinstallation Environment (WinPE).

### Procedimiento

---

Para obtener las instrucciones que describen cómo crear un CD o DVD arrancable de WinPE, consulte los siguientes artículos de la wiki IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

 Sistemas operativos Windows

## Restaurar el sistema operativo de Windows con Automated System Recovery

---

Puede restaurar el sistema operativo de Windows de un equipo con Automated System Recovery (ASR).

### Procedimiento

---

Para obtener las instrucciones que describen cómo restaurar un sistema de Windows mediante ASR, consulte los artículos de la wiki de IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1



## Qué hacer a continuación

---

Ahora puedes restaurar otros volúmenes.

### Tareas relacionadas:

Crear un CD arrancable WinPE

Crear un archivo de opciones del cliente para la recuperación automática del sistema

### Referencia relacionada:

Restore

Restore Systemstate

 Sistemas operativos Windows

## Restauración de archivos y árboles Dfs de Microsoft





---

Para restaurar los puntos de unión Dfs y los datos de cada punto de unión, primero restaure los metadatos de punto de unión Dfs y después restaure separadamente cada punto de unión.

Si los metadatos de punto de unión no se restauran, IBM Spectrum Protect creará un directorio en la raíz Dfs utilizando el mismo nombre que el del punto de unión y restaurará los datos en ese directorio.

### Tareas relacionadas:

Métodos de protección de archivo Microsoft Dfs

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows








## Restauración de una imagen

---

Existen algunos puntos que debe tener en cuenta antes de comenzar a restaurar imágenes en el sistema.




Para poder restaurar una imagen (desactivada o activada), debe tener autorización de administrador del sistema.

A continuación, se muestra una lista de los puntos que debe tener en cuenta antes de restaurar una imagen:

- Al restaurar la imagen de un volumen, los datos se restaurarán al mismo estado en el que estaban cuando se realizó la última copia de seguridad de imagen. Asegúrese por completo de que necesita restaurar una imagen, puesto que sustituirá todo el sistema de archivos o volumen RAW por la imagen del servidor.
-  Sistemas operativos Windows La operación de restauración de imágenes sobrescribe la etiqueta del volumen de destino con la etiqueta que existía en el volumen de origen.
- Asegúrese de que el volumen al que está restaurando la imagen tiene como mínimo el mismo tamaño que la imagen que se está restaurando.
-  Sistemas operativos Linux En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en /etc/fstab, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo /etc/fstab para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El sistema de archivos o volumen que está restaurando tiene que ser del mismo tipo que el original.
-  Sistemas operativos Windows El sistema de archivos o volumen que está restaurando no tiene que ser del mismo tipo que el original. Ni siquiera se tiene que dar formato al volumen. El proceso de restauración de la imagen crea el sistema de archivos con el formato correcto que necesite.
- Asegúrese de que el volumen de destino de la restauración no está utilizándose. El cliente bloquea el volumen antes de iniciar la restauración. El cliente desbloquea el volumen cuando finaliza la restauración. Si el volumen se está utilizando cuando el cliente intenta bloquear el sistema de archivos, la restauración da un error.
- No es posible restaurar una imagen en la ubicación de instalación del programa de cliente de IBM Spectrum Protect.
-  Sistemas operativos Windows Si ha creado una imagen de la unidad del sistema, no puede restaurar la imagen en la misma ubicación, porque el cliente no puede tener un bloqueo exclusivo de la unidad del sistema. Asimismo, debido a las diferentes configuraciones de los componentes del sistema, es posible que la imagen del sistema no sea coherente entre los componentes (como Active Directory). Algunos de estos componentes se pueden configurar para que utilicen volúmenes diferentes, de modo que unos se instalen en la unidad del sistema y otros en volúmenes que no son del sistema.
- Si ejecuta copias de seguridad incrementales de forma progresiva y copias de seguridad de imagen del sistema de archivos, puede realizar una restauración de imagen incremental del sistema de archivos. El proceso restaura los archivos individuales una vez restaurada la imagen completa. Los archivos individuales restaurados son los archivos de los que se ha hecho una copia de


seguridad después de la imagen original. Opcionalmente, si los archivos se hubieran suprimido después de la copia de seguridad original, la restauración incremental puede suprimir estos archivos de la imagen base.

La supresión de archivos se realizará correctamente si el grupo de copia de seguridad del servidor de IBM Spectrum Protect cuenta con suficientes versiones para los archivos existentes y suprimidos. Las copias de seguridad y restauraciones incrementales solamente se pueden realizar en sistemas de archivos montados y no en volúmenes lógicos RAW.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si por algún motivo se daña una imagen restaurada, puede utilizar la herramienta `fsck` para intentar repararla.









Puede utilizar la opción `verifyimage` con el mandato `restore image` para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.

Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción `imagetofile` con el mandato `restore image` para especificar que desea restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

-  Sistemas operativos Windows Si por algún motivo se daña una imagen restaurada, debe ejecutar `chkdsk` para comprobar si hay sectores defectuosos y, en caso afirmativo, repararlos (a menos que el volumen restaurado sea RAW).

Puede utilizar la opción `verifyimage` con el mandato `restore image` para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.





Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción `imagetofile` con el mandato `restore image` para especificar que desea restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Restauración de una imagen mediante la GUI  
Puede utilizar la GUI para restaurar una imagen del sistema de archivos o un volumen lógico RAW.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Restauración de una imagen mediante la línea de mandatos  
Utilice el mandato `restore image` para restaurar una imagen mediante el cliente de línea de mandatos de IBM Spectrum Protect.

#### Referencia relacionada:

Imagetofile

Verifyimage

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows





## Restauración de una imagen mediante la GUI

Puede utilizar la GUI para restaurar una imagen del sistema de archivos o un volumen lógico RAW.

### Acerca de esta tarea

Realice estos pasos para restaurar una imagen del sistema de archivos o volumen lógico RAW:

### Procedimiento





1. Pulse **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios.
3. Localice el objeto del árbol que tiene el nombre **Imagen** y amplíelo. Pulse en las casillas que hay junto a la imagen que desea restaurar. Si desea obtener información detallada sobre el objeto, resáltelo y seleccione **Ver** → **Detalles de archivo** en la ventana principal, o bien pulse el botón **Ver detalles de archivo**.
4. **Opcional:** para realizar una restauración de imagen incremental, pulse el botón **Opciones** para abrir la ventana Opciones de restauración y seleccione la opción **Imagen más directorios y archivos incrementales**. Si desea suprimir archivos inactivos del sistema de archivos local, seleccione la casilla **Suprimir archivos inactivos de sistema local**. Pulse el botón **Aceptar**.
5.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. La imagen se puede restaurar en el volumen con el punto de montaje desde el que se ha hecho originalmente la copia de seguridad. Alternativamente, se puede seleccionar un volumen diferente como ubicación de la restauración.
6.  Sistemas operativos Windows Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. La imagen se puede restaurar en el volumen con la letra de la unidad o el punto de montaje desde el que se ha hecho originalmente la copia de seguridad. Alternativamente, se puede seleccionar un volumen diferente como ubicación de la restauración.

7. Pulse el botón **Restaurar** para iniciar la restauración. Aparecerá la ventana **Lista de tareas**, en la que se muestra el progreso de la restauración. Aparecerá la ventana Informe de restauración.

## Resultados





---

A continuación, figuran algunas cuestiones que deberá tener en cuenta cuando realice una operación de restauración de imagen mediante la GUI:

- Puede seleccionar **Ver** → **Detalles de archivo** en la ventana principal o pulsar el botón **Ver detalles de archivo** para visualizar las imágenes del sistema de archivos de las que el cliente ha realizado una copia de seguridad:
  - Tamaño de imagen - Es el tamaño del volumen del que se ha realizado la copia de seguridad.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tamaño almacenado - Es el tamaño de la imagen real que se ha almacenado en el servidor. La imagen almacenada en el servidor de IBM Spectrum Protect tiene un tamaño que equivale a la capacidad del volumen.
  -  Sistemas operativos Windows Tamaño almacenado - Es el tamaño de la imagen real que se ha almacenado en el servidor. Puesto que la copia de seguridad de imágenes le permite realizar la copia de seguridad únicamente de los bloques utilizados en un sistema de archivos, el tamaño almacenado de la imagen en el servidor de IBM Spectrum Protect podría ser más pequeño que el tamaño del volumen. Para las copias de seguridad de imágenes en línea, la imagen almacenada puede ser más grande que el sistema de archivos, en función del tamaño de los archivos de la caché.
  - Tipo de sistema de archivos
  - Fecha y hora de la copia de seguridad
  - Clase de gestión asignada a la copia de seguridad de imagen
  - Si la copia de seguridad de imágenes es una copia activa o inactiva
- Si desea modificar opciones de restauración específicas, pulse el botón **Opciones**. Las opciones que modifique *sólo* estarán en vigor durante la sesión actual.
- En la ventana Opciones de restauración, puede elegir restaurar sólo la imagen o la imagen y los archivos de los directorios de datos de copia incremental. Si elige **Sólo la imagen**, solo se restaurará la imagen de la última copia de seguridad. Éste es el valor predeterminado.

Si ha ejecutado una copia de seguridad de imagen incremental por fecha en un volumen o copias de seguridad de imagen en un volumen con datos de copia incremental, puede elegir la opción **Imagen más directorios y archivos incrementales**. Si elige **Imagen más directorios y archivos incrementales**, también puede seleccionar **Suprimir archivos inactivos de sistema local** para suprimir los archivos inactivos que se restauren en el sistema de archivos local. Si el único tipo de copia de seguridad que ha realizado en el sistema de archivos ha sido la copia de seguridad de imagen incremental por fecha, no se suprimirán los archivos.


Importante: Debe asegurarse por completo de que necesita realizar una restauración incremental, puesto que se sustituirá todo el sistema de archivos por la imagen del servidor y, a continuación, se restaurarán los archivos de los que ha hecho copia de seguridad con la operación de copia de seguridad de imagen incremental.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Restauración de una imagen mediante la línea de mandatos

---

Utilice el mandato `restore image` para restaurar una imagen mediante el cliente de línea de mandatos de IBM Spectrum Protect.

 Sistemas operativos Windows Puede utilizar la opción `verifyimage` con el mandato `restore image` para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, IBM Spectrum Protect emite un mensaje de aviso en la consola y en el registro de errores.

 Sistemas operativos Windows Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción `imagetofile` con el mandato `restore image` para especificar que desea restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

### Referencia relacionada:

Imagetofile  
Verifyimage

## Restauración de datos desde un conjunto de copias de seguridad

---

El administrador de IBM Spectrum Protect puede generar un conjunto de copias de seguridad, que es una colección de los archivos que residen en el servidor, en soportes portables creados en un dispositivo utilizando un formato compatible con el dispositivo de cliente.

Puede restaurar datos de un juego de copias de seguridad del servidor de IBM Spectrum Protect o cuando el juego de copias de seguridad esté disponible localmente como un archivo o en un dispositivo de cinta.

Puede restaurar conjuntos de copias de seguridad desde las siguientes ubicaciones:

- Desde el servidor de IBM Spectrum Protect
- Desde medios portables de un dispositivo conectado a la estación de trabajo cliente
- Desde un archivo de conjunto de copias de seguridad en la estación de trabajo cliente

Los conjuntos de copias de seguridad pueden proporcionarle las funciones de archivado instantáneo y recuperación rápida, como se describe a continuación.


#### Archivado instantáneo

Esta función permite al administrador crear un juego de copias archivadas a partir de las versiones de copia de seguridad ya almacenadas en el servidor.

#### Recuperación rápida con conjuntos de copias de seguridad locales

Normalmente, las restauraciones se realizan a partir de copias de seguridad de archivos normales almacenados en el servidor de IBM Spectrum Protect fuera de los juegos de copias de seguridad. Este enfoque le ofrece la posibilidad de restaurar la versión de copia de seguridad más reciente de cada archivo. Es posible que un conjunto de copias de seguridad no contenga la versión de copia de seguridad más reciente de los archivos.


En algunos casos, la restauración de datos desde un juego de copias de seguridad puede ser una opción más adecuada que la restauración desde archivos de copia de seguridad normales del servidor de IBM Spectrum Protect. La restauración desde juegos de copias de seguridad puede ser más adecuada por los siguientes motivos:

- Un conjunto de copias de seguridad puede contribuir a una recuperación más rápida porque todos los archivos necesarios para la restauración están dentro de un menor número de volúmenes de almacenamiento.
- Los juegos de copias de seguridad permiten la colección de instante de los archivos. Puede restaurar en un instante específico en vez de restaurar lo que está disponible en ese momento en una restauración a nivel de archivo normal desde el servidor.
-  Sistemas operativos Windows Puede realizar una restauración ASR utilizando un volumen de conjunto de copias de seguridad.

Restaurar un conjunto de copias de seguridad del servidor de IBM Spectrum Protect ofrece un conjunto mayor de opciones de restauración que restaurar a partir de un conjunto de copias de seguridad local. Sin embargo, en algunos casos puede ser preferible restaurar a partir de un conjunto de copias de seguridad local:

- Es posible que tenga que restaurar los datos cuando no haya una conexión de red disponible con el servidor de IBM Spectrum Protect. Esto puede suceder en una situación de recuperación ante siniestro.
- La restauración local puede ser más rápida que la restauración a través de una conexión de red con el servidor de IBM Spectrum Protect.

Un juego de copias de seguridad puede restaurarse desde el servidor de IBM Spectrum Protect mientras los volúmenes de juego de copias de seguridad estén disponibles en dicho servidor, o pueden haberse cambiado al sistema del cliente para una restauración de juego de copias de seguridad local. Puede generarse un conjunto de copias de seguridad con o sin una tabla de contenidos (TOC), y éste puede contener datos de archivos o imágenes.

 Sistemas operativos Windows El conjunto de copias de seguridad contiene datos del estado del sistema.

La posibilidad de restaurar datos de conjuntos de copias de seguridad está restringida por la ubicación del conjunto de copias de seguridad y el tipo de datos de que contiene. El cliente de línea de mandatos puede restaurar algunos datos que la GUI no puede, pero la GUI le permite examinar y elegir los objetos que desea restaurar. Por lo general, los conjuntos de copias de seguridad del servidor con una tabla de contenido ofrecen más opciones durante la restauración. Sin embargo, los juegos de copias de seguridad locales ofrecen opciones que a veces son preferibles a restaurar a partir del servidor de IBM Spectrum Protect.

Las limitaciones para restaurar datos de juegos de copias de seguridad mediante la GUI se resumen en la siguiente tabla. Cada celda interior representa una combinación de tipo de datos y ubicación del conjunto de copias de seguridad. En cada situación, la celda indica si puede utilizar la GUI para restaurar únicamente el conjunto de copias de seguridad completo, seleccionar objetos del conjunto de copias de seguridad o si no puede utilizarla para restaurar el conjunto de copias de seguridad.

Tabla 1. Restricciones de restauración del conjunto de copias de seguridad de la GUI

Tipo de datos del conjunto de copias de seguridad	Ubicación del conjunto de copias de seguridad		
	Local (location=file o location=tape)	Servidor de IBM Spectrum Protect (tabla de contenidos disponible)	Servidor de IBM Spectrum Protect (tabla de contenidos no disponible)

Tipo de datos del conjunto de copias de seguridad	Ubicación del conjunto de copias de seguridad		
	Local (location=file o location=tape)	Servidor de IBM Spectrum Protect (tabla de contenidos disponible)	Servidor de IBM Spectrum Protect (tabla de contenidos no disponible)
archivo	Sólo restauración del conjunto de copias de seguridad completo.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	Sólo restauración del conjunto de copias de seguridad completo.
imagen	No se puede restaurar.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	No se puede restaurar.
estado del sistema	Sólo restauración del conjunto de copias de seguridad completo.	Restauración del conjunto de copias de seguridad completo o de objetos seleccionados.	Sólo restauración del conjunto de copias de seguridad completo.

Las restricciones para restaurar datos de conjuntos de copias de seguridad mediante el cliente de la línea de mandatos se resumen en la tabla que se encuentra a continuación. Cada celda interior representa una combinación de tipo de datos y ubicación del conjunto de copias de seguridad. En cada situación, la celda contiene los mandatos de restauración que puede utilizar. Salvo lo indicado, puede restaurar objetos específicos dentro de un conjunto de copias de seguridad así como el conjunto de copias de seguridad completo.











Tabla 2. Restricciones de restauración de los conjuntos de copias de seguridad de la línea de mandatos

Tipo de datos del conjunto de copias de seguridad	Ubicación del conjunto de copias de seguridad		
	Local (location=file o location=tape)	Servidor de IBM Spectrum Protect (tabla de contenidos disponible)	Servidor de IBM Spectrum Protect (tabla de contenidos no disponible)
archivo	Mandatos: restauración restore backupset	Mandatos: restauración restore backupset	Mandatos: restore backupset
imagen	No se puede restaurar	Mandato: restore image	No se puede restaurar
estado del sistema	Mandato: restore backupset	Mandatos: restore backupset restore systemstate	Mandato: restore backupset







Restricción: Cuando restaura datos del estado del sistema mediante el mandato restore backupset, no puede especificar objetos individuales. Sólo puede restaurar el estado del sistema completo.

- Restauración de conjuntos de copias de seguridad: consideraciones y restricciones  
Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.
- Restauración del conjunto de copias de seguridad  
IBM Spectrum Protect interpreta que un juego de copias de seguridad es un objeto que contiene una estructura de archivos completa. Puede restaurar todo el conjunto de copias de seguridad o, en algunos casos, puede seleccionar partes de él. Los medios del conjunto de copias de seguridad son autodescriptivos y contienen toda la información necesaria para realizar correctamente una restauración.
- Restauración de conjuntos de copias de seguridad mediante la GUI  
La GUI de cliente puede restaurar datos desde un conjunto de copias de seguridad del servidor, desde un archivo local o desde un dispositivo de cinta local. Puede utilizar la GUI para restaurar archivos individuales de un juego de copias de seguridad del servidor de IBM Spectrum Protect con una tabla de contenidos, pero no de un juego de copias de seguridad local ni de un juego de copias de seguridad del servidor sin una tabla de contenidos.
- Restauraciones de los conjuntos de copia de seguridad utilizando una interfaz de línea de mandatos  
La interfaz de línea de mandatos puede restaurar datos de un conjunto de copias de seguridad, desde un archivo local o de un dispositivo de cinta local. Puede utilizar el cliente de interfaz de línea de mandatos para restaurar archivos individuales de los conjuntos de copias de seguridad local y de conjuntos de copia de seguridad configurados sin TOC.

#### Referencia relacionada:

 sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris  
 Sistemas operativos WindowsLocalbackupset  
 Query Backupset  
 sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris  
 Sistemas operativos WindowsQuery Image  
 Restore

Restore Backupset

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos WindowsRestore Image  
 Sistemas operativos WindowsRestore Systemstate

## Restauración de conjuntos de copias de seguridad: consideraciones y restricciones










---

Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.

### Consideraciones de restauración del conjunto de copias de seguridad

---









Al restaurar conjuntos de copias de seguridad, tenga en cuenta lo siguiente:

- Si el objeto que desea restaurar se ha generado desde un nodo cliente cuyo nombre es distinto del nodo actual, especifique el nombre del nodo original con el parámetro `filespace` en cualquiera de los mandatos `restore`.
- Si no puede restaurar un conjunto de copias de seguridad desde el medio portable, póngase en contacto con el administrador de IBM Spectrum Protect para asegurarse de que el medio portable se creó en un dispositivo con un formato compatible con el suyo.
- Si utiliza el mandato `restore backupset` en la línea de mandatos inicial con el parámetro `-location=tape 0 -location=file`, el cliente no intenta ponerse en contacto con el servidor de IBM Spectrum Protect.
- Cuando restaure un grupo a partir de un conjunto de copias de seguridad:
  - Se restaurará todo el grupo, o todos los grupos, del espacio de archivos virtual. Si hay varios grupos en el mismo espacio de archivos virtual, no podrá restaurar un solo grupo especificando el nombre de grupo. No puede restaurar una parte de un grupo especificando una vía de acceso de archivo.
  - Especifique un grupo utilizando los valores siguientes:
    - Especifique el nombre de espacio de archivos individual con el parámetro `filespace`.
    - Utilice la opción `subdir` para incluir subdirectorios.
- Se proporciona soporte limitado para la restauración de conjuntos de copias de seguridad desde dispositivos de cinta conectados al sistema cliente. Se debe utilizar siempre un controlador de dispositivo nativo proporcionado por el fabricante del dispositivo. El controlador de dispositivo proporcionado por IBM para que lo utilice el servidor de IBM Spectrum Protect no se puede utilizar en el sistema cliente para restaurar juegos de copias de seguridad locales.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si un conjunto de copias de seguridad contiene archivos de distintos propietarios, el propio conjunto de copias de seguridad será propiedad del ID de usuario `root` y los ID de usuarios que no sean `root` no verán el conjunto de copias de seguridad. En tal caso, los ID de usuario que no son `root` pueden restaurar sus archivos si el administrador de IBM Spectrum Protect `rd>` les proporciona el nombre del juego de copias de seguridad. Los usuarios que no sean `root` sólo podrán restaurar sus propios archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para permitir que la GUI del cliente restaure un conjunto de copias de seguridad de un dispositivo local, sin que sea necesaria una conexión al servidor, utilice la opción `localbackupset`.

### Consideraciones de restauración del conjunto de copias de seguridad

---

Al restaurar conjuntos de copias de seguridad, tenga en cuenta las siguientes restricciones:


- No es posible restaurar ni utilizar los datos de los conjuntos de copias de seguridad de los que se ha hecho una copia de seguridad mediante la API.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No puede restaurar datos de imagen de un conjunto de copias de seguridad mediante la utilización del mandato `restore backupset`. Sólo puede restaurar datos de imagen de un conjunto de copias de seguridad con el mandato `restore image`.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No puede restaurar datos de imagen de un conjunto de copias de seguridad local (`location=tape 0 location=file`). Sólo puede restaurar datos de imagen de un juego de copias de seguridad del servidor de IBM Spectrum Protect.

## Restauración del conjunto de copias de seguridad

---

IBM Spectrum Protect interpreta que un juego de copias de seguridad es un objeto que contiene una estructura de archivos completa. Puede restaurar todo el conjunto de copias de seguridad o, en algunos casos, puede seleccionar partes de él. Los medios del conjunto de copias de seguridad son autodescriptivos y contienen toda la información necesaria para realizar correctamente una restauración.

Si está conectado a un servidor de Tivoli Storage Manager Versión 5.4 o posterior, el administrador del servidor podrá crear conjuntos de copias de seguridad apiladas. Los juegos de copias de seguridad apilados pueden contener datos de varios nodos y distintos tipos de datos para un nodo cliente en particular. Los tipos de datos pueden ser datos de archivo o datos de imagen.

 Sistemas operativos Windows Si ha realizado la actualización desde Tivoli Storage Manager Express, también estarán admitidos algunos datos de aplicación.

**Restricción:** El proceso de restauración de datos de imagen y datos de aplicación solo está disponible cuando la restauración se realiza desde el servidor. No puede restaurar datos de imagen y datos de aplicación de la restauración de un conjunto de copias de seguridad de un cliente local.

Cuando un juego de copias de seguridad se ha apilado, sólo puede restaurar los datos de su propio nodo. Los datos de todos los demás nodos se pasan por alto. Cuando restaure datos desde un juego de copias de seguridad apilado de un dispositivo local, sólo podrá restaurar los datos de archivo de su propio nodo cliente. Es importante que la opción nodename se configure para que coincida con el nombre de nodo utilizado para generar el conjunto de copias de seguridad de uno de los nodos de la pila.

**Importante:** Debido a la portabilidad de los conjuntos de copias de seguridad locales, deben realizarse pasos adicionales para proteger los conjuntos de copias de seguridad locales de los medios portables. Los medios del conjunto de copias de seguridad deben protegerse físicamente, porque el conjunto de copias de seguridad puede restaurarse localmente sin autenticarse con el servidor. Todos los usuarios disponen de acceso a todos los datos del juego de copias de seguridad apilado, lo que significa que los usuarios disponen de acceso a los datos que no son de su propiedad, cambiando el nombre de nodo o visualizando el juego de copias de seguridad en el formato RAW de éste. Los únicos métodos que garantizan la protección de los datos son la protección física o el cifrado de los medios.

Si desea restaurar datos del conjunto de copias de seguridad desde el servidor, puede restaurar archivos individuales, directorios o los datos del conjunto de copias de seguridad completo en una única operación desde la GUI o desde la línea de mandatos. Si desea restaurar datos del conjunto de copias de seguridad localmente, la GUI sólo podrá visualizar y restaurar un conjunto de copias de seguridad completo. La línea de mandatos se puede utilizar para restaurar archivos o directorios individuales que están almacenados en un conjunto de copias de seguridad localmente.

## Restauración de conjuntos de copias de seguridad mediante la GUI

---











La GUI de cliente puede restaurar datos desde un conjunto de copias de seguridad del servidor, desde un archivo local o desde un dispositivo de cinta local. Puede utilizar la GUI para restaurar archivos individuales de un juego de copias de seguridad del servidor de IBM Spectrum Protect con una tabla de contenidos, pero no de un juego de copias de seguridad local ni de un juego de copias de seguridad del servidor sin una tabla de contenidos.

### Acerca de esta tarea

---

**Importante:** antes de iniciar una operación de restauración, tenga en cuenta que los conjuntos de copias de seguridad pueden contener datos para varios espacios de archivos. Si especifica un destino distinto de la ubicación original, los datos de *todos* los espacios de archivos se restauran en la ubicación especificada.




























Para restaurar un conjunto de copias de seguridad de la GUI, siga los pasos a continuación:

1.  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Pulse Restaurar en la ventana principal de la GUI. Aparecerá la ventana Restaurar.
2. Localice el objeto de árbol de directorios Juegos de copias de seguridad y amplíelo pulsando en el signo más (+) que aparece junto a éste.
  - o  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para restaurar el conjunto de copias de seguridad de un dispositivo local, expanda el objeto Local y aparecerá la ventana para especificar la ubicación de conjunto de copias de seguridad. En la ventana, seleccione Nombre de archivo: o Nombre de cinta: en la lista desplegable y, a continuación, especifique la ubicación del archivo o la cinta. También puede pulsar el botón Examinar para que se abra una ventana de selección de archivos y seleccionar un conjunto de copias de seguridad.
  - o Para restaurar datos del conjunto de copias de seguridad desde el servidor, amplíe primero el objeto Servidor y, a continuación, Nivel de archivo o Imagen, en función del tipo de restauración solicitada.
3. Realice una pulsación en el recuadro que se encuentra junto al conjunto de copias de seguridad o al directorio o archivo del conjunto de copias de seguridad que desea restaurar.

Puede seleccionar archivos de un conjunto de copias de seguridad si el conjunto de copias de seguridad se encuentra en el servidor y tiene una tabla de contenido.

4. Pulse Restaurar. Aparecerá la ventana Destino de restauración. Entre la información pertinente.
5. Pulse Restaurar. La ventana Lista de tareas mostrará el estado del proceso de restauración.

Nota:


- Si el objeto que desea restaurar forma parte de un juego de copias de seguridad generado en un nodo y se cambia el nombre de nodo en el servidor, los objetos del juego de copias de seguridad generados antes del cambio de nombre no coincidirán con el nuevo nombre de nodo. Asegúrese de que el nombre del nodo es el mismo que el nodo para el que se generó el juego de copias de seguridad.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows El cliente puede utilizarse para restaurar un conjunto de copias de seguridad en un dispositivo conectado, con o sin una conexión de servidor. Si no puede establecerse conexión con el servidor, se visualizará un mensaje preguntándole si desea continuar con la restauración de un conjunto de copias de seguridad locales. Asimismo, también puede utilizarse la opción localbackupset para indicar al cliente que no intente establecer conexión con el servidor.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Algunos dispositivos locales, como los dispositivos de cinta (los dispositivos de cinta no se aplican a Mac OS X), requieren la instalación de controladores de dispositivo antes de realizarse la restauración. Consulte el manual del dispositivo para obtener ayuda para realizar esta tarea. También necesita conocer la dirección del dispositivo para llevar a cabo la restauración.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Las siguientes funciones de una restauración de conjunto de copias de seguridad desde el servidor no están disponibles cuando la restauración se realiza localmente:
  1.  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Restaurar una imagen.
  2.  Sistemas operativos Windows Restaurar componentes del estado del sistema individual.
  3.  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Visualización y restauración de la GUI de archivos y directorios individuales. Para restaurar un directorio o archivo individual desde un conjunto de copias de seguridad locales puede utilizarse la línea de mandatos.
  4.  Sistemas operativos Windows Restauración de datos de aplicación si el servidor se ha migrado desde el producto Tivoli Storage Manager Express.

## Restauraciones de los conjuntos de copia de seguridad utilizando una interfaz de línea de mandatos

La interfaz de línea de mandatos puede restaurar datos de un conjunto de copias de seguridad, desde un archivo local o de un dispositivo de cinta local. Puede utilizar el cliente de interfaz de línea de mandatos para restaurar archivos individuales de los conjuntos de copias de seguridad local y de conjuntos de copia de seguridad configurados sin TOC.

Para restaurar la interfaz de línea de mandatos del cliente, utilice el mandato query backupset para visualizar qué datos del conjunto de copias de seguridad están disponibles, a continuación utilice los mandatos de restauración de los datos.





Puede utilizar los mandatos siguientes para restaurar datos de sus conjuntos de copias de seguridad:

- restore
- restore backupset
- restore image
-  Sistemas operativos Windows restore systemstate

Utilice el mandato adecuado para la ubicación del conjunto de copias de seguridad y de los datos del conjunto de copias de seguridad. Para obtener más información, consulte el apartado Tabla 2.





### Referencia relacionada:

Query Backupset


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Query Image

Restore

Restore Backupset

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Restore Image

 Sistemas operativos Windows Restore Systemstate

 Sistemas operativos Windows

## Restaurar compartimientos de Net Appliance CIFS

La restauración de la definición de compartición implica la restauración del directorio raíz del espacio de archivos de compartición que, en la mayoría de las circunstancias, puede realizarse como se indica a continuación: `dsmc rest \\NetAppFiler\CifsShareName\ -dirsonly`



La siguiente salida indica que el directorio raíz (y la definición de compartición) se ha restaurado:

```
Restoring          0 \\NetAppFiler\CifsShareName\ [Done]
```

Si la definición de compartición de CIFS se suprime en el servidor de archivos de Net Appliance, el cliente no podrá restaurar directamente la definición de compartición porque ya no se puede acceder al compartición.

La definición de compartición puede restaurarse indirectamente creando una compartición local temporal y restaurando la definición de compartición en la compartición temporal, tal como se indica a continuación:

```
md c:\tempdir net share tempshare=c:\tempdir
/remark:"Temporary Share for Restoring Deleted CIFS Share"
net use z: \\LocalMachineName\tempshare
dsmc res \\NetAppFiler\CifsShareName\ z:\ -dirsonly
```

Con ello, la definición de compartición original (incluidos los permisos) se restaura en el servidor de archivos.

Puede que las versiones anteriores del servidor de IBM Spectrum Protect experimenten un problema que impida la restauración del directorio raíz y la definición de compartir de CIFS. Si se produce este problema, la situación podrá eludirse utilizando uno de los métodos siguientes:

1. Utilice el indicador de prueba `DISABLENQR` para restaurar el directorio raíz, tal como se indica a continuación:

```
dsmc res \\NetAppFiler\CifsShareName\ -test=disablenqr -dirsonly
```

2. Utilice la opción `-pick` del cliente de línea de mandatos con un mandato de restauración y seleccione el directorio raíz:

```
dsmc res \\NetAppFiler\CifsShareName\ -dirsonly -pick
```


#### Tareas relacionadas:



Copia de seguridad de las definiciones de compartición de Net Appliance CIFS



 Sistemas operativos Linux  Sistemas operativos Windows



## Restauración de datos desde la copia de seguridad de VMware

Puede utilizar diversos métodos para restaurar datos de copias de seguridad en máquinas virtuales VMware. El método de restauración depende del tipo de copia de seguridad y versión del software del cliente de copia de seguridad y archivado que utilice para ejecutar la restauración.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

 Sistemas operativos Linux  Sistemas operativos Windows Restauración completa de VM

 Sistemas operativos Linux  Sistemas operativos Windows Utilice el mandato `restore vm` para restaurar una máquina virtual entera a partir de una copia de seguridad de máquina virtual completa. Al restaurar una copia de seguridad de máquina virtual completa, la imagen restaurada sustituye la máquina virtual o se crea una nueva máquina virtual. En una restauración de máquina virtual completa, restaura todos los archivos VMware y el estado del sistema en sistemas Windows. Si accede a IBM Spectrum Protect Recovery Agent, puede restaurar archivos individuales.

 Sistemas operativos Linux  Sistemas operativos Windows Dependiendo de la versión del cliente de copia de seguridad y archivado que se esté ejecutando en el cliente VMware, utilice el método adecuado para restaurar una copia de seguridad de máquina virtual completa:

Versiones de copia de seguridad y archivado anteriores a la versión 6.2.2:

Restaura la copia de seguridad de máquina virtual completa utilizando VMware Consolidated Backup. Para obtener más información, consulte el siguiente tema:


Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup

Versiones del cliente de copia de seguridad y archivado cliente 6.2.2 o posteriores:

Restaura la copia de seguridad de máquina virtual completa utilizando la API de vStorage. El cliente de IBM Spectrum Protect V6.2.2 o posterior puede restaurar copias de seguridad completas de VMware creadas con versiones del cliente anteriores a V6.2.2. Para obtener más información, consulte el siguiente tema:

Restauración de copias de seguridad de máquina virtual completas


 Sistemas operativos Windows Restauración a nivel de archivo

 Sistemas operativos Windows Utilice el mandato `restore` para restaurar archivos individuales de una copia de seguridad de máquina virtual a nivel de archivos. Utilice este método cuando no pueda restaurar de manera práctica una imagen de VMware

completa. Las operaciones de copia de seguridad a nivel de archivo se han creado con clientes de copia de seguridad y archivado de la versión 7.1 o anterior.

A las restauraciones a nivel de archivos se les aplican las siguientes restricciones:

- Puede utilizar el método de restauración a nivel de archivos solo si existe una copia de seguridad a nivel de archivos de la máquina virtual.
- No puede restaurar una máquina virtual entera a partir de copias de seguridad a nivel de archivos porque el mandato restore no recrear estados de sistema Windows.
- No puede utilizar este método para restaurar archivos individuales desde una copia de seguridad de máquina virtual completa de una máquina virtual.

 Sistemas operativos Windows Dependiendo de la configuración de la máquina virtual en la que restaure los archivos, utilice el método adecuado para restaurar archivos a partir de una copia de seguridad a nivel de archivos:

El cliente de copia de seguridad y archivado no está instalado en la máquina virtual:





Restablezca los archivos desde el servidor de seguridad vStorage que haya realizado la copia de seguridad de la máquina virtual.

El cliente de copia de seguridad y archivado está instalado en la máquina virtual:

Restablezca el archivo desde el cliente de copia de seguridad y archivado instalado en la máquina virtual.

Para obtener más información, consulte el siguiente tema:

Escenario: Restauración de copias de seguridad de máquina virtual completas


-  Sistemas operativos Windows Restauración de copias de seguridad de máquina virtual completas  
Puede restaurar una copia de seguridad VMware completa para volver a crear todos los archivos de la máquina virtual VMware directamente en el servidor VMware. Este método sustituye el método en desuso de restauración de copias de seguridad creadas utilizando herramientas VMware Consolidated Backup (VCB). Este método de restauración no requiere el uso de la herramienta de conversión de VMware antes de restaurar la copia de seguridad en el servidor VMware. No puede utilizar este método para restaurar archivos individuales desde una copia de seguridad de máquina virtual completa.
-  Sistemas operativos Windows Casos de ejemplo para ejecutar el acceso instantáneo de máquina virtual completa y restauración de máquina virtual instantánea completa desde la línea de mandatos del cliente de archivado y copia de seguridad  
Las operaciones de acceso instantáneo a la máquina virtual completa y restauración instantánea de la máquina virtual completa requieren una licencia para IBM Spectrum Protect for Virtual Environments. Puede llevar a cabo cualquiera de estas operaciones desde la línea de mandatos del cliente de archivado y copia de seguridad. Las operaciones y opciones de restauración instantánea y acceso instantáneo solo se admiten para máquinas virtuales VMware que estén alojadas en servidores VMware ESXi 5.1 o versiones posteriores.
-  Sistemas operativos Windows Escenario: Restauración de copias de seguridad de máquina virtual completas  
En sistemas Microsoft Windows, puede restaurar archivos específicos a partir de una copia de seguridad a nivel de archivos de una máquina virtual VMware. Las restauraciones a nivel de archivos son útiles para restaurar archivos individuales que pudieran perderse o dañarse. No puede utilizar este método para restaurar archivos que formasen parte de una copia de seguridad de VM completa. Antes de restaurar archivos desde un servidor de seguridad fuera de host en la máquina virtual VMware, dicho servidor se debe configurar como servidor proxy.
-  Sistemas operativos Windows Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup  
Puede restaurar una copia de seguridad VMware completa para volver a crear todos los archivos de la máquina virtual VMware. Siga estos pasos para restaurar las copias de seguridad de VM completas que se crearon mediante la utilización de VMware Consolidated Backup (VCB) que se ejecuta en IBM Spectrum Protect versión 6.2.0 o anterior.

 Sistemas operativos Linux  Sistemas operativos Windows

## Restauración de copias de seguridad de máquina virtual completas

Puede restaurar una copia de seguridad VMware completa para volver a crear todos los archivos de la máquina virtual VMware directamente en el servidor VMware. Este método sustituye el método en desuso de restauración de copias de seguridad creadas utilizando herramientas VMware Consolidated Backup (VCB). Este método de restauración no requiere el uso de la herramienta de conversión de VMware antes de restaurar la copia de seguridad en el servidor VMware. No puede utilizar este método para restaurar archivos individuales desde una copia de seguridad de máquina virtual completa.

### Antes de empezar

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Para restaurar una copia de seguridad VMware completa creada utilizando las herramientas VCB en IBM Spectrum Protect Versión 6.2.0 o anterior, consulte el tema "Restauración de copias de seguridad de máquina virtual completas creadas con copia de seguridad consolidada de VMware".

## Procedimiento

1. Dependiendo de la ubicación de destino de la restauración, complete los pasos adecuados:
  - Si la restauración de la copia de seguridad de máquina virtual completa va a sobrescribir la máquina virtual VMware existente, suprima dicha máquina virtual.
  - Si restaura la copia de seguridad de máquina virtual completa en una nueva máquina virtual, no necesita suprimir la máquina virtual existente. Puede suprimir la máquina virtual existente o proceder al siguiente paso.
2. Consulte a la máquina virtual acerca de las copias de seguridad de VMware siguiendo los pasos indicados a continuación:
  - a. En el servidor de copia de seguridad fuera de host, ejecute el siguiente mandato:

```
dsmc q vm *
```

El mandato muestra las copias de seguridad disponibles, por ejemplo:

Núm	Fecha	copia	seg	Clase	gest	Tipo	A/I	Máquina virtual
1	12/03/2009	03:05:03		DEFAULT		VSTORFULL	A	vm_guest1
2	09/02/2010	10:45:09		DEFAULT		VSTORFULL	A	vm_guest11
3	09/02/2010	09:34:40		DEFAULT		VSTORFULL	A	vm_guest12
4	09/02/2010	10:10:10		DEFAULT		VSTORFULL	A	vm_guest13
5	12/04/2009	20:39:35		DEFAULT		VSTORFULL	A	vm_guest14
6	09/02/2010	11:15:18		DEFAULT		VSTORFULL	A	vm_guest15
7	09/02/2010	02:52:44		DEFAULT		VSTORFULL	A	vm_guest16
8	08/05/2010	04:28:03		DEFAULT		VSTORFULL	A	vm_guest17
9	08/05/2010	05:20:27		DEFAULT		VSTORFULL	A	vm_guest18
10	08/12/2010	04:06:13		DEFAULT		VSTORFULL	A	vm_guest19
11	09/02/2010	00:47:01		DEFAULT		VSTORFULL	A	vm_guest7
12	09/02/2010	01:59:02		DEFAULT		VSTORFULL	A	vm_guest8
13	09/02/2010	05:20:42		DEFAULT		VSTORFULL	A	vm_guest9

El código de retorno de ANS1900I es 0.

El código de retorno más alto de ANS1901I fue 0.

- b. En los resultados devueltos por el mandato de consulta, identifique la máquina virtual que desea restaurar.
3. Restaure la copia de seguridad de VMware completa utilizando el mandato `restore vm`. Para restaurar una copia de seguridad en una máquina virtual con un nuevo nombre, utilice la opción `-vmname`. Por ejemplo, en el siguiente mandato, se restaura la máquina virtual y se especifica un nuevo nombre para la máquina virtual restaurada:


```
dsmc restore vm my_old_vmname -vmname=new_vm_name -datastore=myPath
```

4. Cuando se termine la restauración, la máquina virtual se apaga. Inicie la máquina virtual desde el vCenter de VMware.

 Sistemas operativos Windows

## Qué hacer a continuación






Si está restaurando copias de seguridad de protección de aplicaciones, consulte Consideraciones sobre la duplicación para la restauración de una copia de seguridad de protección de aplicaciones desde el transportador de datos.

-  Sistemas operativos Windows Consideraciones sobre la duplicación para la restauración de una copia de seguridad de protección de aplicaciones desde el transportador de datos  
Para máquinas virtuales (VM) Windows VMware, si intenta restaurar una copia de seguridad de protección de aplicaciones desde el transportador de datos, tenga en cuenta las restricciones de instantánea al restaurar la copia de seguridad de protección de aplicaciones.

### Tareas relacionadas:

Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup

### Referencia relacionada:

 Sistemas operativos Linux  Sistemas operativos Windows Query VM  
 Sistemas operativos Linux  Sistemas operativos Windows Restore VM  
INCLUDE.VMSNAPSHOTATTEMPTS  
 Sistemas operativos Windows

## Casos de ejemplo para ejecutar el acceso instantáneo de máquina virtual completa y restauración de máquina virtual instantánea completa desde la

## Línea de mandatos del cliente de archivado y copia de seguridad

---

Las operaciones de acceso instantáneo a la máquina virtual completa y restauración instantánea de la máquina virtual completa requieren una licencia para IBM Spectrum Protect for Virtual Environments. Puede llevar a cabo cualquiera de estas operaciones desde la línea de mandatos del cliente de archivado y copia de seguridad. Las operaciones y opciones de restauración instantánea y acceso instantáneo solo se admiten para máquinas virtuales VMware que estén alojadas en servidores VMware ESXi 5.1 o versiones posteriores.

Los siguientes casos de ejemplo demuestran las operaciones de acceso instantáneo a la máquina virtual completa o las operaciones de restauración de la máquina virtual completa que puede llevar a cabo. Antes de poder completar las operaciones que se describen en el siguiente texto, debe configurar al menos un nodo transportador de datos en el servidor de copia de seguridad vStorage para que pueda proteger las máquinas virtuales desde las operaciones de copia de seguridad y restauración de host. Los pasos para configurar los nodos del transportador de datos están descritos en Configuración de nodos del transportador de datos en un entorno de vSphere.

### Caso de ejemplo: desea realizar un acceso instantáneo a máquina virtual completo para verificar la integridad de una imagen de copia de seguridad de una máquina virtual VMware, sin restaurar la máquina virtual o los discos al host ESXi

---

La finalidad de este objetivo es verificar que una imagen de copia virtual puede utilizarse para restaurar correctamente un sistema si se suprime la máquina virtual o si sus discos y datos están dañados o no se pueden utilizar.

En este caso de ejemplo, suponemos que un servidor ESX tiene una máquina virtual llamada Orion ejecutándose. Desea verificar que la imagen de copia de seguridad almacenada por el servidor de IBM Spectrum Protect puede utilizarse para restaurar esta máquina virtual si falla la máquina virtual actual.

Para llevar a cabo una operación de acceso instantáneo a VM, utilice el mandato `restore vm` con las opciones de ubicación del inventario que se especifican para identificar la ubicación para la máquina virtual restaurada. Todas las opciones de ubicación, como `vmname`, `datacenter`, `host`, y `datastore` se han utilizado en combinación con la opción de acceso instantáneo (`-VMRESToretype=INSTANTAccess`) para especificar la ubicación para la máquina virtual (acceso instantáneo).

Ya que la máquina virtual Orion existe en el inventario y se está ejecutando, debe proporcionar un nombre nuevo para una máquina virtual temporal añadiendo el nombre nuevo a la opción `vmname`. También debe añadir la opción `-VMRESToretype=INSTANTAccess` a la línea de mandatos para indicar que se trata de una operación de restauración de acceso instantáneo.

Al introducir el siguiente mandato se prepara una máquina virtual denominada "Orion\_verify" para que esté disponible para el acceso instantáneo. Puede utilizar esta máquina virtual para verificar que la imagen de la que se ha realizado la copia de seguridad se puede restaurar.

```
dsmc restore vm Orion -vmname=Orion_verify -Host=esxi.example.com
-datacenter=mydataCenter -VMRESToretype=INSTANTAccess -VMAUTOSTARTvm=YES
```

La opción `-VMAUTOSTARTvm=YES` indica que la máquina virtual se inicia cuando se restaura. De forma predeterminada, la máquina virtual nueva no se inicia de forma automática. Con este valor predeterminado, puede volver a configurar la máquina virtual antes de iniciarla.

También puede listar las versiones de una máquina virtual de la que se realizó una copia de seguridad utilizando las opciones `inactive` o `pick` o las opciones `pittime` o `pitdate` para seleccionar una copia de seguridad activa o inactiva, desde una fecha u hora particular. Por ejemplo, para mostrar una lista de versiones de copia de seguridad de la máquina virtual Orion, utilice el siguiente mandato:

```
dsmc restore vm Orion -pick
```

Para una máquina virtual que se restaura mediante la opción `-VMRESToretype=INSTANTAccess`, los datos temporales que se crean mediante la máquina virtual se guardan en una instantánea de VMware.

Tras restaurar la máquina virtual temporal, (Orion\_verify), ejecute las herramientas de verificación para verificar la integridad del disco y de los datos. Utilice el programa de utilidad como `chkdsk`, o un programa de utilidad o aplicación que elija, para verificar los discos y los datos. Si la máquina virtual temporal pasa las comprobaciones de integridad, puede eliminar los recursos temporales que se crearon para dar soporte a la operación de restauración de acceso instantáneo.

### Caso de ejemplo: desea determinar si existen máquinas virtuales temporales (acceso instantáneo) para que pueda ejecutar una operación de limpieza para liberar los recursos asociados con ellos

---

Utilice el mandato `query vm` con una de las siguientes opciones que especifica en la línea de mandatos:

```
-VMRESToretype=INSTANTAccess  
-VMRESToretype=ALLtype
```

Donde:

```
-VMRESToretype=INSTANTAccess  
Muestra todas las máquinas virtuales que se están ejecutando en modalidad instantánea, creadas por una operación de restore  
vm -VMRESToretype=INSTANTAccess.  
-VMRESToretype=ALLtype  
Muestra todas las máquinas virtuales con sesiones de acceso instantáneo o restauración instantánea que se iniciaron mediante  
un mandato restore vm que utiliza bien las opciones de -VMRESToretype=INSTANTAccess o VMRESToretype=-  
INSTANTRestore.
```

Los siguientes ejemplos muestran la sintaxis para varias opciones:

```
query vm * -VMREST=INSTANTA  
query vm * -VMREST=ALL
```

Puede añadir una opción `-Detail` a cada uno de los mandatos `query vm` que se muestran para visualizar más información sobre cada una de las máquinas virtuales temporales.

```
query vm vmname -VMREST=INSTANTA -Detail
```

Para eliminar los recursos que se crearon para una máquina virtual temporal llamada "Orion\_verify", ejecute el siguiente mandato:

```
dsmc restore vm Orion -vmname=Orion_verify -VMRESToretype=VMCleanup
```

La opción `-VMRESToretype=VMCleanup` suprime la máquina virtual temporal del host ESXi, desmonta cualquier iSCSI que se montase y limpia la lista del dispositivo iSCSI desde el host de ESX. Todos los datos temporales para la máquina virtual se suprimen de la instantánea de VMware.

## Caso de ejemplo: desea iniciar una operación de restauración instantánea para restaurar una máquina virtual que ha fallado en un host de ESX a partir de una imagen de copia de seguridad creada por IBM Spectrum Protect

---

La ventaja de una restauración instantánea de máquina virtual completa, en oposición a la operación de restauración instantánea hace que la máquina virtual esté disponible para usarse inmediatamente tan pronto como se inicia. No tiene que esperar para que todos los datos se vuelvan a restaurar antes de poder utilizar la máquina virtual. Durante una operación de restauración instantánea, la máquina virtual utiliza los discos iSCSI hasta que los discos locales se restauran completamente. Cuando los discos locales se han restaurado, la máquina virtual cambia la E/S desde los discos iSCSI a los discos locales, sin una interrupción notable del servicio.

Restaurar una máquina virtual llamada Orion mediante el siguiente mandato:



```
dsmc restore vm Orion -Host=esxi.example.com -datacenter=mydatacenter  
-VMTEMPDatastore=temp_datastore -VMRESToretype=INSTANTRestore  
-datastore=mydatastore
```


Este mandato especifica el nombre de la máquina virtual que se va a restaurar, el host y el centro de datos en el que se va a restaurar y el tipo de restauración (`-VMRESToretype=INSTANTRestore`). La opción `VMTEMPDatastore` es un parámetro obligatorio para las operaciones de restauración instantáneas.

El almacén de datos temporales se utiliza mediante vMotion para guardar la configuración de la máquina virtual restaurada durante el proceso de restauración instantánea. El nombre que especifica debe ser único. No puede coincidir con el nombre de ningún almacén de datos original guardado la máquina virtual hubiera utilizado cuando se realizó la copia de seguridad de la misma y no puede ser el mismo que se especifica como nombre en la opción `-datastore`. Si la opción `-datastore` se omite, los archivos de la máquina virtual se restauran a los almacenes de datos que se utilizan cuando se realizó la copia de seguridad de la máquina virtual.

De forma predeterminada, las máquinas virtuales que se restauran de forma instantánea se equipan con discos gruesos. Puede cambiar este comportamiento de discos de suministro ligero añadiendo la opción `-VMDISKProvision=THIN` a la línea de mandatos o en el archivo de opciones del cliente.


Importante: Para las operaciones de restauración instantáneas, asegúrese de que tanto el almacén de datos temporal que especifique con la opción `vmtempdatastore` como el almacén de datos de VMware que especifique mediante la opción `datastore` en el mandato `restore VM` tengan suficiente almacenamiento libre para guardar la máquina virtual que está restaurando, y el archivo de instantáneas que contiene cambios realizados a los datos. Si va a restaurar una máquina virtual y especifica un suministro ligero o grueso (`-vmdiskprovision=thin` o `-vmdiskprovision=thick`), el almacén de datos en el que restaure la máquina virtual debe tener suficiente espacio libre para acomodar la capacidad total del disco de la máquina virtual y no únicamente la cantidad de disco que se utiliza. Por ejemplo, si una máquina virtual tiene 300 GB de capacidad total para el disco, no puede restaurar esa máquina virtual a un almacén de datos que tenga menos de 300 GB disponibles, incluso si solo se utiliza una porción de la capacidad total.

-  Sistemas operativos Windows Casos de ejemplo de limpieza y reparación instantánea de VM completa  
Cuando una operación de restauración instantánea falla después de que se encienda la máquina virtual, se necesita realizar la limpieza y las tareas de reparación manuales.
-  Sistemas operativos Windows Recuperación de condiciones de error no estándar  
Los problemas con dispositivos iSCSI pueden impedir que realice una operación de restauración instantánea o un acceso instantáneo.

 Sistemas operativos Windows

## Casos de ejemplo de limpieza y reparación instantánea de VM completa

Cuando una operación de restauración instantánea falla después de que se encienda la máquina virtual, se necesita realizar la limpieza y las tareas de reparación manuales.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Cuando una operación de restauración instantánea falla con almacenamiento vMotion en ejecución, se crea alguna de las siguientes situaciones:

- La operación de restauración instantánea genera un mensaje de error.
- La operación de restauración instantánea se suspende de forma indefinida y la máquina virtual no responde.

Para determinar la causa del problema, puede realizar una consulta detallada de la máquina virtual utilizando el siguiente mandato:

```
dsmc q vm * -vmrestoretype=instantrestore -detail
```

En la salida que produce este mandato, en cada máquina virtual de la salida, busque la línea que contenga `Action Needed`. Utilice los siguientes párrafos `Action Needed` para recuperarse de la operación de restauración instantánea fallida, dependiendo del estado de `Action Needed`.

### Action Needed: Cleanup

En la salida del mandato `query vm * -vmrestoretype=instantrestore -detail command`, verifique que el estado de vMotion de almacenamiento es correcto (`vMotion Status: Successful`) y que todos los discos de máquina virtual son discos físicos (`Disk Type: Physical`). Este estado confirma que la máquina virtual se ha restaurado y que se necesita limpiar los componentes huérfanos, como los montajes iSCSI.

Este tipo de anomalía sucede debido a alguna de las siguientes situaciones:

- La restauración instantánea ha fallado y se está ejecutando Storage vMotion. VMware vSphere sigue el proceso de vMotion.
- Storage vMotion ha terminado correctamente, pero la limpieza automática del montaje iSCSI falla.

Para realizar la limpieza de los componentes huérfanos, ejecute el mandato `restore vm` con el parámetro `-VMRESToretype=VMCleanup`. Por ejemplo:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCleanup
```

### Acción necesaria: Reparación

En la salida del mandato `query vm * -vmrestoretype=instantrestore -detail`, verifique que el dispositivo iSCSI que se adjunta a la máquina virtual ha fallado (el estado es `Disk Path: Dead`).

Este tipo de anomalía sucede debido a alguna de las tres situaciones siguientes:

- La máquina virtual que se utiliza como transportador de datos o la máquina del transportador de datos física ha fallado.
- Se ha producido un error de red entre el transportador de datos y el host de ESX o el transportador de datos y el servidor de IBM Spectrum Protect.
- La protección para VMware Recovery Agent Service ha fallado.

El dispositivo iSCSI debe devolverse a un estado activo antes de que se intente otra operación instantánea.

Para intentar realizar una recuperación de un error de transportador de datos, siga estos pasos:

1. Investigue la causa del error y reinicie la máquina del transportador de datos si no se inicia automáticamente. Esta acción inicia una recuperación automática de los discos iSCSI montados.
2. En la salida del mandato `query vm * -vmrestoretype=instantrestore -detail`, verifique los discos de máquina virtual están activos (`Disk Path: Active`). Este estado significa que la máquina virtual se ha restaurado y está disponible para

utilizarse.

3. Reinicie vMotion de almacenamiento en el cliente de vSphere y supervise su progreso en la barra de estado del cliente de vSphere.
4. Si el almacenamiento del procesamiento de vMotion se ha completado correctamente, ejecute el mandato `restore vm` con el parámetro `-vmrestoretype=VMCLleanup` para limpiar los discos iSCSI. Por ejemplo:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCLleanup
```

Para intentar realizar la recuperación después de un error de red, siga estos pasos:

1. Repare el problema de red para que la comunicación entre el transportador de datos y el host de ESX, y el transportador de datos y los servidores de IBM Spectrum Protect se reanude.
2. En la salida del mandato `query vm * -vmrestoretype=instantrestore -detail`, verifique los discos de máquina virtual están activos (`Disk Path: Active`). Este estado significa que la máquina virtual se ha restaurado y está disponible para utilizarse.
3. Si el error de red no hizo que vMotion de almacenamiento agotase el tiempo de espera, no es necesario realizar ninguna acción.
4. Si la red falla porque el almacenamiento de vMotion ha superado el tiempo de espera y el mensaje de error indica que el disco de origen no responde, reinicie el almacenamiento de vMotion en el cliente de vSphere. Cuando termina el procesamiento del almacenamiento vMotion, ejecute el mandato `restore vm` con el parámetro `-vmrestoretype=VMCLleanup` para limpiar los discos iSCSI. Por ejemplo:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCLleanup
```

Para intentar realizar una recuperación después del error en el servicio de Data Protection for VMware Recovery Agent, siga estos pasos:

1. Investigue la causa del error y reinicie el servicio de Data Protection for VMware Recovery Agent si no se inicia automáticamente. Esta acción inicia una recuperación automática de los discos iSCSI montados.
2. En la salida del mandato `query vm * -vmrestoretype=instantrestore -detail`, verifique los discos de máquina virtual están activos (`Disk Path: Active`). Este estado significa que la máquina virtual se ha restaurado y está disponible para utilizarse.
3. Si el error del servicio de Data Protection for VMware Recovery Agent no hizo que el almacenamiento de vMotion superase el tiempo de espera, no se requiere ninguna acción.
4. Si el error en el servicio de Data Protection for VMware Recovery Agent provocó que se agotase el tiempo de espera de vMotion, y el mensaje de error indica que el disco de origen no está respondiendo, reinicie el almacenamiento de vMotion en el cliente de vSphere. Cuando termina el procesamiento del almacenamiento vMotion, ejecute el mandato `restore vm` con el parámetro `-vmrestoretype=VMCLleanup` para limpiar los discos iSCSI. Por ejemplo:


```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMCLleanup
```

## Eliminación completa

Si no se puede recuperar de un error y desea eliminar la máquina virtual y sus componentes, ejecute `restore vm` con el parámetro `-vmrestoretype=VMFULLCleanup`. Por ejemplo:

```
dsmc restore vm original_vmname -vmname=new_vm_name -VMRESToretype=VMFULLCleanup
```

Una operación de `VMFULLCleanup` fuerza la eliminación de la máquina virtual y de todos sus componentes, sin tener en cuenta el estado de la máquina virtual. No inicie una operación de limpieza completa mientras que vMotion sigue migrando una máquina virtual.


 Sistemas operativos Windows

## Recuperación de condiciones de error no estándar

Los problemas con dispositivos iSCSI pueden impedir que realice una operación de restauración instantánea o un acceso instantáneo.

### Acerca de esta tarea

Cuando un servidor ESX no puede acceder a un almacén de datos en un disco iSCSI, se emite un mensaje de VMware para indicar que se ha producido un error de "pérdida de dispositivo permanente". El sistema debe ofrecerle una opción para cancelar o reintentar la conexión de iSCSI. Elija la opción de volver a intentar la operación para ver si se trata de un error transitorio y si se puede efectuar la recuperación. Si el reintento no es satisfactorio, pruebe los siguientes pasos de resolución de problemas. Si son satisfactorios, a continuación, intente la operación de acceso instantáneo o de restauración instantánea de nuevo.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

## Procedimiento

---

1. Examine el registro de tareas y sucesos del servidor ESX para ver si hay un error APD (All Paths Down). Es posible que la visualización de este error en los registros se prolongue un poco, pero debe estar presente antes de que el usuario prosiga con los pasos siguientes. Si no espera a que aparezca el error antes de intentar aplicar las soluciones de problemas, es posible que haga que se cuelgue el servidor ESX.
2. Apague la máquina virtual.
3. Vuelva a explorar el adaptador de bus de host (HBA). Es posible que una nueva exploración del HBA en el servidor ESX reactive el dispositivo fallido. Si los bloqueos del kernel de VMware impiden que vuelva a explorar el HBA, efectúe los siguientes pasos:
  - a. En la interfaz de vCenter, seleccione el host de ESX.
  - b. Haga clic en Configuración.
  - c. Pulse con el botón derecho del ratón sobre Adaptador de software iSCSI y seleccione Propiedades.
  - d. Pulse Descubrimiento estático.
  - e. Suprima todas las direcciones estáticas y pulse Cerrar.
  - f. Vuelva a explorar el adaptador de bus de host (HBA).



Sistemas operativos Windows

## Escenario: Restauración de copias de seguridad de máquina virtual completas


---

En sistemas Microsoft Windows, puede restaurar archivos específicos a partir de una copia de seguridad a nivel de archivos de una máquina virtual VMware. Las restauraciones a nivel de archivos son útiles para restaurar archivos individuales que pudieran perderse o dañarse. No puede utilizar este método para restaurar archivos que formasen parte de una copia de seguridad de VM completa. Antes de restaurar archivos desde un servidor de seguridad fuera de host en la máquina virtual VMware, dicho servidor se debe configurar como servidor proxy.

### Antes de empezar

---

Las operaciones de copia de seguridad a nivel de archivo se han creado con clientes de copia de seguridad y archivado de la versión 7.1 o anterior.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Importante: Utilice el mandato restore para ejecutar una restauración a nivel de archivos. No utilice el mandato restore vm. En este escenario de restauración a nivel de archivos se tienen en cuenta las siguientes suposiciones:

- El objetivo es restaurar archivos copiados previamente por el servidor de IBM Spectrum Protect.
- Los archivos se copiaron previamente de una máquina virtual VMware llamada Orion, cuyo nombre de host es orion. En este escenario, la máquina Virtual Orion falla y se deben restaurar algunos de sus archivos.
- Los archivos de Orion se copian en espacios de archivos que coinciden con la forma en minúsculas del nombre de host del sistema. Los nombres del espacio de archivos se expresan en formato de convenio de nomenclatura universal (UNC), por ejemplo:
  - Los archivos copiados desde la unidad C: de Orion, se almacenan en el espacio de archivos \\orion\c\$.
  - Si Orion tiene una unidad D:, los archivos copiados desde esta unidad se almacenan en el espacio de archivos \\orion\d\$.
- En este escenario, los archivos se restauran desde el directorio C:\mydocs de Orion al directorio C:\restore\_temp de un sistema diferente. El sistema en el que restaura el archivo puede ser otra máquina virtual VMware o un sistema físico.
- El sistema que ejecuta la restauración tiene un nombre de host y nombre de nodo diferente a la máquina virtual Orion. Durante la restauración, debe especificar la especificación de archivo origen en el formato UNC completo y utilizar uno de los siguientes parámetros para acceder a Orion:

-virtualnodename

Especifica el nodo cliente para el que está restaurando la copia de seguridad. Utilice este parámetro si está restaurando archivos en un sistema en el que ha iniciado sesión.

-asnodename

Especifica el nodo cliente para el que está restaurando la copia de seguridad. Utilice este parámetro si está restaurando archivos en un sistema para el que tiene autoridad de proxy.

Complete los pasos indicados a continuación para ejecutar una restauración a nivel de archivos del sistema Orion:

## Procedimiento

---



1. Consulte al servidor de IBM Spectrum Protect para determinar los espacios de archivos registrados para Orion:

```
dsmc query filespace -virtualnode=orion
```

2. Restaure los archivos del espacio de archivos de Orion ejecutando uno de los siguientes mandatos:

Restaure los archivos en el sistema en el que ha iniciado sesión actualmente:

Imagine que actualmente ha iniciado sesión en el sistema denominado Orion. Ejecute uno de los siguientes mandatos:

- a. Si sabe la contraseña del nodo que está restaurando, utilice la opción `-virtualnodename` en el mandato de restauración. Por ejemplo, ejecute el siguiente mandato para restaurar los archivos en Orion:

```
dsmc restore \\orion\c$\mydocs\ c:\restore_temp\ -sub=yes
-virtualnodename=orion
```

- b. Si tiene autoridad proxy, puede restaurar archivos en nombre del nodo de destino. La autoridad proxy se debe otorgar desde el nodo de agente, es decir, el nodo del sistema desde el que se ejecuta la restauración. Para poder acceder al nodo de destino debe saber la contraseña del nodo de agente. Por ejemplo, ejecute el siguiente mandato para restaurar los archivos en Orion:

```
dsmc restore \\orion\c$\mydocs\ c:\restore_temp\ -sub=yes
-asnodename=orion
```

Tabla 1. Componentes del mandato restore al restaurar archivos en el mismo sistema

Componente de mandato	Descripción
\\orion\c\$\mydocs\	Especificación de archivo de origen del servidor de IBM Spectrum Protect. Esta ubicación contiene la copia de seguridad de los archivos que está restaurando. La copia de seguridad se realiza de los archivos de la máquina virtual <code>orion</code> , por lo que la especificación de archivo debe estar en formato UNC.
c:\restore_temp\	Especificación del archivo de destino del sistema en el que ha iniciado sesión actualmente. Los archivos se restauran en esta ubicación.
-sub=yes	Especifica que todos los subdirectorios de la especificación de archivo de origen se deben incluir al ejecutar la operación de restauración.
-virtualnodename=orion	Notifica el servidor de IBM Spectrum Protect que está ejecutando la copia de seguridad desde el nodo <code>orion</code> .
-asnodename=orion	Notifica el servidor de IBM Spectrum Protect que está ejecutando la copia de seguridad desde el nodo <code>orion</code> .

Restauración de archivos en un sistema diferente:

Para restaurar archivos desde el servidor de IBM Spectrum Protect en un sistema distinto al sistema en el que ha iniciado sesión, ejecute el mandato indicado a continuación. Puede utilizar este mandato solo si ha iniciado sesión con autoridad para escribir en el sistema remoto controlado por el sistema operativo.

```
dsmc restore \\orion\c$\mydocs\ \\orion\c$\restore_temp\ -sub=yes
-virtualnode=orion
```

Tabla 2. Componentes del mandato restore al restaurar archivos en un sistema diferente

Componente de mandato	Descripción
\\orion\c\$\mydocs\	Identifica la especificación de archivo de origen en el servidor IBM Spectrum Protect. Esta ubicación contiene la copia de seguridad de los archivos que está restaurando. La copia de seguridad se realiza de los archivos de la máquina virtual <code>orion</code> , por lo que la especificación de archivo debe estar en formato UNC.
\\orion\c\$\restore_temp\	Identifica la especificación del archivo de destino del sistema en el que ha iniciado sesión. Está restaurando archivos en la máquina virtual <code>orion</code> en la red utilizando una característica Microsoft que identifica las ubicaciones de red en notación UNC.
-sub=yes	Especifica que todos los subdirectorios de la especificación de archivo de origen se deben incluir al ejecutar la operación de restauración.

Componente de mandato	Descripción
- virtual nodename=orion	Notifica el servidor de IBM Spectrum Protect que está ejecutando la copia de seguridad desde el nodo orion.

**Conceptos relacionados:**








Restauración de datos desde la copia de seguridad de VMware

**Tareas relacionadas:**

Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup

Restauración de copias de seguridad de máquina virtual completas

**Referencia relacionada:**


-  Sistemas operativos Linux
-  Sistemas operativos Windows
-  Query Filespace
-  Sistemas operativos Linux
-  Sistemas operativos Windows
-  Restore
-  Sistemas operativos Windows

## Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup

Puede restaurar una copia de seguridad VMware completa para volver a crear todos los archivos de la máquina virtual VMware. Siga estos pasos para restaurar las copias de seguridad de VM completas que se crearon mediante la utilización de VMware Consolidated Backup (VCB) que se ejecuta en IBM Spectrum Protect versión 6.2.0 o anterior.

### Antes de empezar

Para restaurar una copia de seguridad VMware completa creada utilizando IBM Spectrum Protect Versión 6.2.2 o posterior, consulte el tema "Restauración de copias de seguridad de máquina virtual completas".

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

### Procedimiento

1. Dependiendo de la ubicación de destino de la restauración, complete los pasos adecuados:
  - Si la restauración de la copia de seguridad de máquina virtual completa va a sobrescribir la máquina virtual VMware existente, suprima dicha máquina virtual.
  - Si restaura la copia de seguridad de máquina virtual completa en una nueva máquina virtual, no necesita suprimir la máquina virtual existente. Puede suprimir la máquina virtual existente o proceder al siguiente paso.
2. Consulte a la máquina virtual acerca de las copias de seguridad de VMware completas siguiendo los pasos indicados a continuación:
  - a. En el servidor de copia de seguridad fuera de host, ejecute el siguiente mandato:

```
dsmc q vm *
```

El mandato muestra las copias de seguridad disponibles, por ejemplo:

```

Núm Fecha copia seg Clase gest Tipo A/I Máquina virtual
-----
1 12/03/2009 03:05:03 DEFAULT VMFULL A vm_guest1
2 09/02/2010 10:45:09 DEFAULT VMFULL A vm_guest11
3 09/02/2010 09:34:40 DEFAULT VMFULL A vm_guest12
4 09/02/2010 10:10:10 DEFAULT VMFULL A vm_guest13
5 12/04/2009 20:39:35 DEFAULT VMFULL A vm_guest14
6 09/02/2010 11:15:18 DEFAULT VMFULL A vm_guest15
7 09/02/2010 02:52:44 DEFAULT VMFULL A vm_guest16
8 08/05/2010 04:28:03 DEFAULT VMFULL A vm_guest17
9 08/05/2010 05:20:27 DEFAULT VMFULL A vm_guest18
10 08/12/2010 04:06:13 DEFAULT VMFULL A vm_guest19
11 09/02/2010 00:47:01 DEFAULT VMFULL A vm_guest7
12 09/02/2010 01:59:02 DEFAULT VMFULL A vm_guest8
13 09/02/2010 05:20:42 DEFAULT VMFULL A vm_guest9

```

El código de retorno de ANS1900I es 0.

El código de retorno más alto de ANS1901I fue 0.

- b. En los resultados devueltos por el mandato de consulta, identifique la máquina virtual que desea restaurar.

3. Restaure la copia de seguridad de VMware completa utilizando el mandato `restore vm`. Para restaurar una máquina virtual desde un determinado punto en el tiempo, incluya las opciones `-pitdate` y `-pittime`. por ejemplo:

```
dsmc restore vm my_vm_name destination -pitdate=date -pittime=hh:mm:ss
```

Donde:

*my\_vm\_name*

Nombre de la máquina virtual que va a restaurar.

*destino*

Ubicación del directorio del archivo vmdk restaurado.

*-pitdate*

La fecha en que se creó la copia de seguridad.

*-pittime*

La hora en que se creó la copia de seguridad.

4. Al completarse la restauración, se devolverá el siguiente mensaje. Especifique `Y`.

```
Las herramientas Virtual Infrastructure Client o VMware Converter se pueden utilizar para redefinir la máquina virtual al inventario de VMware Virtual Center.
```

```
¿Desea iniciar el Convertidor de VMware ahora? (Sí (Y)/No (N))
```






Consejo: Si especifica `N`, la línea de mandatos realizará una devolución sin abrir VMware Converter. No obstante, debe convertir la imagen antes de que esta se pueda restaurar.

5. Para convertir la imagen VCB en una imagen virtual en un servidor VMware utilizando la herramienta VMware vCenter Converter, complete los pasos siguientes:
  - a. En el menú Inicio de Windows, abra la herramienta Converter.
  - b. Desde la herramienta Convertidor, pulse en Máquina de Convertidor.
  - c. En el campo Archivo de máquina virtual, especifique la ubicación donde se ha restaurado el archivo `.vmx`.  
Consejo: El archivo `.vmx` se ha restaurado en el directorio especificado por la opción `vmbackdir` del mandato `restore vm`.
  - d. Siga el resto de los pasos del asistente para convertir la copia de seguridad de la máquina virtual completa.
6. Cuando se termine la restauración, la máquina virtual se apaga. Inicie la máquina virtual desde el vCenter de VMware.

#### Tareas relacionadas:

Restauración de copias de seguridad de máquina virtual completas






#### Referencia relacionada:

-  Sistemas operativos Linux
-  Sistemas operativos WindowsQuery VM
-  Sistemas operativos Linux
-  Sistemas operativos WindowsRestore VM
-  Sistemas operativos Windows

## Restaurar objetos individuales de Active Directory en Windows

Puede restaurar objetos individuales de Active Directory para realizar la recuperación después de la supresión o daños accidentales de objetos de Active Directory sin que requieran la conclusión o el reinicio del servidor de Active Directory.

En el cliente Windows Server, utilice el mandato `restore adobjects` para restaurar objetos locales suprimidos de Active Directory (objetos tombstone). También puede restaurar objetos individuales de Active Directory desde las copias de seguridad del estado del sistema en el servidor de IBM Spectrum Protect.

-  Sistemas operativos WindowsReanimar objetos tombstone o restaurar desde la copia de seguridad de estado del sistema  
La reanimación tombstone es un proceso para restaurar un objeto que ha sido eliminado desde el Active Directory. Cuando se suprime un objeto de Active Directory, no se borra físicamente de la base de datos; sólo se marca como suprimido. Entonces, es posible reanimar (restaurar) el objeto.
-  Sistemas operativos WindowsRestauración de objetos de Active Directory mediante la GUI y la línea de mandatos  
Para restaurar los objetos de Active Directory individuales, debe ejecutar el cliente de copia de seguridad y archivado en un controlador de dominio y la cuenta de usuario debe ser un miembro del grupo de administradores. Los objetos de Active Directory no se visualizan en el árbol de directorios si su cuenta de usuario no es miembro del grupo de administradores.
-  Sistemas operativos WindowsRestricciones y limitaciones al restaurar objetos de Active Directory  
Hay restricciones y limitaciones que deberá tener en cuenta al restaurar los objetos de Active Directory.
-  Sistemas operativos WindowsConservación de atributos en objetos tombstone  
Para especificar un atributo para conservarlo en el objeto tombstone, localice en primer lugar este atributo en el esquema de Active Directory y después actualice el atributo `searchFlags` del objeto del esquema.
-  Sistemas operativos WindowsModificación del aceptador de cliente y servicios de agente para utilizar el cliente web  
No puede restaurar objetos individuales de Active Directory utilizando el cliente web de forma predeterminada. Los servicios del

cliente web (agente y aceptador de cliente) se ejecutan en la cuenta del sistema local de forma predeterminada. Esta cuenta no tiene suficientes privilegios para restaurar objetos de Active Directory.

**Tareas relacionadas:**

Restauración del estado del sistema de Windows

**Referencia relacionada:**

Restore Adobjects

 Sistemas operativos Windows

## Reanimar objetos tombstone o restaurar desde la copia de seguridad de estado del sistema

---

La reanimación tombstone es un proceso para restaurar un objeto que ha sido eliminado desde el Active Directory. Cuando se suprime un objeto de Active Directory, no se borra físicamente de la base de datos; sólo se marca como suprimido. Entonces, es posible reanimar (restaurar) el objeto.

Cuando se reanima un objeto, no se conservan todos los atributos de los objetos. Cuando un objeto se convierte en un objeto tombstone, se extraen muchos atributos del mismo automáticamente, y estos atributos extraídos se pierden de forma permanente. No obstante, es posible cambiar el esquema de Active Directory para que tenga más atributos conservados después de la supresión de objetos.

En los objetos tombstone, tampoco se conservan los enlaces entre usuarios y grupos. Por ejemplo, después de la reanimación de un objeto de usuario, la cuenta de usuario no pertenecerá a ningún grupo. Toda esta información debe crearla manualmente de nuevo el administrador de Active Directory.

Cuando un objeto de Active Directory se restaura desde una copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect, prácticamente se restauran todos sus atributos y su pertenencia como miembro del grupo. Esta es la mejor opción de restauración en el controlador de dominio de Windows Server. Cuando se restaura un objeto desde el servidor:

- La base de datos de Active Directory se extrae de una copia de seguridad de estado del sistema y se restaura en una ubicación temporal.
- La base de datos restaurada se abre.
- Seleccione los objetos que desea restaurar. Para cada objeto:
  - Se realiza una búsqueda del objeto tombstone coincidente. Para buscar el objeto tombstone, se utiliza el GUID (Globally Unique Identifier).
  - Si se encuentra el objeto tombstone coincidente, se reanima. En este caso, el objeto restaurado conserva su GUID (Globally Unique Identifier) y su SID (Security Identifier) originales.
  - Si no se encuentra el objeto tombstone coincidente, se crea un objeto nuevo en la base de datos. En este caso, el objeto nuevo tiene un GUID y un SID nuevos diferentes del objeto original.
- Los atributos que faltan se copian de la copia de seguridad al objeto reanimado o creado de nuevo. Los atributos existentes que se han modificado desde que se realizó la copia de seguridad se actualizan para que coincidan con el valor de la copia de seguridad. Los atributos nuevos que se han agregado desde que se realizó la copia de seguridad se suprimen.
- Se restaura la pertenencia a miembros del grupo.

Aunque todos los atributos se pueden establecer de forma programada y se vuelven a crear los enlaces de grupo, es posible que los objetos restaurados no estén inmediatamente disponibles después de la restauración. Es posible que un administrador de Active Directory tenga que actualizar manualmente los objetos restaurados para que estén disponibles. Asegúrese de leer Restricciones y limitaciones al restaurar objetos de Active Directory antes de realizar la restauración.

**Conceptos relacionados:**

Conservación de atributos en objetos tombstone

Restauración de los datos

Restricciones y limitaciones al restaurar objetos de Active Directory

**Tareas relacionadas:**

Restauración del estado del sistema de Windows

**Referencia relacionada:**

Restore Adobjects

 Sistemas operativos Windows

## Restauración de objetos de Active Directory mediante la GUI y la línea de mandatos

---

Para restaurar los objetos de Active Directory individuales, debe ejecutar el cliente de copia de seguridad y archivado en un controlador de dominio y la cuenta de usuario debe ser un miembro del grupo de administradores. Los objetos de Active Directory no se visualizan en el árbol de directorios si su cuenta de usuario no es miembro del grupo de administradores.

Puede restaurar objetos de directorio activo u objetos tombstone mediante la GUI o la línea de mandatos.

Para restaurar objetos individuales desde la GUI:

1. Pulse en Restaurar en la ventana IBM Spectrum Protect. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios si es preciso. Para expandir un objeto del árbol, pulse en el signo más (+) que se encuentra junto al objeto.
3. Localice el nodo de Active Directory en el árbol de directorios. Expándaolo para ver Objetos locales suprimidos. El objeto del servidor también está disponible.
  - Para restaurar objetos tombstone, expanda Objetos locales suprimidos, desplácese hasta los objetos tombstone que desea restaurar y selecciónelos.
  - Para restaurar los objetos de Active Directory de los que se ha realizado una copia de seguridad al servidor de IBM Spectrum Protect:
    - a. Expanda el objeto Servidor. Aparecerá una ventana de diálogo que mostrará una lista de copias de seguridad de estado del sistema (con diferentes indicaciones de hora) en el servidor.
    - b. Seleccione una copia de seguridad del estado del sistema en la lista. La base de datos de Active Directory de ese estado del sistema se restaurará como proceso en segundo plano y el árbol se llenará con objetos de Active Directory.
    - c. Navegue hasta los objetos de Active Directory que desee restaurar y selecciónelos.

Consejo: Si desea ver los atributos para un objeto de Active Directory, siga expandiendo cada objeto de Active Directory del árbol hasta que llegue al que desea. Los atributos para un objeto se muestran en el área de visualización que se encuentra junto al árbol. Puede buscar o filtrar el árbol para ver un objeto de Active Directory en función de su nombre.
4. Pulse en Restaurar para iniciar la operación de restauración. Se abre la ventana Lista de tareas y muestra el progreso de la operación de restauración.

En la línea de mandatos, utilice el mandato query adobjects para consultar y el mandato restore adobjects para restaurar objetos individuales de Active Directory.

#### Referencia relacionada:

Query Adobjects

Restore Adobjects

 Sistemas operativos Windows

## Restricciones y limitaciones al restaurar objetos de Active Directory

Hay restricciones y limitaciones que deberá tener en cuenta al restaurar los objetos de Active Directory.

Antes de restaurar objetos, debe comprender las siguientes restricciones y limitaciones:

- No restaure Active Directory como parte de una operación de restauración del estado del sistema, a menos que tenga previsto utilizarlo en operaciones de restauración a nivel de recuperación ante siniestro de todo Active Directory. Este tipo de operación de restauración requiere que el servidor de Active Directory se detenga y se vuelva a iniciar.
- No puede realizar una restauración a instante específico de objetos tombstone. Puede llevar a cabo una restauración a un instante específico de objetos de Active Directory de los que ha realizado copia de seguridad en el servidor.
- No puede restaurar objetos de Active Directory de juegos de copias de seguridad.

Antes de restaurar objetos, debe comprender las siguientes limitaciones:

- La restauración de objetos de Active Directory del servidor de IBM Spectrum Protect requiere espacio temporal en la unidad de disco duro local. Puede utilizar la opción stagingdirectory para especificar un directorio del disco duro local para almacenar datos temporales del servidor. Dependiendo del tamaño de los datos temporales, el ancho de banda de la red, y tanto del rendimiento óptimo del cliente como del servidor, esta operación puede tardar desde 20 segundos hasta más de una hora en completarse. Es posible que se produzca un retardo al renovar la ventana Restaurar cuando se visualiza el árbol de Active Directory.
- Las contraseñas de usuario no se pueden restaurar de forma predeterminada. Un objeto de usuario restaurado está inhabilitado hasta que el administrador restaura la contraseña y vuelve a habilitar la cuenta. Del mismo modo, si se ha suprimido la cuenta de un sistema del dominio y luego se restaura mediante el cliente de copia de seguridad y archivado, se debe vincular manualmente al dominio después de la restauración. De lo contrario, los usuarios del sistema de destino no pueden iniciar una sesión en el dominio.

Para que un objeto de sistema o usuario esté totalmente operativo después de una restauración, debe modificar los atributos del esquema *Unicode-Pwd* como se describe en **Conservación de atributos en objetos tombstone**.

- El esquema de Active Directory no se vuelve a crear durante la restauración del objeto de Active Directory. Si el esquema se ha modificado después de la copia de seguridad, es posible que el objeto restaurado haya dejado de ser compatible con el nuevo esquema y que algunos atributos del objeto de Active Directory hayan dejado de ser válidos. El cliente emite un mensaje de aviso si alguno no se ha podido restaurar.
- No se pueden restaurar los GPO (Group Policy Objects) y sus enlaces con las unidades organizativas (OU).
- No se restauran las políticas locales para los objetos de Active Directory.
- Cuando restaura un objeto desde el servidor de IBM Spectrum Protect, si el objeto de destino ya existe en Active Directory y lo sustituye por su versión de copia de seguridad, el objeto no se suprime ni se vuelve a crear. Se utiliza el objeto existente como base y la versión de copia de seguridad sobrescribe sus atributos. Algunos atributos como, por ejemplo, el GUID y el SID permanecen en el objeto existente y la versión de copia de seguridad no los sobrescribe.
- Si hay varios objetos tombstone para el mismo contenedor, vuelva a reanimarlos desde la línea de mandatos del cliente de copia de seguridad y archivado mediante el GUID de objeto, en cuyo caso el cliente de línea de mandatos sólo vuelve a reanimar el objeto del contenedor y no a sus hijos. En la GUI del cliente de copia de seguridad y archivado, se puede seleccionar todo el contenedor para reanimarlo.
- Cuando restaure un objeto desde el servidor de IBM Spectrum Protect, si el objeto de Active Directory activo existe y tiene activado el bit que *impide su supresión*, el cliente podrá modificar los atributos del objeto activo. No obstante, si hay un objeto tombstone del mismo nombre pero un GUID de objeto diferente, los Servicios de Directorios devuelven el error de *acceso denegado*.
- Cuando restaura un objeto desde el servidor de IBM Spectrum Protect y se ha cambiado el nombre del contenedor del objeto, el cliente vuelve a crear el contenedor utilizando el nombre original en el momento de la copia de seguridad. En la restauración de un objeto tombstone, el cliente lo restaura en el contenedor con el nombre nuevo, ya que el atributo *lastKnownParent* del objeto tombstone se ha actualizado para que refleje el nuevo nombre del contenedor.

**Conceptos relacionados:**


Conservación de atributos en objetos tombstone

Restauración de los datos

**Referencia relacionada:**

Restore Adobjects

Stagingdirectory

 Sistemas operativos Windows

## Conservación de atributos en objetos tombstone

---

Para especificar un atributo para conservarlo en el objeto tombstone, localice en primer lugar este atributo en el esquema de Active Directory y después actualice el atributo *searchFlags* del objeto del esquema.

Hay un software adquirido por el proveedor (por ejemplo, ADSI Edit) que le permite actualizar el atributo *searchFlags* del objeto del esquema.

Generalmente, ninguno de los bits de la máscara de bits *searchFlags* está establecido (el valor es 0). Establezca *searchFlags* en 8 (0x00000008) si desea que Active Directory guarde el atributo concreto en el objeto tombstone cuando se suprima el objeto original.

**Conceptos relacionados:**

Restauración de los datos

**Referencia relacionada:**

Restore Adobjects

 Sistemas operativos Windows

## Modificación del aceptador de cliente y servicios de agente para utilizar el cliente web

---

No puede restaurar objetos individuales de Active Directory utilizando el cliente web de forma predeterminada. Los servicios del cliente web (agente y aceptador de cliente) se ejecutan en la cuenta del sistema local de forma predeterminada. Esta cuenta no tiene suficientes privilegios para restaurar objetos de Active Directory.

Para habilitar esta operación de restauración en el cliente web, realice estos pasos:

1. Modifique el aceptador de cliente y los servicios de agente de modo que utilicen una cuenta administrativa como, por ejemplo, *Administrador* cuando inicie la sesión en Windows.
2. Puede editar las propiedades del aceptador de cliente y los servicios de agente (normalmente denominados TSM Client Acceptor y TSM Remote Client Agent) en el Panel de control.
3. Modifique el aceptador de cliente y los servicios de agente en la página Opciones de inicio de sesión del asistente de configuración de IBM Spectrum Protect cuando configure el cliente web

Si el cliente web ya está configurado, siga estos pasos:

1. Pulse Iniciar.
2. Pulse Panel de control → Herramientas administrativas → Servicios.
3. Seleccione el servicio del planificador en la lista de servicios Windows.
4. Pulse el separador Iniciar la sesión.
5. Pulse Esta cuenta en la sección Iniciar sesión como.
6. Especifique una cuenta administrativa o pulse Examinar para localizar la cuenta de dominio.
7. Especifique la contraseña para la cuenta de dominio.
8. Pulse Aceptar y, a continuación, pulse Iniciar.

**Referencia relacionada:**

Restore Adobjects

## Restaurar o recuperar datos durante una migración tras error

---

Cuando el cliente se migra a servidor secundario, puede restaurar o recuperar los datos replicados desde servidor secundario.

### Antes de empezar

---

Antes de empezar a restaurar o recuperar los datos durante una operación de migración tras error:

- Asegúrese de que el cliente está configurado para la migración tras error automática.
- Asegúrese de estar conectado a un servidor de IBM Spectrum Protect que replique los nodos de cliente. Para obtener más información sobre los requisitos de la migración tras error, consulte Requisitos para la migración tras error automática del cliente.

Restricción: En la modalidad de migración tras error, no puede realizar la copia de seguridad o archivar los datos en servidor secundario.

### Procedimiento

---

Para restaurar o recuperar los datos durante una migración tras error, siga estos pasos:





1. Compruebe el estado de réplica de los datos del cliente de servidor secundario. El estado de réplica indica si la copia de seguridad más reciente se ha replicado en el servidor secundario.
2. Restaure o recupere los datos como lo haría normalmente desde la GUI del cliente o desde la interfaz de línea de mandatos. Consejo: La función de operaciones de restauración reiniciable funcionan como se esperaba cuando está conectado a servidor secundario. Sin embargo, las operaciones de restauración que se interrumpen cuando el servidor primario se desconecta no se pueden restaurar después de que el cliente realice la migración tras error. Debe ejecutar la operación de restauración completa de nuevo después de que el cliente realice la migración tras error al servidor secundario.

### Resultados

---

Si los datos de réplica del servidor secundario no es actual, se le solicita continuar o detener la restauración o la operación de recuperación.

Por ejemplo, para restaurar el directorio de build.sh en la interfaz de línea de mandato, emita el siguiente mandato:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
dsmc res /build.sh
```

 Sistemas operativos Windows

```
dsmc res C:\build.sh
```

Se visualiza la siguiente salida:

```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.
```

```
Nombre de nodo: MY_NODE_NAME
ANS2106I Connection to primary IBM Spectrum Protect server 192.0.2.1 failed
```

```
ANS2107I Attempting to connect to secondary server TARGET at
192.0.2.9 : 1501
```

```
Nombre de nodo: MY_NODE_NAME
Session established with server TARGET: Windows
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del servidor: 11/16/2016 12:05:35 Último acceso: 11/15/2016 14:13:32
```

```
Session established in failover mode to secondary server
ANS2108I Connected to secondary server TARGET.
Se ha invocado la función de restauración.
```

```
ANS2120W The last store operation date reported by the server TARGET of
05/16/2013 22:38:23 does not match the last store operation date of
05/21/2013 21:32:20 stored by the client.
Continue (Yes (Y)/No (N))
```

Si responde con N, se muestra el siguiente mensaje:

```
ANS1074W The operation was stopped by the user.
```


Si responde con Y, el proceso de restauración continúa como normal, pero es posible que los datos que restaure no sean los más actuales.

#### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

#### Tareas relacionadas:

Determinación del estado los datos replicados del cliente

 Sistemas operativos Windows

## Cómo autorizar a otro usuario para que restaure o recupere archivos

---

Puede autorizar a otro usuario de otro nodo para restaurar las versiones de copia de seguridad o para recuperar las copias archivadas. De esta forma, podrá compartir archivos con otras personas o con otras estaciones de trabajo que utilice con un nombre de nodo distinto.

### Acerca de esta tarea

---

También puede autorizar a otros nodos para que accedan al espacio de archivos de recuperación automática del sistema (ASR).

Se puede utilizar otro nodo para crear el disquete de ASR y poder recuperar la estación de trabajo mediante ASR y el cliente de copia de seguridad y archivado. Utilice el otro nodo si se produce algún problema con la estación de trabajo y el disquete ASR de la disquete no está disponible.

Para autorizar a otro nodo para que restaure o recupere los archivos:

### Procedimiento

---

1. Pulse **Herramientas** → **Lista de acceso al nodo** en la ventana principal.
2. En la ventana **Lista de acceso al nodo**, pulse el botón **Añadir**.
3. En la ventana **Agregar regla de acceso**, seleccione un elemento en el campo **Permitir acceso a** para especificar el tipo de datos al que el otro usuario puede acceder. Puede seleccionar **Objetos de copia de seguridad** o bien **Objetos archivados**.
4. Escriba el nombre de nodo del usuario en el campo **Otorgar acceso a nodo**. Escriba el nombre de nodo de la estación de trabajo host en el campo **Otorgar acceso a nodo**.
5. Escriba el ID de usuario de la estación de trabajo host en el campo **Usuario**.
6. En el campo **Espacio de archivos y directorio**, seleccione el espacio de archivos y el directorio al que el usuario puede acceder. No puede seleccionar más de un espacio de archivos y un directorio al mismo tiempo. Si desea dar al usuario acceso a otro espacio de archivos y otro directorio, debe crear otra regla de acceso.
7. Si desea limitar el acceso del usuario a determinados archivos del directorio, escriba en el campo **Nombre de archivo** el nombre completo o el tipo de los archivos del servidor a los que el otro usuario puede acceder. El campo **Nombre de archivo** solo acepta una entrada. Puede ser un único nombre de archivo o un nombre de archivo con caracteres comodín que corresponde a uno o varios archivos. Puede utilizar un carácter comodín como parte del patrón. La entrada debe coincidir con archivos que se hayan almacenado en el servidor.
8. Si desea otorgar acceso a todos los archivos que coincidan con la especificación del nombre de archivo en el directorio seleccionado, incluidos sus subdirectorios, pulse **Incluir subdirectorios**.
9. Pulse **Aceptar** para guardar la regla de acceso y cerrar la ventana **Agregar regla de acceso**.
10. La regla de acceso que ha creado se muestra en el cuadro de lista de la ventana **Lista de acceso al nodo**. Cuando ya no necesite la ventana **Lista de acceso al nodo**, pulse **Aceptar**. Si no desea guardar los cambios, pulse **Cancelar** o cierre la ventana.

### Resultados

---



Por ejemplo, para otorgar al nodo user2 acceso a todos los subdirectorios y archivos de copia de seguridad en el directorio d:\user1, cree una regla con los valores siguientes:

```
Permitir acceso a: Objetos de copia de seguridad
Otorgar acceso a nodo: user2
Espacio de archivos y directorio: d:\user1
Nombre de archivo: *
Incluir subdirectorios: Seleccionado
```

El nodo que está autorizando debe estar inscrito en su servidor de IBM Spectrum Protect.

En la línea de mandatos del cliente, utilice el mandato set access para autorizar a otro nodo a restaurar o recuperar los archivos. También puede utilizar el mandato query access para ver la lista actual y delete access para suprimir nodos de la lista.

**Referencia relacionada:**

Delete Access

Query Access

Set Access

 Sistemas operativos Windows

## Restauración o recuperación de archivos de otro nodo cliente

---

Después de que los usuarios concedan acceso a los archivos del servidor, puede restaurar o recuperar dichos archivos en el sistema local.

### Acerca de esta tarea

---

Para mostrar espacios de archivos de otro usuario en el servidor, restaurar las versiones de copia de seguridad de otro usuario o recuperar las copias de archivado de otro usuario en el sistema de archivos local, siga estos pasos:

### Procedimiento

---

1. Pulse **Herramientas** en la ventana principal.
2. Pulse **Acceder a otro nodo**.
3. Escriba el nombre de nodo de la estación de trabajo host en el campo **Nombre de nodo** y pulse **Establecer**.

### Resultados

---

Si está utilizando mandatos, utilice la opción fromnode para indicar el nodo. También debe utilizar el nombre del espacio de archivos, en vez de la letra de la unidad, para seleccionar la unidad de restauración/recuperación a la que desea acceder. Incluya el nombre del espacio de archivos entre llaves y especifíquelo como si especificara una letra de unidad. Por ejemplo, para restaurar los archivos del directorio \projx del nodo cougar en el espacio de archivos de disco d en su propio directorio \projx, especifique:

```
dsmc restore -fromnode=cougar \\cougar\d$\projx\* d:\projx\
```

Utilice el mandato query filespace para mostrar una lista de espacios de archivos. Por ejemplo, para mostrar una lista de los espacios de archivos de cougar, escriba:

```
dsmc query filespace -fromnode=cougar
```

**Importante:** El cliente de copia de seguridad y archivado puede utilizar la información de espacio de archivos al restaurar archivos. La información de espacio de archivos puede contener el nombre del sistema desde el que se ha realizado la copia de seguridad de los archivos. Si realiza la restauración de archivos desde otro nodo cliente y no especifica un destino para los archivos restaurados, el cliente utilizará la información de espacio de archivos para restaurar los archivos. En este caso, el cliente intentará restaurar los archivos en la unidad del sistema original. Si el sistema de restauración dispone de acceso a la unidad del sistema original, podrá restaurar archivos en la unidad original. Si el sistema de restauración no puede acceder a la unidad del sistema original, el cliente devolverá un mensaje de error de red. Si desea restaurar la estructura de directorios original pero en un sistema distinto, especifique sólo la unidad de destino cuando restaure los archivos. Esto es cierto cuando se restauran archivos de otro nodo y cuando se recuperan archivos de otro nodo.

**Referencia relacionada:**

Fromnode

Restore

Retrieve

 Sistemas operativos Windows

## Restauración o recuperación de archivos en otra estación de trabajo

---

Si utiliza una estación de trabajo diferente, puede restaurar o recuperar archivos de los que ha efectuado copia de seguridad en su propia estación de trabajo.

Sus versiones de copia de seguridad y copias archivadas se almacenan de acuerdo con su nodo, no con su estación de trabajo específica. La contraseña de IBM Spectrum Protect protege los datos.

Para restaurar o recuperar archivos en otra estación de trabajo, utilice la opción `virtualnodename` para especificar el nombre de nodo de la estación de trabajo desde donde se realizó la copia de seguridad de los archivos. Puede utilizar la opción `virtualnodename` al iniciar IBM Spectrum Protect o bien agregarla al archivo de opciones del cliente `dsm.opt` en la estación de trabajo. Si está utilizando una estación de trabajo de otra persona en lugar de la suya, utilice la opción `virtualnodename` con el mandato `dsm`. Por ejemplo, si el nombre del nodo es `cougar`, entre:

```
start dsm -virtualnodename=cougar
```

Podrá entonces restaurar o recuperar archivos como si estuviera trabajando en la estación de trabajo original.

También puede utilizar la opción `virtualnodename` en los mandatos. Por ejemplo, para restaurar los archivos `\projx` en el directorio local `c:\myfiles`, escriba:

```
dsmc restore -virtualnodename=cougar \\cougar\d$\projx\*. * c:\myfiles\
```

Si no desea restaurar o recuperar los archivos en el mismo nombre de directorio de la estación de trabajo alternativa, escriba un destino distinto.

## Restauración o recuperación de archivos en otro tipo de estación de trabajo

---

Puede restaurar o recuperar archivos de un tipo de sistema en otro. Esto se denomina *cross-client restore*.

Restricción: Debe tener los permisos adecuados para acceder al espacio de archivos de la otra estación de trabajo.

Las unidades NTFS y ReFS permiten nombres de directorios y de archivos más largos de los que se permiten en unidades FAT. Si está recuperando archivos en una unidad FAT con nombres de archivo largos, especifique un archivo de destino para cada archivo.

Cuando se utiliza el cliente Windows para recuperar archivos con nombres largos en un sistema de archivos NTFS o ReFS, se conservan los nombres largos, incluso si el archivo se recupera en un tipo de unidad distinto de la unidad de origen.

### Tareas relacionadas:

Cómo autorizar a otro usuario para que restaure o recupere archivos

Restauración o recuperación de archivos de otro nodo cliente

 Sistemas operativos Windows

## Supresión de espacios de archivos

---

Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor.

### Acerca de esta tarea

---

No puede suprimir copias de seguridad concretas si se conservan en el servidor. Al suprimir un espacio de archivos, estará suprimiendo todos los archivos, tanto las copias de seguridad como las copias archivadas, que se encuentran dentro del mismo. Por ejemplo, si elimina el espacio de archivos de la unidad `C:`, estará eliminando todas las copias de seguridad de todos los archivos que haya en ese disco y de todos los archivos de ese disco que haya archivado.

Atención: Considere detenidamente la acción que va a realizar antes de intentar suprimir un espacio de archivos.

Puede suprimir espacios de archivos mediante la GUI o el cliente de línea de mandatos. Para suprimir espacios de archivos de almacenamiento adjunto de red (NAS), utilice el cliente web o el cliente de línea de mandatos.

Para suprimir un espacio de archivos mediante el cliente GUI, siga estos pasos:

### Procedimiento

---

1. En la ventana principal, pulse **Herramientas** → **Suprimir espacios de archivos**.
2. Seleccione los espacios de archivos que desee suprimir.
3. Pulse **Suprimir**. El cliente le pedirá una confirmación antes de eliminarlos.

### Resultados




---

También puede suprimir un espacio de archivos con el mandato delete filesystem. Utilice la opción class con el mandato delete filesystem para suprimir espacios de archivos NAS.

**Referencia relacionada:**

Class

Delete Filespace

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Restaurar una imagen en archivo

---

Al realizar una copia de seguridad de una imagen, el cliente de archivado y copia de seguridad realiza una copia de seguridad del primer sector del volumen, pero, al restaurar los datos, omite el primer sector para mantener el bloque de control del volumen lógico original del volumen de destino.

Cuando se realiza una restauración de imagen en archivo, en el archivo se restaura el contenido del volumen completo, incluido el primer sector.

Los volúmenes LVM de AIX de grupos de volúmenes originales contienen el bloque de control de volumen lógico (LVCB) en el primer sector (512 bytes) del volumen. El LVCB contiene metadatos específicos del volumen y que deberían conservar las aplicaciones que utilizan el volumen.

Cuando copie el archivo que contenga la imagen en un volumen LVM desde el grupo de volúmenes original, deberá omitir el LVCB del archivo y del volumen de destino. Para llevar esto a cabo, puede utilizar el mandato dd siguiente:

```
dd if=<filename> of=/dev/<vol> bs=512 skip=1 seek=1
```

El mandato dd establece el tamaño de bloque en 512 bytes, lo cual hace que la copia se realice muy lentamente. La mejor opción consiste en utilizar `bs=1m` o una especificación similar. Tenemos una forma alternativa de copiar los datos de imagen:

1. Guarde el primer sector original en un archivo:

```
dd if=/dev/<vol> of=firstblk.tmp bs=512 count=1
```

2. Copie la imagen restaurada:

```
dd if=<filename> of=/dev/<vol> bs=1m
```

3. Restaure el primer sector original:

```
dd if=firstblk.tmp of=/dev/<vol> bs=512 count=1
```

Con la introducción de formatos de grupo de volúmenes grandes y escalables en AIX, es posible que el primer sector del volumen lógico no pueda contener LVCB y esté disponible para los datos. Si utiliza grupos de volumen grandes y escalables en su sistema, y tiene que restaurar todo el volumen incluyendo el primer sector, restaure el volumen a un archivo y después, cópielo a un volumen de destino. Para llevar esto a cabo, puede utilizar el mandato **dd** siguiente:

```
dd if=<filename> of=/dev/<vol> bs=1m
```

**Conceptos relacionados:**

Restauración de una imagen mediante la línea de mandatos

**Tareas relacionadas:**

Restauración de una imagen mediante la GUI

 Sistemas operativos AIX  Sistemas operativos Linux

## Gestión de datos del sistema de archivos GPFS con agrupaciones de almacenamiento

---

Con la tecnología Global Parallel File Systems (GPFS), puede gestionar los datos utilizando agrupaciones de almacenamiento. Una agrupación de almacenamiento es una colección de discos o RAID que tienen propiedades similares y que se gestionan conjuntamente como un grupo.

El grupo en el que se gestionan conjuntamente las agrupaciones de almacenamiento es el sistema de archivos. La ubicación y gestión automatizadas de los archivos de la agrupación de almacenamiento la realizan las políticas. Una política es un conjunto de reglas que describe el ciclo útil de los datos de usuario basándose en los atributos del archivo.

Cuando se crea un archivo, la política de ubicación determina la ubicación inicial de los datos del archivo y asigna el archivo a una agrupación de almacenamiento. Todos los datos que se graban en ese archivo se colocan en la agrupación de almacenamiento

asignada. La política de gestión determina las operaciones de gestión que han de aplicarse al archivo, como la migración y la supresión. Los archivos contenidos en un sistema de archivos GPFS se distribuyen entre diferentes agrupaciones de almacenamiento, en función de las políticas de ubicación y migración habilitadas.

Durante la restauración, los archivos se colocan en la agrupación de almacenamiento correcta. El servidor de IBM Spectrum Protect no está al tanto de las migraciones de agrupación a agrupación, por lo tanto los archivos se colocan en la agrupación de almacenamiento desde la que se ha realizado la copia de seguridad. El motor de política sustituye los archivos en función de las políticas de migración.

Si un ID de agrupación de almacenamiento se ha almacenado en los atributos ampliados del archivo, y esa agrupación de almacenamiento está disponible, el archivo siempre se coloca en esa agrupación de almacenamiento. Si la agrupación de almacenamiento no está disponible, la ubicación del archivo la determina la política de ubicación. Si la política de ubicación no coincide con el archivo, el archivo se coloca en la agrupación del sistema.

GPFS maneja la colocación de archivos después de una restauración como se indica a continuación:

- El archivo se coloca en la agrupación que puede seleccionar haciendo coincidir los atributos del archivo guardado con una regla RESTORE
- El archivo se coloca en la agrupación en la que estaba cuando se ha realizado la copia de seguridad.
- La ubicación en la que ha de colocarse el archivo se basa en la política de ubicación actual.
- El archivo se coloca en la agrupación de almacenamiento del sistema.

La regla GPFS RESTORE permite hacer coincidir archivos según los atributos guardados y no según los atributos del archivo actual. Si los atributos del archivo no coinciden, GPFS intenta restaurar el archivo en la secuencia descrita anteriormente.

Para obtener más información acerca de la regla GPFS RESTORE, lea la documentación GPFS acerca de políticas y reglas.

Se aplican las restricciones siguientes:










- La restauración de los archivos apéndice no funciona cuando se utilizan varias agrupaciones de almacenamiento ni con los archivos que tienen ACL.
- La desvinculación de juegos de archivos no está admitida.
- La opción ctime de GPFS debe establecerse en no (valor predeterminado) para evitar que se realicen operaciones de copia de seguridad/archivado no deseadas de los archivos después de la migración de archivos de GPFS de agrupación a agrupación.

Para obtener información sobre la utilización de las agrupaciones de almacenamiento, consulte la documentación del servidor de IBM Spectrum Protect.

#### Conceptos relacionados:

Almacenamiento de datos en agrupaciones de almacenamiento

#### Información relacionada:

-  Sistemas operativos AIX  Sistemas operativos Linux  Información sobre el producto GPFS
-  Sistemas operativos AIX  Sistemas operativos Linux  Mandato mmbbackup: Requisitos de IBM Spectrum Protect
-  Sistemas operativos AIX  Sistemas operativos Linux  Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbbackup de IBM Spectrum Scale

## Restauración de datos a un instante específico





---




Utilice una restauración a un *instante específico* para restaurar archivos al estado que tenían en una fecha y hora específicos.


### Acerca de esta tarea

---

Una restauración a un instante específico puede eliminar el efecto de los datos dañados mediante la restauración de los datos a un momento anterior al problema o puede recuperar una configuración básica a una condición anterior.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Puede llevar a cabo una restauración a un instante específico de un espacio de archivos, directorio o archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris También puede llevar a cabo una restauración de punto en el tiempo de las copias de seguridad de imagen.

 Sistemas operativos Windows Puede llevar a cabo una restauración a un instante específico de los datos del estado del sistema, un espacio de archivos, un directorio o un archivo. También puede llevar a cabo una restauración de punto en el tiempo de las copias de seguridad de imagen.

Lleve a cabo copias de seguridad incrementales para dar soporte a una restauración a un instante específico. Durante una copia de seguridad incremental, el cliente de copia de seguridad y archivado notifica al servidor el momento en que los archivos se suprimen de un espacio de archivos o directorio de cliente. Las copias de seguridad selectivas e incrementales por fecha no informan al servidor de

los archivos suprimidos. Ejecute copias de seguridad incrementales con una frecuencia coherente con los requisitos de restauración posibles.

Si solicita una restauración a un instante específico con una fecha y una hora anteriores a la versión más antigua mantenida por el servidor de IBM Spectrum Protect, el objeto no se restaura en el sistema. Los archivos que se hayan borrado de la estación de trabajo antes del instante especificado no se restaurarán.

Nota:

1. El administrador debe definir los valores de grupo de copia que mantengan suficientes versiones inactivas de un archivo para garantizar que se puede restaurar un archivo en una fecha y hora específicas. Si no se mantienen suficientes versiones, es posible que el cliente no pueda restaurar todos los objetos en el instante específico que especifique.
2. Si suprime un archivo o un directorio, la próxima vez que ejecute una copia de seguridad incremental, la versión de copia de seguridad activa pasará a inactiva y las versiones más antiguas que excedan el número especificado por el atributo *Versiones si datos suprimidos* se suprimen de la clase de gestión.

Cuando realice una restauración a un instante específico, tenga en cuenta la siguiente información:

- El cliente restaura las versiones de archivos de la copia de seguridad más reciente anterior a la fecha de instante específico especificada. Asegúrese de que el instante específico que especifique no coincida con la fecha y la hora en que se realizó la copia de seguridad.
- Si la fecha y hora especificadas para el objeto que intenta restaurar son anteriores a las de la versión más antigua que existe en el servidor, el cliente no podrá restaurar dicho objeto.
- Una restauración a un instante específico restaura los archivos que se han suprimido de la estación de trabajo cliente después de la fecha especificada, pero no los archivos suprimidos antes de dicha fecha.
- El cliente no puede restaurar un archivo creado después de la fecha y hora del instante específico. Cuando se ejecute la restauración a un instante específico, no se suprimirán los archivos creados en el cliente en fecha posterior a la especificada como instante específico.

## Procedimiento

---

Para llevar a cabo una restauración a un instante específico utilizando la GUI del cliente, siga los pasos siguientes:

1. Pulse el botón Restaurar en la ventana principal. Aparecerá la ventana Restaurar.
2. Pulse el botón Instante específico en la ventana Restaurar. Aparecerá la ventana Restauración a un instante específico.
3. Seleccione el recuadro Utilizar una fecha de instante específico. Seleccione la fecha y hora y pulse Aceptar. El instante especificado aparece en el campo visualización de instante específico en la ventana Restaurar.
4. Visualice los objetos que desea restaurar. Puede buscar un objeto por su nombre, filtrar el árbol de directorios o trabajar con los directorios del árbol de directorios.
5. Pulse en las casillas que se encuentran junto a los objetos que desea restaurar.
6. Pulse el botón Restaurar. Se abrirá la ventana Destino de restauración. Entre la información pertinente.
7. Pulse el botón Restaurar para iniciar la restauración. En la ventana Lista de tareas de restauración se muestra el estado del proceso.

## Resultados

---





Nota: Si no existen versiones de copia de seguridad de un directorio para el instante específico que indique, los archivos que se encuentren en ese directorio no se podrán restaurar desde la GUI. Sin embargo, puede restaurar estos archivos desde la línea de mandatos.


Puede iniciar la restauración a un instante específico desde el cliente de línea de mandatos utilizando las opciones `pitdate` y `pittime` con los mandatos `query backup` y `restore`. Si utiliza las opciones `pitdate` y `pittime` con el mandato `query backup`, se establece el instante específico al que se devuelve la información de archivo. Si utiliza las opciones `pitdate` y `pittime` con el mandato `restore`, los valores de fecha y hora especificados establecen el instante específico al que se devuelven los archivos. Si especifica `pitdate` sin un valor para `pittime`, el valor predeterminado de `pittime` será 23:59:59. Si especifica `pittime` sin un valor para `pitdate`, éste se ignorará.

### Conceptos relacionados:

Políticas de gestión de almacenamiento

### Referencia relacionada:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Backup Image

 Sistemas operativos AIX

## Restauración de archivos cifrados AIX


---

Cuando se realiza una copia de seguridad de archivos en formato en bruto a partir de un Sistema de archivos de cifrado (EFS) de JFS2 de AIX, solamente podrá restaurarla en el mismo EFS de JFS2 o en otro. No se pueden restaurar en ningún otro sistema de archivos distinto, ni en ninguna otra plataforma.

Cuando se realiza una copia de seguridad de los archivos EFS en forma de texto legible, podrá restaurarlos en cualquier lugar. Si los restaura en un EFS de JFS2, se volverán a cifrar automáticamente solo si el directorio en el que se restauran tiene establecida la opción "herencia de EFS" de AIX.

Tras restaurar un archivo del que se ha realizado una copia de seguridad en formato bruto, es posible que observe que el archivo ya no se puede descifrar. Es posible que la clave de cifrado original utilizada para el archivo ya no esté disponible en el almacén de claves de usuario. En tal caso, deberá restaurar el almacén de claves utilizado en el momento de realizar la copia de seguridad.

Para obtener información sobre cómo realizar copias de seguridad de datos EFS, consulte el apartado Copia de seguridad del sistema de archivos cifrado de JFS2 de AIX.

 Sistemas operativos AIX

## Restaurar sistemas de archivos con partición de carga de trabajo de AIX

Todos los archivos que se crean mediante la partición de carga de trabajo local (WPAR) y que se copian mediante un cliente de copia de seguridad y archivado que está instalado en la WPAR global se pueden restaurar mediante el cliente instalado en la WPAR global.

Consulte los siguientes ejemplos de partición global y de configuración de WPAR:

Global partition:

```
system name: shimla
file system: /home /opt
```

WPAR #1 configuration:

```
name: wpar1
file system: /home; name in global WPAR: /wpars/wpar1/home
```

WPAR #2 configuration:

```
name: wpar2
file system: /data; name in global WPAR: /wpars/wpar2/data
```

Existen dos formas de restaurar datos WPAR, dependiendo del método utilizado para realizar la copia de seguridad de los archivos de datos WPAR:

- Restaure todos los sistemas de archivos WPAR como espacios de archivo en la partición global. El nombre de espacio de archivos se debe utilizar para identificar el WPAR al cual pertenece. Todos los datos se gestionan en un nodo utilizando una planificación. Aquí encontrará un archivo de ejemplo, `dsm.sys`, que utiliza la configuración de ejemplo mencionada anteriormente, con una stanza de servidor para todos los sistemas de archivos, tanto globales como lógicos:

```
SERvername  shimla
          TCPPort                1500
          TCPServeraddress        servidor.ejemplo.com
          nodename                 shimla
          PasswordAccess          generate
          Domain                   /wpars/wpar1/home /wpars/wpar2/data /home /opt
```

Utilice el mandato siguiente para restaurar cada espacio de archivos:

```
dsmc restore /wpars/wpar1/home/*
dsmc restore /wpars/wpar2/data/*
dsmc restore /home/*
dsmc restore /opt/
```

- Restaure cada sistema de archivos WPAR desde un nombre de nodo distinto, si se ha realizado la copia de seguridad bajo un nombre de nodo distinto. Cada WPAR debe tener un nombre de nodo independiente y un planificador en ejecución en la partición global. Además, se han de configurar los tres servicios del planificador, utilizando para cada uno de ellos un archivo `dsm.opt`

distinto correspondiente al nombre de la sección del servidor. Este método permite que cada operación de restauración de WPAR se pueda gestionar de forma independiente de las demás. Aquí encontrará un archivo de ejemplo, `dsm.sys`, que utiliza la configuración de ejemplo mencionada anteriormente, con tres secciones de servidor: una para `wpar1`, otra para `wpar2` y otra para la partición global `shimla`:

```

SErvername  shimla_wpar1
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename   wpar1
PasswordAccess  generate
Domain     /wpars/wpar1/home




SErvername  shimla_wpar2
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename   wpar2
PasswordAccess  generate
Domain     /wpars/wpar2/data

SErvername  shimla
TCPPort    1500
TCPSeveraddress  servidor.ejemplo.com
nodename   shimla
PasswordAccess  generate
Domain     /home /opt

```

Tabla 1. mandatos de restauración de WPAR de ejemplo con el archivo `dsm.opt`








En el archivo <code>dsm.opt</code> file	mandato de restauración de ejemplo
<code>servername shimla_wpar1</code>	<code>dsmc restore /wpars/wpar1/home/*</code>
<code>servername shimla_wpar2</code>	<code>dsmc restore /wpars/wpar2/data/*</code>
<code>servername shimla</code>	<code>dsmc restore /home/*</code> <code>dsmc restore /opt/*</code>

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Restaurar sistemas de archivos NAS




Las imágenes del sistema de archivos NAS se restauran mediante el cliente web o la interfaz de línea de mandatos. El interfaz de cliente web está disponible sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.

Puede restaurar imágenes del sistema de archivos NAS completas o diferenciales de las que se ha hecho una copia de seguridad previamente. Si restaura una imagen diferencial, IBM Spectrum Protect restaura automáticamente la imagen de copia de seguridad completa, seguida de una imagen diferencial. No es necesario que un nodo cliente monte un sistema de archivos NAS para realizar operaciones de copia de seguridad o de restauración en dicho sistema de archivos.

-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Restauración de sistemas de archivos NAS utilizando el cliente web  
En esta sección se indican los pasos para restaurar sistemas de archivos NAS mediante la GUI del cliente web.
-  Sistemas operativos Windows Restauración de directorios y archivos NAS mediante el cliente web  
Puede utilizar la opción `toc` con la opción `include.fs.nas` en el archivo de opciones del cliente para especificar si el cliente guarda la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Opciones y mandatos para restaurar sistemas de archivos NAS desde la línea de mandatos.  
Este tema enumera algunos ejemplos de las opciones y mandatos que puede utilizar para restaurar las imágenes del sistema de archivos NAS desde la línea de mandatos.

### Conceptos relacionados:

Descripción general de la configuración del cliente web

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Restauración de sistemas de archivos NAS utilizando el cliente web

En esta sección se indican los pasos para restaurar sistemas de archivos NAS mediante la GUI del cliente web.

### Antes de empezar

El interfaz de cliente web está disponible sólo para conexiones a servidores de IBM Spectrum Protect Versión 8.1.1, V8.1.0, V7.1.7 o anterior.

## Procedimiento

---


1. Pulse el botón **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios si es preciso. Para expandir un nodo del árbol, pulse en el signo más (+) situado junto al objeto del árbol. Los nodos que se muestran son aquéllos de los que se ha hecho copia de seguridad y para los que el administrador tiene autorización. El nodo raíz denominado **Nodos** no se puede seleccionar. Este nodo sólo aparece si hay un complemento NAS presente en la estación de trabajo cliente. Los nodos NAS se muestran en el mismo nivel que el nodo de la estación de trabajo cliente. Sólo aparecen los nodos para los que tiene autorización el administrador.
3. Expanda el nodo NAS para ver el objeto Imagen.
4. Expanda el objeto Imagen para ver los volúmenes que puede restaurar. No puede expandir los objetos Volumen.
5. Pulse las casillas situadas junto a los volúmenes bajo el objeto Imagen que desea restaurar. Si desea restaurar una imagen NAS de la que se ha efectuado una copia de seguridad en una fecha concreta, pulse el botón **Instante específico**. Al seleccionar una fecha, aparece el último objeto del que se hizo copia de seguridad en dicha fecha o anteriormente, incluidos los objetos que estén inactivos. Si desea ver todas las imágenes (incluidas las activas y las inactivas), antes de seleccionarlas, pulse **Ver** → **Visualizar archivos activos/inactivos** en la barra de menús.
6. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. Especifique la información en la ventana Destino de restauración. Si va a realizar la restauración en un destino diferente, sólo podrá restaurar un volumen a la vez. Puede restaurar las imágenes de sistemas de archivos NAS en cualquier volumen del servidor de archivos NAS desde el que se realizó su copia de seguridad. No puede restaurar imágenes en otro servidor de archivos NAS.
7. Pulse **Restaurar**. La ventana **Lista de tareas** de copia de seguridad NAS muestra el estado del proceso y la barra de progreso de la restauración. Si aparece un número junto a la barra de progreso, éste indica el tamaño de la restauración, si se conoce. Una vez finalizada la restauración, la ventana Informe de restauración NAS muestra los detalles del proceso. Si debe cerrar la sesión del navegador web, las operaciones NAS actuales continuarán después de la desconexión. Puede utilizar el botón **Descartar** situado en la ventana **Lista de tareas** de restauración NAS para salir de los procesos de supervisión sin finalizar la operación actual.
8. (Opcional) Para supervisar el procesamiento de una operación, seleccione Acciones > IBM Spectrum Protect Actividades en la ventana principal.

## Resultados

---

Consideraciones:

- Las copias de seguridad de estaciones de trabajo y remotas (NAS) se excluyen mutuamente en una ventana Restaurar. Tras haber seleccionado un elemento para restaurar, el siguiente elemento que seleccione deberá ser del mismo tipo (NAS o no NAS).
- No se mostrarán detalles en el marco derecho de la ventana Restaurar correspondientes a los nodos o imágenes NAS. Para ver información sobre una imagen NAS, resalte la imagen NAS y seleccione Ver > Detalles de archivo en el menú.
- Para suprimir espacios de archivo NAS, seleccione Utilities > Delete Filespaces. Puede suprimir objetos de la estación de trabajo y objetos remotos.

 Sistemas operativos Windows

## Restauración de directorios y archivos NAS mediante el cliente web

---

Puede utilizar la opción toc con la opción include.fs.nas en el archivo de opciones del cliente para especificar si el cliente guarda la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.

### Acerca de esta tarea

---

Si guarda la información de la TOC, puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que deben restaurarse. Para crear una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Tenga en cuenta que, para crear una tabla de contenido, es necesario disponer de un proceso adicional, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad. Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios utilizando el mandato de servidor RESTORE NODE, siempre que conozca el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

Para restaurar archivos y directorios NAS:

## Procedimiento

---

1. Pulse Restaurar en la ventana principal. Aparecerá la ventana Restaurar.



2. Expanda el árbol de directorios si es preciso. Para expandir un nodo del árbol, pulse en el signo más (+) situado junto al objeto del árbol. Los nodos que se muestran son aquéllos de los que se ha hecho copia de seguridad y para los que el administrador tiene autorización. El nodo raíz denominado Nodos no se puede seleccionar. Este nodo sólo aparece si hay un complemento NAS presente en la estación de trabajo cliente. Los nodos NAS aparecen en el mismo nivel que el nodo de la estación de trabajo cliente. Sólo aparecen los nodos para los que tiene autorización el administrador.
3. Expanda el nodo NAS para ver el objeto Nivel de archivo.
4. Expanda el objeto Nivel de archivo para ver los últimos volúmenes, directorios y archivos de los que se ha efectuado una copia de seguridad. Cuando se expande el objeto de volumen y en el servidor existe información completa de tabla de contenido correspondiente a la última copia de seguridad, aparece el diálogo Cargar tabla de contenido. Si no se dispone de la información completa de tabla de contenido correspondiente a la última copia de seguridad, no aparecerá ningún objeto bajo el objeto de volumen. En el paso siguiente se explica cómo visualizar objetos de copias de seguridad que no son las más recientes. Se proporciona información completa de TOC si se realiza cualquiera de las operaciones siguientes: (1) Una copia de seguridad de imágenes diferencial con información TOC y su correspondiente copia de seguridad de imágenes completa con información TOC, o (2) Una copia de seguridad de imágenes completa con información TOC.
5. Seleccione las casillas situadas junto a los directorios o archivos que desea restaurar.
  - a. Si desea restaurar archivos de una imagen NAS de la que se ha efectuado una copia de seguridad en una fecha concreta, o visualizar archivos de varias versiones anteriores, resalte el volumen que desea restaurar y pulse el botón Instante específico.
  - b. Si selecciona Utilizar fecha de instante específico en la ventana Restauración a un instante específico, bajo el objeto Nivel de archivo aparecerán los archivos de la imagen de la que se ha realizado una copia de seguridad en dicha fecha o, si se trata de una imagen diferencial, los archivos de su imagen completa correspondiente.
  - c. Si selecciona Utilizar las imágenes seleccionadas en la ventana Restauración a un instante específico, aparecerá la ventana Seleccionar imágenes para que seleccione imágenes. El contenido de las imágenes seleccionadas aparecerá en el objeto Nivel de archivo.
6. Pulse Restaurar. Aparecerá la ventana Destino de restauración. Especifique la información en la ventana Destino de restauración. Si va a realizar la restauración en un destino diferente, sólo podrá restaurar un volumen a la vez.
7. Pulse Restaurar. La ventana Lista de tareas de copia de seguridad NAS muestra el estado del proceso y la barra de progreso de la restauración. Si aparece un número junto a la barra de progreso, éste indica el tamaño de la restauración, si se conoce. Una vez finalizada la restauración, la ventana Informe de restauración NAS muestra los detalles del proceso. Si debe cerrar la sesión del navegador web, las operaciones NAS actuales continuarán después de la desconexión. Puede utilizar el botón Descartar situado en la ventana Lista de tareas de restauración NAS para salir de los procesos de supervisión sin finalizar la operación actual.
8. (Opcional) Para supervisar el procesamiento de una operación, seleccione Acciones > IBM Spectrum Protect Actividades en la ventana principal.

## Resultados

Consideraciones:

- Las copias de seguridad de estaciones de trabajo y remotas (NAS) se excluyen mutuamente en una ventana Restaurar. Tras haber seleccionado un elemento para restaurar, el siguiente elemento que seleccione deberá ser del mismo tipo (workstation o NAS).
- Para ver información sobre los objetos en el nodo de NAS, resalte el objeto y seleccione View > File Details en el menú.
- Para suprimir espacios de archivo NAS, seleccione Utilities > Delete Filespaces. Puede suprimir objetos de la estación de trabajo y objetos remotos.

**Referencia relacionada:**

Toc










 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows



## Opciones y mandatos para restaurar sistemas de archivos NAS desde la línea de mandatos.


Este tema enumera algunos ejemplos de las opciones y mandatos que puede utilizar para restaurar las imágenes del sistema de archivos NAS desde la línea de mandatos.

Tabla 1. Opciones y mandatos NAS

Opción o mandato	Definición	Página
query node	Muestra todos los nodos en los que un identificador de usuario de administración determinado dispone de autorización para realizar operaciones. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la web.	Query Node

Opción o mandato	Definición	Página
query backup	Utilice el mandato query backup con la opción class para mostrar información sobre las imágenes de sistema de archivos de las que se ha realizado una copia de seguridad para un servidor de archivos NAS.	Query Backup
query filespace	Utilice el mandato query filespace con la opción <b>class</b> para visualizar una lista de espacios de archivos pertenecientes a nodo NAS.	Query Filespace
restore nas	Restaura la imagen de un sistema de archivos que pertenece a un servidor de archivos NAS (Network Attached Storage).	Restore NAS
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows monitor process	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Muestra los procesos de copia de seguridad y de restauración actuales de todos los nodos NAS en los que el administrador dispone de autorización. El usuario de administración puede seleccionar el proceso que desea supervisar.	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Monitor Process
cancel process	Muestra los procesos de copia de seguridad y de restauración actuales de todos los nodos NAS en los que el administrador dispone de autorización. Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar.	Cancel Process
delete filespace	Utilice delete filespace con la opción class para que se visualice una lista de los espacios de archivos que pertenecen a un nodo NAS y para seleccionar el que desea suprimir.	Delete Filespace






 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Independientemente de la plataforma del cliente, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol10.

 Sistemas operativos Windows Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

 Sistemas operativos Windows

- Independientemente de la plataforma del cliente, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol10.
- En el sistema de archivos NAS es necesario utilizar llaves { } como delimitadores de los nombres de sistemas de archivos cuando se utiliza la línea de mandatos; por ejemplo: {/vol/vol10}.

Nota: Cuando se inicia una operación de restauración NAS utilizando el cliente de línea de mandatos o el cliente web, el servidor empieza un proceso para iniciar, controlar y supervisar la operación. Es posible que tarde unos cuantos minutos en observar el progreso en la interfaz de línea de mandatos porque el servidor debe realizar el montaje y otras tareas necesarias antes de que se produzca el traspaso de datos. Puede que el cliente de línea de mandatos de IBM Spectrum Protect visualice un mensaje *Interrumpido...* cuando tiene lugar el montaje. Puede pasar por alto este mensaje.

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  
 Sistemas operativos Oracle Solaris

## Restaurar copias de seguridad activas o inactivas

El administrador determina cuántas versiones de copia de seguridad mantiene IBM Spectrum Protect para cada archivo de la estación de trabajo.

Tener varias versiones de un archivo le permite restaurar versiones anteriores en el caso de que la copia de seguridad más reciente esté dañada. La versión de copia de seguridad más reciente es la versión *activa*. Cualquier otra versión de copia de seguridad es una versión *inactiva*.






Cada vez que IBM Spectrum Protect hace copias de seguridad de archivos, marca la nueva versión de copia de seguridad como copia de seguridad activa y la copia de seguridad activa anterior pasa a ser inactiva. Cuando se alcanza el número máximo de versiones inactivas, IBM Spectrum Protect suprime la versión inactiva más antigua.

Para restaurar una versión de copia de seguridad inactiva, debe visualizar ambas versiones, la activa y la inactiva, pulsando la opción **Visualizar archivos activos/inactivos** del menú **Ver**. Para ver sólo las versiones activas (opción predeterminada), pulse la opción **Visualizar sólo archivos activos** del menú **Ver**. Si intenta restaurar más de una versión a la vez, sólo se restaurará la versión activa.

En la línea de mandatos de IBM Spectrum Protect, utilice la opción *inactive* para visualizar los objetos activos e inactivos.

## Referencia relacionada:

Inactive

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  
 Sistemas operativos Oracle Solaris

## Restauración de datos mediante la GUI

En esta sección figuran los pasos que es necesario seguir para restaurar versiones de copias de seguridad de archivos o subdirectorios individuales.






### Procedimiento

1. Pulse **Restaurar** en la ventana principal. Aparecerá la ventana Restaurar.
2. Expanda el árbol de directorios. Seleccione las casillas situadas junto a los archivos o directorios que desea restaurar. Para buscar o filtrar archivos, pulse el icono **Buscar** de la barra de herramientas.
3. Escriba los criterios de búsqueda en la ventana Buscar archivos (Restaurar).
4. Pulse el botón **Buscar**. Aparecerá la ventana Archivos coincidentes (Restaurar).
5. Pulse las casillas que se encuentran junto a los archivos que se desean restaurar y cierre la ventana Archivos coincidentes (Restaurar).
6. Escriba los criterios de filtrado en la ventana Buscar archivos (Restaurar).
7. Pulse el botón **Filtrar**. La ventana Restaurar muestra los archivos filtrados.
8. Pulse en las casillas que se encuentran junto a los archivos o directorios filtrados que desea restaurar.
9. Si desea modificar opciones de restauración específicas, pulse el botón **Opciones**. Las opciones que modifique *sólo* estarán en vigor durante la sesión actual.
10. Pulse **Restaurar**. Aparecerá la ventana Destino de restauración. Especifique la información en la ventana Destino de restauración.
11. Pulse **Restaurar**. La ventana **Lista de tareas** de restauración muestra el estado del proceso de restauración.

### Resultados

Nota: En Mac OS X, tenga en cuenta las siguientes consideraciones cuando restaure datos mediante la GUI:

1. Cuando se utiliza Herramientas de IBM Spectrum Protect para administradores para iniciar el cliente, este se ejecuta con un ID de usuario de cero. Esto significa que si crea una carpeta en la que restaurar los archivos, dicha carpeta será propiedad del usuario root. Para acceder a los archivos, deberá cambiar los permisos de la carpeta. Podrá cambiar el propietario de la carpeta desde una ventana de terminal con el mandato **sudo chown**. Consulte la documentación relativa al sistema operativo que utilice para obtener más información sobre cómo llevarlo a cabo.
2. Cuando restaure archivos con la opción *replaca* establecida en *no*, los archivos existentes no se sobrescribirán, pero sí los directorios. Para dejar intactos los directorios existentes durante una operación de restauración, seleccione el botón **Opciones**, => después seleccione el menú desplegable **Todos los archivos y directorios seleccionados** y elija la opción **Solo archivos**.
3. Cuando las carpetas se restauran desde un sistema de archivos UFS o HFSX en un sistema de archivos HFS y sólo difieren en el uso de mayúsculas o minúsculas, el cliente restaura el contenido de ambas carpetas en una sola.

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  
 Sistemas operativos Oracle Solaris

## Ejemplos de restauración desde la línea de mandatos









Este tema enumera algunos ejemplos de los mandatos restore para su uso en tareas específicas.

En la tabla siguiente se muestran ejemplos de utilización del mandato restore para restaurar objetos del almacenamiento del servidor de IBM Spectrum Protect.

Tabla 1. Ejemplos de restauración desde la línea de mandatos






Tarea	Mandato	Consideraciones
Restaurar la versión de copia de seguridad más reciente del archivo /Users/monnett/Documents/h1.doc, aunque la copia de seguridad esté inactiva.	<pre>dsmc restore /Users/monnett /Documents/h1. doc -latest</pre>	Si el archivo que está restaurando ya no reside en la estación de trabajo y ha realizado una copia de seguridad incremental después de suprimir el archivo, no habrá ninguna copia de seguridad activa del archivo en el servidor. En este caso, utilice la opción latest para restaurar la versión de copia de seguridad más reciente. IBM Spectrum Protect restaura la versión de copia de seguridad más reciente, ya sea activa o inactiva. Consulte el apartado Latest para obtener más información.

Tarea	Mandato	Consideraciones
Visualizar una lista de versiones de copia de seguridad activas e inactivas para seleccionar las versiones que se restaurarán.	<code>dsmc restore "/Users/monnett/ Documents/*" -pick - inactive</code>	Si intenta restaurar a la vez las versiones activa e inactiva de un archivo, sólo se restaurará la versión activa. Consulte los apartados Pick y Inactive para obtener más información.
Restaurar el archivo <code>/Users/monnett/Documents/h1.doc</code> a su directorio original.	<code>dsmc restore /Users/monnett/ Documents/h1. doc</code>	Si no especifica ningún destino, los archivos se restaurarán en su ubicación original.
Restaurar el archivo <code>/Users/monnett/Documents/h1.doc</code> bajo un nombre y directorio nuevos.	<code>dsmc restore /Users/monnett/ Documents/h1. doc /Users/gordon/ Documents/h2.d oc</code>	Ninguna
Restaurar los archivos del directorio <code>/Users</code> y todos sus subdirectorios.	<code>dsmc restore /Users/ - subdir=yes</code>	Si restaura una vía de acceso y un archivo específicos, IBM Spectrum Protect restaura de forma recursiva <i>todos</i> los subdirectorios de esa vía de acceso y todas las instancias del archivo especificado que haya en <i>cualquiera</i> de esos subdirectorios. Consulte el apartado Subdir para obtener más información sobre la opción <b>subdir</b> .
Restaurar todos los archivos del directorio <code>/Users/gordon/Documents</code> al estado en el que se encontraban a las 13:00 horas del día 17 de agosto de 2003.	<code>dsmc restore - pitd=8/17/2003 -pitt=13:00:00 /Users/gordon/ Documents/</code>	Consulte los apartados Pitdate y Pittime para obtener más información sobre las opciones pitdate y pittime.
Restaurar todos los archivos del directorio <code>/Users/mike/Documents</code> que terminen por <code>.bak</code> al directorio <code>/Users/mike/projectn/</code> .	<code>dsmc restore "/Users/mike/D ocuments/*.bak " /Users/mike/pr ojectn/</code>	si el destino es un directorio, especifique el delimitador ( <code>/</code> ) como el último carácter del destino. Si omite el delimitador y el origen especificado es un directorio o una especificación de archivo con un carácter comodín, recibirá un mensaje de error. Si el directorio <code>projectn</code> no existe, se creará.
Restaurar los archivos especificados en el archivo <code>restorelist.txt</code> en una ubicación distinta.	<code>dsmc restore - filelist=/User s/user2/Docume nts/ restorelist.tx t /Users/NewRest oreLocation/</code>	Consulte el apartado Filelist para obtener más información sobre la restauración de una lista de archivos.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Ejemplos: restauraciones mediante la línea de mandatos para grandes cantidades de datos  
Si debe restaurar un gran número de archivos, puede obtener un rendimiento más rápido si utiliza el mandato restore en lugar de la GUI. Además, puede mejorar el rendimiento especificando varios mandatos restore al mismo tiempo.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicializable  
En este tema se describen los procesos de restauración estándar (o clásica), de restauración sin consulta y de restauración reinicializable.

**Referencia relacionada:**

Restore

-  sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux
-  Sistemas operativos Oracle Solaris

## Ejemplos: restauraciones mediante la línea de mandatos para grandes cantidades de datos

Si debe restaurar un gran número de archivos, puede obtener un rendimiento más rápido si utiliza el mandato restore en lugar de la GUI. Además, puede mejorar el rendimiento especificando varios mandatos restore al mismo tiempo.

Por ejemplo, para restaurar todos los archivos del espacio de archivos /home, escriba:

```
dsmc restore /home/ -subdir=yes -replace=all -tapeprompt=no
```

Sin embargo, si especifica varios mandatos para los directorios del espacio de archivos /home, puede restaurar los archivos más rápidamente.

Por ejemplo, puede especificar estos mandatos:

```
dsmc restore /home/monnett/ -subdir=yes -replace=all -tapeprompt=no  
dsmc restore /home/gillis/ -subdir=yes -replace=all -tapeprompt=no  
dsmc restore /home/stewart/ -subdir=yes -replace=all -tapeprompt=no
```

También puede utilizar la opción quiet con el mandato restore para ahorrar tiempo de proceso. Sin embargo, no recibirá mensajes informativos para archivos individuales.

**Nota:** Si ya tiene el conjunto de valores apropiado para las opciones subdir, replace, tapeprompt y quiet en el archivo de opciones del usuario cliente, no es necesario que las incluya en los mandatos.

Cuando escriba múltiples mandatos para restaurar los archivos, debe especificar una parte exclusiva del espacio de archivos en cada mandato restore. Asegúrese de no utilizar ninguna especificación de archivo que se solape en los mandatos.

Para visualizar una lista de los directorios de un espacio de archivos, utilice el mandato query backup. Por ejemplo:

```
dsmc query backup -dirsonly -subdir=no /Users/
```

Como norma general, puede especificar de dos a cuatro mandatos restore al mismo tiempo. El número máximo que puede ejecutar a la vez sin disminuir el rendimiento depende de factores tales como la memoria disponible y la carga de trabajo de la red.

La velocidad a la cual puede restaurar los archivos también depende del número de unidades de cintas disponible en el servidor y de si el administrador está utilizando la función de proximidad para mantener los espacios de archivos asignados en tan pocos volúmenes como sea posible.













Por ejemplo, si /Users/user1 y /Users/user2 se encuentran en la misma cinta, la restauración para /Users/user2 deberá esperar hasta que se haya completado la restauración para /Users/user1. Sin embargo, si /Users/user3 se encuentra en una cinta distinta y existen, como mínimo, dos unidades de cinta disponibles, la restauración para /Users/user3 puede iniciarse al mismo tiempo que la restauración para /Users/user1.

Establezca en ilimitados (-1) los valores ulimit del sistema si han de restaurarse archivos muy grandes (2 GB) con HSM o con el cliente de copia de seguridad/archivado. El cliente puede restaurar estos archivos grandes con suficientes recursos del sistema. Si los valores de ulimit se establecen en valores más bajos, puede que se produzcan errores en la restauración.

## Restauración estándar de la consulta, sin restauración de la consulta y restauración reinicializable

---

En este tema se describen los procesos de restauración estándar (o clásica), de restauración sin consulta y de restauración reinicializable.

-     Sistemas operativos Oracle Solaris  
Proceso de restauración de consulta estándar  
El proceso de restauración de consulta estándar también se denomina restauración clásica. En este tema se explica cómo instalar los trabajos de restauración de consulta estándar.
-     Sistemas operativos Oracle Solaris  
Sin consulta de proceso de restauración  
En el proceso de restauración sin consulta, se envía una sola solicitud de restauración al servidor en lugar de consultar al servidor para cada objeto que se debe restaurar.
-     Sistemas operativos Oracle Solaris  
Proceso de restauración reinicializable  
Si el proceso de restauración se detiene debido a un corte de la alimentación o a una anomalía de la red, el servidor registra el punto en que se ha interrumpido la restauración.

## Proceso de restauración de consulta estándar

---

El proceso de restauración de consulta estándar también se denomina restauración clásica. En este tema se explica cómo instalar los trabajos de restauración de consulta estándar.


Los trabajos de restauración de consulta estándar funcionan de la siguiente manera:





- El cliente realiza una consulta al servidor para obtener una lista de los archivos de los que se ha hecho copia de seguridad correspondientes al espacio de archivos de cliente que desea restaurar.
- El servidor envía una lista de los archivos de los que se ha hecho copia de seguridad que coinciden con los criterios de la restauración. Si desea restaurar archivos activos e inactivos, el servidor envía información sobre todos los archivos de los que se ha hecho copia de seguridad al cliente.
- La lista de los archivos devuelta desde el servidor se clasifica en la memoria del cliente con el fin de determinar el orden de restauración de los archivos y minimizar el número de montajes de cintas necesarios para ejecutar la restauración.
- El cliente indica al servidor que restaure datos de archivo y objetos de directorio.
- Los directorios y archivos por restaurar se envían del servidor al cliente.


## Sin consulta de proceso de restauración

En el proceso de restauración sin consulta, se envía una sola solicitud de restauración al servidor en lugar de consultar al servidor para cada objeto que se debe restaurar.


1. El cliente indica al servidor que va a realizar una restauración sin consulta y le facilita los detalles sobre directorios, archivos y espacios de archivos.
2. El servidor utiliza una tabla independiente para realizar el seguimiento de entradas que guían la restauración.
3. Los datos por restaurar se envían al cliente. Los objetos de archivo y de directorio que se almacenan en el disco se envían inmediatamente, puesto que no es necesario clasificar dichos datos antes de restaurar el objeto.
4. Puede utilizar varias sesiones para restaurar los datos. Si los datos se encuentran en varias cintas, hay diversos puntos de montaje disponibles en el servidor. La combinación de la opción resourceutilization y MAXNUMMP permite el uso de varias sesiones.

 Sistemas operativos Windows Cuando proporcione una especificación de archivo de origen en el mandato restore y no especifique ninguna de las opciones: inactive, latest, pick, fromdate o todate, el cliente utiliza un método de *restauración sin consulta* para restaurar los archivos y los directorios desde el servidor. Este método se denomina restauración sin consulta ya que en lugar de realizar una consulta al servidor para cada objeto que se debe restaurar, se le envía una única solicitud de restauración. En este caso, el servidor devuelve los archivos y directorios al cliente sin que el cliente tenga que realizar ninguna acción adicional. Éste simplemente acepta los datos procedentes del servidor y los restaura en el destino especificado en el mandato restore.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Cuando proporcione una especificación de archivo de origen en el mandato restore y no especifique ninguna de las opciones: inactive, latest, pick, fromdate, todate, el cliente utiliza un método de *restauración sin consulta* para restaurar los archivos y los directorios desde el servidor. Este método se denomina restauración sin consulta ya que en lugar de realizar una consulta al servidor para cada objeto que se debe restaurar, se le envía una única solicitud de restauración. En este caso, el servidor devuelve los archivos y directorios al cliente sin que el cliente tenga que realizar ninguna acción adicional. Éste simplemente acepta los datos procedentes del servidor y los restaura en el destino especificado en el mandato restore.

 sistemas operativos Mac OS X Utilizando el cliente GUI de IBM Spectrum Protect, un ejemplo de un mandato con carácter comodín sin restricciones sería seleccionar una carpeta de la ventana del árbol de restauración. Un ejemplo de un mandato con carácter comodín con restricciones sería seleccionar archivos individuales de una carpeta.

Utilizando el cliente de línea de mandatos, un ejemplo de un mandato con carácter comodín sin restricciones:

 sistemas operativos Mac OS X

```
"/Users/user1/Documents/2004/*"
```


 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
/home/mydocs/2004/*
```

 Sistemas operativos Windows

```
c:\mydocs\2004\*
```

Un ejemplo de una especificación de archivo con carácter comodín con restricciones sería:

 sistemas operativos Mac OS X

```
/Users/user1/Documents/2004/sales.*
```

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris


```
/home/mydocs/2004/sales.*
```





## Proceso de restauración reiniciable

---






Si el proceso de restauración se detiene debido a un corte de la alimentación o a una anomalía de la red, el servidor registra el punto en que se ha interrumpido la restauración.

El cliente conoce este registro como *restauración reiniciable*. Se puede disponer de varias sesiones de restauración reiniciables. Utilice el mandato query restore o seleccione **restartable restores** en el menú Acciones para averiguar si su cliente tiene alguna sesión de restauración reiniciable en la base de datos del servidor.

 Sistemas operativos Windows Debe completar una restauración reiniciable antes de intentar llevar a cabo más copias de seguridad del sistema de archivos. Si intenta repetir la restauración interrumpida o realizar una copia de seguridad del espacio de archivos de destino, no lo logrará porque no ha concluido la restauración original. Para reiniciar la restauración en el punto en que se interrumpió, utilice el mandato restart restore; para suprimir la restauración reiniciable, utilice el mandato cancel restore. Si reinicia la restauración interrumpida, ésta se reinicia desde la primera transacción, que podría constar de uno o varios archivos, que no se había restaurado por completo en el momento de producirse la interrupción. Por este motivo, puede que reciba algunos mensajes que le preguntarán si han de sustituirse archivos de la transacción interrumpida cuya restauración ya se ha realizado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Debe completar una restauración reiniciable antes de intentar llevar a cabo más copias de seguridad del sistema de archivos. Si intenta repetir la restauración interrumpida o realizar una copia de seguridad del espacio de archivos de destino, no lo logrará porque no ha concluido la restauración original. Para reiniciar la restauración en el punto en que se interrumpió, utilice el mandato restart restore; para suprimir la restauración reiniciable, utilice el mandato cancel restore.

En el cuadro de diálogo **Restauraciones reiniciables** de la GUI de IBM Spectrum Protect, puede seleccionar y suprimir la restauración interrumpida o bien puede reiniciarla. Si reinicia la restauración interrumpida, ésta se reinicia desde la primera transacción, que podría constar de uno o varios archivos, que no se había restaurado por completo en el momento de producirse la interrupción. Por este motivo, puede que reciba algunos mensajes que le preguntarán si han de sustituirse archivos de la transacción interrumpida cuya restauración ya se ha realizado.


 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Para llevar a cabo restauraciones reiniciables mediante la GUI del cliente Web, siga los pasos siguientes:

1. Seleccione **Acciones**→ **Restauraciones reiniciables** en el panel inicial.
2. Seleccione la sesión de restauración reiniciable que desee llevar a cabo.
3. Pulse el botón **Reiniciar** de la parte superior del panel.

### Referencia relacionada:

Resourceutilization

Restore

 Sistemas operativos Oracle Solaris

## Restauración de sistemas de archivos ZFS de Solaris

---

Zettabyte File Systems (ZFS) utiliza las agrupaciones de almacenamiento para gestionar el almacenamiento físico.

La forma como se puede restaurar un sistema de archivos ZFS depende de cómo se haya realizado la copia de seguridad.

- Si se ha hecho la copia de seguridad de todos los archivos y carpetas como objetos separados, se pueden restaurar llevando a cabo una restauración a nivel de archivo. Por ejemplo:

```
dsmc restore /tank/myZFS/ -subdir=yes -replace=all
```

No efectúe una restauración a nivel de archivo en un escenario de recuperación tras desastre. Aunque pueda restaurar satisfactoriamente todos los archivos y carpetas de sistema a partir de una copia de seguridad creada con un cliente de archivado y copia de seguridad, es posible que el sistema restaurado sea inestable o genere un error.

- Si ha hecho la copia de seguridad de una instantánea ZFS completa como un solo archivo, tiene que restaurar el archivo de instantánea del servidor en una ubicación temporal. Por ejemplo:

```
dsmc restore /tmpdir/mySnapshotfile
```

A continuación, puede restaurar el sistema de archivos a partir del archivo de instantánea utilizando los mandatos de Oracle Solaris ZFS. Por ejemplo:

```
zfs receive tank/myZFS@mySnapshot < /tmpdir/mySnapshotFile
```

La ventaja de restaurar ZFS a partir de un archivo de instantánea es que se puede restaurar el sistema de archivos completo en un escenario de recuperación tras desastre.

Para obtener información detallada sobre cómo restaurar datos en sistemas de archivos ZFS, consulte la documentación de producto que está disponible en Oracle. Si va a restaurar una agrupación raíz ZFS, consulte los temas donde se describe cómo volver a crear la agrupación raíz y cómo recuperar instantáneas de agrupación raíz.

#### Tareas relacionadas:






















Realizar la copia de seguridad de sistemas de archivos Solaris Zettabyte






 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Tareas de restauración adicionales

---

En este apartado se indican algunas consideraciones avanzadas para la restauración de datos.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Cómo autorizar a otro usuario para que restaure o recupere archivos  
Puede autorizar a otro usuario de la misma estación de trabajo o de otra para que restaure versiones de copia de seguridad o recupere copias archivadas de los archivos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Restauración o recuperación de archivos de otro nodo cliente  
Después de que los usuarios concedan acceso a los archivos del servidor, puede restaurar o recuperar dichos archivos en el sistema local.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Restaurar o recuperar archivos en otra estación de trabajo  
Desde una estación de trabajo distinta, puede restaurar o recuperar archivos de los que ha realizado copia de seguridad anteriormente en su propia estación de trabajo. Debe conocer la contraseña de IBM Spectrum Protect asignada a su nodo.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Restauración de un disco en caso de pérdida del mismo  
Puede recuperar los archivos si puede ejecutar el cliente. Si el disco que contiene el cliente no se encuentra (porque ha sido robado o por un error en el hardware), debe reinstalar el cliente antes de poder recuperar los archivos. Si pierde el disco que contiene el sistema operativo y el software de comunicación, debe recuperarlos antes de conectarse al servidor IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Supresión de espacios de archivos  
Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor.
-  Sistemas operativos Linux  
Habilite SELinux para restaurar los archivos en el cliente de Red Hat Enterprise Linux 5  
Si es un usuario no root y está intentando restaurar archivos en el cliente Red Hat Enterprise Linux 5, en primer lugar debe activar SELinux.

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Cómo autorizar a otro usuario para que restaure o recupere archivos


---

Puede autorizar a otro usuario de la misma estación de trabajo o de otra para que restaure versiones de copia de seguridad o recupere copias archivadas de los archivos.

### Acerca de esta tarea

---

Esto permite compartir archivos con otras personas o con otras estaciones de trabajo que utilice con un nombre de nodo distinto. Para autorizar a un usuario de otra estación de trabajo para que restaure o recupere los archivos, la otra estación de trabajo debe ejecutarse en uno de los clientes UNIX y debe estar inscrita en el servidor.

 sistemas operativos Mac OS X Nota: Mac OS X *sólo* puede restaurar nodos Mac OS X.

Para autorizar a otro usuario para que restaure o recupere los archivos:

### Procedimiento

---

1. Pulse **Herramientas** → **Lista de acceso al nodo** en la ventana principal. Aparece la ventana Lista de acceso al nodo.
2. Pulse el botón **Agregar**. Aparece la ventana Agregar regla de acceso.



3. En la ventana Agregar regla de acceso, seleccione un elemento en el campo Permitir acceso a para especificar el tipo de datos al que el otro usuario puede acceder. Puede seleccionar Objetos en copia de seguridad o bien Objetos archivados.
4. En el campo Otorgar acceso a nodo, escriba el nombre del nodo de la estación de trabajo host del usuario que puede acceder a sus datos.
5. En el campo Usuario, escriba el nombre del usuario de un nodo que puede acceder a sus datos.
6. En el campo Espacio de archivos y directorio, seleccione el espacio de archivos y el directorio al que el usuario puede acceder. No puede seleccionar más de un espacio de archivos y un directorio al mismo tiempo. Si desea dar al usuario acceso a otro espacio de archivos y otro directorio, debe crear otra regla de acceso.
7. Si desea limitar el acceso del usuario a determinados archivos del directorio, escriba en el campo Nombre de archivo el nombre completo o el tipo de los archivos del servidor a los que el otro usuario puede acceder. El campo Nombre de archivo sólo acepta una entrada. Puede ser un único nombre de archivo o un nombre de archivo con caracteres comodín que corresponda a uno o varios archivos. Puede utilizar un carácter comodín como parte del patrón. La entrada debe coincidir con archivos que se hayan almacenado en el servidor.
8. Para la GUI Java™: si desea dar acceso a todos los archivos del directorio seleccionado que coinciden con la especificación de nombre de archivo, incluidos los archivos de los subdirectorios, pulse **Incluir subdirectorios**.
9. Pulse el botón **Aceptar** para guardar la regla de acceso y cerrar la ventana Agregar regla de acceso.
10. La regla de acceso que ha creado se muestra en el cuadro de lista de la ventana Lista de acceso al nodo. Cuando ya no necesite la ventana Lista de acceso al nodo, pulse el botón **Aceptar**. Si no desea guardar los cambios, pulse **Cancelar** o cierre la ventana.

## Resultados

---

En la interfaz de línea de mandatos, utilice el mandato set access para autorizar otro nodo para restaurar o recuperar los archivos. También puede utilizar el mandato query access para ver la lista actual y delete access para suprimir nodos de la lista.

### Referencia relacionada:

Delete Access

Query Access

Set Access

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Restauración o recuperación de archivos de otro nodo cliente

---

Después de que los usuarios concedan acceso a los archivos del servidor, puede restaurar o recuperar dichos archivos en el sistema local.

## Acerca de esta tarea

---

Puede mostrar espacios de archivos de otro usuario en el servidor, restaurar las versiones de copia de seguridad de otro usuario o recuperar las copias de archivado de otro usuario en el sistema de archivos local:

## Procedimiento

---

1. Pulse **Herramientas** en la ventana principal.
2. Pulse **Acceder a otro nodo**. Aparecerá la ventana Acceder a otro nodo.
3. Escriba el nombre de nodo de la estación de trabajo host en el campo Nombre de nodo. Escriba el nombre del usuario en el campo Nombre usuario.
4. Pulse el botón **Establecer**.

## Resultados

---

Si está utilizando mandatos, utilice las opciones fromnode y fromowner para indicar el nombre del nodo y el nombre del usuario propietario de los archivos.

Por ejemplo, para restaurar archivos en uno de sus propios sistemas de archivos de los que se hizo copia de seguridad en una estación de trabajo denominada `Node1` y propiedad de un usuario cuyo nombre es `Ann`, escriba:

```
dsmc restore -fromn=node1 -fromo=ann "/home/proj/*" /home/gillis/
```

Utilice el mandato query filesystem para obtener una lista de los espacios de archivos. Por ejemplo, para obtener una lista de espacios de archivos propiedad de `Ann` en `Node1`, escriba:

```
dsmc query filesystem -fromn=node1 -fromo=ann
```





### Referencia relacionada:


Fromnode

Query Filespace

Restore

Retrieve

 sistemas operativos Mac OS X  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux

 Sistemas operativos Oracle Solaris

## Restaurar o recuperar archivos en otra estación de trabajo

---

Desde una estación de trabajo distinta, puede restaurar o recuperar archivos de los que ha realizado copia de seguridad anteriormente en su propia estación de trabajo. Debe conocer la contraseña de IBM Spectrum Protect asignada a su nodo.

Para restaurar o recuperar archivos en otra estación de trabajo, utilice la opción `virtualnodename` para especificar el nombre de nodo de la estación de trabajo desde donde se realizó la copia de seguridad de los archivos. La opción `virtualnodename` no puede establecerse en el nombre del host de la estación de trabajo. Puede utilizar la opción `virtualnodename` al iniciar IBM Spectrum Protect o bien puede agregar la opción `virtualnodename` al archivo de opciones del usuario cliente `dsm.opt`. Utilice la opción `virtualnodename` en el mandato **dsmj** si está utilizando la estación de trabajo de otro usuario y no desea actualizar su archivo de opciones del usuario cliente.

IBM Spectrum Protect solicitará la contraseña de su nodo original. Una vez haya escrito la contraseña correcta, todos los sistemas de archivos de su estación de trabajo original aparecerán en la ventana Restaurar o Recuperar. Podrá restaurar o recuperar archivos como si estuviera trabajando en su propia estación de trabajo.

**Importante:** cuando utilice este método para acceder a archivos, tendrá acceso a todos los archivos con copia de seguridad y copias archivadas de su estación de trabajo. Se le considerará un usuario root virtual.

Puede utilizar la opción `virtualnodename` en un mandato. Por ejemplo, para restaurar los archivos de **projx**, escriba:

```
dsmc restore -virtualnodename=nodeone "/home/monnett/projx/*"
```

Si no desea restaurar o recuperar los archivos en el mismo nombre de directorio de la estación de trabajo alternativa, escriba un destino distinto.

Las consideraciones para la recuperación de archivos son las mismas que las de restauración.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Restauración de un disco en caso de pérdida del mismo

---

Puede recuperar los archivos si puede ejecutar el cliente. Si el disco que contiene el cliente no se encuentra (porque ha sido robado o por un error en el hardware), debe reinstalar el cliente antes de poder recuperar los archivos. Si pierde el disco que contiene el sistema operativo y el software de comunicación, debe recuperarlos antes de conectarse al servidor IBM Spectrum Protect.

### Acerca de esta tarea

---

Para protegerse ante estas clases de pérdidas, debe agrupar un conjunto de medios de instalación que pueda utilizar para restaurar el sistema en un estado que le permita conectarse al servidor y empezar a recuperar datos. Los medios de instalación deben contener:

### Procedimiento

---

1. Un sistema operativo iniciable que permita realizar funciones básicas.
2. Un programa de comunicaciones configurado correctamente que permita establecer comunicaciones con el servidor.
3. Un cliente con archivos de opciones personalizadas apropiadas. Puede utilizar la interfaz de línea de mandatos del cliente para completar esta tarea.

### Resultados

---

El paquete de comunicación que utilice determina los archivos que necesita. Consulte los manuales del sistema operativo y el software de comunicación para configurar los medios de instalación.

Si también tiene instalado IBM Spectrum Protect for Space Management en la estación de trabajo, el soporte de instalación debe incluir el cliente de línea de mandatos de HSM.

Nota: El administrador puede planificar operaciones de restauración que pueden resultar muy útiles cuando necesita restaurar un número elevado de archivos.

**Conceptos relacionados:**

## Supresión de espacios de archivos

---

Si el administrador de IBM Spectrum Protect le concede autorización, puede suprimir espacios de archivos completos del servidor.

### Acerca de esta tarea

---

Cuando se suprime un espacio de archivos, está suprimiendo todos los archivos y las imágenes, tanto las versiones de copia de seguridad como las de copias archivadas que hay en ese espacio de archivos. Por ejemplo, si suprime el espacio de archivos del sistema de archivos `/home/monnet`, está suprimiendo todas las copias de seguridad de todos los archivos de ese sistema de archivos y de cada archivo que archivó en el mismo. **Considere detenidamente si desea suprimir un espacio de archivos.** Debe ser un usuario autorizado para poder realizar esta tarea.

Puede suprimir las versiones individuales de copia de seguridad utilizando el mandato `delete backup`.

Puede suprimir espacios de archivos mediante la GUI de cliente de copia de seguridad y archivado o la interfaz de línea de mandatos del cliente. Para suprimir espacios de fila NAS, utilice el cliente web o la interfaz de línea de mandatos.

Para suprimir un espacio de archivos mediante la GUI, siga estos pasos:

### Procedimiento

---

1. Seleccione **Herramientas** → **Suprimir espacios de archivos** en la ventana principal.
2. Pulse en las casillas que se encuentran junto a los espacios de archivos que desea eliminar.
3. Pulse el botón **Suprimir**. El cliente le pedirá una confirmación antes de eliminarlos.

### Resultados

---

También puede suprimir un espacio de archivos con el mandato `delete fileSPACE`. Utilice la opción **class** con el mandato `delete fileSPACE` para suprimir espacios de archivos NAS.

#### Referencia relacionada:

Class

Delete Backup

Delete Filespace

 Sistemas operativos Linux

## Habilite SELinux para restaurar los archivos en el cliente de Red Hat Enterprise Linux 5

---

Si es un usuario no root y está intentando restaurar archivos en el cliente Red Hat Enterprise Linux 5, en primer lugar debe activar SELinux.

Si no activa SELinux, tendrá problemas si restaura los archivos que se han modificado en los atributos ampliados.

## Archivar y recuperar datos con clientes de archivado y copia de seguridad


---





Si desea guardar una copia de un archivo en un almacenamiento a largo plazo en el servidor de IBM Spectrum Protect utilice la función *archive*.

### Acerca de esta tarea


---

Si en alguna ocasión se daña o se pierde el archivo original, utilice la función *restaurar* para recuperar la versión de copia de seguridad del servidor.

-  Sistemas operativos Windows Archivar y recuperar datos (Windows)  
Puede archivar los archivos que se utilizan con poca frecuencia en el servidor de IBM Spectrum Protect y recuperarlos cuando los necesite. Archivar y recuperar archivos es similar a realizar una copia de seguridad y restaurar archivos.

-  sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
 Archivar y recuperar datos (UNIX y Linux)
 

Puede archivar los archivos que se utilizan con poca frecuencia en el servidor de IBM Spectrum Protect y recuperarlos cuando los necesite. Archivar y recuperar archivos es similar a realizar una copia de seguridad y restaurar archivos. Muchas de las ventanas y conceptos son similares.

 Sistemas operativos Windows

## Archivar y recuperar datos (Windows)

---


Puede archivar los archivos que se utilizan con poca frecuencia en el servidor de IBM Spectrum Protect y recuperarlos cuando los necesite. Archivar y recuperar archivos es similar a realizar una copia de seguridad y restaurar archivos.


A menos que se indique lo contrario, las referencias a Windows se aplican a todos los sistemas operativos Windows.

Todos los procedimientos primarios de archivado y recuperación se aplican también al cliente web, excepto las funciones siguientes:

- Editor de preferencias
- Asistente para la instalación

Puede completar las siguientes tareas primarias de archivado y recuperación.

- Archivado de datos con la GUI
- Ejemplos de archivado de datos utilizando la línea de mandatos
- Supresión de datos archivados
- Recuperación de archivos con la GUI
- Recupere las copias de archivado mediante la línea de mandatos
-  Sistemas operativos Windows Copias de archivado
 

Para archivar los archivos, seleccione los archivos que desea archivar. Puede seleccionar los archivos por nombre o descripción o seleccionarlos desde un árbol de directorios.
-  Sistemas operativos Windows Recuperar archivos
 

Seleccione la función Recuperar para recuperar una copia archivada de un archivo o directorio.

### Conceptos relacionados:

Cuándo realizar copias de seguridad y cuándo archivar copias

### Tareas relacionadas:

Inicio de una sesión de cliente web

 Sistemas operativos Windows

## Copias de archivado

---

Para archivar los archivos, seleccione los archivos que desea archivar. Puede seleccionar los archivos por nombre o descripción o seleccionarlos desde un árbol de directorios.

Es posible que el administrador establezca planificaciones para archivar automáticamente determinados archivos de la estación de trabajo. En los apartados siguientes se indica cómo archivar copias sin utilizar una planificación.


Debe asignar una descripción de archivado para todos los archivos de archivado. Una descripción de archivo identifica los datos mediante una descripción significativa que se puede utilizar más tarde para identificar los archivos y directorios. Puede entrar hasta 254 caracteres para describir sus datos archivados. Si no especifica una descripción, se asignará la siguiente descripción de archivo predeterminada:

```
Archive Date: mm/dd/yyyy
```





siendo mm/dd/yyyy la fecha actual.

Cuando selecciona una función de archivado de la GUI del cliente de archivado y copia de seguridad, se muestra una lista con la GUI del cliente de archivado y copia de seguridad y todas las descripciones de archivado utilizadas anteriormente. Estas descripciones de archivado pueden asignarse en posteriores operaciones de archivado.


La copia de seguridad incremental puede recuperar los archivos migrados, mientras que la copia de seguridad/archivado selectiva siempre recupera los archivos migrados si no se utiliza la opción skipmigrated.

-  Sistemas operativos Windows Copia de seguridad o archivo de instantáneas con soporte de archivos abiertos
 

Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).


-  **Sistemas operativos Windows** Archivado de datos con la GUI  
Puede archivar copias específicos o directorios completos de un árbol de directorios. También puede asignar una descripción exclusiva a cada grupo de archivos que archive (paquete de archivado).
-  **Sistemas operativos Windows** Ejemplos de archivado de datos utilizando la línea de mandatos  
Puede archivar datos cuando desee conservar copias de archivos en su estado actual, ya sea para utilizarlos más adelante, ya sea con fines históricos o legales.
-  **Sistemas operativos Windows** Archivado de datos mediante el proxy de nodo cliente  
El archivado de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.
-  **Sistemas operativos Windows** Supresión de datos archivados  
Puede eliminar los objetos de archivado individuales desde el servidor de IBM Spectrum Protect, sin tener que suprimir el espacio de archivos completos al que pertenecen.

**Conceptos relacionados:**

 **Sistemas operativos Windows** Opciones para la copia de seguridad de archivos migrados: skipmigrated, checkreparsecontent, stagingdirectory

**Tareas relacionadas:**

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

 **Sistemas operativos Windows**

## Copia de seguridad o archivo de instantáneas con soporte de archivos abiertos

---

Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).

La instantánea permite realizar el archivado de una copia de instante específico que coincida con el sistema de archivos en el momento en que se toma la instantánea. Los cambios que se realicen posteriormente en el sistema de archivos no se incluirán en la operación de archivado. Puede establecer el parámetro snapshotproviderfs de la opción include.fs en none para especificar qué unidades no utilizan el soporte de archivos abiertos.

Nota:

1. Puede utilizar la opción include.fs para establecer opciones de instantánea para cada sistema de archivos.
2. El soporte de archivos abiertos solo se admite en volúmenes fijos locales, (montados en letras de unidad o en puntos de montaje de volúmenes) con formato de sistemas de archivos FAT, FAT32, NTFS o ReFS. Este soporte incluye los volúmenes conectados con la SAN que satisfacen estos requisitos.
3. Si el cliente no puede crear una instantánea, se recurre a una copia de seguridad que no es OFS; se llevaría a cabo el mismo soporte de copia de seguridad si la característica OFS no estuviera instalada.
4. Para activar el soporte de archivos abiertos en un entorno de clúster, la característica OFS debe estar configurada en todas las estaciones de trabajo del clúster.
5. Cuando se utiliza la función de soporte de archivos abiertos con VSS, el cliente agrega el nombre de volumen de instantánea a la vía de acceso de los objetos que se están procesando. El nombre del volumen de instantánea puede tener un máximo de 1024 bytes. La vía de acceso completa (el nombre del volumen de instantánea más la vía de acceso del objeto) puede ser de 8192 bytes o menos.


Para obtener información sobre restricciones y problemas del soporte de archivos abiertos, busque *TSM Client Open File Support (OFS)* en el sitio web de soporte de IBM®.

**Conceptos relacionados:**

Opciones de proceso

**Tareas relacionadas:**

Configuración del soporte de archivos abiertos

 **Sistemas operativos Windows**

## Archivado de datos con la GUI

---

Puede archivar copias específicos o directorios completos de un árbol de directorios. También puede asignar una descripción exclusiva a cada grupo de archivos que archive (paquete de archivado).


### Acerca de esta tarea

---

Para archivar los archivos, siga estos pasos:

## Procedimiento

1. Pulse en Archive en la GUI de la ventana principal. Aparece la ventana Archive.
2. Expanda el árbol de directorios pulsando el signo más (+) o en un icono de carpeta del árbol. Para buscar o filtrar los archivos, pulse en el icono Search desde la barra de herramientas.
3. Escribir una descripción, aceptar la descripción predeterminada o seleccionar una descripción existente para el paquete de archivado en el campo Description.
4. Para modificar opciones de archivado específicas, pulse en Options. Cualquier opción que se cambie solo es efectiva durante la sesión actual.
5. Pulse en Archive. La ventana Archive Status muestra el progreso de la operación de archivado.

 Sistemas operativos Windows

## Ejemplos de archivado de datos utilizando la línea de mandatos

Puede archivar datos cuando desee conservar copias de archivos en su estado actual, ya sea para utilizarlos más adelante, ya sea con fines históricos o legales.


Puede archivar un archivo, un grupo de archivos o todos los archivos en un directorio o subdirectorío. Después de archivar un archivo, puede suprimir el archivo original de la estación de trabajo. Utilice el mandato archive para archivar copias.

En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato archive para archivar objetos.

Tabla 1. Ejemplos de archivado desde la línea de mandatos

Tarea	Mandato	Consideraciones
Realizar el archivado de todos los archivos en el directorio <code>c:\plan\proj1</code> que tienen la extensión de archivo <code>.txt</code> .	<code>dsmc archive c:\plan\proj1\*.txt</code>	Utilice caracteres comodín para archivar más de un archivo a la vez.
Archivar todos los archivos del directorio <code>c:\small\testdir</code> y borrarlos de la estación de trabajo.	<code>dsmc archive c:\small\testdir\* -deletefiles</code>	Recupere las copias archivadas en la estación de trabajo siempre que las necesite de nuevo. Para obtener más información sobre la opción <code>deletefiles</code> , consulte el apartado <code>Deletefiles</code> .
Archivar el archivo <code>c:\proj1\h1.doc</code> y el archivo <code>c:\proj2\h2.doc</code>	<code>dsmc archive c:\proj1\h1.doc c:\proj2\h2.doc</code>	Puede especificar tantos archivos para archivar como lo permitan los recursos disponibles u otros límites del sistema operativo. Separe los archivos para archivar con un espacio. Para obtener más información sobre la opción <code>filelist</code> , consulte el apartado <code>Filelist</code> .
Archivar una lista de archivos en el archivo <code>c:\filelist.txt</code> .	<code>dsmc archive -filelist=c:\filelist.txt</code>	Utilice la opción <code>filelist</code> para procesar una lista de archivos. Para obtener más información sobre la opción <code>filelist</code> , consulte el apartado <code>Filelist</code> .
Archivar el archivo <code>a:\ch1.doc</code> y asignar una descripción a la copia archivada.	<code>dsmc archive a:\ch1.doc -description="Chapter 1, first version"</code>	Si no especifica una descripción con el mandato <code>archive</code> , el valor predeterminado es <code>Archive Date:x</code> , donde <code>x</code> es la fecha del sistema actual. Para obtener más información sobre la opción <code>description</code> , consulte el apartado <code>Descripción</code> .
Archivar todos los archivos del directorio <code>d:\proj</code> y sus subdirectorios.	<code>dsmc archive d:\proj\ -subdir=yes</code>	Para obtener más información sobre la opción <code>subdir</code> , consulte el apartado <code>Subdir</code> .

Tarea	Mandato	Consideraciones
Utilizar la opción v2archive con el mandato archive para archivar sólo los archivos del directorio c:\relx\dir1.	<code>dsmc archive c:\relx\dir1\ -v2archive</code>	IBM Spectrum Protect archiva sólo las copias del directorio c:\relx\dir1. Los directorios que haya en la vía de acceso no se procesarán. Para obtener más información sobre la opción v2archive, consulte el apartado V2archive.
Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.	<code>dsmc archive -archmc=RET2YRS c:\plan\proj1\ budget.jan\*</code>	Para obtener más información sobre la opción archmc, consulte el apartado Archmc. Para obtener más información acerca de las clases de gestión, consulte el apartado Políticas de gestión de almacenamiento.
Supongamos que inició una instantánea de la unidad C:\ y montó la instantánea como volumen lógico \\florence\c\$\snapshots\ snapshot.0. Archive el árbol del directorio c:\dir1\sub1 desde la instantánea local y gestiónela en el servidor de IBM Spectrum Protect en el nombre de espacio de archivos C:\.	<code>dsmc archive c:\dir1\sub1\* -subdir=yes -snapshotroot=\\florence\c\$\snapshots\ snapshot.0</code>	Para obtener más información, consulte Snapshotroot.

-  Sistemas operativos Windows Asociar una instantánea local con un espacio de archivos del servidor (Windows)  
 Puede asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

#### Referencia relacionada:

Archive

 Sistemas operativos Windows

## Archivado de datos mediante el proxy de nodo cliente

El archivado de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

### Acerca de esta tarea

Esta opción es útil cuando es posible que la estación de trabajo encargada de realizar el archivado cambie con el tiempo, como ocurre con un clúster. La opción asnodename también permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad. Utilice la opción asnodename con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor de IBM Spectrum Protect.

También se realiza una copia de seguridad de los clientes Tivoli Storage Manager FastBack mediante el proxy de nodo de cliente.

Si desea activar esta opción, realice estos pasos:

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
2. Registre cada nodo con el servidor de IBM Spectrum Protect, si éste no existe. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.
3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Éste es el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenan con el nombre de nodo cuando se utiliza la opción asnodename.
4. El administrador de IBM Spectrum Protect debe otorgar la autorización de proxy a todos los nodos del entorno compartido para acceder al nombre de nodo de destino en el servidor de IBM Spectrum Protect, mediante el uso del mandato GRANT PROXYNODE.
5. Utilice el mandato de cliente de administración QUERY PROXYNODE para visualizar los nodos de cliente del usuario autorizado, otorgados mediante el mandato GRANT PROXYNODE.

Efectúe estos pasos para configurar el cifrado con la opción encryptkey=save:

### Procedimiento

1. Especifique encryptkey=save en el archivo de opciones.

2. Realice la copia de seguridad de un archivo como mínimo con `asnode=ProxyNodeName` para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

## Resultados

---

Efectúe estos pasos para configurar el cifrado con la opción `encryptkey=prompt`:

1. Especifique `encryptkey=prompt` en el archivo de opciones.
  2. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.
- Si cambia la clave de cifrado, deberá repetir los pasos anteriores.
  - Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

Realice estos pasos para habilitar el funcionamiento de varios nodos desde la GUI:

1. Compruebe que el nodo de cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) utilizando el mandato de cliente de administración `QUERY PROXYNODE`.
2. Seleccione `Edit > Preferences` para abrir la ventana de preferencias.
3. Seleccione la ficha `General` y rellene el campo `Como nombre de nodo` con el nombre de nodo de destino con autorización de proxy.
4. Pulse `Aplicar` y, a continuación, `Aceptar` para cerrar la ventana de preferencias.

Realice estos pasos para comprobar que el nodo cliente acceda ahora al servidor como nodo de destino:

1. Abra la ventana de árbol y compruebe que aparece el nombre de nodo de destino especificado por el campo `Como nombre de nodo`, o
2. Compruebe el nombre de nodo de destino del campo `Acceder como nodo` de la ventana `Información de conexión`.

Para volver a la operación de nodo único, suprima `Como nombre de nodo` del campo `Acceso como nodo` en la pestaña `General > Preferencias`.


### Consideraciones para una sesión proxy:

- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- Todos los nodos agente del entorno de varios nodos deberían ser del mismo tipo de plataforma.
- No utilice los nodos de destino como nodos tradicionales. Utilícelos únicamente para el proceso de varios nodos.
- no se puede llevar a cabo una copia de seguridad o restauración de objetos del sistema o del estado del sistema.
- No puede acceder a otro nodo (ni desde el menú desplegable de la GUI ni utilizando la opción `fromnode`).
- No se puede utilizar la opción `clusternode`.
- No se puede llevar a cabo una copia de seguridad o una restauración de NAS.

### Referencia relacionada:

Asnodename

Valores de sesión y planificaciones de una operación de proxy

 Sistemas operativos Windows

## Supresión de datos archivados

---

Puede eliminar los objetos de archivado individuales desde el servidor de IBM Spectrum Protect, sin tener que suprimir el espacio de archivos completos al que pertenecen.

### Antes de empezar

---

El administrador de IBM Spectrum Protect debe concederle los permisos para suprimir los objetos archivados. Para determinar si tiene estos permisos, seleccione `File > Información de conexión` desde la GUI del cliente de copia de seguridad y archivado o desde el menú principal del cliente web. La autoridad del estado de supresión de archivado aparece en el campo `Delete Archive Files`. Si este campo muestra `No`, no puede suprimir los objetos archivados de no ser que el administrador le conceda los permisos para hacerlo.

### Procedimiento

---

Para suprimir un objeto archivado desde el servidor, lleve a cabo estos pasos en la GUI o en el cliente web. Como una alternativa a utilizar la GUI o el cliente web, puede suprimir los objetos archivados desde la línea de mandatos mediante el mandato `delete archive`.



1. Seleccione Suprimir datos archivados en el menú Herramientas.
2. En la ventana Archive Delete, expanda el árbol del directorio pulsando en el signo más (+) o en el icono de la carpeta que está al lado del objeto que desea expandir. Los objetos del árbol están agrupados según la descripción del paquete de archivado.
3. Seleccione los objetos archivados que desea suprimir.
4. Pulse Suprimir. El cliente le solicitará que confirme antes de comenzar a suprimir los objetos seleccionados. La ventana Archive Delete Task List muestra el progreso de la operación de supresión.

**Referencia relacionada:**

Delete Archive

 Sistemas operativos Windows

## Recuperar archivos



---

Seleccione la función Recuperar para recuperar una copia archivada de un archivo o directorio.

Nota: Cuando se recupera un directorio, la fecha y la hora de modificación de éste se establecen en la fecha y la hora de la recuperación, no en la fecha y la hora que tenía el directorio cuando se realizó la copia archivada de éste. Esto es así porque primero recupera los directorios y luego añade archivos a dichos directorios.

También se pueden recuperar copias archivadas del árbol de directorios en el árbol de directorios, filtrar el árbol de directorios y recuperar copias archivadas de archivos en propiedad de otro usuario. Para realizar cualquiera de estas acciones, pulse Recuperar en la ventana principal de la GUI del cliente de copia de seguridad y archivado y siga las instrucciones que se proporcionan en la ayuda para tareas de la GUI.

Importante: Cuando recupera un archivo sin especificaciones y existe más de una versión de la copia archivada en el servidor, se recuperan todas las copias. Una vez recuperada la primera copia, se recupera la segunda. Si existe una copia en la estación de trabajo cliente, se le solicitará que la sustituya, la omita o cancele.

-  Sistemas operativos Windows Recuperación de archivos con la GUI  
Puede recuperar los archivos archivados con la GUI del cliente de copia de seguridad y archivado.
-  Sistemas operativos Windows Recupere las copias de archivado mediante la línea de mandatos  
Recupere un archivo cuando desee devolver una copia archivada del servidor a la estación de trabajo. Se muestran algunos ejemplos sobre cómo recuperar los archivos de archivado mediante la línea de mandatos.

**Conceptos relacionados:**

Nombres de archivos duplicados

 Sistemas operativos Windows

## Recuperación de archivos con la GUI

---

Puede recuperar los archivos archivados con la GUI del cliente de copia de seguridad y archivado.

### Procedimiento

---

1. Pulse Retrieve en la GUI de la ventana principal. Aparece la ventana Retrieve.
2. Expanda el árbol de directorios pulsando el signo más (+) o el icono de carpeta junto a un objeto que desee expandir. Para buscar o filtrar los archivos, pulse en el icono Search desde la barra de herramientas.
3. Escriba el criterio de búsqueda en la ventana Find Files.
4. Pulse Search. Aparece la ventana Matching Files.
5. Pulse las casillas de selección de los archivos que desea recuperar y cerrar la ventana Matching Files.
6. Escriba el criterio de filtrado en la ventana Find Files.
7. Pulse Filter. La ventana Retrieve muestra los archivos filtrados.
8. Pulse las casillas de selección de los archivos filtrados o directorios que desea recuperar.
9. Para modificar o recuperar opciones específicas, pulse Options. Cualquier opción que cambie será eficaz solo durante la sesión actual.
10. Pulse Retrieve. Aparece la ventana Retrieve Destination. Puede recuperar archivos en un directorio o una unidad distintos de aquellos en los que se archivaron originalmente. También puede seleccionar qué cantidad de la estructura del directorio padre se recrea en la ubicación de recuperación.
11. Pulse Retrieve. La ventana Retrieve Status muestra el estado de proceso.

 Sistemas operativos Windows

## Recupere las copias de archivado mediante la línea de mandatos

---

Recupere un archivo cuando desee devolver una copia archivada del servidor a la estación de trabajo. Se muestran algunos ejemplos sobre cómo recuperar los archivos de archivado mediante la línea de mandatos.

Puede recuperar un archivo, un grupo de archivos o todos los archivos de un directorio o subdirectorio. Cuando recupere un archivo, el servidor de IBM Spectrum Protect le enviará una copia del mismo. La copia archivada permanece en el almacenamiento.





Utilice el mandato retrieve para recuperar archivos. En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato retrieve.

Tabla 1. Ejemplos de recuperación de archivos desde la línea de mandatos

Tarea	Mandato	Consideraciones
Recuperar el archivo c:\doc\h2.doc en su directorio original.	<code>dsmc retrieve c:\doc\h2.doc</code>	Si no especifica un destino, los archivos se recuperan en su ubicación original.
Recuperar el archivo c:\doc\h2.doc con un nuevo nombre y directorio.	<code>dsmc retrieve c:\doc\h2.doc c:\proj2\h3.doc</code>	Ninguna
Recuperación de todos los archivos archivados con una descripción específica en un directorio denominado retr1 en la ubicación nueva	<code>dsmc retrieve c:\* d:\retr1\ -sub=yes -desc="Mi primera copia archivada"</code>	Ninguna
Recuperar todos los archivos del directorio c:\projecta que finalizan con los caracteres .bak en el directorio c:\projectn.	<code>dsmc retrieve c:\projecta\*.bak c:\projectn</code>	Ninguna
Utilizar la opción pick para ver una lista de copias archivadas en la que puede seleccionar los archivos que desea recuperar.	<code>dsmc retrieve c:\project\* -pick</code>	Para obtener más información sobre la opción pick, consulte Pick.
Recuperación un archivo que originalmente estaba archivado desde un disquete con la etiqueta <i>workathome</i> en la unidad a:, a un disquete en la unidad a: etiquetado como <i>extra</i> .	<code>dsmc retrieve {workathome}\doc\h2.doc a:\doc\h2.doc</code>	Si está recuperando un archivo en un disco que tiene una etiqueta distinta a la del disco desde donde se archivó, utilice el nombre del espacio de archivos (etiqueta) del disco de archivado en vez de la letra de la unidad.
Recuperación de un archivo c:\doc\h2.doc a su directorio original en la estación de trabajo, denominado <i>star</i> .	<code>dsmc retrieve c:\doc\h2.doc \\star\c\$\doc\h2.doc</code> Para recuperar el archivo a <i>star</i> , que se renombró <i>meteor</i> , escriba: <code>dsmc retrieve \\star\c\$\doc\h2.doc \\meteor\c\$\doc\h2.doc</code> También puede escribir: <code>dsmc retrieve \\star\c\$\doc\h2.doc c:\</code> Este ejemplo resulta válido, ya que si el nombre de la estación de trabajo no está incluido en la especificación, se presupone el nombre de la estación de trabajo local ( <i>meteor</i> , en este caso).	En este manual, el nombre de la estación de trabajo forma parte del nombre de archivo. Por lo tanto, si se realizan copias archivadas en una estación de trabajo y se desea recuperarlas en otra estación de trabajo, debe especificarse un destino. Este requisito sucede incluso en el caso de que se recuperen los archivos en la misma estación de trabajo física, pero ésta tiene un nuevo nombre.

**Referencia relacionada:**

Retrieve

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris









## Archivar y recuperar datos (UNIX y Linux)

---

Puede archivar los archivos que se utilizan con poca frecuencia en el servidor de IBM Spectrum Protect y recuperarlos cuando los necesite. Archivar y recuperar archivos es similar a realizar una copia de seguridad y restaurar archivos. Muchas de las ventanas y conceptos son similares.

Todos los procedimientos primarios de archivado y recuperación que aparecen en este tema se aplican también al cliente web, excepto los procedimientos del Editor de preferencias.

Puede completar las siguientes tareas primarias de archivado y recuperación.

- Archivado de datos con la GUI
- Ejemplos de archivado de datos utilizando la línea de mandatos
- Supresión de datos archivados
- Recuperación de datos con la GUI
- Recupere los ejemplos de datos utilizando la línea de mandatos
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Copias de archivado  
Para archivar copias, debe seleccionar los archivos específicos que desea archivar. Puede seleccionar los archivos mediante una especificación de archivos o seleccionándolos en el árbol de directorios.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Recuperar archivos  
Recupere un archivo cuando desee devolver una copia archivada del servidor a la estación de trabajo.

### Conceptos relacionados:

Copia de seguridad de los datos

### Tareas relacionadas:

Inicio de una sesión de cliente web





















 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Copias de archivado

---

Para archivar copias, debe seleccionar los archivos específicos que desea archivar. Puede seleccionar los archivos mediante una especificación de archivos o seleccionándolos en el árbol de directorios.

Es posible que el administrador establezca planificaciones para archivar determinados archivos de la estación de trabajo automáticamente. En los apartados siguientes se indica cómo archivar copias sin utilizar una planificación.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Archivado de datos con la GUI  
Puede archivar un archivo a un grupo de archivos utilizando los nombres de archivo. Puede seleccionar los archivos que coinciden con el criterio de búsqueda utilizando un árbol de directorio.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Ejemplos de archivado de datos utilizando la línea de mandatos  
Puede solicitar servicios de archivado cuando desee conservar copias de archivos en su estado actual, ya sea para utilizarlos más adelante, ya sea para fines históricos o legales. Se muestran ejemplos de archivado de datos mediante la línea de mandatos.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Archivado de datos mediante el proxy de nodo cliente  
El archivado de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Supresión de datos archivados  
Puede eliminar los objetos de archivado individuales desde el servidor de IBM Spectrum Protect, sin tener que suprimir el espacio de archivos completos al que pertenecen.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Tareas de archivado avanzadas  
Los permisos de acceso, los enlaces simbólicos y los enlaces fijos son funciones avanzadas que deberá tener en cuenta al archivar datos.

### Tareas relacionadas:

Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archivado de datos con la GUI

Puede archivar un archivo a un grupo de archivos utilizando los nombres de archivo. Puede seleccionar los archivos que coinciden con el criterio de búsqueda utilizando un árbol de directorio.

### Procedimiento

Archive los archivos mediante el siguiente procedimiento.

1. Pulse Archivar en la ventana principal.
2. En la ventana Archive, expanda el árbol del directorio pulsando la señal (+) más o el icono de la carpeta siguiente a un objeto en el árbol. Para buscar o filtrar los archivos, pulse en el icono Search desde la barra de herramientas.
3. Escriba el criterio de búsqueda en la ventana Find Files.
4. Pulse Search.
5. En la ventana Matching Files, pulse en las casillas de selección que están al lado de los archivos que desea archivar y cerrar la ventana Matching Files.
6. Escriba el criterio de filtrado en la ventana Find Files.
7. Pulse Filter. La ventana Archive muestra los archivos filtrados.
8. Pulse las casillas de selección que están al lado de los archivos filtrados o los directorios que desea archivar.
9. Escriba la descripción, acepte la descripción predeterminada o seleccione una descripción existente para el paquete de archivado en la casilla Description. La longitud máxima de una descripción es de 254 caracteres. Al utilizar una descripción de archivado existente, los archivos o directorios seleccionados se agregan al paquete archivado. Todos los paquetes archivados con la misma descripción se agrupan para las recuperaciones, consultas y supresiones.
10. Para modificar opciones de archivado específicas, pulse en Options. Cualquier opción que se cambie solo es efectiva durante la sesión actual.
11. Pulse en Archive. La ventana de archivado Task List muestra los estados de procesamiento de archivado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Ejemplos de archivado de datos utilizando la línea de mandatos

Puede solicitar servicios de archivado cuando desee conservar copias de archivos en su estado actual, ya sea para utilizarlos más adelante, ya sea para fines históricos o legales. Se muestran ejemplos de archivado de datos mediante la línea de mandatos.





Puede archivar un archivo, un grupo de archivos o todos los archivos en un directorio o subdirectorio. Después de archivar un archivo, puede elegir suprimir el archivo original de la estación de trabajo.

En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato archive para archivar objetos.

Tabla 1. Ejemplos de archivado desde la línea de mandatos

Tarea	Mandato	Consideraciones
Realizar el archivado de todos los archivos en el directorio <code>/home/proj1</code> que tienen la extensión de archivo <code>.txt</code> .	<code>dsmc archive "/home/proj1/*.txt"</code>	Utilice caracteres comodín para archivar más de un archivo a la vez.
Archivar todos los archivos del directorio <code>/home/jones/proj/</code> y borrarlos de la estación de trabajo.	<code>dsmc archive /home/jones/proj/ -deletefiles</code>	Recupere las copias archivadas en la estación de trabajo siempre que las necesite de nuevo. Para obtener más información sobre la opción <code>deletefiles</code> , consulte el apartado <code>Deletefiles</code> .
Archivar los archivos de <code>/home/jones/h1.doc</code> y <code>/home/jones/test.doc</code> .	<code>dsmc archive /home/jones/h1.doc /home/jones/test.doc</code>	Si especifica la opción <code>removeoperandlimit</code> con el mandato <code>archive</code> , el límite de 20 operandos no se aplica y sólo está limitado por los recursos disponibles u otros límites del sistema operativo. Con esta opción, puede especificar más de 20 archivos en un único mandato. Para más información sobre esta opción, consulte <code>Removeoperandlimit</code> .
Archivar una lista de archivos en el archivo <code>/home/avi/filelist.txt</code> .	<code>dsmc archive -filelist=/home/avi/filelist.txt</code>	Utilice la opción <code>filelist</code> para procesar una lista de archivos. Para obtener más información, consulte <code>Filelist</code> .

Tarea	Mandato	Consideraciones
Archivar el archivo <code>/home/jones/ch1.doc</code> y asignarle una descripción.	<code>dsmc archive /home/jones/ch1.doc -description="Capítulo 1, primera versión"</code>	Si no especifica una descripción con el mandato <code>archive</code> , el valor predeterminado es <code>Archive Date:x</code> , donde <code>x</code> es la fecha del sistema actual. Para obtener más información sobre la opción <code>description</code> , consulte el apartado Descripción.
Archivar todos los archivos en el directorio <code>/home/jones/proj/</code> y sus subdirectorios.	<code>dsmc archive /home/jones/proj/ -subdir=yes</code>	Para obtener más información sobre la opción <code>subdir</code> , consulte el apartado Subdir.
Utilice la opción <code>v2archive</code> con el mandato <code>archive</code> para archivar sólo archivos del directorio <code>/home/relx/dir1</code> , pero no los directorios <code>relx</code> o <code>dir1</code> .	<code>dsmc archive "/home/relx/dir1/" -v2archive</code>	El cliente de copia de seguridad y archivado archiva sólo las copias del directorio <code>/home/relx/dir1</code> . Los directorios que haya en la vía de acceso no se procesarán. Para obtener más información sobre la opción <code>v2archive</code> , consulte el apartado V2archive.
Utilice la opción <code>archmc</code> con el mandato <code>archive</code> para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.	<code>dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan</code>	Para obtener más información sobre la opción <code>archmc</code> , consulte el apartado Archmc. Para obtener más información acerca de las clases de gestión, consulte el apartado Políticas de gestión de almacenamiento.
Suponemos que ha iniciado una instantánea del sistema de archivos <code>/usr</code> y montado la instantánea como <code>/snapshot/day1</code> . Archive el árbol del directorio <code>/usr/dir1/sub1</code> desde la instantánea local y gestiónela en el servidor de IBM Spectrum Protect en el nombre de espacio de archivos <code>C:\</code> .	<code>dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1</code>	El cliente considera el valor de <code>snapshotroot</code> como el nombre del espacio de archivos. Para obtener más información, consulte Snapshotroot.

-  sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
- Asociación de una instantánea local a un espacio de archivos del servidor  
 Para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect, utilice la opción `snapshotroot`.

#### Referencia relacionada:

Archive

 sistemas operativos Mac OS X
  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris

## Archivado de datos mediante el proxy de nodo cliente

El archivado de varios nodos que comparten almacenamiento se puede agrupar en un nombre de nodo de destino común en el servidor de IBM Spectrum Protect.

### Antes de empezar

Todos los nodos agente del entorno de varios nodos deberían ser del mismo tipo de plataforma. No utilice los nodos de destino como nodos tradicionales. Utilícelos únicamente para el proceso de varios nodos.


tenga en cuenta las siguientes características de una sesión proxy:

- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- No se puede llevar a cabo una restauración o una copia de seguridad de los servicios del sistema o el estado del sistema.
- No puede acceder a otro nodo (ni desde el menú desplegable de la GUI ni utilizando la opción `fromnode`).
- No se puede llevar a cabo una copia de seguridad o una restauración de NAS.

### Acerca de esta tarea

Resulta útil consolidar archivos archivados a un nombre de nodo de destino común en el servidor cuando la estación de trabajo responsable de llevar a cabo el archivado puede cambiar con el tiempo, como en el caso de un Xsan o clúster. La opción `asnodename` también permite restaurar datos desde un sistema distinto del que se utilizó para realizar la copia de seguridad. Utilice la opción

asnodename con el mandato adecuado para hacer una copia de seguridad, archivar restaurar y recuperar datos bajo el nombre del nodo de destino del servidor de IBM Spectrum Protect. Este soporte está sólo disponible con IBM Spectrum Protect V5.3 y posterior.

 Sistemas operativos Linux También se realiza una copia de seguridad de los clientes Tivoli Storage Manager FastBack mediante el proxy de nodo de cliente.

Configurar el entorno para operaciones con el proxy es un procedimiento de varios pasos que implica definir opciones y mandatos en el cliente de archivado y copia de seguridad y en el servidor.

## Procedimiento

---

Siga los pasos del 1 al 5 para instalar y otorgar autoridad de proxy a los nodos que pueden llevar a cabo procedimientos de archivado en nombre de otro nodo.

1. Instale el cliente de copia de seguridad/archivado en todos los nodos de un entorno de datos compartido.
2. Registre cada nodo con el servidor de IBM Spectrum Protect, si éste no existe. Registre el nombre de nodo de destino común que vaya a compartir cada uno de los nodos agente utilizado en el entorno de datos compartido.
3. Registre cada uno de los nodos en el entorno de datos compartido con el servidor de IBM Spectrum Protect. Éste es el nombre de nodo agente que se utiliza con fines de autenticación. Los datos no se almacenan con el nombre de nodo cuando se utiliza la opción asnodename.
4. Otorgue la autorización de proxy a todos los nodos del entorno compartido para acceder al nombre de nodo de destino en el servidor de IBM Spectrum Protect, mediante el uso del mandato GRANT PROXYNODE (administrador de IBM Spectrum Protect).
5. Utilice el mandato de cliente de administración QUERY PROXYNODE para visualizar los nodos de cliente del usuario autorizado, otorgados mediante el mandato GRANT PROXYNODE.

Con el paso 6 se garantiza que los archivos archivados se cifran en el servidor.

6. Establezca la opción encryptkey en el archivo de opciones.

Especifique encryptkey=save en el archivo de opciones para guardar la clave de cifrado en el archivo de contraseñas de IBM Spectrum Protect. Realice la copia de seguridad de un archivo como mínimo con asnode=ProxyNodeName para crear una clave de cifrado local en cada nodo agente del entorno de varios nodos.

Especifique encryptkey=prompt en el archivo de opciones si desea que los usuarios del nodo gestionen la clave de cifrado. Asegúrese de que los usuarios de los nodos agente del entorno de varios nodos utilicen la misma clave de cifrado.

Si cambia la clave de cifrado, deberá repetir los pasos anteriores. Utilice la misma clave de cifrado para todos los archivos de los que se haya realizado una copia de seguridad en el entorno de nodos compartido.

Lleve a cabo los pasos desde 7 hasta el paso 10 para habilitar el funcionamiento de varios nodos desde la GUI.

7. Compruebe que el nodo de cliente dispone de una autorización de proxy a un nodo de destino (o que está autorizado para actuar como nodo de destino) utilizando el mandato de cliente de administración QUERY PROXYNODE.
8. Seleccione Edit > Preferences para abrir la ventana de preferencias.
9. Seleccione la ficha General y rellene el campo Como nombre de nodo con el nombre de nodo de destino con autorización de proxy.
10. Pulse Aplicar y, a continuación, Aceptar para cerrar la ventana de preferencias.

Lleve a cabo el paso 11 para verificar que el nodo de cliente accede ahora al servidor como nodo de destino.

11. Abra la ventana de árbol y verifique que se visualiza el nodo de destino especificado en el campo Como nombre de nodo. También puede verificar que se muestra el nombre del nodo de destino en el campo Acceso como nodo en la ventana Información de conexión.
12. Opcional: Para volver a la operación de nodo único, suprima Como nombre de nodo del campo Acceso como nodo en la pestaña General > Preferencias.

### Referencia relacionada:

Asnodename

Valores de sesión y planificaciones de una operación de proxy

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Supresión de datos archivados

---

Puede eliminar los objetos de archivado individuales desde el servidor de IBM Spectrum Protect, sin tener que suprimir el espacio de archivos completos al que pertenecen.

### Antes de empezar

---

El administrador de IBM Spectrum Protect debe concederle los permisos para suprimir los objetos archivados. Para determinar si tiene estos permisos, seleccione File > Información de conexión desde la GUI del cliente de copia de seguridad y archivado o desde el menú principal del cliente web. La autoridad del estado de supresión de archivado aparece en el campo `Delete Archive Files`. Si este campo muestra `No`, no puede suprimir los objetos archivados de no ser que el administrador le conceda los permisos para hacerlo.

## Procedimiento

Para suprimir un objeto archivado desde el servidor, lleve a cabo estos pasos en la GUI o en el cliente web. Como una alternativa a utilizar la GUI o el cliente web, puede suprimir los objetos archivados desde la línea de mandatos mediante el mandato `delete archive`.

1. Seleccione Suprimir datos archivados en el menú Herramientas.
2. En la ventana Archive Delete, expanda el árbol del directorio pulsando en el signo más (+) o en el icono de la carpeta que está al lado del objeto que desea expandir. Los objetos del árbol están agrupados según la descripción del paquete de archivado.
3. Seleccione los objetos archivados que desea suprimir.
4. Pulse Suprimir. El cliente le solicitará que confirme antes de comenzar a suprimir los objetos seleccionados. La ventana Archive Delete Task List muestra el progreso de la operación de supresión.













### Referencia relacionada:

Delete Archive

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Tareas de archivado avanzadas

Los permisos de acceso, los enlaces simbólicos y los enlaces fijos son funciones avanzadas que deberá tener en cuenta al archivar datos.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Permisos de acceso  
Al archivar un archivo, el cliente guarda los permisos de acceso estándares de UNIX asignados al archivo.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Archivar y recuperar enlaces simbólicos  
El cliente de copia de seguridad y archivado archiva y recupera los vínculos simbólicos de forma distinta a como maneja los directorios y archivos normales.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Enlaces fijos  
Cuando archive copias que tienen un enlace fijo, el cliente de copia de seguridad y archivado archivará cada instancia del archivo enlazado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Permisos de acceso

Al archivar un archivo, el cliente guarda los permisos de acceso estándares de UNIX asignados al archivo.

En función del sistema operativo, también guarda permisos ampliados. Por ejemplo, para archivos de una estación de trabajo AIX, el cliente guarda listas de control de accesos.

Si usted es un usuario y archiva un archivo para el que dispone de acceso de lectura, pasa a ser el propietario de la copia del archivo. Usted es el único usuario que puede recuperar el archivo archivado a menos que otorgue acceso a otro usuario.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archivar y recuperar enlaces simbólicos

El cliente de copia de seguridad y archivado archiva y recupera los vínculos simbólicos de forma distinta a como maneja los directorios y archivos normales.

La manera en la que el cliente archiva y recupera los enlaces simbólicos depende de la configuración de las opciones, de la posibilidad de acceder o no al directorio de destino y de la forma de especificación de los objetos.

Un *enlace simbólico UNIX* es un archivo que contiene un puntero a otro archivo o directorio. El objeto al que señala el vínculo simbólico se denomina *objeto de destino*.

Se puede realizar una copia de seguridad de un enlace simbólico como información de la vía de acceso a un directorio de destino o como un directorio. Si se realiza una copia de seguridad del enlace simbólico como un directorio, también se podrá hacer una copia de

seguridad de los archivos y carpetas de ese directorio de destino.

La forma de realizar la copia de seguridad del vínculo determina los elementos y el ámbito de la restauración, la configuración de la opción followsymbolic y la posibilidad de acceder al directorio de destino en el momento de la restauración.

Para obtener más información sobre cómo se manejan los vínculos simbólicos durante una operación de archivado, consulte la opción archsymlinkasfile.

Nota: el proceso de los enlaces simbólicos que se describe en este apartado no es aplicable a Mac OS X. El archivado de los enlaces simbólicos se hace siempre como archivos y nunca se siguen.

En la tabla siguiente se muestran las funciones de recuperación y archivado de los vínculos simbólicos y la acción que se lleva a cabo:

Tabla 1. Tabla de gestión de vínculos simbólicos para archivado y recuperación

Función	Acción efectuada
Archivado de un vínculo de archivo.	Archiva el archivo al que hace referencia el vínculo simbólico.
Archivado de un vínculo de directorio.	Archiva el directorio y el contenido de éste.
Archivado de un archivo con subdir=yes.	Archiva el archivo, la vía de acceso del directorio y todos los archivos con nombre parecido en el subárbol.
Archivado de un directorio con subdir=yes.	Archiva el directorio y el contenido de éste y de sus subdirectorios.
Archivado de un vínculo simbólico que hace referencia a un archivo o directorio que no existe.	Archiva el vínculo simbólico.
Recuperación de un vínculo simbólico que hace referencia a un archivo; el archivo y el vínculo existen.	Sustituye el archivo si se ha establecido replace=y.
Recuperación de un vínculo simbólico que hace referencia a un archivo; el vínculo simbólico ya no existe.	Recupera el archivo sustituyendo el nombre del archivo por el nombre del vínculo simbólico y lo coloca en el directorio en el que reside el vínculo simbólico.
Recuperación de un vínculo simbólico que hace referencia a un directorio; el vínculo simbólico y el directorio ya no existen.	Se crea un directorio en el directorio en el que reside el vínculo simbólico y se restauran todos los archivos y subdirectorios en ese directorio. El nombre del vínculo simbólico se utiliza como el nuevo nombre de directorio.
Recuperación de un vínculo simbólico que hace referencia a un directorio; el vínculo simbólico y el directorio todavía existen.	El directorio no se recupera mientras exista el vínculo simbólico.

**Referencia relacionada:**

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris [Archsymlinkasfile](#)  
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Enlaces fijos

Cuando archive copias que tienen un enlace fijo, el cliente de copia de seguridad y archivado archivará cada instancia del archivo enlazado.

Por ejemplo, si archiva dos copias que tienen un enlace fijo, el cliente archiva los datos por duplicado.

Cuando se recuperan archivos con enlace fijo, el cliente restablece los vínculos. Por ejemplo, si se había establecido un enlace fijo entre dos archivos y solo se encuentra uno en su estación de trabajo, al recuperar ambos archivos habrá un enlace fijo entre los dos. La única excepción de este procedimiento se da cuando se archivan dos archivos entre los que hay un enlace fijo y se interrumpe la conexión entre estos en la estación de trabajo. Si recupera los dos archivos desde el servidor, el cliente respeta el sistema de archivos actual y no recupera el enlace fijo.

Consejo: Si no archiva y recupera al mismo tiempo todos los archivos que tienen enlaces fijos, pueden producirse problemas. Para garantizar que los archivos con enlaces fijos permanecen sincronizados, archive y recupere todos los enlaces fijos al mismo tiempo.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris













## Recuperar archivos

Recupere un archivo cuando desee devolver una copia archivada del servidor a la estación de trabajo.

Muchas de las consideraciones avanzadas para la recuperación de archivos son las mismas que las de restauración.



Importante: Cuando recupera un archivo sin especificaciones y existe más de una versión de la copia archivada en el servidor, el cliente recupera todas las copias. Una vez recuperada la primera copia, se recupera la segunda. Si existe una copia en la estación de trabajo cliente, se le solicitará que la sustituya, la omita o cancele.

-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Recuperación de datos con la GUI  
 Puede recuperar un archivo archivado con la GUI.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Recupere los ejemplos de datos utilizando la línea de mandatos  
 Puede recuperar un archivo, un grupo de archivos o todos los archivos de un directorio o subdirectorio.
-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Archivar clases de gestión  
 El cliente de copia de seguridad y archivado comprueba las opciones include de la lista de opciones de inclusión/exclusión para determinar la clase de gestión que debe asignar a los archivos archivados.

**Conceptos relacionados:**

Restaurar o recuperar archivos en otra estación de trabajo

**Tareas relacionadas:**

Cómo autorizar a otro usuario para que restaure o recupere archivos

Restauración o recuperación de archivos de otro nodo cliente

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Recuperación de datos con la GUI

Puede recuperar un archivo archivado con la GUI.

### Procedimiento

1. Pulse Retrieve desde el cliente de la ventana principal de la GUI de Java™. Aparece la ventana Retrieve.
2. Expanda el árbol de directorios pulsando el signo más (+) o el icono de carpeta junto a un objeto que desee expandir. Para buscar o filtrar los archivos, pulse en el icono Search desde la barra de herramientas.
3. Escriba el criterio de búsqueda en la ventana Find Files.
4. Pulse Search. Aparece la ventana Matching Files.
5. Pulse en las cajas de selección que aparecen al lado de los archivos que desea recuperar y cierre la ventana Matching Files.
6. Escriba el criterio de filtrado en la ventana Find Files.
7. Pulse Filter. La ventana Retrieve muestra los archivos filtrados.
8. Pulse las casillas de selección de los archivos filtrados o directorios que desea recuperar.
9. Para modificar o recuperar opciones específicas, pulse Options. Cualquier opción que cambie será eficaz solo durante la sesión actual.
10. Pulse Retrieve. Aparece la ventana Retrieve Destination. Escriba la información apropiada en la ventana Retrieve Destination.
11. Pulse Retrieve. La ventana Task List muestra el estado de recuperación del proceso.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Recupere los ejemplos de datos utilizando la línea de mandatos

Puede recuperar un archivo, un grupo de archivos o todos los archivos de un directorio o subdirectorio.

Cuando recupere un archivo, el servidor IBM Spectrum Protect le enviará una copia del mismo. La copia archivada permanece en el almacenamiento.

Utilice el mandato retrieve para recuperar archivos del almacenamiento de la estación de trabajo. En la tabla siguiente, figuran algunos ejemplos de la utilización del mandato retrieve.

Tabla 1. Ejemplos de recuperación de archivos desde la línea de mandatos

Tarea	Mandato	Consideraciones
Recuperar el archivo /home/jones/h1.doc en su directorio original.	<code>dsmc retrieve /home/jones/h1.doc</code>	Si no especifica un destino, los archivos se recuperan en su ubicación original.
Recuperar el archivo /home/jones/h1.doc con un nuevo nombre y en otro directorio.	<code>dsmc retrieve /home/jones/h1.doc /home/smith/h2.doc</code>	Ninguna.

Tarea	Mandato	Consideraciones
Recuperar todos los archivos del directorio /home/jones que terminen con los caracteres .bak en el directorio /home/smith.	<code>dsmc retrieve "/home/jones/*.bak" /home/smith/</code>	Ninguna.
Recuperar el archivo /home/jones/ch1.doc y asignar una descripción.	<code>dsmc retrieve /home/jones/ch1.doc - description="Capítulo 1, primera versión"</code>	Si no realiza una descripción con el mandato retrieve, el valor predeterminado será Retrieve Date:x, donde x será la fecha actual del sistema.
Utilizar la opción pick para ver una lista de copias archivadas en la que puede seleccionar los archivos que desea recuperar.	<code>dsmc retrieve "/home/jones/*" -pick</code>	Ninguna.
Recuperar una lista de archivos que se han especificados en el archivo retrievalist.txt y colocarlos en su directorio original.	<code>dsmc retrieve - filelist=/home/dir2/retrie velist.txt</code>	Ninguna.

**Referencia relacionada:**

Retrieve

Descripción

Filelist

Pick

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archivar clases de gestión

El cliente de copia de seguridad y archivado comprueba las opciones include de la lista de opciones de inclusión/exclusión para determinar la clase de gestión que debe asignar a los archivos archivados.

Si no asigna una clase de gestión a un archivo mediante la opción include, el cliente asigna al archivo la clase de gestión predeterminada. El cliente puede archivar solo un archivo si la clase de gestión seleccionada contiene un grupo de copia de archivado.

Puede sobrescribir la clase de gestión predeterminada utilizando la opción archmc o si pulsa en Options en la ventana Archive de la GUI, pulsando en Override include/exclude list, y después seleccionando las clases de gestión.

También puede añadir sentencias de inclusión/exclusión la GUI Java™ del cliente de copia de seguridad y archivado o en árbol de directorios del cliente web. Después, puede utilizar la función de Utilities Preview Include-Exclude para obtener la vista previa de la lista de inclusión/exclusión antes de enviar los datos al servidor.

**Conceptos relacionados:**

Asignar una clase de gestión a los archivos

Visualizar información sobre clases de gestión y grupos de copia

**Referencia relacionada:**

Preview Archive

Previsualizar copia de seguridad

## Planificar operaciones para clientes de archivado y copia de seguridad

Pueden planificarse las operaciones de copia de seguridad que protegen los datos del cliente para garantizar que esas operaciones se ejecuten regularmente.

### Acerca de esta tarea

Dispone de un planificador del cliente que interactúa con el planificador central del servidor de IBM Spectrum Protect para hacer una copia automática de sus datos.

- Visión general del planificador de IBM Spectrum Protect  
El planificador central de IBM Spectrum Protect permite llevar a cabo automáticamente operaciones en los plazos especificados.
- Códigos de retorno del cliente  
La interfaz de línea de mandatos de copia de seguridad/archivado y el planificador finalizan con códigos de retorno que reflejan de forma precisa si la operación de cliente se ha realizado correctamente o no.

# Visión general del planificador de IBM Spectrum Protect

El planificador central de IBM Spectrum Protect permite llevar a cabo automáticamente operaciones en los plazos especificados.

Para entender la planificación con IBM Spectrum Protect, es necesario definir varios términos:

## definición de planificación

Una definición de planificación en el servidor de IBM Spectrum Protect especifica las propiedades críticas de una actividad automatizada, incluyendo el tipo de acción, la hora en la que debe llevarse a cabo la acción y la frecuencia de la misma. Se pueden definir otras varias propiedades de una planificación. Para obtener información sobre DEFINE SCHEDULE, consulte la documentación del servidor de IBM Spectrum Protect.

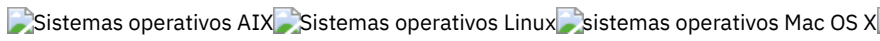
## asociación de planificación


Una asociación de planificación es una asignación de un nodo cliente a una definición de planificación específica. Varias asociaciones de planificación permiten que muchos nodos clientes puedan utilizar definiciones de planificación individuales. Puesto que las definiciones de planificaciones están incluidas en dominios de políticas concretos, sólo es posible asociar los nodos definidos para cierto dominio de políticas con las planificaciones definidas dentro de ese dominio.

## suceso planificado

Un suceso planificado es un caso específico del momento en que se ejecuta una planificación para un nodo. Para que los sucesos planificados automáticos tengan lugar para un cliente, deben satisfacerse las siguientes condiciones:

- Debe existir una definición de planificación para un dominio de políticas específico.
- Debe existir una asociación de planificación para el nodo requerido, que pertenece a dicho dominio de políticas.
- El proceso del planificador cliente debe estar ejecutándose en el sistema cliente.

 Al crear una definición de planificación en el servidor de IBM Spectrum Protect, las acciones de planificación que se pueden llevar a cabo son: incremental, selective, archive, restore, retrieve, image backup (no se aplica a Mac OS X), image restore (no se aplica a Mac OS X), command y macro. La acción planificada que se utiliza más frecuentemente es incremental con el parámetro objects sin definir. Con este valor, el cliente de archivado y copia de seguridad realiza una copia de seguridad incremental del dominio de todos los sistemas de archivo definidos mediante la opción de dominio del cliente. Una definición de planificación mediante la acción command permite que se ejecute un mandato del sistema operativo o un script del shell. Al automatizar tareas para los clientes de IBM Spectrum Protect for Data Protection, se deben utilizar las definiciones de planificación de las acciones de command, que invocan a las herramientas de línea de mandatos de esas aplicaciones.

 Al crear una definición de planificación en el servidor de IBM Spectrum Protect, las acciones de planificación que se pueden llevar a cabo son: incremental, selective, archive, restore, retrieve, imagebackup, imagerestore, command y macro. La acción planificada que se utiliza más frecuentemente es incremental con el parámetro objects sin definir. Con este valor, el cliente de IBM Spectrum Protect realiza una copia de seguridad incremental de todas las unidades definidas mediante la opción domain del cliente. Una definición de planificación mediante la acción command permite que se ejecute un mandato del sistema operativo o un script del shell. Al automatizar tareas para los clientes de IBM Spectrum Protect for Data Protection, se deben utilizar las definiciones de planificación de las acciones de command, que invocan a las herramientas de línea de mandatos de esas aplicaciones.

El *intervalo de inicio* de la planificación indica el período de tiempo aceptable para que se inicie un suceso planificado. El intervalo de inicio se define mediante estos parámetros de definición de planificación: startdate, starttime, durunits y duration. Las opciones startdate y starttime definen el principio del intervalo de inicio para el primer suceso planificado. El principio de los intervalos de inicio para sucesos planificados posteriores varía según los valores de period y perunit de la definición de planificación. Los parámetros duration y durunits definen la duración de la ventana de inicio. La acción de planificación debe empezar obligatoriamente dentro del intervalo de inicio. Para ilustrarlo, considere los resultados de la siguiente definición de planificación:






```
define schedule standard test1 action=incremental starttime=12:00:00 period=1  
perunits=hour dur=30 duru=minutes
```

Suceso	Inicio de ventana	Fin de ventana	Inicio real (es sólo un ejemplo, las horas varían)
1	12:00:00	12:30:00	12:05:33
2	13:00:00	13:30:00	13:15:02
3	14:00:00	14:30:00	14:02:00
etcétera			

La variación en las horas de inicio reales es el resultado de la característica de aleatorización que proporciona el planificador central de IBM Spectrum Protect que ayuda a equilibrar la carga de las sesiones planificadas en el servidor de IBM Spectrum Protect.

- Ejemplos: manejo de espacios en blanco en nombres de archivos de definiciones de planificación  
Al definir o actualizar un parámetro objects de planificación o el parámetro options de planificación con especificaciones de





archivos que contienen espacios en blanco, especifique entre comillas dobles (") cada especificación de archivo que contenga espacios en blanco y entre comillas simples (') todas las especificaciones.

- Horas de inicio preferentes para determinados nodos  
Puede que, de vez en cuando, desee asegurarse de que un nodo en particular inicia la actividad que se ha planificado para éste a una hora lo más cercana posible a la hora de inicio definida de la planificación. Esta necesidad suele darse cuando se utiliza la planificación en modalidad de solicitud.
- Opciones de proceso de planificador  
Las opciones de proceso del planificador determinan las operaciones que se llevan a cabo cuando se inicia un trabajo del planificador.
- Servicios del planificador de aceptación de clientes frente a los servicios del planificador tradicional  
Puede configurar el cliente de IBM Spectrum Protect para gestionar el proceso de planificador utilizando el daemon de aceptación de cliente de IBM Spectrum Protect.
- Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar  
Puede configurar el planificador del cliente de IBM Spectrum Protect para que se ejecute como una tarea de fondo del sistema que se inicie automáticamente al arrancar el sistema.
- Ejemplos: visualización de información sobre trabajo planificado  
Las planificaciones pueden ser clásicas o ampliadas, según como se haya definido el intervalo de la siguiente ejecución.
- Visualizar información sobre el trabajo completado  
Al ejecutar el mandato schedule en primer plano, aparece en pantalla la salida de los mandatos planificados.
- Especificar opciones de planificación  
Puede modificar las opciones de planificación en el archivo de opciones del cliente o la interfaz gráfica de usuario (GUI).
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Opciones del planificador para los mandatos  
El planificador ejecuta mandatos con un identificador de usuario de 0 (root); sin embargo, es posible que algunos mandatos deban ejecutarse con un identificador de usuario que no sea 0.
- Activar o desactivar mandatos planificados  
Puede utilizar la opción schedcmddisabled para desactivar la planificación de mandatos del servidor.
-  Sistemas operativos Windows Cambiar las opciones de proceso utilizadas por el servicio del planificador  
Si configura los servicios de planificación central de IBM Spectrum Protect (el planificador, el aceptador de cliente o el agente de cliente remoto), parte de las opciones de proceso que especifica están definidas en el registro de Windows.
- Gestionar varios requisitos de planificador en un sistema  
En determinadas situaciones es preferible tener más de una actividad planificada para cada sistema cliente.

## Ejemplos: manejo de espacios en blanco en nombres de archivos de definiciones de planificación





---

Al definir o actualizar un parámetro objects de planificación o el parámetro options de planificación con especificaciones de archivos que contienen espacios en blanco, especifique entre comillas dobles (") cada especificación de archivo que contenga espacios en blanco y entre comillas simples (') todas las especificaciones.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Los siguientes ejemplos muestran como delimitar parámetros object de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
objects="/home/proj1/Some file.doc"  
objects="/home/proj1/Some file.doc" "/home/Another file.txt" /home/noblanks.txt'  
objects="/home/My Directory With Blank Spaces/"  
objects="/Users/user1/Documents/Some file.doc"  
objects="/Users/user1/Documents/Some file.doc"  
"/Users/user5/Documents/Another file.txt" /Users/user3/Documents/noblanks.txt'  
objects="/Users/user1/My Directory With Blank Spaces/"
```

Esta sintaxis garantiza que las especificaciones de archivo que contengan un espacio, como /home/proj1/Some file.doc, se traten como un solo nombre de archivo, en vez de como dos archivos distintos (/home/proj1/Some y file.doc).


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Los siguientes ejemplos muestran como delimitar parámetros options de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
options='-preschedulecmd="/home/me/my files/bin/myscript"  
-postschedulecmd="/home/me/my files/bin/mypostscript" -quiet'  
options='-presched="/home/me/my files/bin/precmd" -postsched=finish'
```

 Sistemas operativos Windows  
Los siguientes ejemplos muestran como delimitar parámetros object de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
objects=' "c:\home\proj1\Some file.doc"'
objects=' "c:\home\proj1\Some file.doc" "c:\home\Another file.txt"
  c:\home\noblanks.txt'
objects=' "c:\home\My Directory With Blank Spaces\ "'
objects=' "c:\Users\user1\Documents\Some file.doc"'
objects=' "c:\Users\user1\Documents\Some file.doc"
  "c:\Users\user5\Documents\ Another file.txt" c:\Users\user3\Documents\noblanks.txt'
objects=' "c:\Users\user1\My Directory With Blank Spaces\ "'
```

Esta sintaxis garantiza que las especificaciones de archivo que contengan un espacio, como c:\home\proj1\Some file.doc, se traten como un solo nombre de archivo, en vez de como dos archivos distintos (c:\home\proj1\Some y file.doc).

 Sistemas operativos Windows Los siguientes ejemplos muestran como delimitar parámetros options de planificación cuando las especificaciones de archivo contienen caracteres de espacio:

```
options='-preschedulecmd="c:\home\me\my files\bin\myscript"
  -postschedulecmd="c:\home\me\my files\bin\mypostscript" -quiet'
options='-presched="c:\home\me\my files\bin\precmd" -postsched=finish'
```

También puede consultar la información de los parámetros objects y options de los mandatos DEFINE SCHEDULE y UPDATE SCHEDULE. Para obtener descripciones de estos mandatos y sus parámetros, consulte la documentación del servidor de IBM Spectrum Protect.

### Conceptos relacionados:

Especificación de cadenas de entrada que contengan espacios en blanco o comillas

## Horas de inicio preferentes para determinados nodos

Puede que, de vez en cuando, desee asegurarse de que un nodo en particular inicia la actividad que se ha planificado para éste a una hora lo más cercana posible a la hora de inicio definida de la planificación. Esta necesidad suele darse cuando se utiliza la planificación en modalidad de solicitud.

En función del número de nodos cliente asociados a la planificación y en qué lugar de la secuencia de solicitud se encuentra el nodo, es posible que el nodo reciba la solicitud considerablemente más tarde que la hora de inicio de la planificación.

En este caso, puede realizar los siguientes pasos:

1. Copie la planificación en una nueva planificación con un nombre distinto (o defina una nueva planificación con los atributos preferidos)
2. Establezca el nuevo atributo de prioridad de planificación de modo que tenga una prioridad más alta que la planificación original.
3. Suprima la asociación entre el nodo y la planificación original y luego asocie el nodo a la nueva planificación.

Ahora el servidor de IBM Spectrum Protect procesa primero la nueva planificación.

## Opciones de proceso de planificador


Las opciones de proceso del planificador determinan las operaciones que se llevan a cabo cuando se inicia un trabajo del planificador.





Puede definir la mayoría de estas opciones de proceso del planificador en el archivo de opciones del cliente. No obstante, algunas de estas opciones se pueden definir en el servidor de IBM Spectrum Protect, de forma que afecten a todos los clientes.

En la tabla siguiente se muestran las opciones definidas por el cliente y las del servidor y cuáles sobrescribe el servidor. Una X en una columna indica dónde se puede especificar la opción.

Opción	Cliente definido	Servidor definido	Modificación global de servidor
manageservices	X		
maxcmdretries	X		Mandato SET MAXCMDRETRIES
maxschedsessions		X	
postschedulecmd, postnschedulecmd	X		
preschedulecmd, prenschedulecmd	X		
querschedperiod	X		Mandato SET QUERSCHEDPERIOD
randomize		X	
retryperiod	X		Mandato SET RETRYPERIOD
schedcmddisabled	X		

Opción	Cliente definido	Servidor definido	Modificación global de servidor
schedlogname	X		
schedlogretention	X		
schedmode	X		Mandato SET SCHEDMODES
sessioninitiation	X	X	Mandato UPDATE NODE
tcpclientaddress	X	X (también se define en el servidor cuando <code>sessioninit=serveronly</code> como parte de la definición de nodo)	
tcpclientport	X	X (también se define en el servidor cuando <code>sessioninit=serveronly</code> como parte de la definición de nodo)	

 Sistemas operativos Windows Las opciones que define el cliente están definidas en el archivo `dsm.opt`. El servidor de IBM Spectrum Protect también puede definir algunas opciones en un archivo de opciones del cliente o como parte del parámetro de opciones de la definición de la planificación. El servidor de IBM Spectrum Protect también puede establecer globalmente algunas opciones para todos los clientes. De forma predeterminada, se respeta el valor del cliente para estas opciones. Si se establece la modificación global en el servidor de IBM Spectrum Protect, se ignora el valor del cliente para la opción. La definición de opciones del cliente como parte de la definición de la planificación es útil si desea utilizar opciones específicas para una acción planificada que difiere de los valores de la opción que el nodo cliente utiliza normalmente o que son distintas para cada planificación que el nodo ejecuta.






 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Las definidas por el cliente se definen en el archivo `dsm.sys` o `dsm.opt`. El servidor de IBM Spectrum Protect también puede definir algunas opciones en un archivo de opciones del cliente o como parte del parámetro de opciones de la definición de la planificación. El servidor de IBM Spectrum Protect también puede establecer globalmente algunas opciones para todos los clientes. De forma predeterminada, se respeta el valor del cliente para estas opciones. Si se establece la modificación global en el servidor de IBM Spectrum Protect, se ignora el valor del cliente para la opción. La definición de opciones del cliente como parte de la definición de la planificación es útil si desea utilizar opciones específicas para una acción planificada que difiere de los valores de la opción que el nodo cliente utiliza normalmente o que son distintas para cada planificación que el nodo ejecuta.

La opción `schedmode` controla la interacción de las comunicaciones entre el servidor y cliente de IBM Spectrum Protect. La modalidad de planificación ofrece dos variantes: *sondeo de cliente* y *por solicitud del servidor*. Estas variantes se explican en la documentación del servidor de IBM Spectrum Protect.

- Evaluar códigos de retorno de planificación en scripts de planificación  
Puede utilizar variables de entorno para determinar el código de retorno de IBM Spectrum Protect actual antes de ejecutar un script utilizando las opciones de cliente `preschedulecmd` o `postschedulecmd`.
- Códigos de retorno de los scripts `preschedulecmd` y `postschedulecmd`  
Se describen los códigos de retorno que puede ver al utilizar las opciones `preschedulecmd` y `postschedulecmd`.






## Evaluar códigos de retorno de planificación en scripts de planificación

Puede utilizar variables de entorno para determinar el código de retorno de IBM Spectrum Protect actual antes de ejecutar un script utilizando las opciones de cliente `preschedulecmd` o `postschedulecmd`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows IBM Spectrum Protect proporciona el valor actual del código de retorno en la variable de entorno denominada `TSM_PRE_CMD_RC`. La variable `TSM_PRE_CMD_RC` es el valor actual del código de retorno de IBM Spectrum Protect antes de ejecutar un script de planificación. El valor de la variable `TSM_PRE_CMD_RC` no es necesariamente el mismo que el código de retorno emitido por IBM Spectrum Protect tras la ejecución del script de planificación. La variable `TSM_PRE_CMD_RC` se puede utilizar en scripts de planificación para determinar el estado actual de la planificación.

La variable `TSM_PRE_CMD_RC` se establece en cada una de las siguientes opciones de planificación: `preschedule`, `prenschedule`, `postschedule` y `postnschedule`. `TSM_PRE_CMD_RC` afecta a las planificaciones que tienen especificada la opción `ACTION=COMMAND`.

Un ejemplo de la variable `TSM_PRE_CMD_RC` que se está utilizando:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

```
if [[ -n ${TSM_PRE_CMD_RC} ]] ; then

    if [[ ${TSM_PRE_CMD_RC} == 0 ]] ; then
        echo "The TSM_PRE_CMD_RC is 0"

    elif [[ ${TSM_PRE_CMD_RC} == 4 ]] ; then
        echo "The TSM_PRE_CMD_RC is 4"






    elif [[ ${TSM_PRE_CMD_RC} == 8 ]] ; then
        echo "The TSM_PRE_CMD_RC is 8"

    elif [[ ${TSM_PRE_CMD_RC} == 12 ]] ; then
        echo "The TSM_PRE_CMD_RC is 12"
    else
        echo "The TSM_PRE_CMD_RC is an unexpected value: ${TSM_PRE_CMD_RC}"
    fi





else
    echo "The TSM_PRE_CMD_RC is not set"
fi
```


## Códigos de retorno de los scripts `preschedulecmd` y `postschedulecmd`

Se describen los códigos de retorno que puede ver al utilizar las opciones `preschedulecmd` y `postschedulecmd`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

- Si el mandato especificado por la opción `preschedulecmd` finaliza con un código de retorno distinto de cero, IBM Spectrum Protect supone que el mandato ha fallado. En este caso, no se puede ejecutar el suceso planificado ni ningún mandato `postschedulecmd` o `postnschedulecmd`. El mandato de administración `query event` con la opción `format=detailed` muestra que el suceso no se ha realizado satisfactoriamente con el código de retorno 12.
- Si el mandato especificado por la opción `postschedulecmd` finaliza con un código de retorno distinto de cero, IBM Spectrum Protect considera que el mandato ha fallado. El mandato administrativo `query event` con la opción `format=detailed` muestra que el suceso se ha completado con el código de retorno 8. La excepción es si la operación planificada se ha completado con un código de retorno más alto, en cuyo caso tiene prioridad el código de retorno más alto. Por lo tanto, si la operación planificada finaliza con el código de retorno 0 o 4 y el mandato `postschedulecmd` no se realiza satisfactoriamente, el mandato de administración `query event` muestra que el suceso se ha completado con el código de retorno 8. Si la operación planificada finaliza con el código de retorno 12, dicho código de retorno prevalece y `query event` muestra que el suceso no se ha realizado satisfactoriamente con el código de retorno 12.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Al interpretar el código de retorno desde un mandato, IBM Spectrum Protect considera que 0 significa éxito y cualquier otro valor significa anomalía. Aunque este comportamiento se acepta ampliamente en el sector, no se garantiza al 100%. Por ejemplo, el desarrollador del mandato del widget puede finalizar con un código de retorno 3, si el widget se ha ejecutado correctamente. Por consiguiente, es posible que el mandato `preschedulecmd` o `postschedulecmd` finalice con un código de retorno distinto de cero y sea a pesar de ello satisfactorio. Para evitar que IBM Spectrum Protect trate dichos mandatos como anómalos, puede incluir estos mandatos en un script y codificar el script de modo que interprete los códigos de retorno de mandato correctamente. El script sale con el código de retorno 0 si el mandato se ha ejecutado satisfactoriamente; de lo contrario, sale con un código de retorno distinto de cero. La lógica para un script que ejecuta el widget puede tener el mismo aspecto que este ejemplo:

 Sistemas operativos Windows Al interpretar el código de retorno desde un mandato, IBM Spectrum Protect considera que 0 significa éxito y cualquier otro valor significa anomalía. Aunque este comportamiento se acepta ampliamente en el sector, no se garantiza al 100%. Por ejemplo, es posible que el desarrollador del mandato `widget.exe` salga con el código de retorno 3, si `widget.exe` se ha ejecutado satisfactoriamente. Por consiguiente, es posible que el mandato `preschedulecmd` o `postschedulecmd` finalice con un código de retorno distinto de cero y sea a pesar de ello satisfactorio. Para evitar que IBM Spectrum Protect trate dichos mandatos como anómalos, puede incluir estos mandatos en un script y codificar el script de modo que interprete los códigos de retorno de mandato correctamente. El script debe finalizar con el código de retorno 0 si el mandato se ha realizado satisfactoriamente; de lo contrario, debe

finalizar con un código de retorno distinto de cero. La lógica para un script que ejecuta widget.exe puede tener el mismo aspecto que este ejemplo:













 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
run 'widget'
  if lastcc == 3
    exit 0
  else
    exit 1
```

 Sistemas operativos Windows

```
run 'widget.exe'
  if lastcc == 3
    exit 0
  else
    exit 1
```

#### Referencia relacionada:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows  Postschedulecmd/Postnschedulecmd  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows  Preschedulecmd/Prenschedulecmd

## Servicios del planificador de aceptación de clientes frente a los servicios del planificador tradicional

---

Puede configurar el cliente de IBM Spectrum Protect para gestionar el proceso de planificador utilizando el daemon de aceptación de cliente de IBM Spectrum Protect.

El daemon de aceptación de clientes proporciona un temporizador sencillo que inicia y detiene automáticamente el proceso del planificador cuando resulta necesario. Si no, el método tradicional mantiene el proceso del planificador de IBM Spectrum Protect ejecutándose continuamente. En general, el método preferido para gestionar el planificador es utilizar el daemon de aceptación de clientes.

La información a continuación es una comparación de los métodos de servicios gestionados por el daemon de aceptación de clientes y los servicios del planificador tradicional.

#### Servicios gestionados por el daemon de aceptación de clientes

- Se definen mediante la utilización de la opción `manageservices schedule` y se inician con los servicios del daemon de aceptación de clientes (`dsmcad`).
- El daemon de aceptación de clientes inicia y detiene el proceso del planificador cuando sea necesario para cada acción planificada.
- Requiere menos recursos del sistema cuando está desocupado.
- Las opciones del cliente de IBM Spectrum Protect y las opciones de modificación del servidor de IBM Spectrum Protect se renuevan cada vez que los servicios del daemon de aceptación de clientes inician una copia de seguridad planificada.
- No pueden utilizarse con copias de seguridad `SESSIONINITiation=SERVEROnly`.

#### Servicios del planificador tradicional de IBM Spectrum Protect

- Se inician con el mandato `dsmc sched`.
- Permanecen activos, incluso después de finalizar la copia de seguridad planificada.
- Requieren un mayor uso de los recursos del sistema cuando está desocupado.
- Las opciones del cliente de IBM Spectrum Protect y las opciones de sustitución del servidor de IBM Spectrum Protect sólo se procesan una vez cuando se inicia `dsmc sched`; si elimina una opción de un conjunto de opciones de cliente, debe reiniciar el planificador para que este esté al tanto de la supresión

**Recomendación:** reinicie el planificador tradicional periódicamente para liberar los recursos del sistema que las llamadas al sistema han utilizado anteriormente.

## Establecimiento del proceso del planificador cliente para que se ejecute como una tarea de fondo y se inicie automáticamente al arrancar

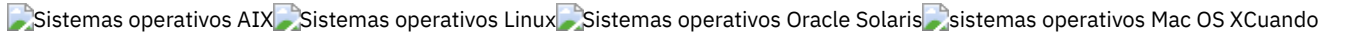
---

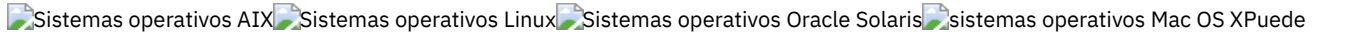


Puede configurar el planificador del cliente de IBM Spectrum Protect para que se ejecute como una tarea de fondo del sistema que se inicie automáticamente al arrancar el sistema.

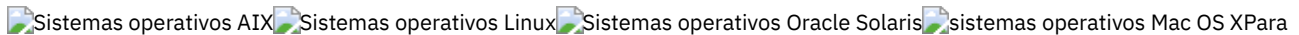
## Acerca de esta tarea

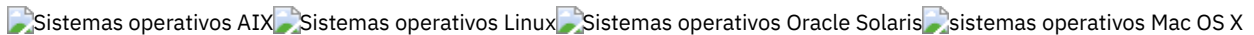
Puede completar esta tarea tanto si utiliza el aceptador de clientes para gestionar el planificador como si utiliza el método tradicional para iniciar el planificador del cliente del planificador.


 Cuando ejecute una planificación gestionada por el aceptador de clientes, establezca el proceso del aceptador de clientes para que se inicie automáticamente en el momento del arranque; no utilice el proceso del planificador. En el método tradicional, establezca el proceso del planificador para que se inicie automáticamente al arrancar.

 Puede configurar el aceptador de clientes para que se ejecute como una tarea de fondo del sistema que se inicie automáticamente al arrancar el sistema. Para configurar el aceptador de clientes para que gestione copias de seguridad planificadas, utilice la opción `managementservices` para especificar si el cliente gestiona únicamente el planificador, únicamente el cliente web o ambos. El método para establecer el aceptador de clientes como una tarea del sistema varía en cada plataforma.

Para que el planificador se inicie de forma desatendida, debe permitir al cliente almacenar su contraseña estableciendo la opción `passwordaccess` en `generate` y almacenar la contraseña ejecutando un mandato simple de cliente como `dsmc query session`. Para fines de prueba, siempre puede iniciar el planificador en primer plano ejecutando `dsmc sched` desde un indicador de mandatos (sin definir ninguna sección `managementservices`).


 Para iniciar el planificador automáticamente durante el arranque, utilice el método gestionado por el aceptador de clientes o el método tradicional.

 Método gestionado por el aceptador de clientes

1. En el archivo `dsm.sys`, establezca la opción `managementservices` en `schedule` o `schedule webclient`.
2. Inicie el aceptador de clientes.
  - a.  Sistemas operativos AIX y Oracle Solaris

En clientes AIX y Solaris, añada la entrada siguiente al archivo de inicio del sistema (`/etc/inittab` en la mayoría de las plataformas):

```
tsm::once:/usr/bin/dsmcad > /dev/null 2>&1 # TSM Client
Acceptor Daemon
```

- b.  Sistemas operativos Linux

En los clientes Linux, el programa de instalación creará un script de inicio para el aceptador de clientes (`dsmcad`) en `/etc/init.d`. El aceptador de clientes (`dsmcad`) debe iniciarse antes de poder gestionar tareas de planificador o gestionar el cliente web. Como `root`, utilice el siguiente mandato para iniciar, detener o reiniciar el aceptador de clientes o para comprobar su estado:

```
>>-service dsmcad--start---+----->>
                                +-stop----+
                                +-restart-+
                                '-status--'
```

Para permitir que el aceptador de clientes se inicie automáticamente tras arrancar el sistema, agregue el servicio como sigue, cuando se lo indique el shell:

```
# chkconfig --add dsmcad
```

Si el sistema operativo Linux ejecuta el servicio de inicialización `systemd`, siga estos pasos para iniciar `dsmcad` y ejecutarlo durante el inicio del sistema:

- i. Copie el archivo de unidad de `systemd` `/opt/tivoli/tsm/client/ba/bin/dsmcad.service` en el directorio `/etc/systemd/system/`.
- ii. Ejecute el siguiente mandato para renovar la lista de unidades `systemd`:


```
systemctl daemon-reload
```

- iii. Ejecute el mandato siguiente para iniciar el aceptador de clientes al arrancar el sistema:

```
systemctl enable dsmsvc.service
```

iv. Ejecute el mandato siguiente para iniciar el aceptador de clientes:





```
systemctl start dsmsvc.service
```





- c.  Sistemas operativos Mac OS X En Mac OS X, el aceptador de clientes debe instalarse como elemento de inicio. Para instalar e iniciar el aceptador de clientes, un administrador del sistema debe utilizar las Herramientas para administradores de IBM Spectrum Protect. Para iniciar, detener o reiniciar el aceptador de clientes, utilice el siguiente mandato:

```
>>-sudo /sbin/SystemStarter--+-start---+--dsmsvc-----><
                                     +-stop----+
                                     '-restart-'
```





3. En el archivo `dsmsvc.sys`, establezca la opción `passwordaccess` en `generate`.

4. Ejecute un mandato como `dsmsvc query sess` para almacenar la contraseña de nodo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Método tradicional:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

1. Establezca la opción `managedservices`.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris En clientes AIX, Linux y Solaris, elimine la opción en su totalidad (el valor predeterminado es `webclient`) o establézcala en `webclient`.
-  sistemas operativos Mac OS X En clientes Mac OS X, establezca la opción `managedservices` en `webclient` o `none`. No establezca la opción en `schedule`.

2. En AIX, Linux y Solaris, añada la entrada siguiente en el archivo de inicio del sistema, por ejemplo, `/etc/inittab`, si está admitido:

```
tmsched::once:/usr/bin/dsmsvc sched > /dev/null 2>&1 # TSM scheduler
```

3. En el archivo `dsmsvc.sys`, establezca la opción `passwordaccess` en `generate`.

4. Ejecute un mandato como `dsmsvc query sess` para almacenar la contraseña de nodo.

5. Para iniciar el planificador cliente en el nodo cliente y conectarlo al planificador del servidor, escriba el siguiente mandato:

```
dsmsvc schedule
```


Si el directorio actual no está en la variable de entorno `PATH`, escriba el siguiente mandato:

```
./dsmsvc schedule
```

Cuando inicie el planificador de cliente, éste se ejecutará continuamente hasta que cierre la ventana, finalice el proceso o cierre la sesión del sistema.

Para ejecutar el mandato `schedule` en segundo plano y seguir ejecutando el planificador de cliente, incluso si finaliza la sesión del sistema, entre el mandato siguiente:

```
nohup dsmsvc schedule 2> /dev/null &
```


 Sistemas operativos Windows En plataformas Windows, el planificador y el aceptador de clientes se ejecutan como servicios. Puede crear y gestionar estos servicios utilizando el asistente de configuración o el programa de utilidad de configuración de servicios de cliente de IBM Spectrum Protect, `dsmsvcutil.exe`.

 Sistemas operativos Windows


- Para iniciar el asistente para la instalación, seleccione **Herramientas > Asistente para la instalación** en la GUI de archivado y copia de seguridad y seleccione una opción **Obtener ayuda para configurar para el servicio adecuado**. Siga las indicaciones para instalar, configurar e iniciar el servicio.
- Para iniciar el programa de utilidad de configuración de servicios de cliente, abra una ventana de indicador de mandatos y emita el siguiente mandato para cambiar al directorio que contiene `dsmsvcutil.exe`:


```
cd /d "c:\Archivos de programa\tivoli\tsm\baclient"
```

Utilice `dsmsvcutil` para gestionar el servicio aceptador de clientes o el servicio del planificador. Para obtener información completa sobre cómo utilizar `dsmsvcutil`, escriba `dsmsvcutil help`.

 Sistemas operativos Windows El planificador cliente puede gestionarse mediante el aceptador de clientes. Al establecer los servicios del planificador para que se ejecuten con la gestión del daemon de aceptación de clientes, deben crearse dos servicios: el servicio de planificador y el servicio del aceptador de clientes. Al instalar el servicio del aceptador de clientes con `dsmsvcutil.exe`, utilice el parámetro

/cadschedname: para identificar qué servicio de planificador gestiona el aceptador de clientes. Si utiliza el asistente de configuración para instalar el planificador, puede seleccionar la casilla de verificación Utilizar el aceptador de cliente para gestionar el planificador, que crea automáticamente ambos servicios y los asocia.

 Sistemas operativos Windows Al utilizar de la herramienta de configuración de servicios de cliente, puede utilizar uno de los siguientes métodos:

 Sistemas operativos Windows

Método gestionado por el aceptador de clientes

1. En el archivo de opciones de cliente (dsm.opt), establezca la opción managedservices en schedule o schedule webclient.
2. En el archivo de opciones de cliente (dsm.opt), establezca la opción passwordaccess en generate.
3. Cree el servicio del planificador:

```
dsmcutil inst /name:"TSM Client Scheduler" /node:tsmclient1  
/password:secret /autostart:no /startnow:no
```

4. Cree el aceptador de clientes y asocie el servicio del planificador con el aceptador de clientes.

```
dsmcutil inst CAD /name:"TSM Client Acceptor" /cadschedname:  
"TSM Client Scheduler" /node:tsmclient1 /password:secret /autostart:yes
```


5. Inicie manualmente el servicio del aceptador de clientes:

```
net start "TSM Client Acceptor"
```

Método tradicional


1. En el archivo de opciones de cliente (dsm.opt), elimine managedservices completamente (el valor predeterminado es webclient) o establézcalo en webclient.
2. En el archivo de opciones de cliente (dsm.opt), establezca la opción passwordaccess en generate.
3. Cree el servicio del planificador:

```
dsmcutil inst /name:"TSM Client Scheduler" /node:tsmclient1  
/password:secret /autostart:yes
```

 Sistemas operativos Windows Para aumentar la fiabilidad del servicio del planificador del cliente en Windows, debe establecer los servicios para que se recuperen automáticamente de una anomalía, como se indica a continuación:

 Sistemas operativos Windows

- Inicie la consola de gestión de servicios de Windows (Inicio > Valores > Panel de control > Herramientas administrativas > Servicios)
- Pulse el botón derecho del ratón en el servicio TSM Client Scheduler y seleccione Propiedades.
- Pulse el separador Recuperación.
- Defina la acción de recuperación como Reiniciar el servicio para la primera, la segunda y las posteriores anomalías.

 Sistemas operativos Windows Si está utilizando aceptador de clientes para gestionar el planificador, debe establecer las propiedades de recuperación para el servicio TSM Client Acceptor, pero dejar los valores de recuperación para TSM Client Scheduler como Take No Action (No realizar ninguna acción) para la primera, la segunda y las posteriores anomalías. Los mismos valores de recuperación también se pueden definir para aumentar la fiabilidad de TSM Journal Service.






#### Referencia relacionada:

Cadlistenonport

## Ejemplos: visualización de información sobre trabajo planificado

Las planificaciones pueden ser clásicas o ampliadas, según como se haya definido el intervalo de la siguiente ejecución.

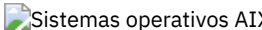
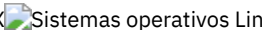
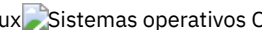


Las planificaciones clásicas permiten que el período de tiempo sea de como máximo una hora. Las planificaciones ampliadas permiten que las acciones se ejecuten en unos determinados días.

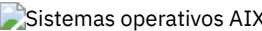
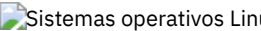
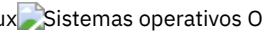

Para visualizar las planificaciones definidas para el nodo cliente, entre:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

```
dsmc query schedule
```

El cliente de copia de seguridad y archivado muestra información detallada sobre todos los trabajos planificados del nodo cliente. En la Tabla 1 se visualiza un ejemplo de la salida clásica de query schedule.

Tabla 1. Ejemplo de la salida clásica de query schedule

 Sistemas operativos AIX	 Sistemas operativos Linux	 Sistemas operativos Oracle Solaris	 sistemas operativos Mac OS X
<p>Nombre de planificación: DAILY_INC                      Descripción: Copia de seguridad diaria de todo el sistema                      Estilo de planificación: Clásico                      Action: Incremental                      Opciones: QUIET                      Objetos:                      Prioridad: 1                      Próxima ejecución: 30 minutos                      Duración: 4 horas                      Período: 1 día                      Día de la semana: Cualquiera                      Mes:                      Día de la semana:                      Semana del mes:                      Caduca: Nunca</p>			
<p>Nombre de planificación: WEEKLY_INC                      Descripción: Copia de seguridad semanal para archivos proyecto                      Estilo de planificación: Clásico                      Action: Incremental                      Opciones: QUIET                      Objetos: /proj                      Prioridad: 1                      Próxima ejecución: 60 minutos                      Duración: 8 horas                      Período: 7 días                      Día de la semana: viernes                      Mes:                      Día de la semana:                      Semana del mes:                      Caduca: Nunca</p>			
 Sistemas operativos Windows			
<p>Nombre de planificación: DAILY_INC                      Descripción: Copia de seguridad diaria de todo el sistema                      Estilo de planificación: Clásico                      Action: Incremental                      Opciones: QUIET                      Objetos:                      Prioridad: 1                      Próxima ejecución: 30 minutos                      Duración: 4 horas                      Período: 1 día                      Día de la semana: Cualquiera                      Mes:                      Día de la semana:                      Semana del mes:                      Caduca: Nunca</p>			
<p>Nombre de planificación: WEEKLY_INC                      Descripción: Copia de seguridad semanal para archivos proyecto                      Estilo de planificación: Clásico                      Action: Incremental                      Opciones: QUIET                      Objetos: e: f:                      Prioridad: 1                      Próxima ejecución: 60 minutos                      Duración: 8 horas                      Período: 7 días                      Día de la semana: viernes                      Mes:                      Día de la semana:                      Semana del mes:                      Caduca: Nunca</p>			

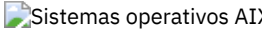
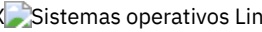
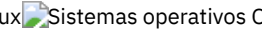

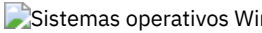
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X La planificación denominada **WEEKLY\_INC** inicia una copia de seguridad incremental semanal en el sistema de archivos /proj.

 Sistemas operativos Windows La planificación denominada **WEEKLY\_INC** inicia una copia de seguridad incremental semanal en las unidades e: y f:.

La planificación denominada **DAILY\_INC** inicia una copia de seguridad incremental diaria. La copia de seguridad incremental siguiente se inicia transcurridos 30 minutos. Como no se listan objetos, el cliente ejecuta la copia de seguridad incremental en el dominio predeterminado. La planificación no tiene fecha de caducidad.

Para determinar de forma más precisa el estado de los sucesos planificados, la salida del mandato query schedule de una planificación ampliada, en clientes de IBM Spectrum Protect versión 5.3 y posteriores, incluye campos nuevos. Estos campos aparecen siempre, tanto si se trata de una planificación clásica como de una sesión de cliente de la versión 5.3 con un servidor de una versión anterior a la 5.3, pero los campos nuevos estarán vacíos. Tenga en cuenta que para un cliente de nivel inferior (anterior a la versión 5.3), el servidor informa de los períodos como indefinidos y el día de la semana es como un día no permitido. En la Tabla 2 se muestra un ejemplo de la salida ampliada de query schedule.

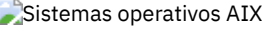
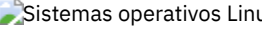
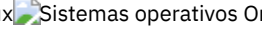

Tabla 2. Ejemplo de salida ampliada del mandato query schedule


 Sistemas operativos AIX	 Sistemas operativos Linux	 Sistemas operativos Oracle Solaris	 sistemas operativos Mac OS X
<p>Nombre de planificación: QUARTERLY_FULL Descripción: Copia de seguridad completa trimestral Estilo de planificación: Ampliado Acción: Selectiva Opciones: subdir=yes Objetos: /* /Volumes/fs2/* Prioridad: 5 Próxima ejecución: 1744 horas y 26 minutos Duración: 1 Día Período: Día de la semana: viernes Mes: marzo, junio, septiembre, diciembre Día del mes: Cualquiera Semana del mes: Última Caduca: Nunca</p>			
<p> Sistemas operativos Windows</p> <p>Nombre de planificación: QUARTERLY_FULL Descripción: Copia de seguridad completa trimestral Estilo de planificación: Ampliado Acción: Selectiva Opciones: subdir=yes Objetos: \* \volumes\fs2\ Prioridad: 5 Próxima ejecución: 1744 horas y 26 minutos Duración: 1 Día Período: Día de la semana: viernes Mes: marzo, junio, septiembre, diciembre Día del mes: Cualquiera Semana del mes: Última Caduca: Nunca</p>			

## Visualizar información sobre el trabajo completado

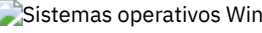
Al ejecutar el mandato schedule en primer plano, aparece en pantalla la salida de los mandatos planificados.

La salida también se dirige al archivo dsmsched.log en el directorio de instalación a menos que modifique el nombre de directorio y de archivo mediante la opción schedlogname.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Cuando se ejecuta el mandato schedule como proceso de fondo, la salida de los mandatos planificados se dirige al archivo dsmsched.log del directorio actual, o a la vía de acceso y el nombre de archivo que se han especificado. El archivo dsmsched.log no puede ser un vínculo simbólico.

 sistemas operativos Mac OS X Nota: En Mac OS X, se puede encontrar el registro por defecto en una de estas ubicaciones:

```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

 Sistemas operativos Windows Cuando se ejecuta el mandato schedule como un servicio, la salida de los mandatos planificados aparece en las anotaciones de sucesos de la aplicación. La salida también se dirige al archivo dsmsched.log en el directorio de instalación a menos que modifique el nombre de directorio y de archivo mediante la opción schedlogname. La cantidad de detalles depende de si la opción *verbose* o *quiet* está establecida en el archivo dsm.opt. El servicio del planificador también envía mensajes a las anotaciones de sucesos de Windows.

Una vez realizado el trabajo planificado, compruebe las anotaciones de planificación para verificar que todo el trabajo ha acabado correctamente.

Cuando se procesa un mandato planificado, las anotaciones de planificación contienen las entradas siguientes:

```
El suceso planificado nombresuceso finalizó satisfactoriamente
```

Si el suceso planificado no se ha completado correctamente, recibirá un mensaje similar al siguiente:

```
ANSI512E El suceso planificado nombre_suceso ha fallado. Código de retorno = código.
```

El cliente indica si IBM Spectrum Protect ha emitido correctamente el mandato planificado que se asocia a *nombre\_suceso* (action=command). No se intenta determinar el motivo de la ejecución correcta o incorrecta del mandato. Puede averiguar el estado del mandato evaluando el código de retorno del mandato planificado de las anotaciones de planificación. La entrada de las anotaciones de planificación correspondiente al código de retorno del mandato está precedida del texto siguiente:

```
Mandato finalizado. El código de retorno es:
```

El tamaño de las anotaciones de planificación sigue aumentando, a menos que podes éstas mediante la utilización de la opción schedlogretention o especifique un tamaño máximo mediante la utilización de la opción schedlogmax.

- Ejemplos: registros de sucesos  
El servicio del planificador registra información en las anotaciones de sucesos de la aplicación y proporciona un número de identificación de suceso (ID de suceso) para cada suceso de las anotaciones. En este tema se muestran ejemplos de sucesos que se han anotado en el archivo de anotaciones de sucesos de la aplicación.

#### Conceptos relacionados:

Especificar opciones de planificación

## Especificar opciones de planificación





---

Puede modificar las opciones de planificación en el archivo de opciones del cliente o la interfaz gráfica de usuario (GUI).

Sin embargo, si el administrador especifica un valor para estas opciones, ese valor prevalece sobre el valor en el cliente.

#### Conceptos relacionados:

Opciones de planificación

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Opciones del planificador para los mandatos

---

El planificador ejecuta mandatos con un identificador de usuario de 0 (root); sin embargo, es posible que algunos mandatos deban ejecutarse con un identificador de usuario que no sea 0.

En este caso, el administrador de IBM Spectrum Protect puede definir planificaciones para mandatos que se ejecutan con un identificador de usuario diferente al identificador de usuario del planificador mediante la opción de servidor schedcmduser.

La opción schedcmduser especifica el nombre de un usuario válido del sistema en el que se ejecuta un mandato planificado. Esta opción sólo puede definirla el administrador del servidor de IBM Spectrum Protect. Si se especifica esta opción, el mandato se ejecuta con la autorización del usuario especificado. De lo contrario, se ejecuta con la autorización del planificador.

```
>>-SCHEDCMDUser----nombre_usuario-----><
```

user\_name

Especifica el nombre de un usuario válido del sistema en el que se ejecuta un mandato especificado.

Nota: La opción schedcmduser *no* afecta al ID de usuario utilizado para los mandatos previos y posteriores a la planificación. Las tareas de planificación previa y posterior siempre se ejecutan como root (ID de usuario 0).

## Activar o desactivar mandatos planificados

---






Puede utilizar la opción schedcmddisabled para desactivar la planificación de mandatos del servidor.

Los mandatos se planifican mediante la opción action=*command* en el mandato del servidor DEFINE SCHEDULE.

La opción `schedcmddisabled` no desactiva los mandatos `preschedulecmd` y `postschedulecmd`. No obstante, puede especificar `preschedulecmd` o `postschedulecmd` con un espacio en blanco o una serie nula para desactivar la planificación de estos mandatos.

Puede utilizar la opción `schedrestretrdisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute operaciones de restauración o recuperación.

Puede utilizar la opción `srvprepostscheddisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute mandatos de planificación previa y posterior al realizar operaciones planificadas.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Puede utilizar la opción `srvprepostsnapdisabled` para evitar que el administrador del servidor de IBM Spectrum Protect ejecute mandatos previos y posteriores a la instantánea al realizar operaciones de copia de seguridad de instantánea planificadas.


**Referencia relacionada:**

`Schedcmddisabled`

`Schedrestretrdisabled`

`Srvprepostscheddisabled`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows `Srvprepostsnapdisabled`

 Sistemas operativos Windows

## Cambiar las opciones de proceso utilizadas por el servicio del planificador

Si configura los servicios de planificación central de IBM Spectrum Protect (el planificador, el aceptador de cliente o el agente de cliente remoto), parte de las opciones de proceso que especifica están definidas en el registro de Windows.

También se pueden especificar las opciones siguientes en el archivo de opciones del cliente (`dsm.opt`).

- `nodename`
- `httpport`
- `tcpserveraddress`
- `tcpport`
- `webports`

Cuando el planificador cliente se ejecuta como un proceso en primer plano con el mandato `dsmc sched`, se utilizan las opciones del archivo de opciones del cliente. No obstante, cuando el planificador se ejecuta como un servicio Windows, se utilizan en su lugar las opciones del registro. Si está utilizando el servicio del planificador y cambia una opción del archivo `dsm.opt`, también debe actualizar el valor correspondiente del registro.

Para actualizar el valor del registro Windows:

Utilice el asistente de configuración en la GUI del cliente. Para obtener más información, consulte el apartado Configuración del planificador.

Alternativamente, puede utilizar la herramienta `dsmcutil` para cambiar el valor del registro. Por ejemplo: `dsmcutil update scheduler /name: <nombre servicio> /node: <nombre nodo nuevo> /password: <contraseña nodo nuevo>`.

Nota: Después de actualizar el registro, debe reiniciar el servicio del planificador para que los cambios entren en vigor. Si va a utilizar la planificación gestionada por el daemon de aceptación de clientes, esto no es necesario porque para cada copia de seguridad el daemon de aceptación de clientes reinicia el planificador.





## Gestionar varios requisitos de planificador en un sistema

En determinadas situaciones es preferible tener más de una actividad planificada para cada sistema cliente.


### Acerca de esta tarea

Normalmente, se puede hacer asociando un nodo con más de una definición de planificación. Es el método estándar de ejecutar varias planificaciones en un sistema.

Debe asegurarse de que los intervalos de planificación para cada planificación no se superponen. Un único proceso de planificador cliente no puede ejecutar simultáneamente varias acciones planificadas; por lo tanto, si se produce una superposición, se ignora la segunda planificación a iniciar si la primera planificación no finaliza antes de la conclusión del intervalo de inicio de la segunda planificación.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Suponga que se debe hacer una copia de seguridad diaria de la mayoría de los sistemas de archivos del sistema cliente y que debe realizarse una

copia de seguridad cada hora de un sistema de archivos que contiene datos críticos. En este caso, sería necesario definir dos planificaciones para manejar este requisito. Para evitar que se produzca un conflicto en la planificación de la copia de seguridad diaria y a cada hora, es necesario que la opción *starttime* de cada planificación sea distinta.

 Sistemas operativos Windows Sponga que se debe hacer una copia de seguridad diaria de la mayoría de las unidades del sistema cliente y que debe realizarse una copia de seguridad cada hora de una unidad que contiene datos críticos. En este caso, sería necesario definir dos planificaciones para manejar este requisito. Para evitar que se produzca un conflicto en la planificación de la copia de seguridad diaria y a cada hora, es necesario que la opción *starttime* de cada planificación sea distinta.

En determinados casos, es necesario ejecutar más de un proceso de planificador en un sistema. Varios procesos requieren un archivo de opciones distinto para cada proceso que debe contener la siguiente información:

- Defina un nombre de nodo exclusivo para cada proceso.
- Especifique anotaciones de planificación y de error exclusivas para cada proceso.
- Cuando se ejecuta en modalidad de solicitud, utilice la opción *tcpclientport* para especificar un puerto exclusivo para cada proceso.





 Sistemas operativos Windows Nota: Cuando el planificador se ejecuta como servicio, las opciones de procesamiento especificadas en el registro de Windows alteran temporalmente las mismas opciones especificadas en el archivo de opciones del cliente.





Las ventajas de utilizar varios procesos de planificación son las siguientes:

- Se puede ejecutar más de una copia de seguridad planificada a la vez.
- Se pueden especificar distintos criterios de copia de seguridad para cada planificación iniciada, mediante el archivo de opciones del cliente o las opciones de modificación del servidor de IBM Spectrum Protect.





Los inconvenientes de utilizar varios procesos de planificación son:





- Se crea un espacio de archivos único para cada nombre de nodo en el servidor de IBM Spectrum Protect.
- Al restaurar los datos, se debe utilizar el mismo nombre de nodo asociado a la copia de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En las plataformas UNIX y Linux, pueden ejecutarse varios procesos de planificación, con el método gestionado por el daemon de aceptación de clientes o con el método tradicional de ejecución del planificador. En cualquiera de los dos casos hay determinados requisitos de instalación:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

- Cada proceso debe ejecutarse utilizando un nombre de nodo distinto.
- Debe crear varias secciones en el archivo *dsm.sys* para cada proceso del planificador. En cada sección, se debe definir un nombre de nodo exclusivo junto con los valores exclusivos para las opciones *errorlogname* y *schedlogname*. También puede optar por definir sentencias *domain*, *include* y *exclude* personalizadas para cada sección.
- En el archivo *dsm.sys*, establezca la opción *passwordaccess* para que se genere en cada sección. Debe generarse una contraseña para cada nombre de nodo que ejecute un proceso de planificador mediante un mandato como *dsmc query sess*.
- Si se ejecuta con la opción *schedmode* establecida en *prompt*, debe establecer un valor *tcpclientport* exclusivo para cada stanza.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Debe empezar cada mandato *dsmc sched* o instancia con la opción *-servername* para hacer referencia al nombre de sección exclusivo en *dsm.sys*. Para *dsmcad*, es necesario definir la variable de entorno *DSM\_CONFIG* para cada instancia de *dsmcad* de modo que haga referencia a su archivo de opciones exclusivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X A continuación se muestra un ejemplo de configuración de los dos procesos de planificación gestionados por el daemon de aceptación de clientes en el archivo *dsm.sys*. Recuerde que debe utilizar vía de accesos completas para los nombres del archivo de anotaciones para evitar que los archivos se graben en el directorio raíz):

```
servername tsm1_sched1
  nodename      aixsvt01_sched1
  tcpserver     firebat
  tcpclientport 1507
  passwordaccess generate
  domain        /svt1
  schedmode     prompted
  schedlogname  /tsm/dsmsched1.log
  errorlogname  /tsm/dsmerror1.log
  managedservices schedule
```

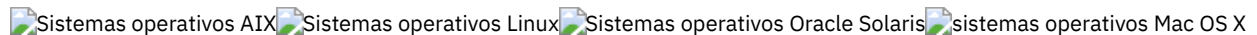
```
servername tsm1_sched2
  nodename      aixsvt01_sched2
  tcpserver     firebat
```

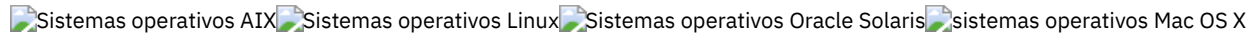


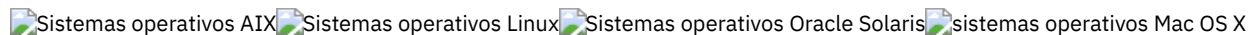
```

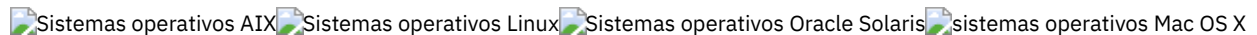
tcpclientport    1508
passwordaccess   generate
domain           /svt1
schedmode        prompted
schedlogname     /tsm/dsmsched2.log
errorlogname     /tsm/dsmerror2.log
managedservices  schedule


```


 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Contenido de /test/dsm.opt1:

 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
servername tsm1\_sched1

 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Contenido de /test/dsm.opt2:

 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
servername tsm1\_sched2

 sistemas operativos Mac OS X Abra dos ventanas de mandatos del shell:

 sistemas operativos Mac OS X

- En la ventana de mandatos del shell 1, escriba:

```

export DSM_CONFIG=/test/dsm.opt1
sudo dsmcad

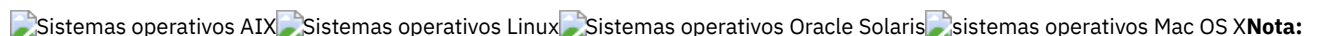
```


- En la ventana de mandatos del shell 2, escriba:

```

export DSM_CONFIG=/test/dsm.opt2
sudo dsmcad

```

 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X **Nota:** Debe escribir estos mandatos en un script de shell si desea que los procesos dsmcad se inicien directamente desde /etc/inittab para poder establecer la variable DSM\_CONFIG antes de iniciar el proceso dsmcad.

 Sistemas operativos Windows Debe crear un servicio distinto para cada proceso de planificación. Si utiliza el daemon de aceptación de clientes para gestionar el planificador, es necesario disponer de un servicio de daemon de aceptación de clientes y un servicio de planificación para cada planificación. A continuación se muestra un ejemplo de cómo establecer dos procesos de planificación de modo que sean gestionados por el daemon de aceptación de clientes:

```


dsmcutil inst /name:"TSM Client Scheduler1"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt1"
/node:tsmcli_sched1 /password:secret /autostart:no /startnow:no

dsmcutil inst CAD /name:"TSM Client Acceptor1"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt1"
/cadschedname:"TSM Client Scheduler1" /node:tsmcli_sched1 /password:secret
/autostart:yes

dsmcutil inst /name:"TSM Client Scheduler2"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt2"
/node:tsmcli_sched2 /password:secret /autostart:no /startnow:no

dsmcutil inst CAD /name:"TSM Client Acceptor2"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt2"
/cadschedname:"TSM Client Scheduler2" /node:tsmcli_sched2 /password:secret
/autostart:yes

```

 Sistemas operativos Windows Es necesario disponer de archivos de opciones exclusivos para cada instancia de planificación que deben identificarse en el momento de la creación del servicio:

Option file #1 (c:\program files\tivoli\tsm\baclient\dsm.opt1)

```

tcps             tsmserve1.example.com
nodename         tsmcli_sched1
passwordaccess   generate
schedlogname     "c:\program files\tivoli\tsm\baclient\dsm\dsmsched1.log"
errorlogname     "c:\program files\tivoli\tsm\baclient\dsm\dsmerror1.log"
schedmode        prompted
tcpclientport    1507

```

```
domain          h:
managementservices schedule
```

Option file #2 (c:\program files\tivoli\tsm\baclient\dsm.opt2)

```
tcps            tmserv1.example.com
nodename        tsmcli_sched2
passwordaccess  generate
schedlogname    "c:\program files\tivoli\tsm\baclient\dsmsched2.log"
errorlogname    "c:\program files\tivoli\tsm\baclient\dsmerror2.log"
schedmode       prompted
tcpclientport   1508
domain          i:
managementservices schedule
```

#### Conceptos relacionados:

Cambiar las opciones de proceso utilizadas por el servicio del planificador

## Códigos de retorno del cliente

La interfaz de línea de mandatos de copia de seguridad/archivado y el planificador finalizan con códigos de retorno que reflejan de forma precisa si la operación de cliente se ha realizado correctamente o no.

Los scripts, los archivos de proceso por lotes y otros recursos de automatización pueden utilizar el código de retorno de la interfaz de línea de mandatos. En operaciones que utilicen el planificador de IBM Spectrum Protect, los códigos de retorno se muestran en la salida del mandato administrativo QUERY EVENT.



En general, el código de retorno hace referencia al mensaje de mayor gravedad durante la operación de cliente.

- Si el mensaje de mayor gravedad es informativo (ANSnnnnI), entonces el código de retorno es 0.
- Si el mensaje de mayor gravedad es un aviso (ANSnnnnW), entonces el código de retorno es 8.
- Si el mensaje de mayor gravedad es un error (ANSnnnnE o ANSnnnnS), entonces el código de retorno es 12.

Se aplica una excepción a estas reglas cuando los mensajes de aviso o de error indican que no se han podido procesar archivos individuales. Para los archivos que no se pueden procesar, el código de retorno es 4. Examine el archivo dsmerror.log para determinar la causa de errores producidos durante las operaciones de cliente. Los errores que se producen durante los sucesos planificados se registran en el archivo dsmsched.log.

La Tabla 1 describe los códigos de retorno y sus significados.

Tabla 1. Códigos de retorno del cliente y significado de éstos

Código	Explicación
0	Todas las operaciones se han completado correctamente.
4	La operación no se ha completado correctamente, aunque algunos archivos no se han procesado. No ha habido más errores ni avisos. Este código de retorno es común. Los archivos no se procesan por varias razones; las siguientes razones son las más comunes. <ul style="list-style-type: none"><li>• El archivo satisface una entrada de una lista de exclusión. Los archivos excluidos generan entradas de registro sólo durante las copias de seguridad selectivas.</li><li>• El archivo estaba siendo utilizado por otra aplicación y el cliente no ha podido acceder al mismo.</li><li>• El archivo ha cambiado durante la operación hasta alcanzar un grado prohibido por el atributo de serialización de copia. Consulte Atributo Serialización de copia.</li></ul>
8	La operación se ha completado con al menos un mensaje de aviso. Para sucesos planificados, el estado es <i>Completed</i> . Revise el archivo dsmerror.log (y dsmsched.log para los sucesos planificados) para determinar qué mensajes de aviso se emitieron y valorar su impacto en la operación.
 Sistemas operativos Windows 12	 Sistemas operativos WindowsLa operación se ha completado con al menos un mensaje de error (excepto los mensajes de error de los archivos omitidos). Para sucesos planificados, el estado es <i>Failed</i> . Revise el archivo dsmerror.log (y dsmsched.log para los sucesos planificados) para determinar qué mensaje se emitieron y valorar su impacto en la operación. Generalmente, este código de retorno significa que el error era tan grave como para impedir que la operación terminase correctamente. Por ejemplo, un error que evita que una unidad completa que esté siendo procesada emita el código de retorno 12.

Código	Explicación
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X 12	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X La operación se ha completado con al menos un mensaje de error (excepto los mensajes de error de los archivos omitidos). Para sucesos planificados, el estado es <code>Failed</code> . Revise el archivo <code>dsmerror.log</code> (y <code>dsm Sched.log</code> para los sucesos planificados) para determinar qué mensaje se emitieron y valorar su impacto en la operación. Generalmente, este código de retorno significa que el error era tan grave como para impedir que la operación terminase correctamente. Por ejemplo, un error que evita que un sistema de archivos que esté siendo procesado emita el código de retorno 12.
<i>otros</i>	Para las operaciones planificadas en las que la acción programada es <code>COMMAND</code> , el código de retorno es el código de retorno desde el mandato que se ejecuta. Si el código de retorno es 0, el estado de la operación planificada es <code>Completed</code> . Si el código de retorno es distinto a cero, el estado es <code>Failed</code> .  Puede que algunos mandatos emitan un código de retorno distinto de cero para indicar que la operación se ha completado correctamente. Para estos mandatos, puede evitar un estado <code>Failed</code> introduciendo el mandato en un script que inicia el mandato, interpreta los resultados y lleva a cabo la salida. El script debería producir un código de retorno de 0 si el mandato es correcto o un código de retorno distinto de cero si el mandato falla. A continuación, pida al administrador del servidor de IBM Spectrum Protect que modifique la definición de planificación para que se ejecute el script en lugar del mandato.

El código de retorno correspondiente a un macro de cliente es el código de retorno más elevado emitido entre los mandatos individuales que componen el macro. Por ejemplo, suponga que una macro consta de estos mandatos:

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X

```
selective "/home/devel/*" -subdir=yes
incremental "/home/devel/TestDriver/*" -subdir=yes
archive "/home/plan/proj1/*" -subdir=yes
```

Sistemas operativos Windows

```
selective c:\MyTools\* -subdir=yes
incremental c:\MyPrograms\TestDriver\* -subdir=yes
archive e:\TSM\* -subdir=yes
```

Si el primer mandato finaliza con un código de retorno de 0, el segundo mandato se completa con un código de retorno de 8 y el tercer mandato finaliza con un código de retorno de 4, el código de retorno para la macro es 8.

Para obtener más información sobre el mandato `QUERY EVENT`, consulte la documentación del servidor de IBM Spectrum Protect.

#### Conceptos relacionados:

Opciones del planificador para los mandatos





## Políticas de gestión de almacenamiento

Las políticas de gestión de almacenamiento son reglas que el administrador define con el fin de gestionar las copias de seguridad y las copias archivadas en el servidor.

Los datos se asocian (o vinculan) a estas políticas, y cuando se realice una copia de seguridad de los datos o cuando éstos se archiven, se gestionarán de acuerdo con los criterios de la política. Los criterios de la política incluyen un dominio de políticas, un juego de políticas, una clase de gestión y un grupo de copia.

Las políticas determinan lo siguiente:

- Si el archivo es elegible para los servicios de copia de seguridad o archivado.
- Cuántas versiones de copia de seguridad deben conservarse.
- Durante cuánto tiempo deben conservarse las versiones de copia de seguridad y las copias archivadas inactivas.
- Dónde deben colocarse las copias en el almacenamiento.
- Para las copias de seguridad incrementales, las políticas también determinan:
  - La frecuencia con que puede hacerse una copia de seguridad de un archivo.
  - Si se debe modificar un archivo antes de volver a hacer una copia de seguridad del mismo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si tiene el cliente de IBM Spectrum Protect for Space Management instalado, el administrador define también reglas que determinan si los archivos son elegibles para la migración desde los sistemas de archivos locales al almacenamiento.

En este tema se explica lo siguiente:

- Criterios de política (dominios de políticas, juegos de políticas, grupos de copia y clases de gestión).
- Cómo visualizar políticas.
- Cómo se asocian los datos a políticas.
  
- Dominios de políticas y juegos de políticas  
Un *dominio de políticas* es un grupo de clientes que tienen unas necesidades similares de copia de seguridad/archivado de datos.
- Clases de gestión y grupos de copia  
Una *clase de gestión* es un conjunto de grupos de copia de seguridad y copia archivada que establece y contiene las necesidades de gestión de almacenamiento específicas para la copia de seguridad y el archivado de datos.
- Visualizar información sobre clases de gestión y grupos de copia  
Puede mostrar información de política con la interfaz de línea de mandatos o con la interfaz gráfica de usuario.
- Seleccionar una clase de gestión para los archivos  
Si la clase de gestión predeterminada satisface las necesidades de copia de seguridad/archivado para todos los archivos de su estación de trabajo, no es necesario emprender ninguna acción para asociar los archivos a dicha clase de gestión. Esto tiene lugar automáticamente cuando realice copia de seguridad o archive los archivos.
- Asignar una clase de gestión a los archivos  
Una clase de gestión define cuándo se incluyen los archivos en una copia de seguridad, durante cuánto tiempo se conservan en el servidor y cuántas versiones del archivo debe conservar el servidor.
- Sustituirla clase de gestión para las copias archivadas  
Al archivar un archivo, puede sustituir la clase de gestión asignada mediante la interfaz gráfica de usuario (GUI), o mediante la opción archmc del mandato archive.
- Seleccionar una clase de gestión para los directorios  
Si la clase de gestión del conjunto de políticas activo que contiene el valor del período más largo para "Retener única versión" (REONLY) satisface los requisitos de copia de seguridad para los directorios, puede que no sea necesario realizar ninguna acción para asociar los directorios a esa clase de gestión. La asociación de clases de gestión se lleva a cabo automáticamente cuando se realiza la copia de seguridad de los directorios.
- Vincular clases de gestión a archivos  
La *vinculación* asocia un archivo a una clase de gestión.
- Revincular las versiones de copias de seguridad a los archivos  
La *revinculación* asocia un archivo o una imagen de volumen lógico a una nueva clase de gestión.
- Período de gracia de retención  
IBM Spectrum Protect también proporciona un *período de gracia de retención de copia de seguridad* y un *período de gracia de retención de copias archivadas* como ayuda para proteger los datos de las copias de seguridad y de las copias archivadas cuando no es posible volver a vincular un archivo con la clase de gestión adecuada.
- Protección de retención de políticas basadas en sucesos  
Todas las clases de gestión que tienen un grupo de copia archivada deben especificar un período de retención; por ejemplo, el número de días que un objeto archivado se almacena en el servidor antes de suprimirse.

## Dominios de políticas y juegos de políticas

---

Un *dominio de políticas* es un grupo de clientes que tienen unas necesidades similares de copia de seguridad/archivado de datos.

Los dominios de políticas contienen uno o varios juegos de políticas. Un administrador utiliza dominios de políticas para gestionar un grupo de nodos cliente de una forma lógica.

Un dominio de políticas puede incluir, por ejemplo:

- Un departamento, como por ejemplo Contabilidad.
- Una ubicación física, como por ejemplo un edificio o un piso concreto.
- Una red de área local, como por ejemplo todos los clientes asociados a un servidor de archivos concreto.

IBM Spectrum Protect incluye un dominio de políticas predeterminado denominado *Standard*. En primer lugar, el nodo cliente puede estar asociado al dominio de políticas predeterminado. Sin embargo, el administrador puede definir dominios de políticas adicionales si hay grupos de usuarios con unas necesidades de copia de seguridad/archivado exclusivas.





Un *juego de políticas* es un grupo de una o varias clases de gestión. Cada dominio de políticas puede contener varios juegos de políticas. El administrador utiliza un juego de políticas para implementar clases de gestión diferentes basándose en las necesidades de la empresa y del usuario. Sólo uno de estos juegos de políticas puede estar activo a la vez. A éste se le conoce como *juego de políticas activo*. Cada juego de políticas contiene una *clase de gestión predeterminada* y un número cualquiera de clases de gestión adicionales.






## Clases de gestión y grupos de copia

Una *clase de gestión* es un conjunto de grupos de copia de seguridad y copia archivada que establece y contiene las necesidades de gestión de almacenamiento específicas para la copia de seguridad y el archivado de datos.

Un administrador puede establecer clases de gestión distintas para satisfacer las necesidades de copia de seguridad/archivado de diferentes tipos de datos, como por ejemplo:

- Datos del sistema que son cruciales para la empresa.
- Datos de la aplicación que cambian a menudo.
- Datos de informe que los encargados de la gestión revisan mensualmente.
- Información legal que debe conservarse indefinidamente, con lo cual se necesita una gran cantidad de espacio de disco.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota: Si tiene instalado IBM Spectrum Protect for Space Management, también puede contener requisitos específicos para migrar archivos al almacén.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows La mayoría del trabajo que se realiza con las políticas de gestión de almacenamiento tiene que ver con las clases de gestión. Cada archivo y directorio del que realice una copia de seguridad y cada archivo del que se realice una copia archivada está asociado a (o *enlazado a*) una clase de gestión de la forma siguiente:

- Si los datos no están asociados con una clase de gestión, IBM Spectrum Protect utiliza la clase de gestión predeterminada del juego de políticas activo.
- Cuando realice una copia de seguridad de los directorios, podrá especificar una clase de gestión con una sentencia *include* o la opción *dirmc*. Si no especifica ninguna clase de gestión, IBM Spectrum Protect utilizará la clase de gestión del juego de políticas activo que especifique el período de retención "Solo retención". Si varias clases de gestión se ajustan a este criterio, IBM Spectrum Protect utiliza el último que haya encontrado, en orden alfabético.
- Para los directorios de copias archivadas, puede especificar una clase de gestión con una sentencia *include.archive* o la opción *archmc*. Si no especifica una clase de gestión, el servidor asigna al directorio archivado la clase de gestión predeterminada. Si la clase de gestión predeterminada no tiene grupo de copia archivada, el servidor asigna la clase de gestión que tiene actualmente el grupo de copia archivada con el período de retención más corto.

Puede utilizar sentencias de *inclusión* en la lista de inclusión/exclusión para asociar los archivos a las clases de gestión. En el archivo de opciones del sistema cliente, puede asociar directorios con una clase de gestión mediante la opción *dirmc*.

Dentro de una clase de gestión, las necesidades específicas de copia de seguridad/archivado se encuentran en *grupos de copia*. Los grupos de copia definen los atributos específicos de gestión de almacenamiento que describen cómo maneja el servidor los datos de los que se ha hecho copia de seguridad o que se han archivado. Los grupos de copia incluyen tanto los *grupos de copia de seguridad* como los *grupos de copia archivada*. Una clase de gestión puede tener un grupo de copia de seguridad, un grupo de copia archivada, ambos grupos, o ninguno.

Un *grupo de copia de seguridad* contiene atributos que se utilizan durante el proceso de copia de seguridad para determinar lo siguiente:

- Cuántos días deben transcurrir para que se vuelva a hacer una copia de seguridad de un archivo.
- Cómo se procesa un archivo durante una copia de seguridad si éste está en uso.

También contiene atributos para gestionar las versiones de copia de seguridad de los archivos en el servidor. Estos atributos controlan lo siguiente:

- En qué tipo de medio almacena el servidor las versiones de copia de seguridad de los archivos y directorios.
- Cuántas versiones de copia de seguridad debe conservar el servidor de los archivos y los directorios.
- Durante cuánto tiempo debe conservar el servidor las versiones de copia de seguridad de los archivos y los directorios.
- Durante cuánto tiempo almacena el servidor las copias de seguridad inactivas.
- Durante cuánto tiempo se almacena la última versión inactiva de un archivo.

Un *grupo de copia archivada* contiene atributos que controlan lo siguiente:

- Si se archiva un archivo que está en uso.
- En qué tipo de medio el servidor almacena las copias archivadas de los archivos.
- Durante cuánto tiempo almacena el servidor las copias archivadas de los archivos.

### Conceptos relacionados:

Seleccionar una clase de gestión para los archivos

Período de gracia de retención

## Visualizar información sobre clases de gestión y grupos de copia

Puede mostrar información de política con la interfaz de línea de mandatos o con la interfaz gráfica de usuario.

En una interfaz gráfica de usuario, pulse **Ver información de políticas** en el menú Programas de utilidad. La ventana **Información de política** muestra las clases de gestión disponibles. En una línea de mandatos, utilice el mandato query mgmtclass para ver las clases de gestión disponibles. La opción detail proporciona más información.

En la Tabla 1 se muestran los valores predeterminados para los grupos de copia de seguridad y copia archivada en la clase de gestión estándar.

Tabla 1. Valores de atributo predeterminados de la clase de gestión estándar

Atributo	Valor predeterminado de copia de seguridad	Valor predeterminado de archivado
Nombre de grupo de copia	Standard	Standard
Tipo de copia	Copia seguridad	Archive
Frecuencia de copia	0 días	CMD (mandato)
Versiones si datos existen	2 versiones	No se aplica
Versiones si datos suprimidos	1 versión	No se aplica
Retener versiones adicionales	30 días	No se aplica
Retener única versión	60 días	No se aplica
Serialización de copia	Estática compartida	Estática compartida
Modalidad de copia	Modificado	Absoluta
Destino de copia	Backuppool	Archivepool
Retener versión	No se aplica	365 días
Sin LAN	Destino	No
Eliminación de duplicados habilitada	No	No

- **Atributo Nombre de grupo de copias**  
El atributo *nombre de grupo de copias* es el nombre del grupo de copias. El valor predeterminado para la copia de seguridad y el archivado es *estándar*.
- **Atributo Tipo de copia**  
El atributo *tipo de grupo de copias* es el tipo del grupo de copias. El valor para la copia de seguridad es siempre *copia de seguridad*; el valor para el archivado es siempre *archivado*.
- **Atributo Frecuencia de copia**  
El atributo *Frecuencia de copia* es el número mínimo de días que deben transcurrir entre las sucesivas copias de seguridad incrementales. Utilice este atributo durante la realización de una copia de seguridad incremental completa.
- **Atributo Versiones si datos existen**  
El atributo *versiones si datos existen* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios.
- **Atributo Versiones si datos suprimidos**  
El atributo *Versiones si datos suprimidos* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios que ha borrados.
- **Atributo Retener versiones adicionales**  
El atributo *Retener versiones adicionales* especifica durante cuántos días deben conservarse todas las versiones de copia de seguridad excepto la más reciente.
- **Atributo Retener única versión**  
El atributo *Retener única versión* especifica durante cuántos días debe conservarse la última versión inactiva restante de un archivo o un directorio.
- **Atributo Serialización de copia**  
El atributo *Serialización de copia* determina si un archivo puede estar en uso durante un proceso de copia de seguridad o archivado y qué se debe hacer en caso afirmativo.
- **Parámetro de modalidad de copia**  
El parámetro *mode* de copia determina si un archivo o directorio se considera para la copia de seguridad incremental sin tener en cuenta si ha cambiado o no desde la última copia de seguridad.
- **Atributo Destino de copia**  
El atributo *destino de copia* designa el destino en el que se almacenan las copias de seguridad o copias archivadas.

- Atributo Retener versiones  
El atributo *retener versiones* especifica el número de días que una copia archivada permanece en el almacenamiento.
- Atributo Eliminar duplicados de datos  
El atributo *Eliminar duplicados de datos* especifica si los datos redundantes se transferirán al servidor de IBM Spectrum Protect durante el proceso de archivado y copia de seguridad.

## Atributo Nombre de grupo de copias

---

El atributo *nombre de grupo de copias* es el nombre del grupo de copias. El valor predeterminado para la copia de seguridad y el archivado es *estándar*.

## Atributo Tipo de copia

---

El atributo *tipo de grupo de copias* es el tipo del grupo de copias. El valor para la copia de seguridad es siempre *copia de seguridad*; el valor para el archivado es siempre *archivado*.



## Atributo Frecuencia de copia


---

El atributo *Frecuencia de copia* es el número mínimo de días que deben transcurrir entre las sucesivas copias de seguridad incrementales. Utilice este atributo durante la realización de una copia de seguridad incremental completa.

Las copias de frecuencia funcionan con el parámetro *mode*. Por ejemplo, si *frequency=0* y *mode=modified*, se hará copia de seguridad de un archivo o directorio únicamente si se ha modificado desde la última copia de seguridad incremental. Si *frequency=0* y *mode=absolute*, se hará copia de seguridad de un objeto cada vez que se haga una copia de seguridad incremental contra el mismo. Si *frequency=0* y *mode=absolute*, las modificaciones y el número de días desde la última copia de seguridad no afectan en la operación de seguridad actual. En las copias de seguridad selectivas no se comprueba el atributo *frequency*.

Para los grupos de copia archivada, la frecuencia de copia es siempre CMD (mandato). No hay ninguna restricción en cuanto a la frecuencia con que se archiva un objeto.

 Sistemas operativos AIX  Sistemas operativos Windows La frecuencia de copia se pasa por alto durante una copia de seguridad con registro por diario.

 Sistemas operativos Windows La copia de seguridad incremental con registro por diario difiere de la copia de seguridad incremental completa tradicional, porque IBM Spectrum Protect no aplica las frecuencias de copia no predeterminadas (diferentes de 0).

## Atributo Versiones si datos existen

---

El atributo *versiones si datos existen* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios.

Si selecciona una clase de gestión que permite más de una versión de copia de seguridad, la versión más reciente recibe el nombre de versión *activa*. Al resto de versiones se las denomina versiones *inactivas*. Si el número máximo de versiones permitidas es cinco, y se ejecuta una copia de seguridad que crea una sexta versión, la versión más antigua se suprime del almacenamiento del servidor.

## Atributo Versiones si datos suprimidos

---

El atributo *Versiones si datos suprimidos* especifica el número máximo de las diferentes versiones de copia de seguridad que se conservan para los archivos y directorios que ha borrados.

Este parámetro se ignora hasta que elimina el archivo o directorio.

Si borra el archivo o el directorio, la próxima vez que ejecute una copia de seguridad incremental, la versión de copia de seguridad activa pasará a estar inactiva. El servidor de IBM Spectrum Protect suprime la versión más antigua por encima del número especificado por este parámetro.

La fecha de caducidad para el resto de versiones depende de los parámetros *Retener versiones adicionales* y *Retener única versión*.

## Atributo Retener versiones adicionales

---

El atributo *Retener versiones adicionales* especifica durante cuántos días deben conservarse todas las versiones de copia de seguridad excepto la más reciente.

La versión más reciente es la versión activa, y las versiones activas no pueden borrarse. Si se especifica *Nolimit*, las versiones de copia de seguridad adicionales se suprimen según el valor del parámetro *versiones si datos existen* o *versiones si datos suprimidos*. En este caso, la versión adicional más antigua se suprime de forma inmediata.

## Atributo Retener única versión

---

El atributo *Retener única versión* especifica durante cuántos días debe conservarse la última versión inactiva restante de un archivo o un directorio.

Si se especifica *Sin límite*, la última versión se conserva indefinidamente.

Este parámetro surte efecto durante la siguiente copia de seguridad incremental después de que se haya suprimido un archivo del sistema cliente. Las actualizaciones posteriores de este parámetro no afectarán a los archivos que ya estén inactivos. Por ejemplo: Si este parámetro está establecido en 10 días cuando se desactiva un archivo durante una copia de seguridad incremental, el archivo se eliminará del servidor a los 10 días.

## Atributo Serialización de copia

---

El atributo Serialización de copia determina si un archivo puede estar en uso durante un proceso de copia de seguridad o archivado y qué se debe hacer en caso afirmativo.

El valor de este atributo puede ser uno de los siguientes:


- **Estática.** Durante una operación de copia de seguridad o archivado, no deben modificarse ni los archivos ni los directorios. Si se modifica un objeto durante un intento de copia de seguridad o archivado, dichos procesos no se realizarán.
- **Estático compartido.** Durante una operación de copia de seguridad o archivado, no deben modificarse ni los archivos ni los directorios. El cliente intenta realizar una copia de seguridad o un archivado hasta cuatro veces más, según el valor especificado en la opción *changinorettries* de su archivo de opciones. Si se modifica un objeto durante cada intento de copia de seguridad o archivado, dichos procesos no se realizarán.
- **Dinámica.** Se realiza una copia de seguridad o una copia archivada de un archivo o un directorio en el primer intento independientemente de si éste cambia durante dichos procesos.
- **Dinámico compartido.** Se realiza una copia de seguridad o una copia archivada de un archivo o un directorio independientemente de si éste cambia durante dichos procesos. El cliente intenta realizar una copia de seguridad o archivado hasta cuatro veces más. El número de intentos depende del valor que se haya especificado en la opción *changinorettries* del archivo de opciones, sin que el archivo cambie durante el intento. En el último intento, se hace copia de seguridad o se archiva el archivo aunque éste haya cambiado.

Si selecciona una clase de gestión que permite realizar una copia de seguridad o archivado mientras el archivo objeto de dichas operaciones está en uso, la versión de copia de seguridad o la copia archivada que está almacenada en el servidor puede ser una copia difusa. Una *copia difusa* es una versión de copia de seguridad o copia archivada que no refleja de forma precisa el contenido real del archivo. Puede que contenga los cambios, pero no todos. Si esto no es aceptable, seleccione una clase de gestión que cree una versión de copia de seguridad o copia archivada sólo si el archivo no cambia durante la copia de seguridad o el archivado. Cuando se utiliza la serialización estática, las aplicaciones no pueden abrir un archivo para el acceso de escritura mientras se hace una copia de seguridad del archivo.


Si restaura o recupera un archivo que contiene una copia difusa, puede que el archivo no sea utilizable. No utilice la serialización dinámica ni la serialización dinámica compartida para hacer copias de seguridad de archivos salvo que esté totalmente seguro de que puede utilizarse una copia difusa restaurada.

Importante: Si selecciona una clase de gestión con un grupo de copia que especifique dinámica compartida o copia de seguridad dinámica de serialización, debe ir con cuidado.

### Conceptos relacionados:

 Sistemas operativos Windows Soporte de archivos abiertos para las operaciones de copia de seguridad

### Tareas relacionadas:

 Sistemas operativos Windows Configuración del soporte de archivos abiertos

### Referencia relacionada:

Snapshotproviderimage

## Parámetro de modalidad de copia

---

El parámetro *mode* de copia determina si un archivo o directorio se considera para la copia de seguridad incremental sin tener en cuenta si ha cambiado o no desde la última copia de seguridad.








El cliente no comprueba el parámetro de modalidad cuando ejecuta copias de seguridad selectivas.

El valor para este parámetro puede ser uno de los siguientes ajustes:

#### Modificados

El objeto se tiene en cuenta para la copia de seguridad incremental solo si este ha cambiado desde la última copia de seguridad. Se considera que un objeto ha cambiado cuando se cumple una de las condiciones siguientes:

- La fecha u hora de la última modificación es distinta.
- El tamaño es distinto.
-  Sistemas operativos Windows Los atributos, excepto el atributo de archivado, son diferentes.
- Si sólo han cambiado los metadatos (como por ejemplo los permisos de acceso), es posible que el cliente sólo haga copia de seguridad de los metadatos.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X El propietario es distinto.

#### absolute

El objeto se tiene en cuenta para la copia de seguridad incremental independientemente de si ha cambiado desde la última copia de seguridad. Para los grupos de copia archivada, la modalidad es siempre Absoluta, lo cual indica que un objeto se archiva independientemente de si ha cambiado desde la última solicitud de archivado.

## Atributo Destino de copia

---

El atributo *destino de copia* designa el destino en el que se almacenan las copias de seguridad o copias archivadas.

El destino puede ser una agrupación de almacenamiento de dispositivos de disco o una agrupación de almacenamiento de dispositivos que admiten medios extraíbles, como por ejemplo una cinta.

## Atributo Retener versiones

---

El atributo *retener versiones* especifica el número de días que una copia archivada permanece en el almacenamiento.

Cuando transcurre el número de días especificado para una copia archivada de un archivo, ésta se suprime del almacenamiento del servidor.

## Atributo Eliminar duplicados de datos

---

El atributo *Eliminar duplicados de datos* especifica si los datos redundantes se transferirán al servidor de IBM Spectrum Protect durante el proceso de archivado y copia de seguridad.

#### Conceptos relacionados:

Deduplicación de datos del lado del cliente

#### Referencia relacionada:

Eliminación de duplicados

Enablededupcache

Opciones exclude

## Seleccionar una clase de gestión para los archivos

---

Si la clase de gestión predeterminada satisface las necesidades de copia de seguridad/archivado para todos los archivos de su estación de trabajo, no es necesario emprender ninguna acción para asociar los archivos a dicha clase de gestión. Esto tiene lugar automáticamente cuando realice copia de seguridad o archive los archivos.

Si selecciona una clase de gestión diferente para los archivos, tenga en cuenta las tres preguntas siguientes:

- ¿La clase de gestión contiene un grupo de copia de seguridad?

Si intenta realizar una copia de seguridad de un archivo asociado a una clase de gestión que no contiene un grupo de copia de seguridad, la copia de seguridad no se realizará.

- ¿La clase de gestión contiene un grupo de copia archivada?

No puede archivar un archivo asociado a una clase de gestión que no contenga un grupo de copia archivada.

- ¿El grupo de copia de seguridad contiene atributos que realizan copias de seguridad de los archivos con la frecuencia suficiente?

La modalidad y la frecuencia funcionan conjuntamente para controlar con qué frecuencia se realiza copia de seguridad de un archivo cuando se utiliza la copia de seguridad incremental. Estos atributos no se comprueban para copias de seguridad selectivas.

- ¿Qué método de serialización utiliza el grupo de copia?

El método de serialización determina cómo funciona IBM Spectrum Protect cuando un archivo cambia mientras se realiza una copia de seguridad de él.

- ¿El grupo de copia de seguridad especifica un número adecuado de versiones de copia de seguridad para conservar y una cantidad adecuada de tiempo de conservación?
- ¿El grupo de copia archivada especifica una cantidad adecuada de tiempo para conservar las copias archivadas de los archivos?

#### Conceptos relacionados:

Atributo Serialización de copia

## Asignar una clase de gestión a los archivos

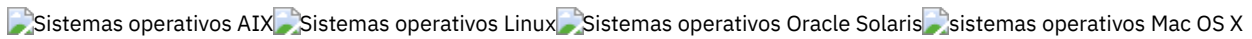
Una clase de gestión define cuándo se incluyen los archivos en una copia de seguridad, durante cuánto tiempo se conservan en el servidor y cuántas versiones del archivo debe conservar el servidor.

El administrador del servidor selecciona una clase de gestión predeterminada. Puede especificar su propia clase de gestión para sustituir la clase de gestión predeterminada.

Para asignar una clase de gestión distinta de la predeterminada a los directorios, utilice la opción `dirmc` en el archivo de opciones de cliente.

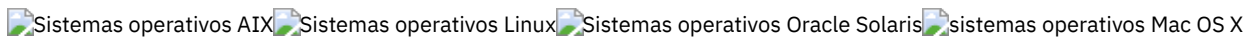
Puede asignar una clase de gestión a un archivo o grupo de archivos utilizando una sentencia `include` en el archivo de opciones. También puede asignar una clase de gestión utilizando una sentencia `include` en el archivo de inclusión-exclusión especificado por la opción `inlexcl`. Los nombres de clase de gestión no son sensibles a mayúsculas y minúsculas.

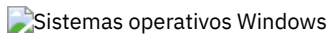
Mediante el uso del cliente de línea de mandatos, para asociar todos los archivos del directorio `costs` con la clase de gestión denominada `budget`, deberá entrar:

 `include /home/proj2/costs/* budget`

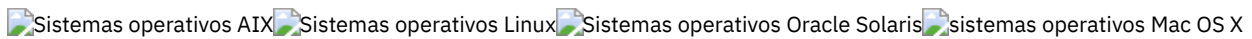
 `include c:\adsm\proj2\costs\* budget`

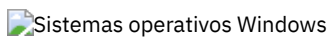
Para especificar una clase de gestión denominada `managall` que se utilice para todos los archivos a los que no se asigne de forma explícita una clase de gestión, deberá especificar lo siguiente:

 `include ../../* managall`

 `include ?:\..\* managall`

Los ejemplos siguientes muestran cómo asignar una clase de gestión a archivos:

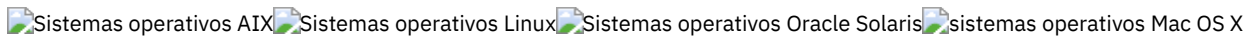
 `exclude ../../*.sno  
include /home/winter/../../*.ice mcweekly  
include /home/winter/december/*.ice mcdaily  
include /home/winter/january/*.ice mcmonthly  
include /home/winter/february/white.sno`

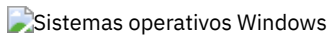
 `exclude ?:\..\*.sno  
include c:\winter\..\*.ice mcweekly  
include c:\winter\december/*.ice mcdaily  
include c:\winter\january/*.ice mcmonthly  
include c:\winter\february\white.sno`

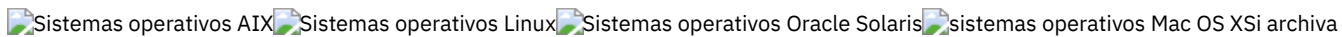
El proceso sigue estos pasos:

1. Se hace una copia de seguridad del archivo `white.sno` del directorio `february` del directorio `winter` siguiendo las reglas de proceso ascendente. Puesto que no se ha especificado ninguna clase de gestión en esta sentencia, el archivo se asigna a la clase de gestión predeterminada.
2. Cualquier archivo con una extensión de `ice` en el directorio `january` se asigna a la clase de gestión denominada `mcmmonthly`.
3. Cualquier archivo con una extensión de `ice` en el directorio `december` se asigna a la clase de gestión denominada `mcdaily`.
4. Los demás archivos con una extensión de `ice` en cualquier directorio bajo el directorio `winter` se asignan a la clase de gestión denominada `mcweekly`.
5. Los archivos que tengan una extensión `sno` de cualquier directorio quedarán excluidos de la copia de seguridad. La excepción a esta regla es `white.sno` en el directorio `february`, que está en el directorio `winter`.

Para especificar su propia clase de gestión predeterminada `mgmt_class_name` para los archivos que no se incluyen de forma explícita, ponga la siguiente sentencia en la parte superior de la lista de inclusión:

 `include ../../* nombre_clase_gestión`

 `include ?:\..\* mgmt_class_name`

 Si archiva un archivo mediante la interfaz gráfica de usuario (GUI), puede seleccionar otra clase de gestión para que sustituya la asignada al archivo.

#### Referencia relacionada:

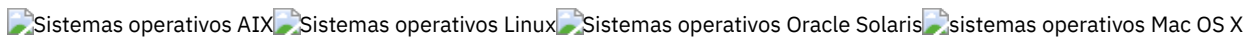
Dirmc  
Opciones include


## Sustituirla clase de gestión para las copias archivadas

Al archivar un archivo, puede sustituir la clase de gestión asignada mediante la interfaz gráfica de usuario (GUI), o mediante la opción `archmc` del mandato `archive`.

Sustituir la clase de gestión mediante la GUI equivale a utilizar la opción `archmc` en el mandato `archive`. Para utilizar la GUI, pulse el botón **Opciones** en el árbol de archivado para sustituir la clase de gestión y seleccionar una clase de gestión distinta.

En la línea de mandatos, para asociar el archivo `budget.jan` a la clase de gestión **ret2yrs**, debería escribir este mandato:

 `dsmc archive -archmc=ret2yrs /home/jones/budget.jan`

 `dsmc archive -archmc=ret2yrs c:\plan\proj1\budget.jan`

## Seleccionar una clase de gestión para los directorios

Si la clase de gestión del conjunto de políticas activo que contiene el valor del período más largo para "Retener única versión" (RETONLY) satisface los requisitos de copia de seguridad para los directorios, puede que no sea necesario realizar ninguna acción para asociar los directorios a esa clase de gestión. La asociación de clases de gestión se lleva a cabo automáticamente cuando se realiza la copia de seguridad de los directorios.

Si hay más de una clase de gestión con el valor RETONLY más largo, el cliente de IBM Spectrum Protect selecciona la clase de gestión cuyo nombre ocupe, por orden alfabético, la última posición.

Si la clase de gestión predeterminada no satisface los requisitos, seleccione una clase de gestión para la que se especifique un período de retención adecuado en el parámetro Retener única versión. Por ejemplo, si la clase de gestión realiza la copia de seguridad de los datos directamente en cinta, pero desea que las copias de seguridad de directorio se dirijan al disco, debe seleccionar una clase de gestión distinta. Debe conservar los directorios como mínimo durante el mismo tiempo que conserva los archivos asociados a estos directorios.

Para los directorios de copia de seguridad, utilice la opción `dirmc` para especificar la clase de gestión a la que se vinculan los directorios.

Para los directorios de archivado, utilice la opción `archmc` con el mandato `archive`.

A continuación se indican los métodos que puede utilizar para ver las clases de gestión disponibles y los atributos de éstas:

- GUI o cliente web: seleccione Ver información de políticas en el menú Herramientas.
- Cliente de línea de mandatos: ejecute `dsmc query mgmtclass -detail`.

Nota: En un servidor de IBM Spectrum Protect, durante el proceso de caducidad, si un directorio archivado reúne los requisitos para la aplicación de la caducidad, el servidor comprueba si alguna de las copias archivadas existentes necesita que se conserve el directorio archivado. En caso afirmativo, al directorio archivado no se le aplica la caducidad, y el cliente de copia de seguridad y archivado actualiza la fecha de inserción del directorio archivado para garantizar que la caducidad del directorio no se producirá antes de que caduquen los archivos que éste contiene.

## Vincular clases de gestión a archivos

---

La *vinculación* asocia un archivo a una clase de gestión.

Cuando se realiza una copia de seguridad de un archivo por primera vez, IBM Spectrum Protect lo enlaza a la clase de gestión predeterminada o bien a la clase de gestión especificada en la lista de inclusión/exclusión.

Si el grupo de copia de seguridad de la clase de gestión especifica que deben conservarse varias versiones de copia de seguridad del archivo, y se solicitan varias copias de seguridad, el servidor siempre tiene una versión de copia de seguridad activa (la versión actual) y una o varias versiones de copia de seguridad del archivo inactivas. Todas las versiones de copia de seguridad de un archivo se vinculan a la misma clase de gestión y se gestionan de acuerdo con los atributos especificados en el grupo de copia de seguridad.

Cuando se archiva un archivo por primera vez, IBM Spectrum Protect lo enlaza a la clase de gestión predeterminada, a la clase de gestión especificada en la lista de inclusión/exclusión o a la clase de gestión indicada al modificar las opciones de archivado durante una operación de archivado.

Las copias archivadas nunca se vuelven a vincular a otra clase de gestión. Si cambia la clase de gestión de un archivo con una sentencia `include.archive`, la opción `archmc` o mediante una interfaz gráfica de usuario del cliente de copia de seguridad y archivado, las copias anteriores de dicho archivo seguirán estando vinculadas a la clase de gestión especificada cuando se archivaron.

Si se suprime un archivo en el sistema cliente, los objetos inactivos del archivo no se vuelven a vincular.

Para obtener información sobre cómo asociar archivos y directorios con clases de gestión, consulte la documentación del servidor de IBM Spectrum Protect.

## Revincular las versiones de copias de seguridad a los archivos

---

La *revinculación* asocia un archivo o una imagen de volumen lógico a una nueva clase de gestión.

Las copias de seguridad de los archivos se vuelven a vincular a una clase de gestión diferente en las condiciones siguientes. En todas estas condiciones, los archivos (activos e inactivos) no se vuelven a vincular hasta la próxima operación de copia de seguridad.

- Se especifica una clase de gestión distinta en una sentencia de inclusión para cambiar la clase de gestión del archivo. Las copias de seguridad se gestionan de acuerdo con la clase de gestión antigua hasta que se ejecute otra copia de seguridad.
- El administrador suprime la clase de gestión del juego de políticas activo. Se utiliza la clase de gestión predeterminada para gestionar las versiones de copia de seguridad cuando se vuelva a hacer una copia de seguridad del archivo.
- El administrador asigna el nodo cliente a un dominio de políticas diferente, y el juego de políticas activo del dominio no contiene una clase de gestión con el mismo nombre. Se utiliza la clase de gestión predeterminada del nuevo dominio de políticas para gestionar las versiones de copia de seguridad.

Para obtener información sobre cómo asociar archivos y directorios con clases de gestión, consulte la documentación del servidor de IBM Spectrum Protect.

## Período de gracia de retención

---

IBM Spectrum Protect también proporciona un *período de gracia de retención de copia de seguridad* y un *período de gracia de retención de copias archivadas* como ayuda para proteger los datos de las copias de seguridad y de las copias archivadas cuando no es posible volver a vincular un archivo con la clase de gestión adecuada.

El período de gracia de retención de copia de seguridad se utiliza en los siguientes casos:

- Se cambia la clase de gestión de un archivo, pero ni la clase de gestión predeterminada ni la nueva clase de gestión contienen un grupo de copia de seguridad.
- La clase de gestión a la que se vincula un archivo ya no existe, y la clase de gestión predeterminada no contiene un grupo de copia de seguridad.

El período de gracia de retención de copia de seguridad, definido en el dominio de políticas, se inicia al ejecutarse una copia de seguridad incremental. El valor predeterminado es 30 días. Sin embargo, el administrador puede ampliar o reducir este período.

Cuando el servidor de IBM Spectrum Protect gestiona un archivo mediante el período de gracia de retención de copia de seguridad, no crea versiones de copia de seguridad del archivo nuevas. Todas las versiones de copia de seguridad del archivo existentes caducan a los 30 días (o el número de días especificado en el dominio de políticas) a partir del día en el que se marcan como inactivas.

Las copias archivadas nunca se vuelven a vincular porque cada operación de archivado crea una copia archivada distinta. Las copias archivadas permanecen vinculadas al nombre de clase de gestión especificado cuando el usuario las archivó. Si la clase de gestión a la que está vinculada una copia archivada ya no existe o ya no contiene un grupo de copia archivada, el servidor utiliza la clase de gestión predeterminada. Si más adelante se cambia o restituye la clase de gestión predeterminada, el servidor utiliza la clase de gestión predeterminada actualizada para gestionar la copia archivada. Si la clase de gestión predeterminada no contiene un grupo de copia archivada, el servidor utiliza el período de gracia de retención de copias archivadas especificado para el dominio de políticas.

## Protección de retención de políticas basadas en sucesos

---

Todas las clases de gestión que tienen un grupo de copia archivada deben especificar un período de retención; por ejemplo, el número de días que un objeto archivado se almacena en el servidor antes de suprimirse.

La política basada en sucesos ofrece la opción de iniciar el período de retención en el momento de archivarse el objeto o bien posteriormente, cuando se envía un suceso de activación relacionado con ese objeto al servidor.

Si se establece el valor `RETINIT=CREATE` para el grupo de copias, el período de retención de datos se inicia cuando se archiva el archivo. Si se utiliza el valor de grupo de copias `RETINIT=EVENT` el período de retención de datos se inicia cuando el servidor recibe la notificación de que se ha producido el suceso.

Este concepto se demuestra en el ejemplo siguiente:

El usuario tiene dos archivos, `create.file` y `event.file`. El usuario dispone de dos clases de gestión; `CREATE`, con `RETINIT=CREATE`, y `EVENT`, con `RETINIT=EVENT`. Las dos clases de gestión tienen un período de retención de 60 días. El usuario realiza el archivado de ambos archivos el mismo día:

```
dsmc archive create.file -archmc=CREATE
dsmc archive event.file -archmc=EVENT
```

Diez días después, el usuario emite el mandato `set event -type=hold` para el archivo `create.file`, por lo que el archivo no puede suprimirse. El mismo día, el usuario emite el mandato `set event -type=activate` para el archivo `event.file`. En ese momento, el período de retención restante de `create.file` es de 50 días y el de `event.file` es de 60 días. Si no se realiza ninguna otra acción, `create.file` se conserva en el servidor indefinidamente y `event.file` caduca 70 días después de haberse creado (60 días después de que se haya producido el suceso de éste). Sin embargo, si transcurren 20 días desde la realización del archivado inicial, el usuario emite `set event -type=release` para el archivo `create.file`. Han transcurrido treinta días del período de retención de éste y, por lo tanto, el archivo caduca en 30 días (la ejecución de la retención, `hold`, no amplía el período de retención).

Para obtener información sobre el valor de grupo de copias `RETINIT`, consulte la documentación del servidor de IBM Spectrum Protect.

- Archivar archivos en un servidor de retención de datos  
Hasta ahora, no se ha mostrado que existan diferencias entre el archivado de los archivos en un servidor normal o en un servidor de retención de datos.

### Referencia relacionada:


Set Event

## Opciones y mandatos del cliente de copia de seguridad/archivado

---

Utilice las opciones del cliente para ajustar el proceso de cliente de archivado y copia de seguridad para que se adapte a sus necesidades. Utilice la interfaz de línea de mandatos de cliente (CLI) como alternativa a la interfaz gráfica de usuario (GUI). Se proporciona información de referencia para las opciones, mandatos y otra información adicional del cliente.

- Lectura de diagramas de sintaxis  
Para leer un diagrama de sintaxis para especificar un mandato, siga la vía de acceso de la línea. Lea de izquierda a derecha y de arriba abajo.
- Opciones de proceso  
Puede utilizar valores predeterminados de las opciones de proceso de cliente o bien puede ajustar las opciones de proceso para adaptarlas a sus necesidades específicas. Consulte la información general sobre opciones de proceso y la guía de referencia de opciones, que contiene información detallada sobre cada una de las opciones.

- Utilización de los mandatos  
El cliente de copia de seguridad y archivado proporciona una interfaz de línea de mandatos (CLI) que puede utilizar como alternativa a la interfaz gráfica de usuario (GUI). En este tema se describe cómo iniciar o finalizar una sesión de mandatos de cliente y cómo escribir los mandatos.
-  Sistemas operativos Windows Programa de utilidad de configuración del servicio del cliente IBM Spectrum Protect  
Se pueden instalar los siguientes servicios del cliente cuando instala el cliente de archivado y copia de seguridad o si utiliza el programa de utilidad de configuración del servicio del cliente de IBM Spectrum Protect:

**Conceptos relacionados:**

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

**Tareas relacionadas:**

Configuración de clientes de copia de seguridad/archivado

Copias de seguridad y restauración de datos con clientes de archivado y copia de seguridad

Archivar y recuperar datos con clientes de archivado y copia de seguridad

## Lectura de diagramas de sintaxis

---

Para leer un diagrama de sintaxis para especificar un mandato, siga la vía de acceso de la línea. Lea de izquierda a derecha y de arriba abajo.

- El símbolo ►►—— indica el comienzo de un diagrama de sintaxis.
- El símbolo ——► al final de una línea indica que el diagrama de sintaxis continúa en la siguiente línea.
- El símbolo ►—— al principio de un línea indica que un diagrama de sintaxis continúa desde la línea anterior.
- El símbolo ——► indica el final de un diagrama de sintaxis.

Elementos de sintaxis, como una palabra clave o una variable, puede estar:

- En la línea (elemento obligatorio)
- Por encima de la línea (elemento predeterminado)
- Por debajo de la línea (elemento opcional)

## Símbolos

---

Especifique estos símbolos *exactamente* como aparecen en el diagrama de sintaxis.

- \* Asterisco
- { } Llaves
- : Dos puntos
- , Coma
- = Signo de igual
- - Guión
- () Paréntesis
- . Punto
- Espacio
- " comillas
- ' comillas simples

## Variables

---

Los elementos en minúscula y en cursiva, como <nombre\_var>, indican variables. En este ejemplo, puede especificar un <nombre\_var> cuando indique el mandato **nombre\_man**.

```
>>-nombre_mand--<nombre_var>-----><
```

## Repetición

---

Una flecha que gira hacia la izquierda indica que el elemento se puede repetir. Un carácter dentro de una flecha significa que debe separar los elementos repetidos con un carácter.

```

      .-|-----|
      v          |
>>--repetir-+-----><

```

Una nota a pie de página (1) junto a la flecha se refiere a un límite que indica el número de veces que se puede repetir un elemento.

```
      .-,-----.  
      v (1)      |  
>>-----repetir+-----<<
```

Notas:

1. Especifique repetir hasta un máximo de cinco veces.

## Opciones necesarias

---

Cuando hay uno o varios elementos en una pila y uno de ellos se encuentra en la línea, *debe* especificar un elemento.

En este ejemplo, debe elegir A, B o C.

```
>>-nombre_mandato---+A+-----<<  
                    +-B-+  
                    '-C-'
```

## Opciones opcionales

---

Cuando un elemento está *por debajo* de la línea, ese elemento es opcional. En el primer ejemplo, puede seleccionar A o nada.

```
>>-nombre_mand---+-----<<  
                    '-A-'
```

Cuando dos o más elementos están en una pila debajo de la línea, todos los elementos son opcionales. En el segundo ejemplo, puede elegir A, B, C o nada en absoluto.

```
>>-nombre_mandato---+-----<<  
                    +-A-+  
                    +-B-+  
                    '-C-'
```

## Opciones repetibles

---

Una pila de elementos seguida de una flecha que gira hacia la izquierda indica que puede seleccionar más de un elemento, o en algunos casos, repetir un elemento individual.

En este ejemplo, puede seleccionar cualquier combinación de A, B o C.

```
      .-,-----.  
      v      |  
>>-nombre_mandato---+A+-----<<  
                    +-B-+  
                    '-C-'
```

## Valores predeterminados

---

Los valores predeterminados se encuentran por encima de la línea. El valor predeterminado se selecciona a menos que lo sustituya o puede seleccionarlo de forma explícita. Para sustituir el valor predeterminado, incluya una opción de la pila debajo de la línea.





En este ejemplo, A es el valor predeterminado. Seleccione B o C para modificar A.

```
      .-A-.  
>>-nombre_mandato---+-----<<  
                    +-B-+  
                    '-C-'
```

## Opciones de proceso

---

Puede utilizar valores predeterminados de las opciones de proceso de cliente o bien puede ajustar las opciones de proceso para adaptarlas a sus necesidades específicas. Consulte la información general sobre opciones de proceso y la guía de referencia de opciones, que contiene información detallada sobre cada una de las opciones.

- **Visión general de las opciones de proceso**  
IBM Spectrum Protect utiliza las *opciones de proceso* para controlar las comunicaciones, el proceso de copia de seguridad/archivado y otros tipos de proceso.
- **Opciones de comunicación**  
Las opciones de comunicación se utilizan para especificar cómo se comunica su nodo cliente con un servidor de IBM Spectrum Protect. Este tema proporciona información sobre los tipos de opciones de comunicación que se pueden utilizar.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **sistemas operativos Mac OS X**  **Sistemas operativos Oracle Solaris**  
**Opciones de servidor**  
Utilice la opción `servername` del archivo `dsm.sys` para empezar un grupo de opciones (secciones) que se utilizan para conectarse al servidor de IBM Spectrum Protect.
- **Opciones de proceso de copia de seguridad/archivado**  
Puede especificar opciones de cliente para controlar algunos aspectos del proceso de archivado y copia de seguridad.
- **Opciones de proceso de restauración y recuperación**  
Puede utilizar opciones de cliente para controlar algunos aspectos del proceso de restauración y recuperación.
- **Opciones de planificación**  
En este tema se explican las opciones que puede utilizar para regular la planificación central. El cliente de copia de seguridad y archivado sólo utiliza las opciones de planificación cuando el planificador está en ejecución.
- **Opciones de formato e idioma**  
Las opciones de formato e idioma le permiten seleccionar formatos diferentes para fecha, hora y números para idiomas diferentes.
- **Opciones de proceso de mandatos**  
En este tema se explican las opciones que puede utilizar con los mandatos del cliente de copia de seguridad y archivado.
- **Opciones de autorización**  
Las opciones de autorización controlan el acceso al servidor de IBM Spectrum Protect.
- **Opciones de proceso de errores**  
Las opciones de proceso de errores especifican el nombre del archivo de registro de errores y cómo el cliente de copia de seguridad y archivado trata las entradas del archivo de registro.
- **Opciones de proceso de transacciones**  
Las opciones de proceso de transacciones controlan el modo en que se procesan las transacciones entre el servidor y el cliente de IBM Spectrum Protect.
- **Opciones de cliente Web**  
Para configurar el cliente web IBM Spectrum Protect se utilizan varias opciones de cliente de archivado y copia de seguridad.
- **Utilización de opciones con mandatos**  
Puede modificar temporalmente diversas opciones del archivo de opciones del cliente (`dsm.opt`) especificándolas con los mandatos adecuados del cliente de copia de seguridad y archivado.
- **Consulta de opciones del cliente**  
Las secciones siguientes contienen información detallada sobre cada una de las opciones de proceso de IBM Spectrum Protect.

### **Conceptos relacionados:**

Utilización de opciones con mandatos


### **Referencia relacionada:**





Lectura de diagramas de sintaxis

## Visión general de las opciones de proceso

---

IBM Spectrum Protect utiliza las *opciones de proceso* para controlar las comunicaciones, el proceso de copia de seguridad/archivado y otros tipos de proceso.











 **Sistemas operativos Windows** Puede especificar opciones de proceso en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Puede especificar opciones de proceso en el archivo de opciones de sistema del cliente (`dsm.sys`), en el archivo de opciones de usuario del cliente (`dsm.opt`) o en la línea de mandatos.


Puede definir los siguientes tipos de opciones:

- Opciones de comunicación



-  Sistemas operativos Windows Opciones de nodo
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Opciones de servidor y nodo
- Opciones de proceso de copia de seguridad/archivado
- Opciones de proceso de restauración y recuperación
- Opciones de planificación
-  Sistemas operativos Windows Opciones de formato e idioma
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Opciones de formato
- Opciones de proceso de mandatos
- Opciones de autorización
- Opciones de proceso de errores
- Opciones de proceso de transacciones
- Opciones de cliente Web
- Opciones de diagnóstico







El cliente de copia de seguridad y archivado también incluye un grupo de opciones de mandatos de cliente que pueden entrarse únicamente en la línea de mandatos con mandatos específicos. Pueden modificarse temporalmente algunas de las opciones del archivo de opciones, entrando dichas modificaciones con mandatos de copia de seguridad/archivado adecuados.

 Sistemas operativos Windows Nota: Algunas de las opciones de procesamiento que utiliza el planificador central de IBM Spectrum Protect se definen en el registro de Windows cuando se configuran los servicios de planificación. Estas opciones también se pueden especificar en el archivo de opciones del cliente. Cuando el planificador se ejecuta como servicio, las opciones de procesamiento que se han especificado en el registro sobrescriben las opciones equivalentes especificadas en el archivo de opciones del cliente.

**Conceptos relacionados:**





Especificación de opciones con un mandato



**Tareas relacionadas:**


-  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris
-  sistemas operativos Mac OS X Creación y modificación del archivo opciones del sistema del cliente
-  Sistemas operativos Windows Creación y modificación del archivo de opciones del cliente


## Opciones de comunicación

Las opciones de comunicación se utilizan para especificar cómo se comunica su nodo cliente con un servidor de IBM Spectrum Protect. Este tema proporciona información sobre los tipos de opciones de comunicación que se pueden utilizar.






 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Para clientes UNIX y Linux, utilice uno de los protocolos de comunicación siguientes:

- TCP/IP
-  Sistemas operativos AIX  Sistemas operativos Linux Memoria compartida (AIX, Linux)







 Sistemas operativos Windows Para todos los clientes de Windows, utilice uno de los protocolos siguientes:

 Sistemas operativos Windows

- TCP/IP
- Named pipes
- Memoria compartida

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Utilice la opción commmethod para especificar el protocolo de comunicación.

Para establecer sus opciones de comunicación, solicite asistencia al administrador de IBM Spectrum Protect.

- Opciones de TCP/IP  
Para utilizar el protocolo de comunicaciones TCP/IP, debe incluir la opción TCP/IP tcpserveraddress en el archivo de opciones de cliente.
-  Sistemas operativos Windows Opción de Named Pipes  
Este tema proporciona información sobre la opción de comunicación namedpipename.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Opciones de memoria compartida  
En este tema se proporciona información sobre las opciones de memoria compartida que se pueden utilizar.

**Referencia relacionada:**





















Commmethod

## Opciones de TCP/IP

Para utilizar el protocolo de comunicaciones TCP/IP, debe incluir la opción TCP/IP tcpserveraddress en el archivo de opciones de cliente.

Las demás opciones de TCP/IP tienen valores predeterminados que pueden modificarse si se desea cambiar el valor predeterminado. Este tema proporciona información sobre los tipos de opciones de comunicación que se pueden utilizar.

Tabla 1. Opciones de TCP/IP

Opción	Descripción
httpport	Especifica una dirección de puerto TCP/IP para el cliente web.
lanfreetcppport	Especifica el número de puerto TCP/IP en el que el agente de almacenamiento de IBM Spectrum Protect está a la escucha.
lanfreetcpsaddress	Especifica la dirección TCP/IP para el agente de almacenamiento IBM Spectrum Protect.
tcpbuffsize	Especifica el tamaño en kilobytes del búfer de comunicaciones TCP/IP interno.
 Sistemas operativos Windows tcpnodelay	 Sistemas operativos Windows Especifica si el servidor y el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X tcpnodelay	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica si el servidor y el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red. Esta opción es para todos los clientes UNIX..
tcpadminport	Especifica un número de puerto TCP/IP independiente en el que el servidor espera solicitudes de sesiones de cliente de administración, lo que permite sesiones de administración seguras dentro de una red privada.
tcpaddress	Especifica una dirección TCP/IP para dsmcad.
tcpport	Especifica la dirección del puerto TCP/IP para un servidor de IBM Spectrum Protect.
tcpserveraddress	Especifica la dirección TCP/IP para un servidor de IBM Spectrum Protect.
tcpwindowsize	Especifica el tamaño en kilobytes de la ventana deslizante de TCP/IP para el nodo cliente.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X webports	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el daemon de aceptación de clientes y el servicio de agente de cliente web (el agente de cliente web no se aplica a Mac OS X) para las comunicaciones con la GUI web.
 Sistemas operativos Windows webports	 Sistemas operativos Windows Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el servicio de aceptación de clientes y el servicio de agente de cliente web para las comunicaciones con el cliente web.

### Referencia relacionada:






Nfstimeout

 Sistemas operativos Windows

## Opción de Named Pipes

Este tema proporciona información sobre la opción de comunicación namedpipename.

Tabla 1. Opción de comunicación de Named Pipes





Opción	Descripción
namedpipename Namedpipename	Especifica el nombre de un conducto con nombre que utilizar para las comunicaciones entre un cliente y un servidor de IBM Spectrum Protect en el mismo dominio de servidor Windows.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows	

## Opciones de memoria compartida

En este tema se proporciona información sobre las opciones de memoria compartida que se pueden utilizar.

Tabla 1. Opciones de comunicación de memoria compartida

Opción	Descripción
lanfreeshmport Lanfreeshmport	Especifica el número exclusivo que el cliente y el agente de almacenamiento utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.
lanfreeshmport Shmport	Especifica el número exclusivo que el cliente y el servidor utilizarán para identificar el área de memoria compartida utilizada para las comunicaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Opciones de servidor

Utilice la opción `servername` del archivo `dsm.sys` para empezar un grupo de opciones (secciones) que se utilizan para conectarse al servidor de IBM Spectrum Protect.

Puede establecer varios grupos de secciones en el archivo `dsm.sys` para la conexión con distintos servidores. Debajo de cada sección de `servername` debe aparecer todas las secciones de opciones de clientes necesarias para establecer comunicación con un servidor. La lista de secciones también puede contener otras opciones para las operaciones de copia de seguridad/archivado.

*Si el archivo de opciones del sistema cliente contiene sólo una sección:* el nodo de cliente contacta con el servidor que se especifique en esa sección para todos los servicios.

*Si el archivo de opciones del sistema cliente contiene más de una sección:* puede especificar un servidor predeterminado con la opción `defaultserver`. No especifique un servidor predeterminado, IBM Spectrum Protect establece contacto con el servidor en la primera sección del archivo `dsm.sys`.

Establezca la opción `defaultserver` al principio del archivo `dsm.sys` delante de cualquier sección del servidor. Para obtener más información, consulte el apartado `Defaultserver`.

Utilice la opción `servername` en el archivo de opciones del usuario cliente (`dsm.opt`) o en la línea de mandatos para especificar un servidor con el que se desea contactar para los servicios de copia de seguridad/archivado. Esto altera temporalmente el servidor predeterminado especificado en el archivo (`dsm.sys`).

**Nota:** No puede sustituir el servidor de migración especificado en el archivo de opciones del sistema cliente.

Tabla 1 muestra un archivo `dsm.sys` de ejemplo.

Tabla 1. Archivo de opciones del sistema cliente de ejemplo

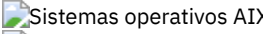
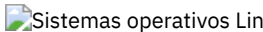
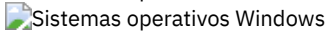
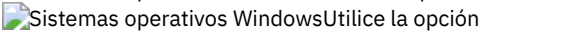
Archivo dsm.sys de ejemplo	
<code>DEFAULTServer</code>	<code>server2</code>
<code>SERvername</code>	<code>server1</code>
<code>NODename</code>	<code>node1</code>
<code>COMMMethod</code>	<code>TCPip</code>
<code>TCPPort</code>	<code>1500</code>
<code>TCPServeraddress</code>	<code>node.domain.company.com</code>
<code>PASSWORDAccess</code>	<code>generate</code>
<code>GRoups</code>	<code>system adsm</code>
<code>USERS</code>	<code>ashton stewart kaitlin</code>
<code>INCLExcl</code>	<code>/adm/adsm/backup1.excl</code>
<code>SERvername</code>	<code>server2</code>
<code>COMMMethod</code>	<code>SHAREdmem</code>
<code>shmport</code>	<code>1520</code>
<code>PASSWORDAccess</code>	<code>prompt</code>
<code>GRoups</code>	<code>system adsm</code>
<code>USERS</code>	<code>danielle derek brant</code>
<code>INCLExcl</code>	<code>/adm/adsm/backup2.excl</code>

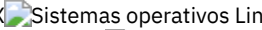
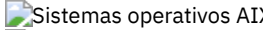
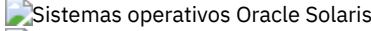
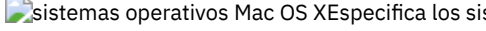
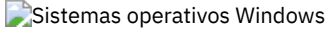
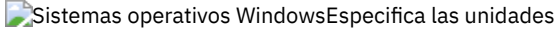

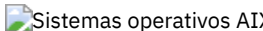
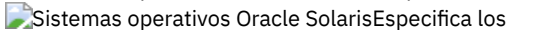

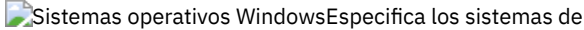

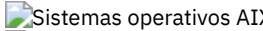
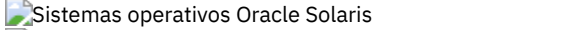
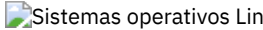
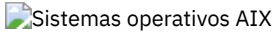
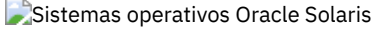
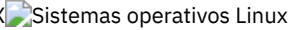
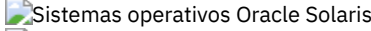
## Opciones de proceso de copia de seguridad/archivado

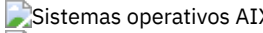
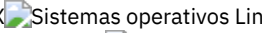
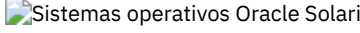
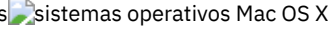
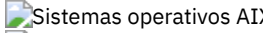
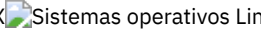
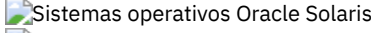
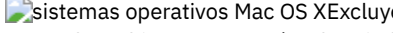
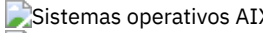
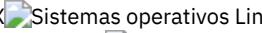
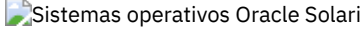
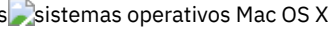
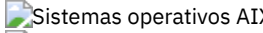
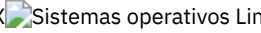
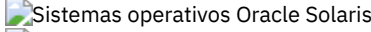
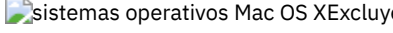
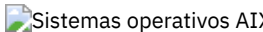
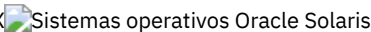
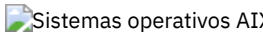



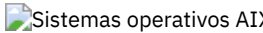
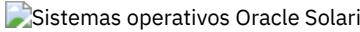
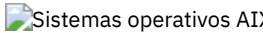
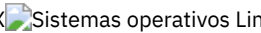
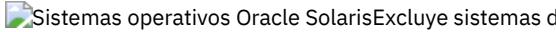
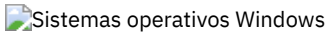
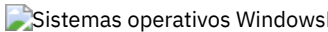
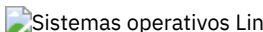

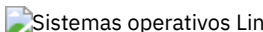

Puede especificar opciones de cliente para controlar algunos aspectos del proceso de archivado y copia de seguridad.

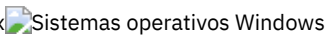
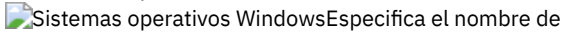
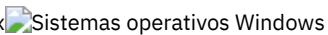
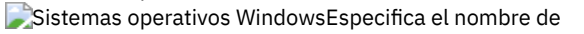
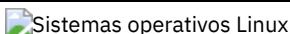
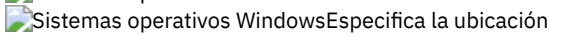
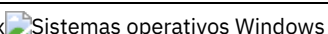
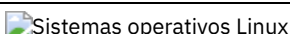
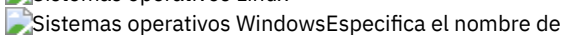
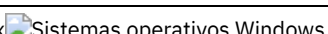
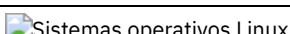

Tabla 1. Opciones de proceso de copia de seguridad/archivado

Opción	Descripción
  afmskipuncachedfiles	  Utilice la opción afmskipuncachedfiles para especificar si los archivos no almacenados en memoria caché y sucios de conjuntos de archivos de Active File Management de General Parallel File System (GPFS™) se procesan para operaciones de copia de seguridad, archivado y migración.
archmc	Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular las copias archivadas.
    archsymlinkasfile	    Especifica si desea que el cliente siga un enlace simbólico y archive el archivo o directorio al que éste hace referencia o que sólo archive el enlace simbólico.
asnodename	Utilice la opción asnodename para permitir a nodos agente realizar copias de seguridad o restauración de datos en nombre de otro nodo (el nodo de destino). Esta opción permite realizar operaciones simultáneas desde varios nodos para almacenar datos en el mismo nodo de destino y espacio de archivos en paralelo.
    automount	    Utilice esta opción con la opción domain para especificar todos los sistemas de archivos montados automáticamente que el cliente intentará montar en las circunstancias siguientes: <ul style="list-style-type: none"> <li>• Cuando se inicia el cliente de copia de seguridad y archivado</li> <li>• Cuando se inicia la copia de seguridad</li> <li>• Cuando el cliente de copia de seguridad y archivado alcanza a un sistema de archivos montado automáticamente durante la operación de copia de seguridad</li> </ul>
autofsrename	Especifica si debe renombrarse un espacio de archivos existente en un servidor activado para Unicode de modo que pueda crearse un espacio de archivos activado para Unicode para la operación actual.
 backmc	 Especifica la clase de gestión que se debe aplicar al submandato backup fastback con propósito de retención.
changingretries	Especifica el número de veces que el cliente intenta realizar una copia de seguridad o archivar un archivo que está en uso.
 class	 Especifica si se hace una lista de NAS o los objetos del servidor de aplicaciones del cliente durante una operación de query backup, query filespace, o delete filespace.
compressalways	La opción compressalways especifica si se debe continuar la compresión si el objeto aumenta de tamaño durante la compresión. Utilice esta opción con la opción compression.

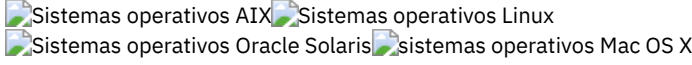
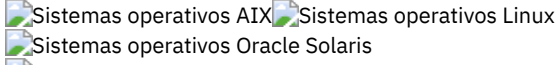
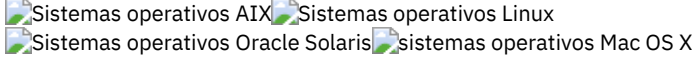
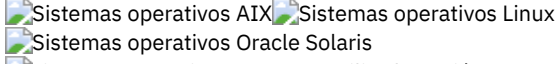
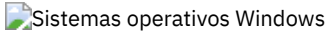







Opción	Descripción
compression	La opción compression comprime los archivos antes de enviarlos al servidor. La compresión de archivos reduce el almacenamiento de datos necesario para almacenar versiones de copia de seguridad y copias archivadas de los archivos.
   createnewbase Createnewbase	   La opción createnewbase crea una instantánea de base y la utiliza para ejecutar una copia de seguridad incremental completa. Al definir esta opción se garantiza que se hace copia de seguridad de cualquier archivo que se haya omitido durante la copia de seguridad incremental por diferencia de instantánea.
eliminación de duplicados Eliminación de duplicados	Especifica si deben eliminarse los datos redundantes en el lado del cliente cuando éste transfiere datos al servidor de IBM Spectrum Protect durante el proceso de archivado o copia de seguridad.
dedupcachepath Dedupcachepath	Especifica la ubicación en la que se creará la base de datos de memoria caché de deduplicación de datos del lado del cliente si se establece la opción enablededupcache=yes durante el proceso de archivado o copia de seguridad.
dedupcachesize Dedupcachesize	Determina el tamaño máximo del archivo de la memoria caché de eliminación de duplicados de datos.
enablededupcache Enablededupcache	Especifica si se desea habilitar la memoria caché de eliminación de duplicados de datos del lado del cliente para que el cliente de copia de seguridad y archivado obtenga los datos modificados de la memoria caché.
deletefiles	Utilice la opción deletefiles con el mandato archive para suprimir archivos de la estación de trabajo después de haber realizado el archivado de éstos.      También puede utilizar esta opción con el mandato restore image y la opción incremental para suprimir archivos de la imagen restaurada si éstos se han suprimido después de haber creado la imagen.
description	La opción description asigna o especifica una descripción para los archivos cuando el cliente efectúa operaciones de archivado, supresión, recuperación, consulta de archivado, o consulta de juegos de copias de seguridad.
detail	Utilice la opción detail para listar información sobre la clase de gestión, el espacio de archivos, las copias de seguridad y las copias archivadas, según el mandato con el que se utilice.
   diffsnapshot	   Utilice la opción diffsnapshot para determinar si el cliente crea una instantánea diferencial.
dirmc	Especifica la clase de gestión que debe utilizarse para los directorios. Si no especifica esta opción, el cliente utiliza la clase de gestión del juego de políticas activo del dominio de políticas cuyo período de retención sea más largo.
dirsonly	Realiza copias de seguridad, restaura, archiva, recupera o efectúa consultas sólo de directorios.















Opción	Descripción
diskcachelocation	Especifica la ubicación en la que se creará la base de datos de caché en disco si se establece la opción <code>memoryefficient=diskcachemethod</code> durante la realización de una copia de seguridad incremental.
    domain	    Especifica los sistemas de archivo que se van a incluir en el dominio de cliente predeterminado en una copia de seguridad incremental.
 domain	 Especifica las unidades que se van a incluir en el dominio de cliente predeterminado en una copia de seguridad incremental.
   domain.image	   Especifica los sistemas de archivos montados y los volúmenes lógicos RAW que desea incluir en el dominio de cliente para una copia de seguridad de imagen. Esta opción es únicamente para AIX, Linux x86_64, Linux on POWER y Solaris.
 domain.image	 Especifica los sistemas de archivos y los volúmenes lógicos RAW que desea incluir en el dominio de cliente para una copia de seguridad de imagen. Esta opción es válida para todos los clientes Windows.
   domain.nas	   Especifica los volúmenes que deben incluirse en el dominio predeterminado para las copias de seguridad de imagen NAS.
  domain.vmfull Domain.vmfull	  Especifica las máquinas virtuales que se van a incluir en copias de seguridad a nivel completo de máquinas virtuales de VMware.
 efsdecrypt	 Especifica si los archivos cifrados por un sistema de archivos de cifrado (EFS) de AIX se leerán en formato cifrado o descifrado.
enablearchiveretentionprotection	Permite al cliente conectar con un servidor de retención de datos.
    enablelanfree Enablelanfree	    Especifica si debe activarse una vía de acceso disponible fuera de la LAN para un dispositivo de almacenamiento conectado a una red de área de almacenamiento (SAN).
 exclude exclude.backup exclude.file exclude.file.backup	 Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad.
    exclude exclude.backup exclude.file exclude.file.backup	    Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción <code>exclude.backup</code> sólo excluye archivos de la copia de seguridad normal, no de HSM.

Opción	Descripción
encryptiontype	Seleccione el cifrado de datos de bits AES-256 o AES-128. El cifrado de datos AES de 256 bits proporciona el nivel más alto de cifrado de datos.
encryptkey	Especifica si se debe guardar la contraseña de clave de cifrado localmente cuando el cliente hace una operación de archivado y copia de seguridad o si se debe pedir la contraseña de la clave de cifrado.
exclude.archive	Excluye sólo de los servicios de archivado el archivo o grupo de archivos que coincidan con el patrón.
    exclude.attribute.symlink	    Excluye un archivo o un grupo de archivos que son vínculos simbólicos o alias (los alias se aplican a Mac OS X) sólo del proceso de copia de seguridad.
exclude.compression	Excluye archivos del proceso de compresión si define la opción compression a yes. Esta opción se aplica a copias de seguridad y copias archivadas.
exclude.dir	Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad.
exclude.encrypt	Excluye archivos especificados del proceso de cifrado.
    exclude.fs	    Excluye los espacios de archivos que coinciden con un patrón. Esta opción es válida para todos los clientes UNIX.
  exclude.fs.nas	  Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas. Esta opción es únicamente para los clientes AIX y Solaris.
 exclude.fs.nas	 Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato backup nas.
   exclude.image	   Excluye sistemas de archivos montados y volúmenes lógicos RAW que coinciden con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. Esta opción es válida únicamente para clientes AIX, Solaris y todos los de Linux.
 exclude.image	 Excluye sistemas de archivos montados y volúmenes lógicos RAW que coinciden con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. exclude.image no afectará a las operaciones de copia de seguridad de imágenes incremental.
  fbbranch	  Especifica el ID de ramificación del servidor remoto de FastBack para el cual se va a iniciar un proceso de copia de seguridad o archivado.









































Opción	Descripción
 Sistemas operativos Linux  Sistemas operativos Windows fbclientname	 Sistemas operativos Linux  Sistemas operativos Windows Especifica el nombre de uno o varios clientes de FastBack cuya copia de seguridad se va a realizar desde el proxy de copia de seguridad.
 Sistemas operativos Linux  Sistemas operativos Windows fbpolicyname	 Sistemas operativos Linux  Sistemas operativos Windows Especifica el nombre de una o más políticas de Tivoli Storage Manager FastBack de las que se desea hacer una copia de seguridad desde el proxy de copia de seguridad.
 Sistemas operativos Linux  Sistemas operativos Windows fbreposlocation	 Sistemas operativos Linux  Sistemas operativos Windows Especifica la ubicación del repositorio de Tivoli Storage Manager FastBack para el proxy del cliente de IBM Spectrum Protect para conectarse y emitir los mandatos MOUNT DUMP, MOUNT ADD y MOUNT DEL.
 Sistemas operativos Linux  Sistemas operativos Windows fbserver	 Sistemas operativos Linux  Sistemas operativos Windows Especifica el nombre de host de la estación de trabajo del servidor FastBack o de la estación de trabajo FastBack Disaster Recovery Hub que es propietaria del repositorio especificado por la opción fbreposlocation.
 Sistemas operativos Linux  Sistemas operativos Windows fbvolumename	 Sistemas operativos Linux  Sistemas operativos Windows Especifica el nombre de uno o más volúmenes de Tivoli Storage Manager FastBack para hacer una copia de seguridad desde el proxy de copia de seguridad.
filelist	Especifica una lista de archivos para que los procese el mandato. El cliente abre la lista de archivos designada y procesa los archivos que contiene la lista de acuerdo con el mandato.
filesonly	Realiza copias de seguridad, restaura, recupera o efectúa consultas sólo de archivos.
groupname	Utilice esta opción con el mandato backup group para especificar el nombre completo del líder de un grupo.
ieobjtype Ieobjtype	Especifica un tipo de objeto para la operación de eliminación de duplicación de datos del lado del cliente. Esta opción se utiliza con las opciones include.dedup y exclude.dedup.
 Sistemas operativos AIX imagegapsize	 Sistemas operativos AIX Especifica el tamaño mínimo de las regiones vacías en un volumen que desee omitir durante una copia de seguridad de imagen. Esta opción es válida para clientes AIX JFS2.
 Sistemas operativos Windows imagegapsize	 Sistemas operativos Windows Especifica el tamaño mínimo de las regiones vacías en un volumen que desee omitir durante una copia de seguridad. Esta opción es válida para todos los clientes Windows.
inclxcl	Especifica la vía de acceso y el nombre de archivo de un archivo de opciones de inclusión/exclusión.
include include.backup include.file	Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad.
include.archive	Incluye archivos o asigna clases de gestión para los procesos de archivado.













































Opción	Descripción
 include.attribute.symlink	 Incluye un archivo o un grupo de archivos que son vínculos simbólicos o alias (los alias se aplican a Mac OS X) de un grupo amplio de archivos excluidos en el proceso de copia de seguridad.
include.compression	Incluye archivos para el proceso de compresión si establece la opción compression en yes. Esta opción se aplica a copias de seguridad y copias archivadas.
include.encrypt	Incluye los archivos especificados para el proceso de cifrado. De forma predeterminada, el cliente no realiza el proceso de cifrado.
 include.fs	 Utilice la opción include.fs para controlar cómo el cliente procesa el espacio de archivos en la copia de seguridad incremental.
 include.fs	 Utilice la opción include.fs para especificar opciones de proceso para un sistema de archivos. Utilice la opción include.fs para especificar qué unidades utilizan el soporte de archivos abiertos y para controlar cómo han de procesarse las copias de seguridad incrementales de espacio de archivo completas.
 include.fs.nas	 Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, utilizando la opción toc con la opción include.fs.nas en el archivo dsm.sys. Para obtener más información, consulte el apartado Toc. Esta opción solo es válida para los clientes AIX y Solaris.
 include.fs.nas	 Utilice la opción include.fs.nas para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imagen del sistema de archivos NAS, utilizando la opción toc con la opción include.fs.nas en el archivo de opciones del cliente (dsm.opt). Para obtener más información, consulte Toc.
 include.image	 Especifica el sistema de archivos o el volumen lógico que debe incluirse para el proceso de copia de seguridad de imagen. Esta opción también proporciona un método para especificar una asignación de clase de gestión explícita para un sistema de archivos o un volumen lógico específico. El mandato backup image ignora todas las demás opciones de inclusión. Esta opción es válida para AIX, Solaris y todos los clientes Linux.

























Opción	Descripción
 Sistemas operativos Windows include.image	 Sistemas operativos Windows Especifica el sistema de archivos o el volumen lógico que debe incluirse para el proceso de copia de seguridad de imagen. Esta opción también proporciona un método para especificar una asignación de clase de gestión explícita para un sistema de archivos o un volumen lógico específico. El mandato backup image ignora todas las demás opciones de inclusión. Utilice la opción include.fs para especificar qué unidades utilizan el soporte de archivos abiertos y para controlar cómo han de procesarse las copias de seguridad incrementales de espacio de archivo completas.
 Sistemas operativos Windows include.systemstate	 Sistemas operativos Windows Asigna clases de gestión para la copia de seguridad del estado del sistema Windows. El valor predeterminado es vincular el objeto del sistema a la clase de gestión predeterminada.
incrbydate	Para solicitar una copia de seguridad incremental por fecha, utilice esta opción con el mandato incremental.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris incremental	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice esta opción con el mandato restore image para asegurarse de que los cambios efectuados en la imagen base también se apliquen a la imagen restaurada. Esta opción es válida para clientes AIX, Solaris y todos los de Linux.
 Sistemas operativos Windows incremental	 Sistemas operativos Windows Utilice esta opción con el mandato restore image para asegurarse de que los cambios efectuados en la imagen base también se apliquen a la imagen restaurada.
 Sistemas operativos Windows incrthreshold	 Sistemas operativos Windows La opción incrthreshold especifica el valor de umbral para el número de directorios de cualquier espacio de archivos con registro por diario que pueda tener objetos activos en el servidor, pero no objetos equivalentes en la estación de trabajo.
memoryefficientbackup	Especifica un algoritmo de copia de seguridad de bajo consumo de memoria para copias de seguridad incrementales cuando se utiliza con el mandato incremental.


Opción	Descripción
mode	<p>Utilice la opción mode con estos mandatos, como se indica a continuación:</p> <ul style="list-style-type: none"> <li>    backup image <ul style="list-style-type: none"> <li></li> <li></li> <li></li> <li> Para especificar si ha de realizarse una copia de seguridad de imagen selectiva o incremental de los sistemas de archivos de cliente.</li> </ul> </li> <li>   backup nas <ul style="list-style-type: none"> <li></li> <li></li> <li> Para especificar si ha de realizarse una copia de seguridad de imagen completa o diferencial de los sistemas de archivos NAS.</li> </ul> </li> </ul> <p>backup group</p> <p>Para especificar si ha de realizarse una copia de seguridad de grupo completa o diferencial que contenga una lista de archivos de uno o más orígenes de espacio de archivos.</p> <ul style="list-style-type: none"> <li> backup vm <ul style="list-style-type: none"> <li> Para especificar si se debe realizar una copia de seguridad selectiva o incremental de sistemas VMware.</li> </ul> </li> <li> backup vm <ul style="list-style-type: none"> <li> Para especificar si se debe realizar una copia de seguridad completa o incremental de una máquina virtual VMware cuando vmbackuptype=fullvm y cuando ha instalado IBM Spectrum Protect for Virtual Environments.</li> </ul> </li> </ul>
 monitor	 Especifica si desea supervisar una copia de seguridad de imagen de los sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).
 noprompt	 Suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire y set event.
 noprompt	 Suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire, restore image y set event.
 nojournal	 Utilice esta opción con el mandato incremental para especificar que desea realizar la copia de seguridad incremental completa tradicional, en lugar de realizar la copia de seguridad con registro por diario predeterminada.

Opción	Descripción
 Sistemas operativos Windows nojournal	 Sistemas operativos Windows Utilice esta opción con el mandato incremental para especificar que desea realizar la copia de seguridad incremental completa tradicional, en lugar de realizar la copia de seguridad con registro por diario predeterminada.
 Sistemas operativos Windows optfile	 Sistemas operativos Windows Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X optfile	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.
 Sistemas operativos AIX  Sistemas operativos Linux postsnapshotcmd	 Sistemas operativos AIX  Sistemas operativos Linux Durante una copia de seguridad basada en instantáneas, esta opción le permite abrir de forma manual una aplicación después de crear la instantánea. Esta opción es válida sólo para las operaciones basadas en instantáneas de JFS2 de AIX o LVM de Linux.
 Sistemas operativos Windows postsnapshotcmd	 Sistemas operativos Windows Durante la copia de seguridad de la imagen en línea abra una operación de soporte de archivos, esta opción le permitirá abrir de forma manual una aplicación después de que el proveedor de instantáneas empiece una instantánea. Esta opción sólo es válida si se ha activado OFS o el soporte de imagen activada.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows preservelastaccessdate	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Puede utilizar esta opción durante una operación de copia de seguridad o archivado para especificar si debe restablecer la fecha del último acceso de cualquier archivo especificado a su valor original tras una after operación de copia de seguridad o archivado. De forma predeterminada, el cliente no reinicia la última fecha de acceso de ningún archivo de copia de seguridad o archivado a su valor original antes de realizar la operación de archivado o copia de seguridad.
 Sistemas operativos AIX  Sistemas operativos Linux presnapshotcmd	 Sistemas operativos AIX  Sistemas operativos Linux Durante una operación de copia de seguridad basada en instantáneas, esta opción permite detener manualmente una aplicación antes de crear la instantánea. Esta opción es válida solo para operaciones basadas en instantánea de AIX JFS2 o Linux LVM.
 Sistemas operativos Windows presnapshotcmd	 Sistemas operativos Windows Durante una copia de seguridad de imagen activada o de soporte de archivos abiertos, esta opción permite detener manualmente una aplicación antes de que el proveedor de instantáneas inicie una instantánea. Esta opción sólo es válida si se ha activado OFS o el soporte de imagen activada.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X removeoperandlimit	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica que el cliente ha de eliminar el límite de 20 operandos. Si especifica la opción removeoperandlimit con los mandatos incremental, selective o archive, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

Opción	Descripción
 Sistemas operativos Windows  resetarchiveattribute	 Sistemas operativos Windows Especifica si el cliente restablece el atributo de archivado de Windows en los archivos de los que realizó correctamente una copia de seguridad en el servidor de IBM Spectrum Protect. Esta opción es válida para todos los clientes Windows.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  skipacl	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica si se debe omitir completamente el proceso de ACL.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  skipaclupdatecheck	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica si se debe realizar la suma de comprobación y las comparaciones de tamaño antes y después de la copia de seguridad y durante el proceso incremental.
 Sistemas operativos Windows  skipntpermissions	 Sistemas operativos Windows Especifica si realizar la copia de seguridad, archivado, recuperación o restauración de la información de seguridad de Windows.
 Sistemas operativos Windows  skipntsecuritycrc	 Sistemas operativos Windows Especifica si debe calcularse el CRC de seguridad para la comparación de permisos durante las copias de seguridad posteriores. Utilice esta opción en todos los clientes Windows.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows  snapdiff	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Especifica una copia de seguridad incremental de los archivos que NetApp ha notificado como cambiados en lugar de explorar el volumen y buscar los archivos que han cambiado. Utilice esta opción con una copia de seguridad incremental de volumen completa de NAS.
 Sistemas operativos AIX  Sistemas operativos Linux  snapshotcachesize	 Sistemas operativos AIX  Sistemas operativos Linux Linux y AIX únicamente: utilice esta opción para especificar un tamaño de instantánea adecuado para que se puedan almacenar todos los bloques de datos anteriores durante la modificación y supresión de archivos. Un tamaño de instantánea del 100% asegurará que la instantánea sea válida. El valor predeterminado es 100 por ciento.
 Sistemas operativos AIX  snapshotproviderfs	 Sistemas operativos AIX Utilice la opción snapshotproviderfs para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas, y para especificar un proveedor de instantáneas. Debe ser un usuario root para poder realizar una operación de archivado o de copia de seguridad de archivos basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.
 Sistemas operativos Windows  snapshotproviderfs	 Sistemas operativos Windows Utilice la opción snapshotproviderfs para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas y para especificar un proveedor de instantáneas.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  snapshotproviderimage	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice la opción snapshotproviderimage para activar la copia de seguridad de imágenes basada en instantánea y para especificar un proveedor de instantáneas. Debe ser usuario root para realizar una operación de copia de seguridad de imagen basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.

Opción	Descripción
 Sistemas operativos Windows snapshotproviderimage	 Sistemas operativos Windows Utilice la opción snapshotproviderimage para habilitar la copia de seguridad de imágenes en línea basada en instantáneas, y para especificar un proveedor de instantáneas.
 Sistemas operativos Windows snapshotroot	 Sistemas operativos Windows Utilice la opción snapshotroot con los mandatos incremental, selective o archive con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X snapshotroot	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice la opción snapshotroot con los mandatos incremental, selective o archive con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. Esta opción es válida para todos los clientes UNIX y Linux.
subdir	Especifica si deben incluirse los subdirectorios de un directorio especificado.
tapeprompt	Especifica si el cliente debe esperar el montaje de la cinta cuando éste sea necesario en un proceso de copia de seguridad, archivado, restauración o recuperación, o si se debe preguntar al usuario.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows toc	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Utilice la opción toc con el mandato backup nas o la opción include.fs.nas para especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, podrá utilizar el mandato de servidor QUERY TOC para determinar el contenido de la copia de seguridad de un sistema de archivos con el mandato de servidor RESTORE NODE para restaurar archivos individuales o árboles de directorios. También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse.
type	Utilice la opción type con el mandato query node para especificar el tipo de nodo que ha de consultarse.
v2archive	Utilice la opción v2archive con el mandato archive para realizar el archivado sólo de los archivos en el servidor. El cliente no procesa los directorios que existen en la vía de acceso de la especificación de archivo de origen.
virtualfsname (no se aplica a Mac OS X)	Utilice esta opción con el mandato backup group para especificar el nombre del contenedor del grupo en el que desea realizar la operación.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris virtualmountpoint	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Define un punto de montaje virtual para un sistema de archivos si desea realizar una copia de seguridad de los archivos que empiezan en un directorio determinado de dicho sistema de archivos.



Opción	Descripción
 Sistemas operativos Linux  Sistemas operativos Windows vmchost	 Sistemas operativos Linux  Sistemas operativos Windows Utilizado con los mandatos backup VM, restore VM o query VM para especificar el nombre de host del servidor de VMware VirtualCenter o ESX donde se dirigen los mandatos.
 Sistemas operativos Linux  Sistemas operativos Windows vmcpw	 Sistemas operativos Linux  Sistemas operativos Windows Utilizado con los mandatos backup VM, restore VM o query VM para especificar la contraseña de VirtualCenter o del usuario ESX que se especifica con la opción vmcuser.
 Sistemas operativos Linux  Sistemas operativos Windows vmcuser	 Sistemas operativos Linux  Sistemas operativos Windows Utilizado con los mandatos backup VM, restore VM o query VM para especificar el nombre de usuario del servidor de VMware VirtualCenter o ESX donde se dirigen los mandatos.
 Sistemas operativos Linux  Sistemas operativos Windows vmmaxvirtualdisks	 Sistemas operativos Linux  Sistemas operativos Windows Se utiliza con el mandato backup VM para especificar el tamaño máximo de los discos de máquina virtual (VMDK) VMware a incluir en una operación de copia de seguridad.
 Sistemas operativos Linux  Sistemas operativos Windows vmskipmaxvirtualdisks	 Sistemas operativos Linux  Sistemas operativos Windows Se utiliza con el mandato backup VM para especificar cómo la operación de copia de seguridad procesa los discos de máquina virtual (VMDK) VMware que superan el tamaño de disco máximo. En V7.1.3 y anterior, la opción vmskipmaxvirtualdisks se llamaba vmskipmaxvmdks.
 Sistemas operativos Linux  Sistemas operativos Windows	 Sistemas operativos Linux  Sistemas operativos Windows



 Sistemas operativos Windows Las siguientes opciones son opciones del cliente de copia de seguridad y archivado que solo se aplican a los archivos migrados de IBM Spectrum Protect HSM for Windows.

 Sistemas operativos Windows

- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

**Conceptos relacionados:**

 Sistemas operativos Windows  Opciones para la copia de seguridad de archivos migrados: skipmigrated, checkreparsecontent, stagingdirectory



 Sistemas operativos Windows  Opciones para restaurar archivos migrados: restorecheckstubaccess, restoremigstate



























## Opciones de proceso de restauración y recuperación

Puede utilizar opciones de cliente para controlar algunos aspectos del proceso de restauración y recuperación.

Tabla 1 enumera las opciones de proceso de restauración y recuperación que están disponibles.

Tabla 1. Opciones de proceso de restauración y recuperación

Opción	Descripción
 Sistemas operativos Windows asrmode	 Sistemas operativos Windows Utilice esta opción con los mandatos restore y restore systemstate para especificar si debe realizarse una operación de restauración en la modalidad de recuperación ASR del sistema. Esta opción se utiliza en el contexto de los mandatos restore que se generan en el archivo asr.sif solo por medio de la ejecución del mandato backup asr. No utilice esta opción fuera del contexto de la modalidad de recuperación ASR.

Opción	Descripción
 Sistemas operativos Windows backupsetname	 Sistemas operativos Windows La opción backupsetname especifica el nombre del conjunto de copias de seguridad o bien el nombre del archivo o del dispositivo de cinta que contiene el conjunto de copias de seguridad. Esta opción se utiliza junto con la opción location.
dirsonly	Califica la operación (copia de seguridad, archivado, restauración, recuperación) para que procese sólo directorios.
disablenqr	Especifica si el cliente de copia de seguridad y archivado puede utilizar el método de restauración sin consulta para restaurar archivos y directorios desde el servidor.
filelist	Especifica un archivo que contiene una lista de archivos que deben procesarse mediante el mandato especificado.
filesonly	Califica la operación (copia de seguridad, archivado, restauración, recuperación) para que procese sólo archivos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X followsymbolic	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica si desea restaurar archivos en vínculos simbólicos o utilizar un vínculo simbólico como punto de montaje virtual.
fromdate	Utilice la opción fromdate con la opción fromtime para especificar una fecha y una hora a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
fromnode	Permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato set access para permitirle consultar, restaurar o recuperar archivos o imágenes del otro nodo.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Muestra los espacios de archivos de un propietario alternativo. También especifica un propietario alternativo desde el que restaurar o recuperar archivos.
fromtime	Utilice la opción fromtime con la opción fromdate para especificar una fecha a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
ifnewer	Sustituye un archivo existente por la última versión de copia de seguridad si ésta es más reciente que el archivo existente.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris imagetofile	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice la opción imagetofile con el mandato restore image para especificar que desea restaurar la imagen de origen en un archivo. Puede que tenga que restaurar la imagen de un archivo en caso de que existan sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen. Esta opción es válida para clientes AIX, Linux y Solaris.
 Sistemas operativos Windows imagetofile	 Sistemas operativos Windows Utilice la opción imagetofile con el mandato restore image para especificar que desea restaurar la imagen de origen en un archivo. Puede que tenga que restaurar la imagen de un archivo en caso de que existan sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen.
inactive	Muestra una lista de los archivos activos e inactivos cuando se utiliza con la opción pick.
latest	Restaura la última versión de copia de seguridad de un archivo independientemente de que esté activa o inactiva.
localbackupset	Especifica si la GUI del cliente de copia de seguridad y archivado pasa por alto la conexión inicial con el servidor para restaurar un juego de copias de seguridad locales en una estación de trabajo independiente.



Opción	Descripción
 (no se aplica a Mac OS X)	 Utilice la opción makesparsefile con los mandatos restore o retrieve para especificar el modo en que los archivos esparcidos se volverán a crear.
	 Especifica si desea supervisar una restauración de imagen de uno o más sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).
	 Suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire y set event.
	 Suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire, restore image y set event.
	 Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.
	 Especifica el archivo de opciones del cliente que desea utilizar para iniciar una sesión del cliente de copia de seguridad y archivado.
pick	 Crea una lista de versiones de copia de seguridad, imágenes o copias archivadas que coinciden con la especificación de archivo que se entre. En esta lista, puede seleccionar las versiones que se desee procesar. Incluya la opción inactive para ver los objetos activos e inactivos.
pitdate	 Utilice la opción pitdate con la opción pittime para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.
pittime	 Utilice la opción pittime con la opción pitdate para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.
preservepath	 Especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.
replace	 Especifica si debe sustituirse un archivo existente o si debe solicitarse su elección al restaurar o recuperar archivos.
(no se aplica a Mac OS X)	 Visualiza todos los miembros de un grupo.
subdir	 Especifica si desea incluir los subdirectorios de un directorio especificado.
tapeprompt	 Especifica si desea que el cliente de copia de seguridad y archivado espere el montaje de una cinta que es necesaria para una operación de restauración o recuperación, o si debe preguntarse al usuario.
todate	 Utilice la opción todate con la opción totime para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
totime	 Utilice la opción totime con la opción todate para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
type	 Utilice la opción type con el mandato query node para especificar el tipo de nodo que ha de consultarse.

Opción	Descripción
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris verifyimage	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Utilice la opción verifyimage con el mandato restore image para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.
Sistemas operativos Windows verifyimage	Sistemas operativos Windows Utilice la opción verifyimage con el mandato restore image para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.

Las siguientes opciones son opciones del cliente de copia de seguridad y archivado que se aplican a los archivos migrados de IBM Spectrum Protect HSM for Windows. Para obtener más información sobre estas opciones, consulte los temas del IBM® Knowledge Center en [http://www.ibm.com/support/knowledgecenter/SSERFH\\_8.1.2/hsmwin/welcome.html](http://www.ibm.com/support/knowledgecenter/SSERFH_8.1.2/hsmwin/welcome.html).

- Checkreparsecontent
- Restorecheckstubaccess
- Restoremigstate
- Skipmigrated

Las siguientes opciones son opciones del cliente de copia de seguridad y archivado que se aplican a los archivos migrados de IBM Spectrum Protect for Space Management. Para obtener más información sobre estas opciones, consulte los temas del IBM Knowledge Center en [http://www.ibm.com/support/knowledgecenter/SSERBH\\_8.1.2/hsmul/welcome.html](http://www.ibm.com/support/knowledgecenter/SSERBH_8.1.2/hsmul/welcome.html).

- Restoremigstate
- Skipmigrated



















## Opciones de planificación

En este tema se explican las opciones que puede utilizar para regular la planificación central. El cliente de copia de seguridad y archivado sólo utiliza las opciones de planificación cuando el planificador está en ejecución.

Tabla 1 enumera las opciones de planificación que están disponibles.

Tabla 1. Opciones de planificación

Opción	Descripción
cadlistenonport	Especifica si se deben abrir puertos de escucha para el aceptador de clientes cuando este se utiliza para gestionar planificaciones en modalidad de sondeo.
managedservices	Especifica si el aceptador de clientes gestiona el cliente web, el planificador o ambos programas.
maxcmdretries	Especifica el número máximo de veces que el planificador cliente intenta procesar un mandato planificado que da error.
sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows postschedulecmd/postnschedulecmd	sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows Especifica un mandato que debe procesarse después de la ejecución de una planificación.
sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows preschedulecmd/prenschedulecmd	sistemas operativos Mac OS X Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows Especifica un mandato que debe procesarse antes de la ejecución de una planificación.
querschedperiod	Especifica el número de horas que el planificador cliente espera entre intentos de establecer contacto con el servidor para realizar trabajos planificados.

Opción	Descripción
retryperiod	Especifica el número de minutos que el planificador cliente debe esperar entre los intentos de procesar un mandato planificado que da error o entre los intentos fallidos de informar de los resultados al servidor.
 Sistemas operativos Windowsrunasservice	 Sistemas operativos WindowsObliga a que siga el proceso de mandatos del cliente, aunque la cuenta que inició el cliente se desconecte. Utilice esta opción en todos los clientes Windows.
schedcmddisabled	Especifica si debe desactivarse la planificación de mandatos genéricos especificados por el administrador de IBM Spectrum Protect.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS Xschedcmduser (solo servidor definido)	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XEl planificador ejecuta mandatos con el identificador de usuario 0; sin embargo, puede que haya otros usuarios que tengan identificadores de usuario distintos. En ese caso, con esta opción el administrador de IBM Spectrum Protect puede definir planificaciones y permitir que éstas se ejecuten bajo un identificador de usuario diferente de 0. La API de cliente de IBM Spectrum Protect no admite esta opción.
schedlogmax Schedlogmax	Especifica el tamaño máximo de las anotaciones del planificador y las anotaciones de cliente web, en megabytes.
schedlogname Schedlogname	Especifica la vía de acceso y el nombre de archivo donde desea almacenar la información de anotaciones de planificación.
schedlogretention	Especifica el número de días que se van a mantener las entradas del archivo de anotaciones en las anotaciones de planificación y las anotaciones del cliente web, y si se guardan las entradas eliminadas.
schedmode	Especifica qué modo de planificación se va a utilizar <i>polling</i> o <i>prompted</i> .
schedrestretdisabled	Especifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute las operaciones planificadas de restauración o recuperación.
sessioninitiation	Utilice la opción sessioninitiation para controlar si el servidor o el cliente ha de iniciar las sesiones a través de un cortafuegos. El valor predeterminado es que el cliente puede iniciar sesiones.
srvprepostscheddisabled	Especifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute los mandatos de preplanificación y postplanificación al realizar operaciones planificadas.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowssrvprepostsnapdisabled	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos WindowsEspecifica si se va a impedir que el administrador del servidor de IBM Spectrum Protect ejecute los mandatos previos y posteriores a la instantánea al realizar operaciones planificadas de copia de seguridad de instantáneas de imagen.
tcpclientaddress	Especifica una dirección TCP/IP si el nodo cliente tiene más de una dirección y desea que el servidor contacte con una dirección distinta de la utilizada para realizar el primer contacto del servidor. El servidor utilizará esta dirección cuando comience la operación planificada por solicitud de servidor. Consulte schedmode prompted (Schedmode) para obtener información detallada.
tcpclientport	Especifica un número de puerto TCP/IP para que el servidor contacte con el cliente cuando el servidor comience la operación planificada por solicitud de servidor. Consulte schedmode prompted (Schedmode) para obtener información detallada.

## Opciones de formato e idioma

Las opciones de formato e idioma le permiten seleccionar formatos diferentes para fecha, hora y números para idiomas diferentes.







 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Las opciones de formato le permiten seleccionar formatos diferentes para fecha, hora y números.

Tabla 1. Opciones de formato e idioma

Opción	Descripción
dateformat	Especifica el formato para visualizar fechas.
 Sistemas operativos Windows language	 Sistemas operativos Windows Especifica el idioma utilizado para los mensajes.
numberformat	Especifica el formato para visualizar números.
timeformat	Especifica el formato para visualizar la hora.

## Opciones de proceso de mandatos

En este tema se explican las opciones que puede utilizar con los mandatos del cliente de copia de seguridad y archivado.

Opciones de proceso de mandato que permiten controlar parte del formateo de datos en la pantalla terminal.

Tabla 1. Opciones de proceso de mandatos



















Opción	Descripción
quiet	Limita el número de mensajes que se muestran en la pantalla durante el proceso. Esta opción puede ser modificada temporalmente por el servidor.
scrolllines	Especifica el número de líneas de información que deben aparecer en pantalla a la vez. Utilice esta opción sólo si scrollprompt está establecida en yes.
scrollprompt	Especifica si se desea que el cliente de copia de seguridad y archivado se detenga y espere después de visualizar el número de líneas de información que ha especificado con la opción scrolllines o bien si se desea que se desplace hasta el final de la lista de información y se detenga.
setwindowtitle	Especifica si se visualizará el nombre de servidor de IBM Spectrum Protect y el nombre de servidor de host en el título de la ventana de mandatos de cliente administrativo.
verbose	Especifica que la información de proceso debe visualizarse en la ventana. La alternativa es quiet. Esta opción puede ser modificada temporalmente por el servidor.

















## Opciones de autorización

Las opciones de autorización controlan el acceso al servidor de IBM Spectrum Protect.

Tabla 1 enumera las opciones de autorización que están disponibles.

Tabla 1. Opciones de autorización

Opción	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows	 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Especifica si desea habilitar o inhabilitar un despliegue automático del cliente si es necesario un reinicio.
autodeploy	
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica los grupos de la estación de trabajo a los que se desea autorizar para que soliciten los servicios de IBM Spectrum Protect al servidor.
password	Especifica la contraseña de IBM Spectrum Protect.

Opción	Descripción
passwordaccess	Especifica si se desea utilizar una contraseña generada o si debe aparecer una solicitud para la contraseña cada vez que inicie el cliente.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X passworddir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica el directorio en el que desea almacenar la contraseña generada automáticamente para su nodo cliente. La clave de cifrado y la contraseña se cifran y almacenan en el archivo TSM.sth.
revokeremoteaccess	Impide que un administrador con privilegios de acceso a cliente acceda a una estación de trabajo a través del cliente web.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X users	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Autoriza a determinados usuarios de la estación de trabajo a que soliciten servicios de un servidor.

## Opciones de proceso de errores

Las opciones de proceso de errores especifican el nombre del archivo de registro de errores y cómo el cliente de copia de seguridad y archivado trata las entradas del archivo de registro.

Tabla 1 enumera las opciones de proceso de errores que están disponibles.

Tabla 1. Opciones de proceso de errores

Opción	Descripción
errorlogmax	Especifica el tamaño máximo de las anotaciones de errores, en megabytes.
errorlogname Errorlogname	Especifica la vía de acceso completa y el nombre de archivo donde desea almacenar información acerca de los errores que se produzcan durante el proceso.
errorlogretention	Especifica durante cuántos días van a conservarse las entradas de las anotaciones de errores antes de eliminarlas y si se van a guardar las entradas eliminadas.































## Opciones de proceso de transacciones

Las opciones de proceso de transacciones controlan el modo en que se procesan las transacciones entre el servidor y el cliente de IBM Spectrum Protect.

Tabla 1 enumera las opciones de proceso de transacciones que están disponibles.

Tabla 1. Opciones de proceso de transacciones

Opción	Descripción
collocatebyfilespec	Especifica que se desea que el cliente de copia de seguridad y archivado utilice solamente una sesión de servidor para enviar objetos generados desde una especificación de archivo. El establecimiento de la opción collocatebyfilespec en yes eliminará la entremezcla de archivos de distintas especificaciones de archivo, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).
commrestartduration	Especifica el número máximo de minutos durante los que se desea que el cliente intente volver a conectarse al servidor de IBM Spectrum Protect después de producirse un error en la comunicación.
commrestartinterval	Especifica el número de segundos que el cliente debe esperar entre los reintentos de conexión al servidor de IBM Spectrum Protect después de producirse un error de comunicación.
diskbuffsize	Especifica el tamaño máximo de búfer de E/S del disco (en kilobytes) que el cliente puede utilizar al leer archivos.





















Opción	Descripción
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows largecommbuffers	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Esta opción se ha sustituido por la opción diskbuffsize. En este momento, el cliente de archivado y copia de seguridad sigue aceptando la opción largecommbuffers para facilitar la transición a la nueva. No obstante, el valor especificado por largecommbuffers se omite en favor del valor de diskbuffsize. Importante: Deje de utilizar largecommbuffers, ya que es posible que releases posteriores del cliente no acepten esta opción.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X xnfstimeout	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica el número de segundos que el servidor espera a que se reciba una llamada de estado del sistema en un sistema de archivos NFS antes de que se exceda el tiempo de espera.
 Sistemas operativos Windows resourceutilization	 Sistemas operativos Windows Utilice la opción resourceutilization con el archivo de opciones de cliente, dsm.opt, para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X resourceutilization	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice la opción resourceutilization en el archivo dsm.sys para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.
txnbytelimit	Especifica el número de kilobytes que el programa cliente guarda en el búfer antes de enviar una transacción al servidor.
 Sistemas operativos Windows usedirectory	 Sistemas operativos Windows Proporciona una manera práctica de simplificar la configuración de comunicación del cliente modificando los parámetros commmethod establecidos en el archivo de opciones del cliente y realizará una consulta a Active Directory para saber qué método de comunicación debe utilizar y a qué servidor debe conectarse.

## Opciones de cliente Web

Para configurar el cliente web IBM Spectrum Protect se utilizan varias opciones de cliente de archivado y copia de seguridad.





Tabla 1 enumera las opciones de cliente web que están disponibles.

Tabla 1. Opciones de cliente Web

Opción	Descripción
httpport	Especifica una dirección de puerto TCP/IP para el cliente web.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X managedservices	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica si el daemon de aceptación de clientes gestiona el cliente web, el planificador o ambos programas.
 Sistemas operativos Windows managedservices	 Sistemas operativos Windows Especifica si el servicio de aceptación de clientes gestiona el cliente web, el planificador o ambos programas.
revokeremoteaccess	Restringe el acceso de un administrador a una estación de trabajo cliente a través del cliente web.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X webports	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el daemon de aceptación de clientes y el servicio de agente de cliente web para las comunicaciones con el cliente web.
 Sistemas operativos Windows webports	 Sistemas operativos Windows Permite utilizar el cliente web fuera de un cortafuegos especificando el número de puerto TCP/IP utilizado por el servicio de aceptación de clientes y el servicio de agente de cliente web para las comunicaciones con el cliente web.

## Utilización de opciones con mandatos

Puede modificar temporalmente diversas opciones del archivo de opciones del cliente (dsm.opt) especificándolas con los mandatos adecuados del cliente de copia de seguridad y archivado.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Puede modificar temporalmente diversas opciones del archivo dsm.sys o del archivo de opciones del usuario cliente (dsm.opt) especificándolas con los mandatos adecuados del cliente de copia de seguridad y archivado.

El cliente procesa las opciones siguiendo este orden (precedencia):





1. Opciones definidas en el servidor con opciones del cliente obligadas por el servidor. El servidor modifica los valores del cliente.
  2. Opciones escritas localmente en la línea de mandatos.
  3. Opciones definidas en el servidor para una planificación utilizando los parámetros de las opciones.
  4. Opciones escritas localmente en el archivo de opciones.
  5. Opciones recibidas del servidor con opciones del cliente no establecidas como implementadas por el servidor. El servidor *no* modifica los valores del cliente si no se le fuerza a ello.
  6. Valores predeterminados de la opción.
- Especificación de opciones con un mandato  
Debe seguir las reglas generales que se aplican a la especificación de opciones con un mandato.
  - Opciones que sólo son válidas en la línea de mandatos inicial  
Un subconjunto de las opciones de cliente que solo es válido en la línea de mandatos inicial. Muchas de estas opciones establecen el entorno de ejecución, como las opciones commmethod u optfile. Las opciones de esta categoría no son válidas en las modalidades interactiva, de macro ni de planificador. Estas opciones generan un error y hacen que el proceso se detenga.
  - Opciones del cliente que pueden establecerse con el servidor de IBM Spectrum Protect  
Algunas opciones del cliente pueden establecerse con el servidor de IBM Spectrum Protect.

## Especificación de opciones con un mandato

Debe seguir las reglas generales que se aplican a la especificación de opciones con un mandato.

- Escriba un mandato, un guión (-), el nombre de la opción, un signo de igual (=) y un parámetro o valor para la opción. No incluya ningún espacio a ambos lados del signo =.

A continuación, se muestran algunos ejemplos de esta sintaxis en distintos clientes:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc archive -description="year end 1999" /home/
```





 Sistemas operativos Windows

```
dsmc archive -description="Project A" c:\devel\proj1\*
```

- Para opciones que no incluyen parámetros, escriba un mandato, un guión (-) y el nombre de la opción. Por ejemplo:

```
dsmc incremental -quiet
```

Nota: utilice un guión (-) para indicar que el texto que sigue es el nombre de una opción. Si un nombre de objeto empieza con un guión, deberá especificar éste entre comillas simples (') o bien entre comillas dobles ("). La mayoría de los procesadores de línea de mandatos del sistema eliminan las comillas antes de enviar los argumentos de la línea de mandatos a la aplicación cliente de IBM Spectrum Protect. En esos casos, puede utilizar caracteres de escape o indicar el doble de comillas para que el cliente pueda recibir un nombre de objeto entre comillas. En la modalidad de bucle, especifique este tipo de objetos entre comillas simples (') o bien entre comillas dobles (").





- Puede escribirse el nombre de opción o una abreviatura del nombre de opción. Por ejemplo, para la opción latest, escriba `-lat` o `-latest`. En la sintaxis de la opción, las letras mayúsculas indican la abreviatura mínima del nombre de dicha opción.
- Entre las opciones antes o después de los parámetros del mandato. Por ejemplo, puede entrar la opción antes o después de una especificación de archivo:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc selective -subdir=yes "/home/devel/proj1/*"  
dsmc selective "/home/devel/proj1/*" -subdir=yes
```

 Sistemas operativos Windows

```
dsmc selective -subdir=yes c:\devel\proj1\  
dsmc selective c:\devel\proj1\* -subdir=yes
```





- Si especifica varias opciones en un mandato, separe cada una de ellas con un espacio en blanco.
- Si el valor de la opción que entre contiene un espacio en blanco, especifique el valor entre comillas ( " "). Por ejemplo:


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X



```
dsmc archive -description="Project A" "/home/devel/proj1/*"
```

 Sistemas operativos Windows

```
dsmc archive -description="Project A" c:\devel\proj1\*
```

- La mayor parte de opciones que se especifican en la línea de mandatos alteran temporalmente el valor establecido en el archivo de preferencias. Sin embargo, cuando utiliza la opción domain con el mandato incremental, ésta se añade al dominio especificado en el archivo de opciones del cliente en lugar de modificar temporalmente el valor actual.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En AIX, Solaris, Linux on z y Mac: el número máximo de caracteres de un nombre de archivo es 255. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.
-  Sistemas operativos Linux En Linux: la longitud máxima de un nombre de archivo es de 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 4096 bytes. Esta longitud coincide con el valor PATH\_MAX soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación real es el número de bytes de los componentes de vía de acceso y archivo, que puede corresponder o no a un número de caracteres igual.

 Sistemas operativos Linux En Linux: para las operaciones de archivado o recuperación, la longitud máxima que se puede especificar para una vía de acceso y un nombre de archivo (combinados) se mantiene en 1024 bytes.

-  Sistemas operativos Windows El número máximo de bytes para el conjunto formado por un nombre de archivo y una vía de acceso de archivo es 6255. Sin embargo, el nombre de archivo propiamente dicho no puede sobrepasar los 255 bytes, y la vía de acceso al archivo no puede sobrepasar los 6000 bytes. Asimismo, los nombres de los directorios (incluido el delimitador de directorio) de una vía de acceso tienen un límite de 255 bytes. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.
-  sistemas operativos Mac OS X Para Mac OS X, la longitud máxima de un nombre de archivo se limita a 504 bytes (no caracteres). La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres que un nombre de archivo contiene puede variar.

## Opciones que sólo son válidas en la línea de mandatos inicial




































Un subconjunto de las opciones de cliente que solo es válido en la línea de mandatos inicial. Muchas de estas opciones establecen el entorno de ejecución, como las opciones commmethod u optfile. Las opciones de esta categoría no son válidas en las modalidades interactiva, de macro ni de planificador. Estas opciones generan un error y hacen que el proceso se detenga.

Tabla 1 lista las opciones que sólo son válidas en la línea de mandatos inicial.

Tabla 1. Opciones que sólo son válidas en la línea de mandatos inicial

<b>Opciones válidas en la línea de mandatos inicial</b>	
---	--



Opciones válidas en la línea de mandatos inicial	
<ul style="list-style-type: none"> <li>•  Sistemas operativos Windowsasrmode</li> <li>•  Sistemas operativos Windowsbackupregistry</li> <li>• commmethod</li> <li>•  Sistemas operativos Windowscomputername</li> <li>• eliminación de duplicados</li> <li>• diskbuffsize</li> <li>• editor</li> <li>• enablededupcache</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  Sistemas operativos Windowsenablelanfree</li> <li>• errorlogmax</li> <li>• errorlogname</li> <li>• errorlogretention</li> <li>•  Sistemas operativos Windowsincrthreshold</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  Sistemas operativos Windowslanfreecommmethod</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  Sistemas operativos Windowslanfreeshmport</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  Sistemas operativos Windowslanfreetcport</li> <li>• maxcmdretries</li> <li>•  Sistemas operativos Windowsnamedpipename</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  sistemas operativos Mac OS Xnfstimeout</li> <li>• nodename</li> <li>• optfile</li> <li>• password</li> <li>• postschedulecmd/postnschedulecmd (puede incluirse en la definición de planificación)</li> <li>•  Sistemas operativos Windowspostsnapshotcmd</li> </ul>	<ul style="list-style-type: none"> <li>• preschedulecmd/prenschedulecmd (puede incluirse en la definición de planificación)</li> <li>•  Sistemas operativos Windowspresnapshotcmd</li> <li>• querschedperiod</li> <li>• resourceutilization</li> <li>• retryperiod</li> <li>•  Sistemas operativos Windowsrunasservice</li> <li>• schedlogmax</li> <li>• schedlogname</li> <li>• schedlogretention</li> <li>• schedmode</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux</li> <li>•  Sistemas operativos Oracle Solaris</li> <li>•  sistemas operativos Mac OS Xservername</li> <li>• sessioninitiation</li> <li>• setwindowtitle</li> <li>• tcpbuffsize</li> <li>• tcpcadaddress</li> <li>• tcpclientaddress</li> <li>• tcpclientport</li> <li>•  Sistemas operativos Windowstcport</li> <li>•  Sistemas operativos Windowstcpserveraddress</li> <li>• tcpwindowsize</li> <li>• txnbytelimit</li> <li>•  Sistemas operativos Windowsusedirectory</li> <li>• virtualnodename</li> </ul>

## Opciones del cliente que pueden establecerse con el servidor de IBM Spectrum Protect

Algunas opciones del cliente pueden establecerse con el servidor de IBM Spectrum Protect.

Tabla 1 enumera las opciones que pueden establecerse con el servidor.

Tabla 1. Opciones que pueden establecerse con el servidor de IBM Spectrum Protect

Opciones que pueden establecerse con el servidor de IBM Spectrum Protect
--

Opciones que pueden establecerse con el servidor de IBM Spectrum Protect	
<ul style="list-style-type: none"> <li>•  Sistemas operativos AIX  Sistemas operativos Linux Afmskipuncachedfiles</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Archsymlinkasfile</li> <li>•  Sistemas operativos Windows  Casesensitiveaware</li> <li>• Changingretries</li> <li>• Collocatebyfilespec</li> <li>• Compressalways</li> <li>• Compression</li> <li>• Eliminación de duplicados</li> <li>• Dirmc</li> <li>• Disablenqr</li> <li>• Diskcachelocation</li> <li>• Domain</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Domain.image</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Domain.nas</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Encryptiontype</li> <li>• Encryptkey</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Opciones exclude</li> <li>• Inclexcl</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Opciones include</li> <li>• maxcandprocs</li> <li>• maxmigrators</li> <li>• Memoryefficientbackup</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nfstimeout</li> <li>• Postschedulecmd/Postnschedulecmd</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Postsnapshotcmd</li> <li>• Preschedulecmd/Prenschedulecmd</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Preservelastaccessdate</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Presnapshotcmd</li> </ul>	<ul style="list-style-type: none"> <li>• Queryschedperiod</li> <li>• Quiet</li> <li>•  Sistemas operativos Windows Resetarchiveattribute</li> <li>• Resourceutilization</li> <li>• Retryperiod</li> <li>• Schedmode</li> <li>• Scrolllines</li> <li>• Scrollprompt</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux Snapshotcachesize</li> <li>•  Sistemas operativos AIX  Sistemas operativos Windows Snapshotproviderfs</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Snapshotproviderimage</li> <li>•  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Stagingdirectory</li> <li>• Subdir</li> <li>• Tapeprompt</li> <li>• Txnbytelimit</li> <li>• Verbose</li> <li>•  Sistemas operativos Linux  Sistemas operativos Windows  Vmchost</li> <li>•  Sistemas operativos Linux  Sistemas operativos Windows  Vmcuser</li> <li>•  Sistemas operativos Linux  Sistemas operativos Windows Vmprocessvmwithindependent</li> <li>•  Sistemas operativos Linux  Sistemas operativos Windows Vmprocessvmwithprdm</li> </ul>

Nota:

1. Consulte la documentación del producto IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en el IBM® Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERBW/welcome>.

**Tareas relacionadas:**

Control de operaciones de cliente mediante conjuntos de opciones de cliente


## Consulta de opciones del cliente

Las secciones siguientes contienen información detallada sobre cada una de las opciones de proceso de IBM Spectrum Protect.

La información sobre cada una de las opciones incluye:


























- Una descripción
- Un diagrama de sintaxis
- Descripciones detalladas de los parámetros.
- Ejemplos de uso de la opción en el archivo de opciones de cliente (si procede)
- Ejemplos de uso de la opción en la línea de mandatos (si procede)




























Las opciones en cuyo ejemplo de línea de mandatos se indica **No se aplica** no pueden utilizarse con la línea de mandatos ni con mandatos planificados.

 sistemas operativos Mac OS X Nota:

















1. No indique un valor de opción entre comillas, salvo que el valor sea una especificación de archivo que contenga espacios o caracteres comodín. Por ejemplo, la siguiente opción no es válida:

```
passwordaccess "generate"
```

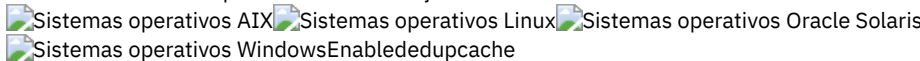
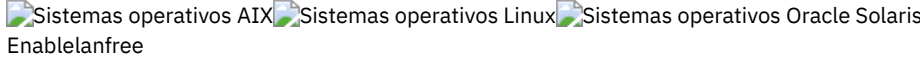
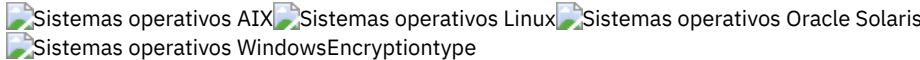
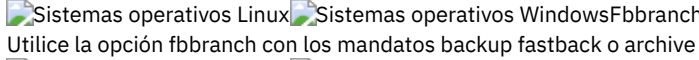
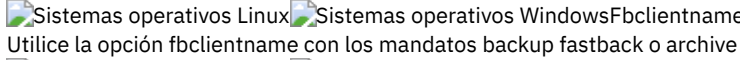
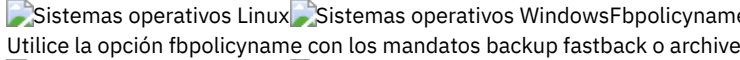
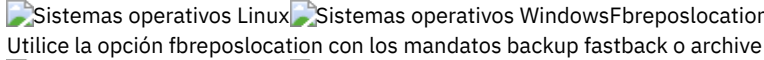
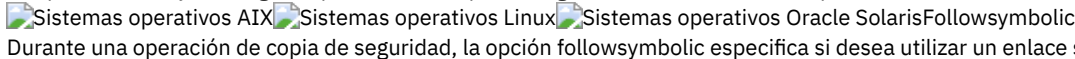
2.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Todas las opciones del archivo dsm.sys, excepto para la opción defaultserver, se deben colocar dentro de una stanza de servidor. Una stanza de servidor es una colección de sentencias de opciones en dsm.sys que comienzan con una opción SERVERName y terminan bien con la siguiente opción SERVERName bien con el final del archivo.
- Absolute  
Utilice la opción absolute con el mandato incremental para imponer una copia de seguridad de todos los archivos y directorios que coincidan con la especificación de archivo o domain, aunque los objetos no se hayan modificado desde la última copia de seguridad incremental.
  -  Sistemas operativos Windows Adlocation  
Puede utilizar la opción adlocation con los mandatos query adobjects o restore adobjects para indicar si los objetos de Active Directory van a consultarse o restaurarse desde el contenedor de objetos suprimidos de Active Directory local o desde la copia de seguridad de estado del sistema del servidor de IBM Spectrum Protect.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Afmskipuncachedfiles  
La opción afmskipuncachedfiles especifica si los archivos no almacenados en memoria caché y socios de conjuntos de archivos de Active File Management de General Parallel File System (GPFS) se procesan para operaciones de copia de seguridad, archivado y migración.
  - Archmc  
Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular los directorios o las copias archivadas.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archsymlinkasfile  
La opción archsymlinkasfile especifica si el cliente de copia de seguridad y archivado sigue un vínculo simbólico y archiva el directorio o el archivo al que hace referencia, o bien si archiva únicamente el vínculo simbólico. Utilice esta opción con el mandato archive.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Asnodename  
Utilice la opción asnodename para permitir a nodos agente realizar copias de seguridad o restauración de datos en nombre de otro nodo (el nodo de destino). Esto permite realizar operaciones simultáneas desde varios nodos para almacenar datos en el mismo nodo de destino y espacio de archivos en paralelo.
  -  Sistemas operativos Windows Asnodename  
Utilice la opción asnodename para permitir que un nodo agente realiza una copia de seguridad, archivado, restauración, recuperación y consulta de datos en nombre de un nodo de destino.
  -  Sistemas operativos Windows Asrmode  
Utilice la opción asrmode con los mandatos restore y restore systemstate para especificar si debe realizarse una operación de restauración en la modalidad de recuperación ASR del sistema.
  - Auditlogging  
Use la opción auditlogging para generar una anotación de auditoría que contenga una entrada para cada archivo que se procese durante una operación incremental, de selección, de archivado, de restauración o recuperación.
  - Auditlogname  
La opción auditlogname especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de auditoría. Esta opción se aplica cuando se habilita la anotación de auditoría.
  -  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Autodeploy  
Utilice la opción autodeploy para habilitar o inhabilitar un despliegue automático del cliente si es necesario un reinicio.
  - Autofsrename  
La opción autofsrename cambia el nombre de un espacio de archivos existente que no está activado para Unicode en el servidor de IBM Spectrum Protect para que pueda crearse un espacio de archivos activado para Unicode con el nombre original para la operación actual.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Automount  
La opción automount añade al dominio un sistema de archivos montado automáticamente montándolo. Utilice esta opción con la

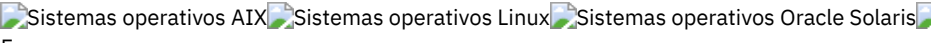
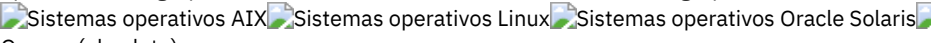
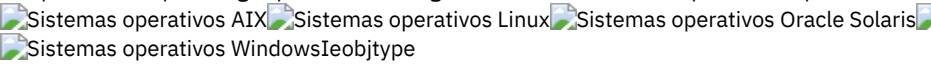
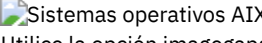
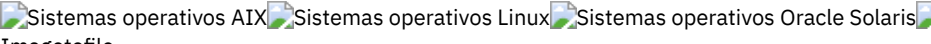
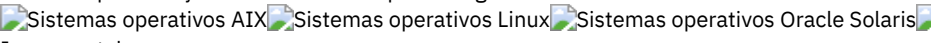


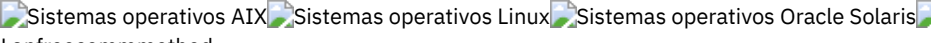
- opción domain.
-  Sistemas operativos Linux  Sistemas operativos Windows  Backmc  
 La opción backmc especifica la clase de gestión que aplicar al mandato backup fastback para fines de retención.
  - Backupsetname  
 La opción backupsetname especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect.
  - Basesnapshotname  
 La opción basesnapshotname especifica la instantánea a utilizar como instantánea base, cuando se realiza una copia de seguridad diferencial de instantánea (snapdiff) de un volumen de archivador NetApp. Si especifica esta opción, también debe utilizar la opción snapdiff o se produce un error. Si no se especifica basesnapshotname, la opción useexistingbase selecciona la instantánea más reciente en el volumen de archivador como la instantánea base.
  - Cadlistenonport  
 La opción cadlistenonport especifica si se debe abrir un puerto de escucha para el aceptador de clientes.
  -  Sistemas operativos Windows  Casesensitiveaware  
 La opción casesensitiveaware especifica si el cliente de copia de seguridad/archivado de Windows debe filtrar objetos de archivo y directorio cuyos nombres están en conflicto por el uso de las mayúsculas y minúsculas.
  - Changingretries  
 La opción changingretries especifica cuántas veces se desea que el cliente intente efectuar copia de seguridad o archivado de un archivo que se esté utilizando en ese momento. Utilice esta opción con los mandatos archive, incremental y selective.
  -  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  Class  
 La opción class especifica si ha de visualizarse una lista de objetos NAS o de cliente al utilizar los mandatos delete filespace, query backup y query filespace.
  -  Sistemas operativos Windows  Clientview  
 La opción clientview está disponible para usuarios que hayan actualizado desde el cliente de copia de seguridad de IBM® Tivoli Storage Manager Express al cliente de archivado y copia de seguridad.
  -  Sistemas operativos Windows  Clusterdisksonly  
 La opción clusterdisksonly especifica si el cliente de archivado y copia de seguridad permite realizar una copia de seguridad únicamente de discos en clúster en entornos específicos.
  -  Sistemas operativos Windows  Clusternode  
 La opción clusternode especifica el modo en que el cliente de copia de seguridad y archivado gestiona las unidades de clúster.
  - Collocatebyfilespec  
 Utilice la opción collocatebyfilespec para especificar si el cliente de copia de seguridad y archivado utiliza solamente una sesión de servidor para enviar objetos generados a partir de especificación de archivo.
  - Commmethod  
 La opción commmethod especifica el método de comunicación que se utiliza para proporcionar conectividad en la comunicación entre cliente y servidor.
  - Commrestartduration  
 La opción commrestartduration especifica el número máximo de minutos durante los que el cliente intentará conectarse de nuevo al servidor de IBM Spectrum Protect después de producirse un error de comunicación.
  - Commrestartinterval  
 La opción commrestartinterval especifica el número de segundos que deben transcurrir entre los intentos que realiza el cliente para volver a conectarse al servidor de IBM Spectrum Protect después de producirse un error de comunicación.
  - Compressalways  
 La opción compressalways especifica si se debe continuar la compresión si el objeto aumenta de tamaño durante la compresión.
  - Compression  
 La opción compression comprime los archivos antes de enviarlos al servidor.
  - Console  
 Utilice la opción console con el mandato query systeminfo para que la información del sistema se visualice en la consola.
  - Createnewbase  
 La opción createnewbase crea una instantánea base y la utiliza como fuente para ejecutar una copia de seguridad incremental completa.
  - Datacenter  
 Especifica la ubicación de destino del centro de datos que contendrá los datos de la máquina restaurada.
  - Datastore  
 Especifica el destino del almacén de datos que utilizar durante la operación de restauración de VMware.
  - Dateformat  
 La opción dateformat especifica el formato que desea utilizar para visualizar o especificar fechas.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Dedupcachepath  
 Utilice la opción dedupcachepath para especificar la ubicación donde se creó la base de datos de la memoria caché de eliminación de duplicados de datos del lado del cliente.
    -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows  Dedupcachesize  
 Utilice la opción dedupcachesize para determinar el tamaño máximo del archivo de la caché de la eliminación de duplicados de


































datos. Cuando el archivo de la caché alcanza su tamaño máximo, se elimina el contenido de la caché y se añaden las entradas nuevas.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Eliminación de duplicados  
Utilice la opción deduplication para especificar si habilita la eliminación de datos redundantes por parte del cliente cuando se transfieren los datos al servidor IBM Spectrum Protect durante el proceso de copia de seguridad y archivado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Defaultserver  
Utilice la opción defaultserver para especificar el nombre del servidor de IBM Spectrum Protect a contactar para los servicios de copia de seguridad/archivado si se ha definido más de un servidor en el archivo dsm.sys.
- Deletfiles  
Utilice la opción deletfiles con el mandato archive para suprimir archivos de la estación de trabajo después de haber realizado el archivado de éstos.
- Descripción  
La opción description asigna o especifica una descripción para los archivos cuando se efectúan operaciones de archivado, supresión de archivado, recuperación, consulta de archivado o consulta de juego de copias de seguridad.
- Detail  
Utilice la opción detail para ver información sobre la clase de gestión, el espacio de archivos, las copias de seguridad, las copias archivadas y otra información adicional en función del mandato con el que se utilice.
- Diffsnapshot  
La opción diffsnapshot controla si cliente de copia de seguridad y archivado debe crear la instantánea diferencial al ejecutar una copia de seguridad incremental por diferencia de instantánea.
- Diffsnapshotname  
La opción diffsnapshotname permite especificar qué instantánea diferencial, en el volumen de archivador de destino, debe utilizarse durante una copia de seguridad diferencial de instantáneas. Esta opción sólo se especifica si también se especifica diffsnapshot=latest.
- Dirmc  
La opción dirmc especifica la clase de gestión que desea utilizar para los directorios.
- Dirsonly  
La opción dirsonly *sólo* procesa directorios. El cliente no procesa archivos.
- Disablenqr  
La opción disablenqr especifica si el cliente de archivado y copia de seguridad puede usar el método de restauración sin consulta para restaurar archivos y directorios del servidor.
- Diskbuffsize  
La opción diskbuffsize especifica el tamaño máximo de memoria intermedia de E/S de disco (en kilobytes) que el cliente puede utilizar al leer archivos. La opción diskbuffsize sustituye a la opción largecommbuffers.
- Diskcachelocation  
La opción diskcachelocation especifica la ubicación en la que se crea la base de datos de memoria caché de disco si la opción memoryefficientbackup=diskcachemethod se especifica durante una copia de seguridad incremental.
- Domain  
La opción domain especifica lo que desea incluir en la copia de seguridad incremental.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Domain.image  
La opción domain.image especifica lo que desea incluir en el dominio de cliente para una copia de seguridad de imágenes.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Domain.nas  
La opción domain.nas especifica los volúmenes que deben incluirse en las copias de seguridad de imagen de NAS.
-  Sistemas operativos Linux  Sistemas operativos Windows Domain.vmfull  
La opción domain.vmfull especifica las máquinas virtuales (VM) a incluir en las operaciones de copia de seguridad de imagen de máquina virtual completa.
-  Sistemas operativos Linux Dontload  
Los clientes Linux x86\_64 pueden utilizar la opción dontload para evitar que se carguen las bibliotecas de plug-in específicas cuando se inicia el cliente de copia de seguridad-archivado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Dynamicimage  
Utilice la opción dynamicimage con el mandato backup image o la opción include.image para especificar que desea realizar una copia de seguridad de imagen dinámica.
-  Sistemas operativos AIX Efsdecrypt  
La opción efsdecrypt permite controlar si los archivos cifrados mediante un sistema de archivos cifrados (EFS) de AIX se leen con formato cifrado o descifrado.
-  Sistemas operativos Windows Enable8dot3namesupport  
La opción enable8dot3namesupport especifica si el cliente realiza copias de seguridad y restauraciones de los nombres cortos de la versión 8.3 de los archivos que tienen nombres largos en los sistemas de archivos NTFS.
- Enablearchiveretentionprotection  
La opción enablearchiveretentionprotection permite al cliente conectarse al servidor de IBM Spectrum Protect for Data































Retention. Esto garantiza que los objetos de archivado no se eliminarán del servidor mientras no se cumplan los requisitos de retención basados en políticas de dicho objeto.







-  **Enablededupcache**  
Utilice la opción `enablededupcache` para especificar si desea utilizar una memoria caché durante la eliminación de duplicados de datos por parte del cliente. El uso de una memoria caché local puede reducir el tráfico de red entre el servidor y el cliente de IBM Spectrum Protect.
- **Enableinstrumentation**  
De forma predeterminada, el cliente de copia de seguridad y archivado y la API de IBM Spectrum Protect recopilan automáticamente datos de instrumentación para identificar los cuellos de botella de rendimiento durante el proceso de copia de seguridad y restauración. Para inhabilitar o habilitar más tarde la instrumentación, utilice la opción `enableinstrumentation`.
-  **Enablelanfree**  
La opción `enablelanfree` especifica si debe activarse una vía de acceso disponible sin LAN a un dispositivo de almacenamiento conectado a una red de área de almacenamiento (SAN).
-  **Encryptiontype**  
Utilice la opción `encryptiontype` para especificar el algoritmo para el cifrado de datos.
- **Encryptkey**  
El cliente de copia de seguridad y archivado admite la opción que permite cifrar los archivos cuya copia de seguridad o archivado se realiza en el servidor de IBM Spectrum Protect. Esta opción se activa con la opción `include.encrypt`.
- **Errorlogmax**  
La opción `errorlogmax` especifica el tamaño máximo del registro de errores, en megabytes. El nombre predeterminado para el registro de errores es `dsmerror.log`.
- **Errorlogname**  
Esta opción especifica la vía de acceso totalmente calificada y el nombre de archivo en el que se deben guardar los mensajes de error.
- **Errorlogretention**  
La opción `errorlogretention` especifica durante cuántos días van a conservarse las entradas de las anotaciones de errores antes de eliminarlas y si se van a guardar las entradas eliminadas en otros archivos.
- **Opciones exclude**  
Utilice las opciones `exclude` para excluir objetos de la imagen de copia de seguridad o de los servicios de archivado.
-  **Fbbranch**  
Utilice la opción `fbbranch` con los mandatos `backup fastback` o `archive fastback`.
-  **Fbclientname**  
Utilice la opción `fbclientname` con los mandatos `backup fastback` o `archive fastback`.
-  **Fbpolicyname**  
Utilice la opción `fbpolicyname` con los mandatos `backup fastback` o `archive fastback`.
-  **Fbreposlocation**  
Utilice la opción `fbreposlocation` con los mandatos `backup fastback` o `archive fastback`.
-  **Fbserver**  
Utilice la opción `fbserver` con los mandatos `backup fastback` o `archive fastback`.
-  **Fbvolumename**  
Utilice la opción `fbvolumename` con los mandatos `backup fastback` o `archive fastback`.
- **Filelist**  
Utilice la opción `filelist` para procesar una lista de archivos.
- **Filename**  
Utilice la opción `filename` con el mandato `query systeminfo` para especificar un nombre de archivo en el que almacenar la información.
- **Filesonly**  
La opción `filesonly` restringe los procesos de copia de seguridad, restauración, recuperación o consulta a *sólo* los archivos.
-  **Followsymbolic**  
Durante una operación de copia de seguridad, la opción `followsymbolic` especifica si desea utilizar un enlace simbólico como punto de montaje virtual. Durante una operación de restauración o recuperación, la opción `followsymbolic` especifica cómo el cliente de copia de seguridad y archivado restaura un directorio cuyo nombre coincide con un enlace simbólico en el sistema de archivos de destino de restauración.
- **Forcefailover**  
La opción `forcefailover` permite al cliente migrar tras error inmediatamente al servidor secundario.
- **Fromdate**  
Utilice la opción `fromdate` con la opción `fromtime` para especificar una fecha y una hora a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
- **Fromnode**  
La opción `fromnode` permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato `set access` para permitirle consultar, restaurar o recuperar archivos para el otro nodo.































- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Fromowner  
 La opción fromowner especifica un propietario alternativo del que restaurar versiones de copia de seguridad o copias archivadas o imágenes. El propietario debe otorgar acceso a otro usuario para que éste utilice los archivos o imágenes.
- Fromtime  
 Utilice la opción fromtime con la opción fromdate para especificar una fecha a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
- Groupname  
 Utilice la opción groupname con el mandato backup group para especificar el nombre de un grupo. Sólo podrá realizar operaciones en grupos nuevos o en la versión actualmente activa del grupo.
- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Grupos (obsoleto)  
 Esta opción está obsoleta.
- Host  
 El host especifica la ubicación del servidor ESX de destino donde se crea la máquina virtual durante una operación de restauración de VMware.
- Httpport  
 La opción httpport especifica una dirección de puerto TCP/IP para el cliente web.
- Hsmreparsetag  
 La opción hsmreparsetag especifica un código de reanálisis exclusivo que crea un producto HSM instalado en el sistema.
- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Sistemas operativos Windows  
 Ieobjtype  
 Utilice la opción ieobjtype para especificar un tipo de objeto para la operación de eliminación de duplicación de datos por parte del cliente dentro de las sentencias de inclusión/exclusión.
- Ifnewer  
 La opción ifnewer sustituye un archivo existente por la última versión de copia de seguridad si ésta es más reciente que el archivo existente.
- 
 Sistemas operativos AIX Sistemas operativos Windows  
 Imagegapsize  
 Utilice la opción imagegapsize con el mandato backup image, en el archivo de opciones, o con la opción include.image para especificar el tamaño mínimo de las regiones vacías de un volumen que desea pasar por alto durante la realización de la copia de seguridad de imágenes.
- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Sistemas operativos Windows  
 Imagetofile  
 Utilice la opción imagetofile con el mandato restore image para especificar que desea restaurar la imagen de origen en un archivo.
- Inactive  
 Utilice la opción inactive para que se visualicen los objetos activos e inactivos.
- Inclexcl  
 La opción inclexcl especifica la vía de acceso y el nombre de archivo de un archivo de opciones de inclusión/exclusión.
- Opciones include  
 Las opciones include especifican los objetos que desea incluir para los servicios de copia de seguridad y archivado.
- Incrbydate  
 Utilice la opción incrbydate con el mandato incremental para realizar la copia de seguridad de los archivos nuevos y cambiados que tienen una fecha de modificación posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que excluya el archivo de la copia de seguridad.
- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Sistemas operativos Windows  
 Incremental  
 Utilice la opción incremental con el mandato restore image para asegurarse de que los cambios que se han realizado en la imagen base también se aplicarán a la imagen restaurada.
- 
 Sistemas operativos Windows  
 Incrthreshold  
 La opción incrthreshold especifica el valor de umbral para el número de directorios de cualquier espacio de archivos con registro por diario que pueda tener objetos activos en el servidor, pero no objetos equivalentes en la estación de trabajo.
- Instrlogmax  
 La opción instrlogmax especifica el tamaño máximo del registro de instrumentación (dsminstr.log) en MB. Los datos de rendimiento del cliente se recopilan en el archivo dsminstr.log durante el proceso de copia de seguridad o restauración cuando la opción enableinstrumentation tiene el valor yes.
- Instrlogname  
 La opción instrlogname especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información que recopila el cliente de copia de seguridad y archivado.
- 
 Sistemas operativos Windows  
 Journalpipe  
 La opción journalpipe especifica el nombre de pipe de un gestor de sesión de daemon de registro por diario al que se adjuntarán los clientes de copia de seguridad.
- 
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Sistemas operativos Windows  
 Lanfrecommmethod

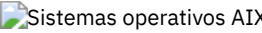
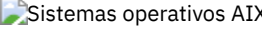
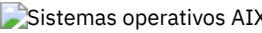
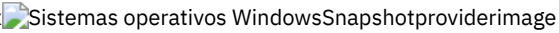
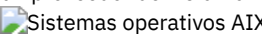
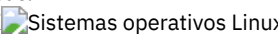
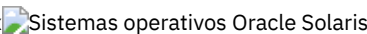
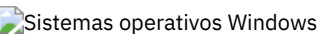
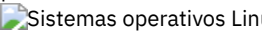
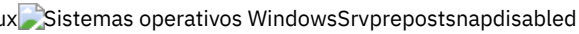

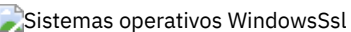
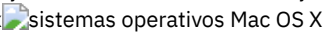
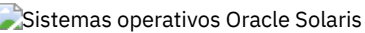
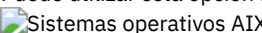
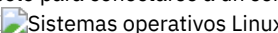
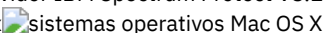


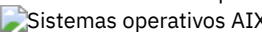

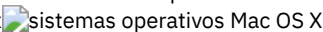
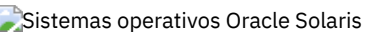

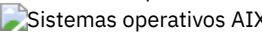

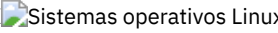
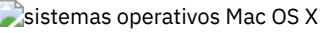
- La opción `lanfreecommmethod` especifica el protocolo de comunicaciones entre el cliente y el agente de almacenamiento de IBM Spectrum Protect. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Lanfreshmport`  
Utilice la opción `lanfreshmport` cuando se haya especificado `lanfreecommmethod=SHAREdmen` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Lanfreetcpsport`  
La opción `lanfreetcpsport` especifica el número de puerto TCP/IP en el que está escuchando el agente de almacenamiento de IBM Spectrum Protect.
  -  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Lanfreesssl`  
Utilice la opción `lanfreesssl` para habilitar SSL (Secure Sockets Layer) para proporcionar comunicaciones seguras de cliente y de agente de almacenamiento. Esta opción está en desuso si se conecta a un servidor IBM Spectrum Protect V8.1.2 o posterior.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Lanfreetcpserveraddress`  
La opción `lanfreetcpserveraddress` especifica la dirección TCP/IP del agente de almacenamiento de IBM Spectrum Protect.
  -  Sistemas operativos Windows `Idioma`  
La opción `language` especifica el idioma para la presentación de mensajes del cliente.
  - `Latest`  
Utilice la opción `latest` para restaurar la versión de copia de seguridad más reciente de un archivo, aunque la copia de seguridad no esté activa.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows `Localbackupset`  
La opción `localbackupset` especifica si la GUI del cliente de copia de seguridad y archivado pasa por alto la conexión inicial con el servidor de IBM Spectrum Protect, para restaurar un juego de copias de seguridad locales en una estación de trabajo independiente.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `Makesparsefile`  
Utilice la opción `makesparsefile` con los mandatos `restore` o `retrieve` para especificar el modo en que los archivos esparcidos se volverán a crear.
  - `Managedservices`  
La opción `managedservices` especifica si el servicio de aceptación de clientes de IBM Spectrum Protect ha de gestionar el planificador, el cliente web o ambos.
  - `Maxcmdretries`  
La opción `maxcmdretries` especifica el número máximo de veces que el planificador cliente (en la estación de trabajo del usuario) intenta procesar un mandato planificado que da error.
  - `Mbobjrefreshthresh`  
La opción `mbobjrefreshthresh` (umbral de renovación de objeto megablock) es un número que define un umbral. Cuando el número de objetos de IBM Spectrum Protect necesarios para describir cualquier megabloque de 128 MB supera este valor, se renueva el megabloque completo y caducan los objetos utilizados para representar esta área, en las copias de seguridad anteriores.
  - `Mbpctrefreshthresh`  
La opción `mbpctrefreshthresh` (umbral de renovación de porcentaje de megablock) es un número que define un umbral. Cuando el porcentaje de objetos de IBM Spectrum Protect necesarios para describir que algún megabloque de 128 MB supera este valor, se renueva el megabloque entero y caducan los objetos utilizados para representar esta área, en las copias anteriores.
  - `Memoryefficientbackup`  
La opción `memoryefficientbackup` especifica el algoritmo de reserva de memoria que ha de utilizarse para procesar las copias de seguridad de espacio de archivos completas.
  - `Mode`  
Utilice la opción `mode` para especificar la modalidad de copia de seguridad que desea utilizar al realizar operaciones de copia de seguridad específicas.
  -  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Monitor`  
La opción `monitor` especifica si se supervisará una copia de seguridad o una restauración de imagen de sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).
  -  Sistemas operativos Windows `Myprimaryserver`  
La opción `myprimaryserver` especifica el nombre de servidor primario que utiliza el cliente para iniciar la sesión en el servidor secundario en modalidad de migración tras error.
  - `Myreplicationserver`  
La opción `myreplicationserver` especifica qué stanza de servidor secundario utiliza el cliente durante una migración tras error.
  -  Sistemas operativos Windows `Namedpipename`  
La opción `namedpipename` especifica el nombre de named pipe para las comunicaciones entre un cliente y un servidor en el mismo dominio de servidor de Windows.
  -  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Nasnodename`  
La opción `nasnodename` especifica el nombre de nodo del servidor de archivos NAS cuando se procesan sistemas de archivos











- NAS. El cliente le solicita un ID de administrador.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Nfstimeout  
La opción nfstimeout especifica el número de segundos que el cliente espera a que se reciba una llamada de sistema de estado en un sistema de archivos NFS antes de que exceda el tiempo de espera.
  - Nodename  
Utilice la opción nodename en el archivo de opciones de cliente para identificar la estación de trabajo en el servidor. Puede utilizar nombres de nodo diferentes para identificar varios sistemas operativos en la estación de trabajo.
  -  Sistemas operativos WindowsNojournal  
Utilice la opción nojournal con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario predeterminada.
  -  Sistemas operativos AIXNojournal  
Utilice la opción nojournal con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional, en lugar de la copia de seguridad basada en registro por diario predeterminada.
  - Noprompt  
La opción noprompt suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire, restore image y set event.
  - Nrtablepath  
La opción nrtablepath especifica la ubicación de la tabla de réplica de nodo en el cliente. El cliente de copia de seguridad y archivado utiliza esta tabla para almacenar la información acerca de cada operación de copia de seguridad o archivado en el servidor de IBM Spectrum Protect.
  - Numberformat  
La opción numberformat especifica el formato que desea utilizar para visualizar los números.
  - Optfile  
La opción optfile especifica el archivo de opciones de cliente que se ha de utilizar cuando inicia una sesión del cliente de copia de seguridad y archivado.
  - Contraseña  
La opción password especifica una contraseña para IBM Spectrum Protect.
  - Passwordaccess  
La opción passwordaccess especifica si desea generar la contraseña automáticamente o establecerla mediante una solicitud al usuario.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Passworddir  
La opción passworddir especifica el directorio donde debe almacenarse el archivo de la contraseña cifrada.
  - Pick  
La opción pick crea la lista de versiones de copia de seguridad o copias archivadas que coinciden con la especificación de archivo que ha especificado.
  - Pitdate  
Utilice la opción pitdate con la opción pittime para establecer un instante específico para visualizar o restaurar la última versión de las copias de seguridad.
  - Pittime  
Utilice la opción pittime con la opción pitdate para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsPostschedulcmd/Postnschedulcmd  
La opción postschedulcmd/postnschedulcmd especifica un mandato que el programa cliente procesa después de ejecutar una planificación.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsPostsnapshotcmd  
La opción postsnapshotcmd le permite ejecutar scripts o mandatos de shell del sistema operativo después de que el cliente de copia de seguridad y archivado haya iniciado una instantánea durante una operación de copia de seguridad basada en instantánea.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsPreschedulcmd/Prenschedulcmd  
La opción preschedulcmd especifica un mandato que el programa cliente procesa antes de ejecutar una planificación.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Preservelastaccessdate  
Utilice la opción preservelastaccessdate para especificar si una operación de copia de seguridad o de archivado cambia la última hora de acceso.
  - Preservepath  
La opción preservepath especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsPresnapshotcmd  
La opción presnapshotcmd le permite ejecutar mandatos del sistema operativo antes de que el cliente de copia de seguridad y archivado inicie una instantánea.

































- **Queryschedperiod**  
La opción queryschedperiod especifica el número de horas que se desea que espere el planificador cliente entre los intentos de establecer contacto con el servidor para realizar trabajos planificados.
- **Querysummary**  
La opción querysummary proporciona estadísticas sobre los archivos, directorios y objetos que devuelven los mandatos query backup o query archive.
- **Quiet**  
La opción quiet limita el número de mensajes que se muestran en la pantalla durante un proceso.
- **Quotesareliteral**  
La opción quotesareliteral especifica si las comillas simples (') o las comillas dobles (") se interpretan literalmente cuando se incluyen en la especificación de una lista de archivos en una opción filelist.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
**Removeoperandlimit**  
La opción removeoperandlimit especifica que el cliente elimina el límite de 20 operandos.
- **Replace**  
La opción replace especifica si ha de grabarse encima de los archivos existentes en la estación de trabajo o si ha de solicitarse al usuario que realice la selección deseada al restaurar o recuperar archivos.
- **Replserverguid**  
La opción replserverguid especifica el GUID (Globally Unique Identifier) que se utiliza cuando el cliente se conecta al servidor secundario durante la migración tras error. El GUID se utiliza para validar el servidor secundario para asegurarse de que es el servidor esperado.
- **Replservername**  
La opción replservername especifica el nombre del servidor secundario al que se conecta el cliente durante una migración tras error.
- **Replsslport**  
La opción replsslport especifica el puerto TCP/IP en el servidor secundario que está habilitado para SSL. La opción replsslport se utiliza cuando el cliente se conecta al servidor secundario durante una migración tras error. Esta opción está en desuso si se conecta a un servidor IBM Spectrum Protect V8.1.2 o posterior.
- **Repltcpport**  
La opción repltcpport especifica el puerto TCP/IP en el servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.
- **Repltcpserveraddress**  
La opción repltcpserveraddress especifica la dirección TCP/IP del servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.
-  Sistemas operativos Windows **Resetarchiveattribute**  
Utilice la opción resetarchiveattribute para especificar si el cliente de copia de seguridad y archivado restablecerá el atributo de archivado de Windows en los archivos de los que se realiza correctamente una copia de seguridad en el servidor de IBM Spectrum Protect.
- **Resourceutilization**  
Utilice la opción resourceutilization con el archivo de opciones para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.
- **Retryperiod**  
La opción retryperiod especifica el número de minutos que debe esperar el planificador cliente entre intentos de procesar un mandato planificado que da error, o entre intentos infructuosos de informar al servidor de los resultados. Utilice esta opción sólo si el planificador se encuentra en ejecución.
- **Revokeremoteaccess**  
La opción revokeremoteaccess impide que un administrador con privilegio de acceso a cliente acceda a una estación de trabajo cliente donde se esté ejecutando el cliente web.
-  Sistemas operativos Windows **Runasservice**  
La opción runasservice obliga a que siga el proceso de mandatos del cliente, aunque la cuenta que inició el cliente se desconecte.
- **Schedcmddisabled**  
La opción schedcmddisabled especifica si ha de desactivarse la planificación de los mandatos mediante la opción action=command del servidor en el mandato de servidor define schedule.
- **Schedcmdexception**  
La opción schedcmdexception se utiliza conjuntamente con la opción schedcmddisabled para desactivar la planificación de mandatos mediante la opción action=command del servidor en el mandato del servidor DEFINE SCHEDULE, excepto para series de mandatos específicas.
- **Schedgroup**  
La opción schedgroup asigna una planificación a un grupo.
- **Schedlogmax**  
La opción schedlogmax especifica el tamaño máximo del registro de planificación (dsmsched.log) y de registro del cliente web (dsmwebcl.log), en megabytes.

- **Schedlogname**  
La opción schedlogname especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de planificación.
- **Schedlogretention**  
La opción schedlogretention especifica el número de días que se mantienen las entradas en el registro de planificación (dsmsched.log) y el registro del cliente web (dsmwebcl.log), y si deben guardarse las entradas eliminadas en otro archivo.
- **Schedmode**  
La opción schedmode especifica si se desea utilizar la modalidad de sondeo de cliente (el nodo cliente periódicamente consulta al servidor sobre los trabajos planificados), o bien la modalidad de solicitud de servidor (el servidor contacta con el nodo cliente en el momento de iniciar una operación planificada).
- **Schedrestretrdisabled**  
La opción schedrestretrdisabled especifica si se debe inhabilitar la ejecución de las operaciones de restauración o recuperación planificadas.
- **Scrolllines**  
La opción scrolllines especifica el número de líneas de información que deben aparecer en pantalla a la vez.
- **Scrollprompt**  
La opción scrollprompt especifica si desea que el cliente de copia de seguridad y archivado se detenga y espere después de visualizar el número de líneas de información especificado en la opción scrolllines, o desea que se desplace hasta el final de la lista de información.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
**Servername**  
En el archivo dsm.sys, la opción servername especifica el nombre que desea utilizar para identificar un servidor y para iniciar una sección que contenga opciones para ese servidor. Puede identificar y especificar opciones para varios servidores.
- **Sessioninitiation**  
Utilice la opción sessioninitiation para controlar si el servidor o el cliente ha de iniciar las sesiones a través de un cortafuegos. El valor predeterminado especifica que el cliente ha de iniciar las sesiones. Puede utilizar esta opción con el mandato schedule.
- **Setwindowtitle**  
Utilice la opción setwindowtitle para modificar el título de la ventana de mandatos de cliente administrativo durante el proceso.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
**Shmport**  
La opción shmport especifica la dirección del puerto TCP/IP de un servidor al utilizar la memoria compartida. Todas las comunicaciones de memoria compartida comienzan con una conexión TCP/IP.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
**Showmembers**  
Utilice la opción showmembers para visualizar todos los miembros de un grupo.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
**Skipacl**  
La opción skipacl permite incluir o excluir datos de la lista de control de acceso (ACL) durante una operación de copia de seguridad o archivado; se incluyen los datos de ACL de forma predeterminada.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
**Skipaclupdatecheck**  
La opción skipaclupdatecheck desactiva la suma de comprobación y las comparaciones de tamaño de los datos de ACL.
-  Sistemas operativos Windows  
**Skipmissingsyswfiles**  
Utilice la opción Skipmissingsyswfiles para especificar si el cliente de archivado y copia de seguridad omite determinados archivos de VSS Writer que faltan y continúa la copia de seguridad del estado del sistema.
-  Sistemas operativos Windows  
**Skipntpermissions**  
La opción skipntpermissions pasa por alto el proceso de la información de seguridad del sistema de archivos de Windows.
-  Sistemas operativos Windows  
**Skipntsecuritycrc**  
La opción skipntsecuritycrc controla el cálculo de la comprobación de redundancia cíclica (CRC) de seguridad para obtener una comparación de la información de seguridad de NTFS o ReFS durante la realización de una operación de copia de seguridad incremental o de copia de seguridad selectiva, una operación de archivado, de restauración o de recuperación.
-  Sistemas operativos Windows  
**Skipsystemexclude**  
Utilice la opción skipsystemexclude para especificar cómo procesar sentencias de exclusión para determinados archivos del sistema operativo que el cliente de IBM Spectrum Protect for Virtual Environments omite de forma predeterminada.
-  Sistemas operativos Linux  Sistemas operativos Windows  
**Snapdiff**  
Si se utiliza la opción snapdiff con el mandato incremental el proceso de copia de seguridad a incrementos se realiza de forma transparente. El mandato ejecuta una copia de seguridad a incrementos de los archivos modificados, según los informes de NetApp, en lugar de explorar todo el volumen en busca de archivos modificados.
-  Sistemas operativos Linux  Sistemas operativos Windows  
**Snapdiffchangelogdir**  
La opción snapdiffchangelogdir define la ubicación donde el cliente almacena los registros de cambios utilizados para operaciones de copia de seguridad diferencial de instantánea.
-  Sistemas operativos Linux  Sistemas operativos Windows  
**Snapdiffhttps**  
Especifique la opción snapdiffhttps para utilizar una conexión HTTPS segura para comunicarse con un archivador NetApp durante una copia de seguridad diferencial de instantánea.

-  Sistemas operativos AIX  Sistemas operativos Linux `Snapshotcachesize`  
Utilice la opción `snapshotcachesize` para especificar un tamaño adecuado para crear una instantánea.
-  Sistemas operativos AIX  Sistemas operativos Windows `Snapshotproviderfs`  
Utilice la opción `snapshotproviderfs` para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas, y para especificar un proveedor de instantáneas.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows `Snapshotproviderimage`  
Utilice la opción `snapshotproviderimage` para activar la copia de seguridad de imágenes basada en instantánea y para especificar un proveedor de instantáneas.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Snapshotroot`  
Utilice la opción `snapshotroot` con los mandatos `incremental`, `selective` o `archive` con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.
- `Srvoptsetencryptiondisabled`  
La opción `srvoptsetencryptiondisabled` permite que el cliente ignore las opciones de cifrado en el conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect.
- `Srvprepostscheddisabled`  
La opción `srvprepostscheddisabled` especifica si ha de impedirse que los mandatos de preplanificación y de postplanificación que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas.
-  Sistemas operativos Linux  Sistemas operativos Windows `Srvprepostsnapdisabled`  
La opción `srvprepostsnapdisabled` especifica si ha de impedirse que los mandatos de previos y posteriores a la instantánea que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Ssl`  
Utilice la opción `ssl` para habilitar Secure Sockets Layer (SSL) para proporcionar comunicaciones de servidor y de cliente seguro. Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.1 o V8 anterior, o V7.1.7 o anterior, el cliente determina si SSL está habilitado. Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.2 o posterior, siempre se utiliza SSL y esta opción controla si se cifran o no los datos de objeto. Por motivos de rendimiento, puede ser aconsejable no cifrar los datos de objeto.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Sslacceptcertfromserv`  
Utilice la opción `sslacceptcertfromserv` para controlar si el cliente de archivado y copia de seguridad o la aplicación de API aceptan y confían en el certificado público de SSL (Capa de sockets seguros) del servidor de IBM Spectrum Protect la primera vez que se conectan. Esta opción sólo se aplica la primera vez que el cliente de archivado y copia de seguridad o la aplicación de API se conectan al servidor de IBM Spectrum Protect. Una vez que el certificado público SSL se ha aceptado, los cambios futuros en el certificado no se aceptarán automáticamente y deben importarse manualmente al cliente de archivado y copia de seguridad. Puede utilizar esta opción solo para conectarse a un servidor IBM Spectrum Protect V8.1.2 y posterior.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Ssldisablelegacytls`  
Utilice la opción `ssldisablelegacytls` para no permitir el uso de protocolos SSL que son inferiores a TLS 1.2.
- `Sslfipsmode`  
La opción `sslfipsmode` especifica si el cliente utiliza la modalidad de SSL Federal Information Processing Standards (FIPS) para comunicaciones de capa segura de sockets (SSL) con el servidor. El valor predeterminado es no.
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `Sslrequired`  
La opción `sslrequired` especifica las condiciones en que SSL es o no necesario cuando el cliente inicia la sesión en el servidor o en los agentes de almacenamiento de IBM Spectrum Protect. Para habilitar realmente SSL para que las comunicaciones de cliente a servidor y de cliente a almacenamiento sean seguras, debe configurar la opción de cliente `ssl` en yes. Cuando se comunica con un servidor IBM Spectrum Protect V8.1.2 y posterior, esta opción ya no se aplica ya que se utiliza SSL.
-  Sistemas operativos AIX  Sistemas operativos Windows `Stagingdirectory`  
La opción `stagingdirectory` define la ubicación donde el cliente almacena los datos que genera a fin de realizar sus operaciones. Una vez finalizado el proceso se suprimen los datos.
- `Subdir`  
La opción `subdir` especifica si desea incluir subdirectorios de los directorios especificados para el proceso.
-  Sistemas operativos Windows `Systemstatebackupmethod`  
Utilice la opción `systemstatebackupmethod` para especificar qué método de copia de seguridad utilizar para realizar una copia de seguridad de la parte del grabador del sistema de los datos de estado del sistema. El método seleccionado se utiliza cuando se hace una copia de seguridad de los datos de estado del sistema.
- `Tapeprompt`  
La opción `tapeprompt` especifica si el cliente de copia de seguridad y archivado debe esperar el montaje de la cinta cuando éste sea necesario en un proceso de copia de seguridad, archivado, restauración o recuperación, o si se debe preguntar al usuario.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows `Tcpadminport`


Utilice la opción `tcpadminport` para especificar un número de puerto TCP/IP por separado en el que el servidor está a la espera de las solicitudes de sesiones de cliente de administración, lo que permite establecer sesiones de administración seguras dentro de una red privada.

- **Tcpbuffsize**  
La opción `tcpbuffsize` especifica el tamaño del almacenamiento intermedio de comunicaciones TCP/IP interno utilizado para transferir datos entre el nodo cliente y el servidor. Aunque utilice más memoria, un almacenamiento intermedio de mayor tamaño puede mejorar el rendimiento en las comunicaciones.
- **Tpcadaddress**  
La opción `tpcadaddress` especifica una dirección TCP/IP para `dsmcad`. Esta opción no suele ser necesaria. Utilice esta opción sólo si el nodo cliente tiene más de una dirección TCP/IP o bien si TCP/IP no es el método de comunicación predeterminado.
- **Tcpclientaddress**  
La opción `tcpclientaddress` especifica una dirección TCP/IP si el nodo cliente tiene más de una dirección y quiere que el servidor contacte con una dirección distinta de la utilizada para realizar el primer contacto del servidor.
- **Tcpclientport**  
La opción `tcpclientport` especifica un número de puerto TCP/IP para que el servidor contacte con el cliente cuando el servidor comience la operación planificada por solicitud de servidor.
- **Tcpnodelay**  
La opción `tcpnodelay` especifica si el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red, por transacción.
- **Tcpport**  
La opción `tcpport` especifica una dirección de puerto TCP/IP para el servidor de IBM Spectrum Protect. Puede obtenerse esta dirección del administrador.
- **Tcpserveraddress**  
La opción `tcpserveraddress` especifica la dirección TCP/IP del servidor de IBM Spectrum Protect. Puede obtener esta dirección de servidor solicitándosela al administrador.
- **Tcpwindowsize**  
Utilice la opción `tcpwindowsize` para especificar el tamaño en kilobytes que desea que tenga la ventana deslizante de TCP/IP para el nodo cliente.
- **Timeformat**  
La opción `timeformat` especifica el formato en el que desea ver y especificar la hora del sistema.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos WindowsToc  
Utilice la opción `toc` con el mandato `backup nas` o la opción `include.fs.nas` para especificar si el cliente de copia de seguridad y archivado ha de guardar la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.
- **Todate**  
Utilice la opción `todate` con la opción `totime` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.
- **Totime**  
Utilice la opción `totime` con la opción `todate` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta. El cliente de copia de seguridad y archivado pasa por alto esta opción si no especifica la opción `todate`.
- **Txnbytelimit**  
La opción `txnbytelimit` especifica el número de kilobytes que el programa de cliente guarda en el almacenamiento intermedio antes de enviar una transacción al servidor.
- **Type**  
Utilice la opción `type` con el mandato `query node` para especificar el tipo de nodo que ha de consultarse. Utilice esta opción con el mandato `set event` para activar, retener o liberar.
- **Updatectime**  
Utilice la opción `updatectime` para comprobar el atributo de cambio de hora (`ctime`) durante una operación de copia de seguridad incremental.
-  Sistemas operativos WindowsUsedirectory  
La opción `usedirectory` consulta a Active Directory con qué método de comunicación y a qué servidor debe conectarse.
- **Useexistingbase**  
La opción `useexistingbase` se utiliza cuando se hacen copias de seguridad de instantáneas que se encuentran en volúmenes de archivador NetApp. La opción `useexistingbase` indica que la instantánea más reciente que existe en el volumen del que se está realizando una copia de seguridad, debe utilizarse como la instantánea base durante una operación de copia de seguridad diferencial de instantáneas.
- **Usereplicationfailover**  
La opción `usereplicationfailover` especifica si se produce la migración tras error automatizada del cliente de un nodo cliente.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Usuarios (obsoleto)  
Esta opción está obsoleta.
- **V2archive**  
Utilice la opción `v2archive` con el mandato `archive` para realizar el archivado sólo de los archivos en el servidor.


- **Verbose**  
La opción verbose especifica que se desea visualizar información detallada de proceso en la pantalla. Éste es el valor predeterminado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
**Verifyimage**  
Utilice la opción verifyimage con el mandato restore image para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino.
- **Virtualfsname**  
Utilice la opción virtualfsname con el mandato backup group para especificar el nombre del espacio de archivos virtual para el grupo en el que desea realizar la operación. El valor de la opción virtualfsname no puede ser igual a un nombre de espacio de archivos existente.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
**Virtualmountpoint**  
La opción virtualmountpoint define un punto de montaje virtual para un sistema de archivos, si desea que se realice una copia de seguridad de los archivos que empiezan en un directorio determinado de dicho sistema de archivos.
- **Virtualnodename**  
La opción virtualnodename especifica el nombre de nodo de la estación de trabajo cuando desea restaurar o recuperar archivos en una estación de trabajo diferente.
-  Sistemas operativos Windows **Vm autostartvm**  
Utilice la opción vm autostartvm con el mandato restore VM vmrestoretype=instantaccess para especificar si la máquina virtual creada durante el proceso de acceso instantáneo se ha encendido automáticamente.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm backupdir**  
La opción vmbackdir especifica la ubicación del disco temporal en el que el cliente guarda los archivos de control que se han creado durante las operaciones de copia de seguridad y restauración de VM completa de máquinas virtuales .
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm backuplocation**  
Utilice la opción vmbackuplocation con los mandatos backup vm o restore vm para especificar la ubicación de copia de seguridad para las operaciones de copia de seguridad y restauración de máquinas virtuales.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm backupmailboxhistory**  
La opción vmbackupmailboxhistory especifica si el historial del buzón se carga automáticamente con la copia de seguridad de la máquina virtual (VM) cuando se detecta IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en una máquina virtual.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm backuptype**  
Utilice la opción vmbackuptype con el mandato backup VM o restore VM para especificar el tipo de copia de seguridad de máquina virtual para completar. También puede utilizar esta opción en mandatos query VM para filtrar los resultados de la consulta e incluir solo máquinas virtuales cuya copia de seguridad haya sido realizada por un tipo de copia de seguridad específico. Para obtener ejemplos, consulte la descripción del mandato query VM.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm chost**  
Utilice la opción vmchost con los mandatos backup VM, restore VM o query VM para especificar el nombre de host de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm cpw**  
Utilice la opción vmcpw con los mandatos backup VM, restore VM o query VM para especificar la contraseña del ID de usuario de VMware VirtualCenter o de ESX que se ha especificado con la opción vmcuser.
- **Vmctlmc**  
Esta opción especifica la clase de gestión que utilizar al hacer copias de seguridad archivos de control de máquina virtual.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm cuser**  
Utilice la opción vmcuser con los mandatos backup VM, restore VM o query VM para especificar el nombre de usuario de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm datastorethreshold**  
Utilice la opción vmdatstorethreshold para establecer el porcentaje de umbral de uso de espacio de cada almacén de datos de VMware de una máquina virtual.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm defaultdvportgroup**  
Utilice esta opción para especificar el grupo de puertos que utilizarán las NIC durante las operaciones restore vm para una máquina virtual que estaba conectada a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no contiene un grupo de puerto virtual distribuido similar.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm defaultdvswitch**  
Utilice esta opción para especificar el conmutador virtual distribuido (dvSwitch) que contiene el grupo de puertos que establezca en la opción vmdefaultdvportgroup. La opción no tiene efecto a menos que también especifique la opción vmdefaultdvportgroup.
-  Sistemas operativos Linux  Sistemas operativos Windows **Vm defaultnetwork**  
Utilice esta opción para especificar la red para que utilizarán las NIC durante una operación restore vm, para una máquina virtual que se había conectado a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no tiene ningún grupo de puerto conmutador distribuido configurado.
-  Sistemas operativos Windows **Vm diskprovision**  
Utilice la opción vmdiskprovision para especificar una política de suministro para el archivo de disco virtual que se utiliza para

restaurar los datos de la máquina virtual VMware. Esta opción es válida sólo para las operaciones restore vm donde se especifique `vmrestoretype=instantrestore`.

- **Vmenabletemplatebackups**


La opción `vmenabletemplatebackups` especifica si el cliente realiza una copia de seguridad de máquinas virtuales de plantillas de VMware cuando protege máquinas virtuales en un servidor vCenter. No se puede realizar la copia de seguridad de las máquinas virtuales de plantillas de VMware cuando éstas están en un host ESXi porque ESXi no soporta plantillas.
-  **Sistemas operativos WindowsVmexpireprotect**

Utilice esta opción para proteger instantáneas de máquina virtual, de forma que no puedan caducar mientras está en curso una operación de restauración instantánea o acceso instantáneo de máquinas virtuales VMware o una restauración de nivel de archivo de una máquina virtual VMware. Utilice esta opción para proteger instantáneas de máquina virtual, de forma que no puedan caducar mientras está en curso una operación de restauración instantánea o acceso instantáneo de máquinas virtuales Hyper-V o una restauración de nivel de archivo de una máquina virtual Hyper-V.
- **Vmiscsiadapter**

Esta opción especifica qué adaptador iSCSI, en el host ESX, se debe utilizar para la restauración instantánea y las operaciones de acceso instantáneo de máquinas virtuales VMware.
-  **Sistemas operativos WindowsVmiscsiserveraddress**


Utilice la opción `vmiscsiserveraddress` con el mandato `restore VM` para especificar el nombre de host o la dirección IP del servidor iSCSI que proporciona los destinos iSCSI para las operaciones de restauración instantánea y de acceso instantáneo.
- **Vmlimitperdatastore**

La opción `vmlimitperdatastore` especifica el número de máquinas virtuales (VM) y discos virtuales en un almacén de datos que se pueden procesar durante una operación de copia de seguridad optimizada.
- **Vmlimitperhost**

La opción `vmlimitperhost` especifica el número de máquinas virtuales (VM) y discos virtuales de un host que se pueden procesar en paralelo durante una operación de seguridad optimizada.
-  **Sistemas operativos WindowsVmlist**


La opción `vmlist` está en desuso para operaciones de copia de seguridad de Hyper-V. Para especificar que una o más máquinas virtuales (VM) de Hyper-V se incluyan en operaciones de copia de seguridad de Data Protection for Microsoft Hyper-V, utilice la opción `domain.vmfull` o especifique las máquinas virtuales cuando ejecute el mandato `backup vm`.
- **Vmmaxbackupsessions**

La opción `vmmaxbackupsessions` especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que trasladan de la máquina virtual (VM) al servidor datos que se pueden incluir en una operación de seguridad optimizada.
- **Vmmaxparallel**



La opción `vmmaxparallel` se utiliza para configurar copias de seguridad optimizadas de varias máquinas virtuales utilizando una sola instancia del cliente de archivado y copia de seguridad. Esta opción especifica el número máximo de máquinas virtuales de las que se puede hacer una copia de seguridad en el Servidor de IBM Spectrum Protect en cualquier momento dado.
-  **Sistemas operativos WindowsVmmaxpersnapshot**

Utilice la opción `vmmaxpersnapshot` para especificar el número máximo de máquinas virtuales (VM) que deben incluirse en una instantánea de Hyper-V. La copia de seguridad de las máquinas virtuales de la instantánea se realiza en el servidor de IBM Spectrum Protect.
- **Vmmaxrestoresessions**



La opción `vmmaxrestoresessions` especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que se pueden incluir en una operación de restauración optimizada para una máquina virtual (VM).
- **Vmmaxrestoreparalleldisks**

La opción `vmmaxrestoreparalleldisks` permite que un Cliente IBM Spectrum Protect restaure varios discos virtuales al mismo tiempo.
-  **Sistemas operativos WindowsVmmaxsnapshotretry**





















Utilice la opción `vmmaxsnapshotretry` para especificar el número máximo de veces que se debe reintentar una operación de instantánea de una máquina virtual (VM) si la instantánea inicial falla con una condición recuperable.
- **Vmmaxvirtualdisks**

La opción `vmmaxvirtualdisks` especifica el tamaño máximo de los discos de máquina virtual VMware (VMDK) para incluir en una operación de copia de seguridad.
-  **Sistemas operativos Linux**  **Sistemas operativos WindowsVmmc**




Utilice la opción `vmmc` para almacenar las copias de seguridad de máquina virtual con una clase de gestión distinta a la clase de gestión predeterminada. Para copias de seguridad de VM de VMware, la opción `vmmc` sólo es válida si se ha establecido la opción `vmbackuptype=fullvm`.
- **Vmmountage**

Utilice la opción `vmmountage` con el mandato `restore VM "*" -vmrestoretype=mountcleanupall` para especificar el número de horas durante las cuales debe estar activo un montaje de restauración de nivel de archivo de MV para borrar.
-  **Sistemas operativos Linux**  **Sistemas operativos WindowsVmnoprmdisks**

Esta opción permite al cliente restaurar la información de configuración para los volúmenes pRDM que están asociados con una máquina virtual VMware, aunque no se puedan encontrar las LUN que estaban asociadas con los volúmenes. Dado que los volúmenes pRDM no se incluyen en la instantánea de máquina virtual, solo se puede restaurar la información de configuración y no los datos que estaban en los volúmenes.

-  Sistemas operativos Linux  Sistemas operativos Windows `Vmnovrdm`disks  
Esta opción permite al cliente restaurar la información de configuración y los datos para volúmenes de pRDM asociados a una máquina virtual VMware virtual, incluso si no se encuentran los LUN que estaban asociados a los volúmenes.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmpreferdag`passive  
La opción `vmpreferdag`passive especifica si se debe realizar una copia de seguridad de una copia activa o pasiva de una base de datos que forma parte de un grupo de disponibilidad de base de datos (DAG) de Microsoft Exchange Server.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmprocessvmwith`independent  
Utilice esta opción para controlar si las copias de seguridad completas de máquinas virtuales de VMware son procesadas si la máquina se suministra con uno o más volúmenes de discos independientes.
- `Vmprocessvmwith`physdisks  
Utilice la opción `vmprocessvmwith`physdisks para controlar si las copias de seguridad de máquina virtual (VM) Hyper-V RCT se procesan si la VM tiene uno o más discos físicos (discos de paso a través) suministrados.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmprocessvmwith`prdm  
Utilice esta opción para controlar si las copias de seguridad de máquina virtual de VMware completa son procesadas si la máquina tiene uno o más volúmenes RDM (dispositivos de correlación RAW) proporcionados en modalidad de compatibilidad física (pRDM).
-  Sistemas operativos Windows `Vmrestore`type  
Utilice la opción `vmrestore`type con los mandatos `query VM` o `restore VM` para especificar el tipo de operación de restauración a realizar o consultar.
-  Sistemas operativos Windows  Sistemas operativos Linux `Vmskipctl`compression  
Utilice la opción `vmskipctl`compression para copias de seguridad de máquina virtual para especificar si los archivos de control (\*.ctl) se comprimen durante una copia de seguridad de máquina virtual. La opción no afecta a la compresión de los archivos de datos (\*.dat)
- `Vmskipmax`virtualdisks  
La opción `vmskipmax`virtualdisks especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDKs) que exceden el tamaño máximo de disco.
- `Vmskipmax`vmdks  
La opción `vmskipmax`vmdks especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDK) que exceden el tamaño máximo de disco.
- `Vmskip`physdisks  
Utilice la opción `vmskip`physdisks para restaurar la información de configuración para los discos físicos (discos de paso a través) que están asociados con una máquina virtual (VM) Hyper-V, si los números de unidad lógica (LUN) que están asociados con los volúmenes en los discos físicos están disponibles.
-  Sistemas operativos Windows `Vmstorage`type  
Utilice la opción `vmstorage`type con el mandato `restore VM` para especificar el tipo de dispositivo de almacenamiento desde el que se monta la instantánea con Agente de recuperación de IBM Spectrum Protect.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmtag`datamover  
Utilice la opción `vmtag`datamover para habilitar el soporte de codificación en el cliente de archivado y copia de seguridad (transportador de datos). Cuando esta opción está habilitada, el cliente gestiona copias de seguridad de máquinas virtuales en objetos de inventario de VMware de acuerdo con los códigos de protección de datos que se han establecido mediante la Plug-in de cliente de IBM Spectrum Protect vSphere del cliente web vSphere, o que se establecen con herramientas como VMware vSphere PowerCLI Versión 5.5 R2 o posterior.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmtag`defaultdatamover  
Utilice la opción `vmtag`defaultdatamover para proteger máquinas virtuales definidas en una planificación que no tengan una categoría o código Transportador de datos asignada o heredada.
-  Sistemas operativos Windows `Vmtemp`datastore  
Utilice la opción `vmtemp`datastore con el mandato `restore VM` para definir un almacén de datos temporal en el host de ESX para una operación de restauración instantánea.
- `Vmverify`ifaction  
Utilice esta opción para especificar la acción a realizar si el transportador de datos detecta problemas de integridad con los archivos CTL y bitmap más recientes para una máquina virtual.
- `Vmverify`iflatest  
Esta opción solo se aplica a operaciones de copia de seguridad de máquina virtual VMware que utilicen la modalidad de copia de seguridad incremental-constante-incremental (es decir, un mandato a `backup vm` con `-mode=IFIncremental` especificado). Si se habilita esta opción `vmverifyiflatest`, el transportador de datos ejecuta una comprobación de integridad en los archivos CTL y bitmap que se crearon en un servidor durante la última copia de seguridad, si la última copia de seguridad fue una copia de seguridad incremental-constante-incremental.
-  Sistemas operativos Linux  Sistemas operativos Windows `Vmstort`transport  
La opción `vmstort`transport especifica el orden de transportes preferido (jerarquía) que utilizar cuando se realizan copias de seguridad de o restaurar máquinas virtuales de VMware. Si no incluye un transporte determinado utilizando esta opción, se excluirá el transporte y no se utilizará para transferir los datos.
-  Sistemas operativos Windows `Vssalt`stagingdir  
La opción `vssalt`stagingdir especifica la vía de acceso totalmente calificada que contiene la caché de exclusión del sistema y datos temporales para el funcionamiento de instantáneas de VSS.



-  Sistemas operativos WindowsVssusesystemprovider  
La opción vssusesystemprovider especifica si se debe utilizar el proveedor de sistemas de Windows, o permitir a Windows decidir qué proveedor es más apropiado utilizar.
-  Sistemas operativos Linux  Sistemas operativos WindowsVmtimeout  
VMTIMEOut especifica el tiempo máximo, en segundos, que se debe esperar antes de abandonar una operación backup vm, cuando se utiliza la opción INCLUDE.VMTSMVSS para proporcionar protección de aplicaciones. Para utilizar esta opción, debe haber instalado la licencia de IBM Spectrum Protect para entornos virtuales.
- Webports  
La opción webports habilita el uso del cliente web fuera de un cortafuegos.
- Wildcardsareliteral  
La opción wildcardsareliteral especifica si los signos de interrogación (?) y los asteriscos (\*) se interpretan literalmente, cuando están incluidos en una especificación de una lista de archivos en una opción filelist.

## Absolute

---

Utilice la opción absolute con el mandato incremental para imponer una copia de seguridad de todos los archivos y directorios que coincidan con la especificación de archivo o domain, aunque los objetos no se hayan modificado desde la última copia de seguridad incremental.

Esta opción modifica el parámetro mode del grupo de copia de clase de gestión para grupos de copia de seguridad; no afecta al parámetro frequency ni a ninguno de los otros parámetros del grupo de copia de seguridad. Esta opción no modifica las sentencias exclude, de modo que los objetos que se excluyen de la copia de seguridad no son aptos para copia de seguridad, aunque se especifique la opción absolute.


Importante: Antes de utilizar la opción absolute, tenga en cuenta los siguientes efectos que puede tener esta opción sobre copias de seguridad y operaciones del servidor de IBM Spectrum Protect:

- Las copias de seguridad consumen más recursos de base de datos y almacenamiento del servidor.
- Las copias de seguridad consumen más ancho de banda de red.
- Las operaciones del servidor, como por ejemplo caducidad del inventario, copia de seguridad de agrupación de almacenamiento, migración de agrupación de almacenamiento, reclamación y réplica de nodo, requieren más tiempo en completarse. La optimización de datos puede ayudar a mitigar algunos de estos efectos, pero no evita el proceso necesario para reconstituir los datos optimizados a su formato original cuando la agrupación de almacenamiento se migra o se copia en almacenamiento no optimizado.

Esta opción sólo es válida como un parámetro de línea de mandatos para el mandato incremental cuando se realizan las siguientes operaciones:

- Copias de seguridad incrementales progresivas completas o parciales de sistemas de archivos o unidades de disco.
- Copias de seguridad de diferencial de instantánea cuando también se especifica createnewbase=yes.

Para imponer una copia de seguridad completa de un sistema de archivos que utiliza copia de seguridad basada en registro por diario, especifique las opciones nojournal y absolute en el mandato incremental.

 Sistemas operativos Windows Durante una copia de seguridad incremental de dominio, donde se especifica systemstate como parte del dominio, la opción absolute no impone una copia de seguridad completa de objetos de estado del sistema. Para imponer una copia de seguridad incremental de dominio para crear una copia de seguridad completa de objetos de estado del sistema, debe añadir systemstatebackupmethod full al archivo de opciones del cliente.

Para utilizar la opción absolute en copias de seguridad incrementales planificadas, el administrador del servidor de IBM Spectrum Protect debe crear una planificación de copia de seguridad separada que incluya la opción absolute en el parámetro options de la planificación.

## Clientes soportados

---

Esta opción es válida para todos los clientes como parámetro de línea de mandatos para el mandato incremental. Esta opción no se pueden añadir a un conjunto de opciones de cliente en el servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-ABSolute-----><
```

## Parámetros





---


No hay parámetros para esta opción.


## Ejemplos

---

Línea de mandatos:

     
dsmc incr -absolute "/Users/sparky/source/\*.c"

  
dsmc incr -absolute c:\foo\\*.c



## Adlocation

---

Puede utilizar la opción adlocation con los mandatos query adobjects o restore adobjects para indicar si los objetos de Active Directory van a consultarse o restaurarse desde el contenedor de objetos suprimidos de Active Directory local o desde la copia de seguridad de estado del sistema del servidor de IBM Spectrum Protect.

## Clientes soportados

---

Esta opción es válida para los clientes de Windows Server soportados. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
..-local--.  
>>-ADLOCation--+-+-----+----->>  
                '-server-'
```

## Parámetros

---

server

Indica si los objetos de Active Directory se consultarán o restaurarán desde una copia de seguridad de estado del sistema en el servidor de IBM Spectrum Protect. Válido para todos los clientes soportados del servidor Windows.

local

Especifica que los objetos de Active Directory se consultarán o restaurarán desde el contenedor de objetos suprimidos de Active Directory local. Éste es el valor predeterminado.

## Ejemplo

---

Línea de mandatos:

```
query adobjects "cn=Jim Smith" -adlocation=server
```

## Afmskipuncachedfiles

---

La opción afmskipuncachedfiles especifica si los archivos no almacenados en memoria caché y sucios de conjuntos de archivos de Active File Management de General Parallel File System (GPFS) se procesan para operaciones de copia de seguridad, archivado y migración.

Los estados de archivos de GPFS Active File Management, *no almacenado en memoria caché* y *sucio* se explican en Información sobre el producto GPFS.

La ejecución de HSM en sistemas de archivos GPFS que utilizan conjuntos de archivos de Active File Management se explica en Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect .

Si realiza una copia de seguridad, archiva o migra archivos de un sistema de archivos que contiene conjuntos de archivos de Active File Management, establezca afmskipuncachedfiles=yes.

Restricción: Si Active File Management se ejecuta en modalidad de actualización local (LU), la opción afmskipuncachedfiles del archivo de caché se debe establecer en No.

## Cientes soportados

---

Esta opción es válida para clientes de archivado y copia de seguridad que se ejecutan en sistemas AIX y Linux.

## Archivo de opciones

---

Ponga esta opción en el archivo dsm.sys antes de cualquier stanza de servidor.

## Sintaxis

---

```
>>-AFMSKIPUNCACHEDFILES--+-NO-- .
                                     +-----+-----><
                                     '-YES-'
```

## Parámetros

---

NO

El estado de archivo de Active File Management se ignora durante las operaciones de copia de seguridad, archivado y migración. Las operaciones de migración en archivos no almacenados en memoria caché o sucios fallan y producen el mensaje de error ANS9525E. Las operaciones de copia de seguridad y archivado en archivos no almacenados en memoria caché necesitan operaciones de captación de Active File Management. Las operaciones de captación pueden producir tráfico de red significativo entre el inicio y la memoria caché de Active File Management. Este parámetro es el predeterminado.

YES

Los archivos no almacenados en memoria caché o sucios en conjuntos de archivos de Active File Management se saltan durante el proceso de copia de seguridad, archivado y migración.






## Archmc

---

Utilice la opción archmc con el mandato archive para especificar la clase de gestión disponible para el dominio de políticas a la que desea vincular los directorios o las copias archivadas.





Cuando realice una copia archivada, podrá modificar temporalmente la clase de gestión asignada mediante la utilización de la opción archmc en el mandato archive o bien mediante la utilización del cliente web. La modificación temporal de la clase de gestión que se realiza mediante el cliente web equivale a la utilización de la opción archmc en el mandato archive.


Si no utiliza la opción archmc, el servidor vincula los directorios archivados a la clase de gestión. Si la clase de gestión predeterminada no tiene grupo de copias archivadas, el servidor vincula los directorios archivados a la clase de gestión con el período de retención más reducido.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Cientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción es válida para todos los clientes UNIX y Linux. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-ARCHMc = -clasegestión-----><
```

## Parámetros

---


clasegestión

Especifica una clase de gestión disponible en el conjunto de políticas activo del dominio de políticas. Esta clase de gestión modifica temporalmente la clase de gestión predeterminada y cualquier sentencia incluye que se haya especificado para los archivos y directorios cuya copia archivada está realizando.





## Ejemplos

---


Línea de mandatos:

 sistemas operativos Mac OS X




```
dsmc archive -archmc=ret2yrs /Users/van/Documents/budget.jan
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc archive -archmc=ret2yrs /home/plan/proj1/budget.jan
```

 Sistemas operativos Windows

```
dsmc archive -archmc=ret2yrs c:\plan\proj1\budget.jan\*
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Archsymlinkasfile

---

La opción archsymlinkasfile especifica si el cliente de copia de seguridad y archivado sigue un vínculo simbólico y archiva el directorio o el archivo al que hace referencia, o bien si archiva únicamente el vínculo simbólico. Utilice esta opción con el mandato archive.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX, a excepción de Mac OS X. El servidor también puede definir esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (dsm.opt).

## Sintaxis

---

```
>>-ARCHSYMLinkasfile-+-.-Yes-.-----+<<
                    |'-No--'|
```

## Parámetros

---

Yes

Especifica que el cliente debe seguir un vínculo simbólico y archiva el archivo o directorio asociado. Éste es el valor predeterminado.

No

Especifica que el cliente archiva el vínculo simbólico y no el archivo o directorio asociado.

## Ejemplos





---

Archivo de opciones:

```
archsymlinkasfile no
```

Línea de mandatos:

```
-archsyml=no
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Asnodename

---

Utilice la opción asnodename para permitir a nodos agente realizar copias de seguridad o restauración de datos en nombre de otro nodo (el nodo de destino). Esto permite realizar operaciones simultáneas desde varios nodos para almacenar datos en el mismo nodo de destino y espacio de archivos en paralelo.

El nodo cliente debe tener garantizado el acceso al nodo de destino a través del mandato grant proxynode del cliente administrativo del servidor de IBM Spectrum Protect, y debe ser un usuario root para utilizar la opción asnodename.

Cuando el administrador de IBM Spectrum Protect ha otorgado autorización a un proxy de nodo y se utiliza la opción asnodename para convertirse en ese nodo, pueden consultarse y restaurarse todos los archivos como si se dispusiera de autorización de usuario root.

Un nodo de agente es un nodo cliente al que se ha otorgado autorización para realizar operaciones de cliente en nombre de un nodo de destino.

Un nodo de destino es un nodo cliente que otorga autorización a uno o varios nodos de agente para realizar operaciones en nombre de éste.

Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, maxnummp y deduplication) y las planificaciones que se definen en el servidor. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.

Por ejemplo, puede utilizar el siguiente mandato para realizar la copia de seguridad de los datos compartidos para el espacio de archivos que se ha almacenado en el nombre de nodo MyCluster:

```
/cluster1/mydata  
dsmc incremental /Users -asnodename=MyCluster
```

También puede utilizar la opción asnodename para restaurar los datos bajo otro nombre de nodo en el servidor. Sólo puede restaurar los datos que son de su propiedad.

La opción asnodename difiere de la opción nodename en lo siguiente:

- Cuando utiliza la opción nodename, debe escribir la contraseña del nombre de nodo que especifica.
- Cuando utiliza la opción asnodename, debe especificar la contraseña del nodo de agente cliente para poder acceder a los datos que se han almacenado para el nodo de destino cliente.

**Restricciones:** no puede utilizar la opción asnodename con -fromnode ni puede realizar una copia de seguridad de NAS mediante la utilización de asnodename. La opción asnodename puede utilizarse para sistemas de clústeres, aunque no se admite ningún software de clúster específico.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux.

## Archivo de opciones

---

Incluya esta opción en el archivo dsm.sys dentro de una stanza de servidor. Puede establecer esta opción en la ficha **General** del editor de preferencias.

## Sintaxis

---

```
>>-ASNODENAME- --targetnode-----<<
```

## Parámetros

---

targetnode

Especifica el nombre de nodo en el servidor de IBM Spectrum Protect bajo el que se desea realizar la copia de seguridad o restaurar los datos.

## Ejemplos

---





Archivo de opciones:

```
asnodename mycluster
```

Línea de mandatos:

```
-asnodename=mycluster
```

Esta opción no es válida en modalidad interactiva, pero puede definirse en la parte de opciones de una definición de planificación.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Valores de sesión y planificaciones de una operación de proxy  
Una operación de proxy se produce cuando un nodo de agente utiliza la opción asnodename nombre\_nodo\_destino para realizar operaciones en nombre del nodo de destino especificado.

 Sistemas operativos Windows

## Asnodename

---

Utilice la opción `asnodename` para permitir que un nodo agente realiza una copia de seguridad, archivado, restauración, recuperación y consulta de datos en nombre de un nodo de destino.

Un *nodo de agente* es un nodo cliente al que el administrador de IBM Spectrum Protect otorga autorización para realizar operaciones de cliente en nombre de un *nodo de destino*. El nodo de destino es el nodo de cliente para el cual el nodo de agente realiza las acciones. El administrador utiliza el mandato `grant proxynode` en el servidor de IBM Spectrum Protect para otorgar esta autorización.

Los nodos de agente se pueden utilizar para distribuir la carga de trabajo de realizar la copia de seguridad de los volúmenes de un sistema, en diversos sistemas cliente. Cada sistema que está involucrado en la copia de seguridad utiliza su propio nombre de nodo de agente, pero los datos de copia de seguridad se almacenan en un espacio de archivos común que es propiedad del nodo de destino.

Por ejemplo, supongamos que tiene la intención de realizar la copia de seguridad de cuatro volúmenes que pertenecen a un nodo que se denomina SCORPIO, pero la operación de copia de seguridad tarda demasiado en ejecutarse. Puede distribuir parte de la carga de trabajo a otras tres máquinas: TAURUS, ARIES, y LEO. SCORPIO y las otras tres máquinas cada una realiza la copia de seguridad de uno de los volúmenes de SCORPIO. Cada nodo que esté involucrado en la copia de seguridad se conecta al servidor por medio de su propio nombre de nodo de agente, y cada nodo especifica un valor único para la opción `asnodename`. No utilice un nombre de sistema o nombre de clúster para el valor `asnodename`. La tabla siguiente muestra un ejemplo de configuración.

Tabla 1. Configurar el valor de la opción `asnodename` para distribuir copias de seguridad.

Host servidor	NODENAME valor de opción	ASNODENAME valor de opción	Volumen con copia de seguridad	Nombre de espacio de archivo de servidor
SCORPIO	SCORPIO	TARGET_SCORPIO	\\scorpio\r\$	\\target_scorpio\r\$
TAURUS	TAURUS	TARGET_SCORPIO	\\scorpio\s\$	\\target_scorpio\s\$
ARIES	ARIES	TARGET_SCORPIO	\\scorpio\t\$	\\target_scorpio\t\$
LEO	LEO	TARGET_SCORPIO	\\scorpio\u\$	\\target_scorpio\u\$

Para crear las relaciones entre el nodo de destino y los nodos proxy, el administrador del servidor IBM Spectrum Protect debe realizar las acciones siguientes:

1. Registrar los nodos SCORPIO, TAURUS, ARIES, LEO y TARGET\_SCORPIO.
2. Otorgar a los nodos SCORPIO, TAURUS, ARIES y LEO la autoridad de proxy para el nodo TARGET\_SCORPIO

Cuando realiza una copia de seguridad o archivado de datos sin la opción `asnodename`, los datos de la copia de seguridad realizada se almacenan en un espacio de archivos en el servidor que coincide con el nombre de UNC de la unidad en la que existen los datos originales.

Cuando se utiliza la opción `asnodename` para realizar una copia de seguridad de los datos en nombre de un nodo de destino, los datos se almacenan en un espacio de archivos propiedad del nodo de destino. Sin embargo, en lugar de utilizar el nombre de host en el nombre de espacio de archivos, el nombre del nodo de destino se utiliza en el nombre de espacio de archivos. Por ejemplo, si TAURUS realiza la copia de seguridad de los datos en la unidad S de SCORPIO y configura el valor de opción `asnodename` en `asnodename=target_scorpio`, los datos de copia de seguridad se almacenan en un espacio de archivos denominado `\\target_scorpio\s$`. El espacio de archivos será propiedad del nodo TARGET\_SCORPIO.

Al restaurar o recuperar datos, el comportamiento predeterminado es restaurar o recuperar los datos en una ubicación que coincida con el nombre de espacio de archivos.

Continuando con el ejemplo anterior, si el nodo SCORPIO utiliza `asnodename=target_scorpio` para restaurar datos de `\\target_scorpio\s$`, el cliente intentará restaurar los datos a la unidad S en un sistema denominado TARGET\_SCORPIO. Esta operación no genera los resultados esperados porque en esta configuración de muestra, no hay ningún sistema que se denomine TARGET\_SCORPIO.

En el ejemplo siguiente, se especifica el mandato `restore` en el nodo SCORPIO. El mandato restaura todos los archivos y subdirectorios del directorio `Users\andy\education` del espacio de archivos `\\target_scorpio\s$` en la unidad S en el sistema denominado SCORPIO:

```
dsmc restore \\target_scorpio\s$\users\andy\education\* s:\
-subdir=yes -asnodename=target_scorpio
```

Se aplican las siguientes consideraciones cuando utiliza un nodo proxy para realizar una copia de seguridad o restaurar datos en otros nodos:

- Una operación de proxy utiliza los valores del nodo de destino (por ejemplo, `maxnummp` y `deduplication`) y las planificaciones que se definen en el servidor de IBM Spectrum Protect. Los valores del nodo de servidor de IBM Spectrum Protect y las planificaciones del nodo de agente se ignoran.
- No puede utilizar `asnodename` con el mandato `backup nas`.
- No puede utilizar `asnodename` con la opción `fromnode`.

- Si utiliza asnodename para realizar copias de seguridad y restaurar volúmenes que se encuentran en una configuración de clúster, no utilice clusternode yes.
- No puede utilizar asnodename para realizar la copia de seguridad o restaurar el estado del sistema.
- Si un nodo de agente restaura los datos de un conjunto de copias de seguridad, no se restaura el objeto de estado del sistema en el conjunto de copias de seguridad.
- Puede utilizar asnodename con el mandato backup image, pero debe especificar el volumen mediante un nombre UNC. No puede utilizar la letra de unidad.
- Si utiliza los mismos valores asnodename para realizar la copia de seguridad de archivos de distintas máquinas, necesitará realizar un seguimiento de qué archivos o volúmenes tienen una copia de seguridad de cada sistema para que pueda restaurarlos en la ubicación correcta.
- Todos los nodos de agente de un entorno de varios nodos deben tener el mismo tipo de plataforma.
- No utilice nodos de destino como nodos tradicionales, especialmente si cifra los archivos antes de hacer una copia de seguridad en el servidor.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo dsm.opt. Puede establecer esta opción en la ficha General del editor de preferencias.

## Sintaxis

---

```
>>-ASNODENAME- --targetnode-----<<
```

## Parámetros

---

targetnode

Especifica el nombre de nodo en el servidor de IBM Spectrum Protect bajo el que se desea realizar la copia de seguridad o restaurar los datos.

## Ejemplos

---

Archivo de opciones:


```
asnodename target_scorpio
```

Línea de mandatos:

Este mandato realiza una copia de seguridad de toda la unidad F: en un espacio de archivos del servidor denominado \\target\_scorpio\f\$.

```
dsmc incremental f: -asnodename=target_scorpio
```

Esta opción no es válida en modalidad interactiva, pero puede definirse en la parte de opciones de una definición de planificación.

-  Sistemas operativos Windows Valores de sesión y planificaciones de una operación de proxy  
Una operación de proxy se produce cuando un nodo de agente utiliza la opción asnodename nombre\_nodo\_destino para realizar operaciones en nombre del nodo de destino especificado.

 Sistemas operativos Windows

## Asrmode

---

Utilice la opción asrmode con los mandatos restore y restore systemstate para especificar si debe realizarse una operación de restauración en la modalidad de recuperación ASR del sistema.

Esta opción se utiliza en el contexto de los mandatos restore que se generan en el archivo asr.sif solo por medio de la ejecución del mandato backup asr.

## Clientes soportados

---

Esta opción es válida para clientes Windows soportados que se están ejecutando en un Windows Preinstallation Environment; las arquitecturas de arranque BIOS y UEFI reciben soporte.

```
>>-ASRMODE = -+-----+-----><
              +-No--+
              '-Yes-'
```

## Parámetros

---

No

Especifica que el cliente no realiza la operación de restauración en modalidad de recuperación ASR del sistema.

Yes

Especifica que el cliente realiza la operación de restauración en modalidad de recuperación ASR. Es el valor predeterminado para clientes Windows durante una recuperación de ASR. Estos clientes se ejecutan en Windows Preinstallation Environment (WinPE) durante la recuperación ASR.

## Ejemplos

---

Línea de mandatos:

```
restore systemstate -asrmode=yes
restore systemstate -asrmode=yes -inactive -pick
```

Esta opción es válida para una sesión interactiva, pero no se puede cambiar entrando la opción mientras se ejecuta una sesión interactiva.

## Auditlogging

---





Use la opción `auditlogging` para generar una anotación de auditoría que contenga una entrada para cada archivo que se procese durante una operación incremental, de selección, de archivado, de restauración o recuperación.

La anotación de auditoría se puede configurar para que capture un nivel básico de información o un nivel de información más inclusivo (completo).

El nivel básico de la función de anotación de auditoría captura la información que se encuentra en la anotación de planificación y registra la información de que se ha hecho una copia de seguridad de un archivo, se ha archivado, actualizado, restaurado, recuperado, caducado, eliminado, omitido o ha fallado durante una operación de copia de seguridad incremental, de copia de seguridad selectiva, de archivado, de restauración o de recuperación. Asimismo, el nivel básico de la anotación de auditoría captura el mandato de entrada de los mandatos que se ejecutan mediante la línea de mandatos de copia de seguridad/archivado o los clientes del planificador.

El nivel completo de anotación de auditoría graba una acción de cada archivo que procesa el cliente de copia de seguridad/archivado. Además de todos los sucesos grabados mediante el nivel básico de la anotación de auditoría, el nivel completo de anotación de auditoría graba información de un archivo que se ha excluido o no se ha enviado durante una operación de copia de seguridad incremental progresiva porque el archivo no ha cambiado.

A continuación puede ver un ejemplo de los mensajes que se emiten cuando la anotación de auditoría se configura para que capture el nivel básico de información:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X





```
04/21/07 15:25:05 ANS1650I Command:
  sel /home/spike/test/*
04/21/07 15:25:05 ANS1651I Backed Up:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1652I Archived:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1653I Updated:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1654E Failed:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1655I Restored:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1656I Retrieved:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1657I Expired:
  /home/spike/test/file.txt
04/21/07 15:25:05 ANS1658I Deleted:
  /home/spike/test/file.txt
```







04/21/07 15:25:05 ANS1659I Skipped:  
/home/spike/test/file.txt


#### Sistemas operativos Windows

04/21/07 15:25:05 ANS1650I Command:  
sel c:\test\file.txt  
04/21/07 15:25:05 ANS1651I Backed Up:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1652I Archived:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1653I Updated:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1654E Failed:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1655I Restored:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1656I Retrieved:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1657I Expired:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1658I Deleted:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1659I Skipped:  
\\spike\c\$\test\file.txt

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Los siguientes mensajes se pueden emitir cuando el registro de auditoría se ha configurado para capturar el nivel completo de información (además de todos los mensajes emitidos para el nivel básico del registro de auditoría):

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

04/21/07 15:25:05 ANS1660I Excluded:  
/home/spike/test/file.txt  
04/21/07 15:25:05 ANS1661I Unchanged:  
/home/spike/test/file.txt


 Sistemas operativos Windows A continuación, puede ver un ejemplo de los mensajes que se emiten cuando la anotación de auditoría se configura para que capture el nivel completo de información (además de todos los mensajes emitidos para el nivel básico de la anotación de auditoría):


#### Sistemas operativos Windows

04/21/07 15:25:05 ANS1660I Excluded:  
\\spike\c\$\test\file.txt  
04/21/07 15:25:05 ANS1661I Unchanged:  
\\spike\c\$\test\file.txt


La anotación de auditoría no es un sustituto ni un reemplazo de la anotación de errores estándar (`dsmererror.log`) ni de la anotación de planificación (`dsmsched.log`). Si se produce un error que impide que un archivo pueda procesarse, en el registro de auditoría aparecerá un mensaje que indicará que se ha producido un error, aunque el mensaje no indicará la naturaleza del error. Para diagnósticos de problemas se debe usar todavía la anotación de errores estándar.




Las entradas de la anotación de auditoría sólo contienen una indicación de la hora y un nombre de objeto. No hay información para distinguir entre archivos y directorios ni tampoco ninguna información sobre el tamaño de un objeto.


 sistemas operativos Mac OS X El cliente de archivado y copia de seguridad de Mac OS X creará el registro de auditoría en formato de archivo Unicode (UTF-16).

 Sistemas operativos Windows Cuando se utilice el cliente de copia de seguridad/archivado de Windows, todos los nombres de objetos se grabarán en formato UNC. El cliente de copia de seguridad/archivado de Windows creará el registro de auditoría en formato de archivo Unicode.

De forma predeterminada, el nombre de la anotación de auditoría es `dsmaudit.log` y se incluye en el mismo directorio que la anotación de error, `dsmererror.log`. El nombre y la ubicación de la anotación de auditoría se pueden configurar mediante la opción `auditlogname`. No existe ningún parámetro que permita controlar el tamaño de la anotación de auditoría ni realizar la operación de poda de ésta. La opción `auditlogname` no se puede definir como opción en un conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 sistemas operativos Mac OS X El mandato `auditlogging` se admite con mandatos de copia de seguridad que interactúan con objetos de nivel de archivo como `backup groups`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris El mandato `auditlogging` no se admite con los mandatos de copia de seguridad que interactúan con objetos de nivel de imagen como `backup image` o `restore image`. El mandato `auditlogging` se admite con mandatos de copia de seguridad que interactúan con objetos de nivel de archivo como `backup groups`.

 Sistemas operativos Windows El mandato `auditlogging` no se admite con los mandatos de copia de seguridad que interactúan con objetos de nivel de imagen como `backup image` o `restore image`. El mandato `auditlogging` se admite con mandatos de copia de seguridad que interactúan con objetos de nivel de archivo como `backup groups` y `backup systemstate`.

Si ha activado el registro de auditoría para una operación y se produce una anomalía al intentar grabar en el registro de auditoría (por ejemplo, el disco en el que reside la anotación de auditoría no dispone de espacio suficiente), el registro de auditoría se desactivará para el resto de la operación y el código de retorno de la operación se establecerá en 12, con independencia del resultado de la operación.


## Clientes soportados





---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo `dsm.opt`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

## Sintaxis

---

```

      .-off---.
>>-AUDITLOGGING--+-+-----+-----><
                  +-basic-+
                  '-full--'
```

## Parámetros

---

- `off`  
Especifica que el recurso de anotación de auditoría no está ocupado. Éste es el valor predeterminado.
- `basic`  
Especifica que la anotación de auditoría captura un nivel básico de información.
- `full`  
Especifica que la anotación de auditoría captura un nivel más amplio de información.

## Ejemplos

---

Ejecutar una copia de seguridad incremental con la anotación de auditoría activada.

Línea de mandatos:

```
dsmc i -auditlogging=basic
```

Realizar la copia de seguridad de una lista de archivos mediante la utilización del nivel máximo de auditoría, que permite que otra aplicación, como un script Perl, verifique los resultados.

 Sistemas operativos Windows

```
dsmc i -filelist=file.lst -auditlogging=full
      -auditlogname="c:\program files\tivoli\tsm\baclient\
      temp_audit001.log"
```

## Auditlogname

---

La opción `auditlogname` especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de auditoría. Esta opción se aplica cuando se habilita la anotación de auditoría.





## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Sistemas operativos Windows Coloque esta opción en el archivo dsm.opt.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

## Sintaxis


```
>>-AUDITLOGName--filespec-----<<
```

## Parámetros

### filespec





Especifica la vía de acceso y el nombre de archivo donde quiere que el cliente de copia de seguridad y archivado almacene la información de anotación de auditoría.





Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio actual. El valor predeterminado es el directorio de instalación con el nombre de archivo dsmaudit.log. El archivo dsmaudit.log no puede ser un enlace simbólico.

 Sistemas operativos Windows En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo, la vía de acceso contiene la letra de la unidad D\$: \\computer7\D\$\logs\tsmaudit.log.

## Ejemplos

Ejecutar una copia de seguridad incremental con la anotación de auditoría activada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Salida de ejemplo

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X A continuación puede ver una muestra de ejecución y un archivo de salida:

```
> dsmc inc /SMSVT/mfs1 -auditlogging=full
-auditlogname=/home/cliv3/audit.log
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016.
Reservados todos los derechos.

Nombre de nodo: NAXOS_CLUSTER
Sesión establecida con servidor
ODINHSMSESV: AIX-RS/6000
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
Último acceso: 11/15/2016 12:01:57

Copia de seguridad incremental del volumen '/SMSVT/mfs1'
Directory--> 4,096 /SMSVT
 /mfs1/ [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test0 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test1 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test2 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test3 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test4 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test5 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test6 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test7 [Sent]
Normal File--> 32,768 /SMSVT
 /mfs1/test8 [Sent]
```


```
Normal File-->          32,768 /SMSVT
/mfsl/test9 [Sent]
La copia de seguridad incremental de '/SMSVT/mfsl'
se ha realizado correctamente
```

```
Número total de objetos inspeccionados:   11
Número total de objetos de copia de seguridad: 11
Número total de objetos actualizados:     0
Número total de objetos revinculados:     0
Número total de objetos suprimidos:       0
Número total de objetos caducados:        0
Número total de objetos con errores:      0
Número total de bytes transferidos:       320,31 KB
Tiempo de transferencia de datos:         0,01 s
Velocidad de transferencia de datos de red: 17.141,84 KB/s
Velocidad de transferencia de datos compuesta: 297,43 KB/s
Objetos comprimidos al:                   0%
Tiempo transcurrido en el proceso: 00:00:01
```

A continuación puede ver el contenido de la anotación de auditoría:


```
07/03/07 12:05:14 ANS1650I Command:
inc /SMSVT/mfsl
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test0
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test1
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test2
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test3
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test4
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test5
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test6
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test7
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test8
07/03/07 12:05:15 ANS1651I Backed Up:
/SMSVT/mfsl/test9
```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows Almacenar la anotación de auditoría en una vía de acceso distinta de la vía de acceso predeterminada.

```
auditlogname c:\mypath\myaudit.log
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Realizar la copia de seguridad de una lista de archivos mediante la utilización del nivel máximo de auditoría, que permitía que otra aplicación, como un script Perl, verificara los resultados:

```
dsmc i -filelist=file.lst -auditlogging=full
-auditlogname="c:\program files\tivoli\tsm\baclient\
temp_audit001.log"
```

 Sistemas operativos Windows Salida de ejemplo

 Sistemas operativos Windows A continuación puede ver una muestra de ejecución y un archivo de salida:

```
C:\Archivos de programa\Tivoli\TSM\baclient>dsmc i
c:\test\* -sub=yes -auditlogging=full
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 11/16/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016.
Reservados todos los derechos.
```

```
Nombre de nodo: PATMOS
Sesión establecida con el servidor PATMOS_5331: Windows
Versión de servidor 8, release 1, nivel 0.0
```

Fecha/hora del cliente: 11/16/2016 12:05:35  
Último acceso: 11/15/2016 15:52:06

```
Copia de seguridad incremental del volumen 'c:\test\*'
Normal File-->      1,048,576 \\patmos\c$\test
  \dir1\file1 [Sent]
Normal File-->      1,048,576 \\patmos\c$\test
  \dir1\file2 [Sent]
Normal File-->          1,024 \\patmos\c$\test
  \dir1\file3 [Sent]
Normal File-->      1,048,576 \\patmos\c$\test
  \dir2\file1 [Sent]
Normal File-->      1,048,576 \\patmos\c$\test
  \dir2\file2 [Sent]
Normal File-->          1,024 \\patmos\c$\test
  \dir2\file3 [Sent]
Successful incremental backup of '\\patmos\c$\test\*'
```

```
Número total de objetos inspeccionados: 12
Número total de objetos de copia de seguridad: 6
Número total de objetos actualizados: 0
Número total de objetos revinculados: 0
Número total de objetos suprimidos: 0
Número total de objetos caducados: 0
Número total de objetos con errores: 0
Número total de bytes transferidos: 400,85 KB
Tiempo de transferencia de datos: 0,00 s
Velocidad de transferencia de datos de red: 0,00 KB/s
Velocidad de transferencia de datos compuesta: 382,85 KB/seg
Objetos comprimidos por: 91%
Tiempo transcurrido en el proceso: 00:00:01
El código de retorno de ANS1900I es 0.
El código de retorno más alto de ANS1901I fue 0.
```

A continuación puede ver el contenido de la anotación de auditoría:

```
04/21/2007
15:52:25 ANS1650I Command:
  i c:\test\*
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test\dir1
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test\dir2
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test\file1
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test\file2
04/21/2007 15:52:26 ANS1661I Unchanged:
  \\patmos\c$\test\file3
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir1\file1
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir1\file2
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir1\file3
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir2\file1
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir2\file2
04/21/2007 15:52:26 ANS1651I Backed Up:
  \\patmos\c$\test\dir2\file3
```





## Autodeploy

---

Utilice la opción autodeploy para habilitar o inhabilitar un despliegue automático del cliente si es necesario un reinicio.

## Clientes soportados


---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Esta opción es válida para clientes AIX, Linux, Mac y Solaris.

 Sistemas operativos Windows Esta opción es válida para los clientes Windows.


## Archivo de opciones

También puede establecer esta opción incluyéndola en el archivo de opciones del cliente. También puede establecer la interfaz gráfica de usuario de Java pulsando Editar > Cliente y seleccionando la opción apropiado en la ficha General.

 Sistemas operativos Windows

## Sintaxis

```
. -Yes----- .  
>>-AUTODEPLOY--+-----+-----><  
+ -No-----+  
' -NOReboot-'
```

 Sistemas operativos Windows

## Parámetros

Yes

Especifica que el cliente se despliega automáticamente desde el servidor. Yes es el valor predeterminado.  
Importante:

- Cuando se establece autodeploy en yes, si se necesita un reinicio de la estación de trabajo del cliente para completar el despliegue, no puede inhabilitar el reinicio. Se reiniciará la estación de trabajo del cliente. Si es importante que la estación de trabajo no se reinicie automáticamente, establezca autodeploy en noreboot. El despliegue se cancelará si es necesario el reinicio. El cliente actual no se ve afectado.
- Si es necesario reiniciar, el gestor de despliegue comienza el reinicio del sistema cliente y sale. Sin embargo, es posible cancelar o interrumpir el reinicio. Como el gestor de despliegue ya ha terminado, no se envía ningún mensaje al servidor para indicar el error de reinicio. El resultado del despliegue sigue siendo correcto. Debe reiniciar el sistema de manera que el despliegue del nuevo cliente se complete.

No





Especifica que el cliente no se despliega automáticamente desde el servidor.

NOReboot

Especifica que el gestor de despliegue nunca reinicie de forma automática el sistema cliente, aunque sea necesario un reinicio. Si es necesario un reinicio, permitir el despliegue automático en muchas máquinas con el parámetro NOReboot puede hacer que solo se realice una actualización parcial de, potencialmente, muchos clientes.





Para solucionar este problema, el gestor de despliegue intenta detectar si se necesita reiniciar. Si es necesario reiniciar, el gestor de despliegue cancelará el despliegue antes de instalar el cliente nuevo. Esto garantiza que el sistema cliente siga teniendo un cliente de archivado y copia de seguridad activo y se pueda volver a programar el despliegue del cliente nuevo.

Hay casos excepcionales en los que el gestor de despliegue no puede detectar el reinicio; por ejemplo, si los procesos de cliente se inician desde un script. En estos casos, continuará la instalación del cliente nuevo, pero será necesario reiniciar de forma manual el sistema cliente.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Sintaxis

```
. -Yes- .  
>>-AUTODEPLOY--+-----+-----><  
' -No--'
```

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Parámetros






Yes

Especifica que el cliente se despliega automáticamente desde el servidor. Yes es el valor predeterminado.

No

Especifica que el cliente no se despliega automáticamente desde el servidor.

## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows






Archivo de opciones:  
autodeploy no

Línea de mandatos:  
  
No se aplica.

 Sistemas operativos Windows

Archivo de opciones:  
autodeploy noreboot

Línea de mandatos:  
  
No se aplica.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows


Importante: Utilice la opción `schedmode prompted` junto con la opción `autodeploy` para habilitar el planificador a fin de procesar la planificación del despliegue del cliente de forma inmediata.

### Conceptos relacionados:


Despliegue automático del cliente de copia de seguridad y archivado


## Autofsrename


La opción `autofsrename` cambia el nombre de un espacio de archivos existente que no está activado para Unicode en el servidor de IBM Spectrum Protect para que pueda crearse un espacio de archivos activado para Unicode con el nombre original para la operación actual.


 sistemas operativos Mac OS X Cuando especifica `autofsrename yes` en el archivo de opciones del cliente y el valor del servidor `autofsrename` se ha establecido en `client`, el servidor de IBM Spectrum Protect genera un nombre exclusivo añadiendo `_OLD` al nombre del espacio de archivos que especifica en la operación actual. Por ejemplo, el servidor cambiará el nombre del espacio de archivos `Jaguar` por `Jaguar_OLD`. Si el nuevo nombre del espacio de archivos es demasiado largo, el sufijo sustituirá los últimos caracteres del nombre del espacio de archivos. Por ejemplo, el nombre del espacio de archivos `nombrelargosistemaarchivos` se cambiará por:

```
nombrelargosistemaarchivos_OLD
```


 sistemas operativos Mac OS X Si el nuevo nombre del espacio de archivos ya existe en el servidor, el servidor cambiará el nuevo nombre del espacio de archivos por `Jaguar_OLDX`, donde la `x` es un número exclusivo.


 sistemas operativos Mac OS X El servidor creará nuevos espacios de archivos activados para Unicode que sólo contengan los datos que se especifican en la operación actual. Por ejemplo, imaginemos que `Jaguar` es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos `.log` en el directorio `/Users/user5/Documents`. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por `Jaguar_OLD`. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado `Jaguar`. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `/Users/user5/logs` y los archivos `*.log` especificados en la operación. El servidor almacena todas las posteriores copias de seguridad selectivas incrementales completas y parciales y archiva los datos en los nuevos espacios de archivos activados para Unicode.

 sistemas operativos Mac OS X Por ejemplo, imaginemos que `Jaguar` es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos `.log` en el directorio `/Users/user5/Documents`. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por `Jaguar_OLD`. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado `Jaguar`. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `/Users/user5/logs` y los archivos `*.log` especificados en la operación. Los siguientes datos incrementales completos y parciales, de copia de seguridad selectiva y de archivado se almacenan en los nuevos espacios de archivos activados para Unicode.


 Sistemas operativos Windows Cuando especifica `autofsrename yes` en el archivo de opciones del cliente y el valor del servidor `autofsrename` se ha establecido en `client`, el servidor de IBM Spectrum Protect genera un nombre exclusivo añadiendo `_OLD` al nombre del espacio de archivos que especifica en la operación actual. Por ejemplo, el servidor cambiará el nombre del espacio de archivos `\\nombre-nodo\h$` por `\\nombre-nodo\h$_OLD`. Si el nombre de espacio de archivos nuevo es demasiado largo, el sufijo sustituye los últimos caracteres del nombre del espacio de archivos, como se muestra a continuación:

```
\\nombre-de-nodo_OLD
```

 Sistemas operativos Windows Si el nuevo nombre del espacio de archivos ya existe en el servidor, el servidor cambiará el nuevo nombre del espacio de archivos por `\\nombre-nodo_OLDx`, donde la `x` es un número exclusivo.

 Sistemas operativos Windows El servidor creará nuevos espacios de archivos activados para Unicode que sólo contengan los datos que se especifican en la operación actual. Por ejemplo, para realizar el archivado de archivos desde el disco `H:` denominado `\\nodo\h$`, emita el mandato de archivado siguiente:

```
arc h:\logs\*.log
```


 Sistemas operativos Windows Antes de que tenga lugar el archivado, el servidor cambiará el nombre del espacio de archivos por `\\nodo\h$_OLD`. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado `\\nodo\h$`. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio `\logs` y los archivos `*.log` especificados en la operación. Los siguientes datos incrementales completos y parciales, de copia de seguridad selectiva y de archivado se almacenan en los nuevos espacios de archivos activados para Unicode.


Los espacios de archivos red denominados permanecen en el servidor como espacios de archivos estabilizados. *Estos espacios de archivos contienen todos los datos originales, que pueden restaurarse siempre que permanezcan en el servidor.*

Nota: Cuando, durante la conversión de Unicode, se cambia el nombre de un espacio de archivos existente, las reglas de acceso que se han definido para el espacio de archivos siguen aplicándose al espacio de archivos original. Deberán definirse nuevas reglas de acceso para aplicarlas al nuevo espacio de archivos Unicode.

Después de la instalación, realice una copia de seguridad incremental completa y cambie el nombre de todos los espacios de archivos existentes que no están activados para Unicode y realice la copia de seguridad de los archivos y directorios que éstos contienen en los nuevos espacios de archivos activados para Unicode. Esta operación implica un mayor tiempo de proceso y almacenamiento en el servidor.


Los espacios de archivos que no están activados para Unicode pueden verse en el juego de caracteres del entorno local desde el que se ha realizado realizar la copia de seguridad de los archivos. Puede que una estación de trabajo que se ejecute en otro entorno regional diferente no vea estos espacios de archivos ni efectúe operaciones de restauración. Los espacios de archivos activados para Unicode de los que se hace copia de seguridad en un entorno regional, están visibles en los demás entornos regionales, siempre que la estación de trabajo tenga instaladas las fuentes adecuadas.


 Sistemas operativos Windows Para realizar la restauración o recuperación desde un espacio de archivos no activado para Unicode, especifique el origen en el servidor y el destino en el cliente. Consulte

 sistemas operativos Mac OS X El servidor puede definir la opción `autofsrename` y modificar temporalmente el valor `autofsrename` del cliente.

## Cientes soportados


---


 sistemas operativos Mac OS X Esta opción sólo es válida para Mac OS X. El servidor puede definir la opción `autofsrename` y modificar temporalmente el valor `autofsrename` del cliente. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. El servidor puede definir la opción `autofsrename` y modificar temporalmente el valor `autofsrename` del cliente. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha General, en el cuadro de lista desplegable Cambiar nombre de espacios de archivos no Unicode durante la copia de seguridad/archivado del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha General, en el cuadro de lista desplegable Cambiar nombre de espacios de archivos no Unicode durante la copia de seguridad/archivado del Editor de preferencias.

## Sintaxis

---

```
.-Prompt-.
>>-AUTOFsrename----->>
+-Yes-----+
'-No-----'
```

## Parámetros

---



Yes

Especifica que el servidor de IBM Spectrum Protect cambia automáticamente el nombre de todos los espacios de archivos que no están activados para Unicode en la operación de copia de seguridad o archivado actual.





No

Especifica que el servidor no cambia el nombre de los espacios de archivos que no están activados para Unicode en la operación de copia de seguridad o archivado actual.

Prompt

Especifica que se le preguntará si desea cambiar el nombre de los espacios de archivos no activados para Unicode en la operación actual. Éste es el valor predeterminado.

Consideraciones:




- Esta opción solo se aplica cuando el servidor establece la opción `autofsrename` en `client`.
- Cuando el planificador cliente está en ejecución, el procedimiento predeterminado consiste en no presentar ninguna solicitud de información. La siguiente sesión interactiva solicita al usuario que cambie el nombre del espacio de archivos.
- El cliente *sólo* le presentará una única solicitud de información por espacio de archivos. Si especifica `no` en el indicador, más adelante el cliente no puede cambiar el nombre de los espacios de archivos. Sin embargo, el administrador de IBM Spectrum Protect podrá cambiar el nombre de los espacios de archivos en el servidor.
-  Sistemas operativos Mac OS X  Sistemas operativos Windows Cuando la copia de seguridad de los archivos se realiza en un espacio de archivos no activado para Unicode, el cliente activado para Unicode pasa por alto los archivos y directorios que tienen nombres que contienen caracteres de una página de códigos que es distinta de la del entorno regional actual.
-  Sistemas operativos Mac OS X  Sistemas operativos Windows Si las copias de seguridad de archivos y directorios cuyos nombres contenían caracteres de una página de códigos distinta de la del entorno regional actual se habían realizado con un cliente no habilitado para Unicode, es posible que hayan caducado. El cliente activado para Unicode hará caducar estos archivos si no se realiza una migración del espacio de archivos a un espacio de archivos activado para Unicode. Puede hacer una copia de seguridad de estos archivos y archivarlos en un espacio de archivos Unicode.

## Ejemplos

---

Archivo de opciones:

```
autofsrename yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Automount

---

La opción `automount` añade al dominio un sistema de archivos montado automáticamente montándolo. Utilice esta opción con la opción `domain`.

Utilice esta opción para especificar todos los sistemas de archivos montados automáticamente que el cliente de copia de seguridad y archivado intenta montar en las siguientes situaciones:

- Cuando se inicia el cliente
- Cuando se inicia la copia de seguridad
- Cuando el cliente ha accedido a un sistema de archivos montado automáticamente durante la copia de seguridad

Monte el sistema de archivos antes de que el cliente realice una copia de seguridad de dicho sistema. Si el sistema de archivos siempre se monta antes de realizar la copia de seguridad, no es necesario especificar explícitamente un sistema de archivos montado automáticamente en la opción `automount`. Sin embargo, añada este sistema de archivos en la opción `automount` para asegurarse de que dicho sistema se ha montado en todas las circunstancias mencionadas anteriormente. Los sistemas de archivos montados automáticamente se vuelven a montar si se han desactivado mientras se realizaba una operación de copia de seguridad.

## Clientes soportados

---

Esta opción es válida para todas las plataformas UNIX, a excepción de Mac OS X. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`).

## Sintaxis

---

.- - - - - .

```
>>-AUTOMount-----filespacename-+-----><
```

## Parámetros

---

filespace

Especifica uno o más sistemas de archivos montados automáticamente completamente cualificados que se montan y se añaden al dominio.

## Ejemplos

---

Archivo de opciones:

```
automount /home/Fred /home/Sam
```

Línea de mandatos:

No se aplica.

 Sistemas operativos Linux  Sistemas operativos Windows

## Backmc

---


La opción backmc especifica la clase de gestión que aplicar al mandato backup fastback para fines de retención.


Utilice la opción backmc con el mandato backup fastback.

Si realiza una copia de seguridad de un objeto en varias ocasiones y especifica una clase de gestión diferente para cada copia de seguridad, todas las versiones de copia de seguridad del objeto se vuelven a enlazar con la última clase de gestión especificada.

## Clientes soportados

---

 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Ninguno. Esta opción sólo puede especificarse en la línea de mandatos o en el planificador.

## Sintaxis

---

```
>>-BACKMc---nombre_clase_gestión-----><
```

## Parámetros

---

nombre\_clase\_gestión

Especifica el nombre de la clase de gestión.

## Ejemplos

---

Línea de mandatos:






```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1 -backmc=ret2yrs
```





## Backupsetname

---

La opción backupsetname especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect.

Puede utilizar la opción backupsetname con los mandatos siguientes:

- query backup
- query filespace
-  Sistemas operativos Windows query image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris query image
-  Sistemas operativos Windows query systemstate




-  Sistemas operativos Windows restore image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris restore image


Nota: Los mandatos siguientes toman backupsetname como parámetro de posición. El parámetro de posición backupsetname tiene un comportamiento distinto que la opción backupsetname. Para ver una descripción de cómo afecta el parámetro de posición backupsetname a cada uno de estos mandatos consulte las explicaciones del mandato:

- query backupset
- restore
- restore backupset

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para todos los clientes UNIX y Linux. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

## Sintaxis

---

```
>>-BACKUPSETName--nombre_conjunto_copias-----><
```

## Parámetros

---

nombrejuego copias

Especifica el nombre de un juego de copias de seguridad del servidor de IBM Spectrum Protect. No puede utilizar caracteres comodín.





## Ejemplos

---



Línea de mandatos:

 sistemas operativos Mac OS X



```
dsmc query backup /Volumes/bkSets/file.1
-backupsetname=YEAR_END_ACCOUNTING.12345678
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc query backup /usr/projects -subdir=yes
-backupsetname=YEAR_END_ACCOUNTING.12345678
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
dsmc restore image /home/proj
-backupsetname=ACCOUNTING_2007.12345678
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

```
dsmc query image -backupsetname=WEEKLY_BSET.21435678
```

 Sistemas operativos Windows

```
dsmc query backup c:\* -subdir=yes
-backupsetname=weekly_accounting_data.32145678
```

 Sistemas operativos Windows

```
dsmc restore image e:
-backupsetname=weekly_backup_data.12345678
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Basesnapshotname


---


La opción `basesnapshotname` especifica la instantánea a utilizar como instantánea base, cuando se realiza una copia de seguridad diferencial de instantánea (`snappdiff`) de un volumen de archivador NetApp. Si especifica esta opción, también debe utilizar la opción `snappdiff` o se produce un error. Si no se especifica `basesnapshotname`, la opción `useexistingbase` selecciona la instantánea más reciente en el volumen de archivador como la instantánea base.

Si no se puede encontrar la instantánea especificada, se notifica un error y la operación de copia de seguridad falla.

## Cientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows compatibles.

## Archivo de opciones

---

Esta opción puede especificarse en el archivo de opciones del cliente o bien en la línea de mandatos.

## Sintaxis

---

```
>>-BASESNAPSHOTName-- --nombre_instantánea----->>
```

## Parámetros

---

### *nombre\_instantánea*

Especifica el nombre de una instantánea existente que utilizar como instantánea base. El nombre especificado puede ser un nombre de instantánea, por ejemplo `vol1_snap`, o puede ser el nombre de una copia de seguridad de NetApp planificada con un nombre como `nocturno.x`, donde `x` es el número de secuencia (donde `nightly.0` es la instantánea más antigua).

También puede utilizar un patrón con caracteres comodín para seleccionar una instantánea. Los caracteres comodín pueden ser los siguientes:

\*

Un asterisco (\*) coincide con cualquier carácter.

?

El signo de interrogación (?) coincide con un solo carácter.

Los caracteres comodín son útiles si las instantáneas siguen un patrón, por ejemplo incluir la fecha o la fecha y hora como parte del nombre de instantánea. Por ejemplo, una instantánea creada el 12 de noviembre de 2012 a las 11:10:00 AM puede guardarse como `UserDataVol_121103111000_snapshot`. La instantánea más reciente que coincide con el patrón se selecciona como la base existente. Por ejemplo, si hay dos instantáneas guardadas (`UserDataVol_121103111000_snapshot` y `UserDataVol_121103231000_snapshot`), se selecciona `UserDataVol_121103231100_snapshot` porque es 12 horas posterior a la otra instantánea.

```
-basesnapshotname="UserDataVol_*_snapshot"
```

Los signos de interrogación funcionan bien para las copias de seguridad planificadas que siguen un patrón de nombre coherente. Esta sintaxis selecciona la copia de seguridad "nocturno" más frecuente como la instantánea que debe utilizarse como base existente.

```
-basenameshotname="nightly.?"
```

## Ejemplos

---

Archivo de opciones:

```
basesnapshotname nightly.?
```

```
basesnapshotname volum_base_snap
```

Línea de mandatos:

```
dsmc incr \\DRFileer\UserDataVol_Mirror_Share -snappdiff  
-useexistingbase -basesnapshotname="nightly.?"
```

### Referencia relacionada:

Useexistingbase

## Cadlistenonport

---

La opción cadlistenonport especifica si se debe abrir un puerto de escucha para el aceptador de clientes.

Cuando un puerto de escucha está abierto, puede aceptar cualquier conexión de entrada. Sin embargo, el puerto no se utiliza si el aceptador de clientes solo gestiona el planificador y este se ejecuta en modalidad de sondeo. Puede utilizar esta opción para evitar que el aceptador abra el puerto no utilizado.

El valor predeterminado de esta opción es yes. Utilice cadlistenonport no solo si se utilizan managedservices schedule y schedmode polling.





## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Coloque esta opción en el archivo de opciones del cliente (dsm.sys) de una stanza de servidor.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-CADLISTENONPort--+-Yes-  
                        '-No--'
```

## Parámetros

---

Yes

Especifica que el aceptador de clientes debe abrir un puerto de escucha. Este parámetro es el predeterminado.

No

Especifica que el aceptador de clientes no debe abrir un puerto de escucha. Utilice este valor cuando utilice el aceptador de clientes solo para gestionar el planificador en modalidad de sondeo.

Este valor inhabilita otras características que dependen del aceptador de clientes, como las operaciones de copia de seguridad y restauración de clientes, IBM Spectrum Protect for Virtual Environments: operaciones de la GUI de Data Protection for VMware vSphere y operaciones de copia de seguridad y restauración de IBM Spectrum Protect Snapshot.

## Ejemplo

---

Archivo de opciones:  
cadlistenonport no  
Línea de mandatos:  
No se aplica.

### Referencia relacionada:

Managedservices  
Schedmode

 Sistemas operativos Windows

## Casesensitiveaware

---

La opción casesensitiveaware especifica si el cliente de copia de seguridad/archivado de Windows debe filtrar objetos de archivo y directorio cuyos nombres están en conflicto por el uso de las mayúsculas y minúsculas.

Los volúmenes NTFS y ReFS son sensibles a mayúsculas y minúsculas y permiten almacenar nombres de archivo sensibles a mayúsculas y minúsculas. Aunque el sistema operativo Windows no es sensible a las mayúsculas y minúsculas, aplicaciones como Windows Services para UNIX (SFU) utilizan convenios POSIX y permiten utilizar nombres de archivos sensibles a las mayúsculas y minúsculas. SFU se suele incluir con sistemas operativos Windows como as Windows Powered OS y Windows Storage Server. Estos sistemas operativos normalmente se despliegan en hardware (por ejemplo, hardware NAS) que actúa como un servidor de archivos dedicado en un entorno heterogéneo.

Si existen clientes UNIX que almacenan archivos en volúmenes NTFS o ReFS en estos entornos de servidor de archivos Windows, utilice la opción `casesensitiveaware`. Si no se utiliza esta opción en estos entornos, se producirán resultados imprevisibles durante las operaciones de copia de seguridad y de archivado si se producen conflictos de nombres de archivos sensibles a las mayúsculas y minúsculas. Para los entornos de servidor de archivos Windows homogéneos, la opción `casesensitiveaware` no es necesaria.

Por ejemplo, si existe un conjunto de objetos denominados 'MyWork.xls', 'MYWORK.xls' y 'mywork.xls', puesto que el sistema operativo Windows no es sensible a las mayúsculas y minúsculas, las aplicaciones no podrán distinguir entre dos objetos denominados 'mywork.xls' y 'MyWork.xls'.

Por este motivo, el cliente de copia de seguridad y archivado de Windows no podrá garantizar la integridad de la restauración de estos objetos. Cuando surge un conflicto relacionado con la utilización de mayúsculas y minúsculas en un nombre, el cliente de copia de seguridad y archivado sólo puede garantizar la integridad de la restauración del primer archivo en orden alfabético. En un sistema operativo basado en ASCII, como Windows, esto significa que los nombres que se indican en letras mayúsculas aparecerán alfabéticamente antes que sus homólogos en minúsculas, por ello 'MySwork.xls' debería preceder alfabéticamente a 'mywork.xls'.

En este ejemplo, si se utilizara la opción `casesensitiveaware`, sólo se procesaría 'MyWork.xls'. Se emite un mensaje de error para 'mywork.xls' y se pasa por alto. Si 'mywork.xls' es un directorio, se pasaría por alto el subárbol de directorios 'mywork.xls'. En todos los casos, los mensajes se grabarán en las anotaciones de error locales y en la consola del servidor de IBM Spectrum Protect para indicar los nombres de archivos exactos de los objetos que se pasan por alto.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones de cliente (`dsm.opt`).

## Sintaxis

---

```

>>-CASESENSITIVEAware-----<<
      .-No--
      +-----+
      '-Yes-'
```

## Parámetros

---

yes

Especifica que el cliente debe intentar identificar los nombres de los objetos que sólo difieren en la utilización de mayúsculas y minúsculas y filtrar los objetos en los que existen conflictos relacionados con la utilización de mayúsculas y minúsculas y cuya correcta restauración no puede garantizarse.

no

Especifica que el cliente debe intentar identificar los nombres de los objetos que sólo difieren en la utilización de mayúsculas y minúsculas. Éste es el valor predeterminado.

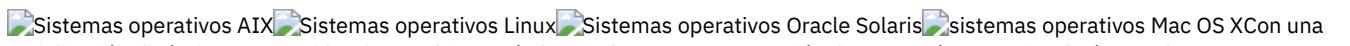
## Changingretries


---






La opción `changingretries` especifica cuántas veces se desea que el cliente intente efectuar copia de seguridad o archivado de un archivo que se esté utilizando en ese momento. Utilice esta opción con los mandatos `archive`, `incremental` y `selective`.

Esta opción sólo se aplica cuando serialización de copia (atributo de un grupo de copias de clase de gestión) es estática compartida o dinámica compartida.

Con una serialización estática compartida, si un archivo está abierto durante una operación, la operación se repite el número de veces que especifique. Si el archivo está abierto durante cada uno de los intentos, no se realiza la operación.





 Con una serialización dinámica compartida, si un archivo está abierto durante una operación, la operación se repite el número de veces que especifique. La operación de copia de seguridad o archivado tiene lugar durante el último intento tanto si el archivo está abierto como si no.


 Con una serialización dinámica compartida, si un archivo está abierto durante una operación, la operación se repite el número de veces que especifique. La operación de copia de seguridad o archivado tiene lugar durante el último intento tanto si el archivo está abierto como si no. El soporte de archivos abiertos se puede usar para hacer copias de seguridad de archivos que están bloqueados o en uso.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados





---


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha Copia de seguridad, en el campo Número de reintentos si el archivo se está utilizando del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Copia de seguridad, en el campo Número de reintentos si el archivo se está utilizando del Editor de preferencias.

## Sintaxis

---

```
>>-CHAngingretries- numberretries-----<<
```

## Parámetros

---

númeroreintentos





Especifica el número de veces que se intenta una operación de copia de seguridad o de archivado si se está utilizando el archivo. El rango de valores es de 0 a 4, siendo 4 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
changingretries 3

Línea de mandatos:  
-cha=3

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Class

---



La opción class especifica si ha de visualizarse una lista de objetos NAS o de cliente al utilizar los mandatos delete filespace, query backup y query filespace.


Por ejemplo, para mostrar una lista de los espacios de archivos que pertenezcan a un nodo NAS, especifique el mandato siguiente:

```
query filespace -class=nas
```

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción solo es válida para clientes AIX, Linux y Oracle Solaris. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

## Sintaxis

---

```
      .-client-.
>>-CLASS = -+-----+-----><
          '-nas----'
```

## Parámetros

---

- client**  
Especifica que se desea visualizar una lista de espacios de archivos para un nodo cliente. Éste es el valor predeterminado.
- nas**  
Especifica que se desea visualizar una lista de espacios de archivos para un nodo NAS.

## Ejemplos

---

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

Línea de mandatos:

```
q backup -nasnodename=nodename -class=nas
```

 Sistemas operativos Windows

## Clientview

---

La opción `clientview` está disponible para usuarios que hayan actualizado desde el cliente de copia de seguridad de IBM® Tivoli Storage Manager Express al cliente de archivado y copia de seguridad.

Para poder utilizar esta opción, deberá conectarse con el servidor de Tivoli Storage Manager Versión 5.4 o posterior. La opción `clientview` permite seleccionar la vista `express` o la vista estándar de la interfaz gráfica de usuario (GUI).

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Coloque esta opción en el archivo `dsm.opt`. Para cambiar a la vista `Express`:

1. En la GUI del cliente de copia de seguridad y archivado, seleccione `Editar > Preferencias` en la barra de menús.
2. En la ficha `General` del editor de preferencias, en el campo `Vista de cliente`, pulse en `Express`.
3. Pulse `Aceptar` para guardar los cambios.

Para cambiar a la vista `Estándar`:

1. En la GUI del cliente de copia de seguridad y archivado, pulse `Modificar valores`.
2. En la ficha `General` del Editor de preferencias, en el campo `Vista de cliente`, pulse `Estándar`.
3. Pulse `Aceptar` para guardar los cambios.

## Sintaxis

---

```
      .-standard-.
>>-CLIENTVIEW = -+-----+-----><
                '-express--'
```

## Parámetros

---

- standard**  
Especifica que debe utilizarse la vista estándar o de empresa de la GUI del cliente de copia de seguridad y archivado. La vista estándar contiene las características avanzadas de la GUI de cliente de copia de seguridad/archivado. Éste es el valor predeterminado.
- express**  
Especifica que debe utilizarse la vista `express` de la GUI del cliente de copia de seguridad y archivado. La vista `express` contiene las mismas funciones que la GUI del cliente de copia de seguridad de `Express`.

 Sistemas operativos Windows



## Clusterdiskonly

---

La opción clusterdiskonly especifica si el cliente de archivado y copia de seguridad permite realizar una copia de seguridad únicamente de discos en clúster en entornos específicos.

El cliente de copia de seguridad y archivado permite realizar una copia de seguridad únicamente de discos en clúster cuando el cliente se ejecuta en los siguientes entornos:

- En Microsoft Cluster Server (MSCS)
- Cuando se emplea la migración tras error en un cliente de Windows Server soportado
- En un entorno de VERITAS Cluster Server (VCS), si configura clusternode yes

Anteriormente, el cliente de copia de seguridad y archivado sólo permitía copias de seguridad y restauraciones de los datos de las unidades en clúster que estaban montadas como una letra de unidad.

Es común encontrar unidades en clúster montadas como puntos de montaje de volúmenes. Los sistemas operativos Windows Server permiten a los usuarios exceder la limitación de 26 letras de unidad permitiendo definir puntos de montaje de volumen en un servidor en clúster. El cliente puede proteger los datos en discos de clúster montados como letras de unidad en máquinas de sistema operativo Windows Server. El cliente también puede proteger los datos en discos de clúster montados como puntos de montaje de volumen. El cliente de copia de seguridad y archivado puede determinar automáticamente si un volumen que utiliza un punto de montaje de volúmenes es un volumen de clúster.

Si configura clusterdiskonly yes, el cliente de copia de seguridad y archivado continúa segregando las unidades locales desde unidades de clúster incluso cuando evalúa la opción de dominio ALL-LOCAL. Cuando se especifica clusterdiskonly no, debe definir de forma explícita los dominios de copia de seguridad. Cuando se especifica clusterdiskonly no, el cliente de copia de seguridad y archivado también omite la enumeración de recursos de clúster para determinar los recursos que representan unidades de clúster.

## Clientes soportados

---

Esta opción es válida para todos los clientes de Windows Server soportados.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
.-Yes-.
>>-CLUSTERDISKOnly--+-+-----+-----<<
                    '-No--'
```

## Parámetros

---

Yes

Especifica que el cliente sólo permitirá el proceso de las unidades de clúster. El valor predeterminado es Yes.

No

Especifica que el cliente permite el proceso de cualquier disco cuando se define clusternode yes.

## Ejemplos

---

Caso 1: Realizar la copia de seguridad de un nodo que gestiona las unidades locales (no de clúster) y la información del estado del sistema

Este es el nodo que se ha dedicado a la restauración del sistema físico en caso de producirse una anomalía de hardware. No hay unidades de clúster que aparezcan como puntos de montaje de volúmenes..

Archivo de opciones:

```
CLUSTERNODE NO (predeterminado)
CLUSTERDISKONLY YES (predeterminado)
DOMAIN ALL-LOCAL (predeterminado)
EXCLUDE c:\...\file.txt
```

Caso 1b: Realizar la copia de seguridad de un nodo que gestiona las unidades locales (no de clúster) y la información del estado del sistema y omite la enumeración de los recursos de clúster

Este es un caso similar al caso 1, que puede desplegarse si el cliente de copia de seguridad y archivado emplea una cantidad de tiempo no adecuada durante el proceso de arranque. Durante la inicialización del cliente de copia de seguridad/archivado, se enumeran todos los recursos de clúster para determinar cuáles representan dispositivos de disco de clúster. Este proceso se puede emitir si se establece clusterdisksonly no.

Archivo de opciones:

```
CLUSTERNODE NO (predeterminado)
CLUSTERDISKSONLY NO
DOMAIN C: D: (las unidades locales deben enumerarse explícitamente)
EXCLUDE c:\...\file.txt
```

Caso 2: Realizar la copia de seguridad de un nodo que gestiona las unidades en clúster de un grupo de recursos de clúster y omite la enumeración de los recursos de clúster

Este caso de ejemplo se puede desplegar si el cliente de archivado y copia de seguridad tarda un periodo de tiempo inadecuado durante el proceso de arranque. Durante la inicialización del cliente de copia de seguridad/archivado, se enumeran todos los recursos de clúster para determinar cuáles representan dispositivos de disco de clúster. Este proceso se puede emitir si se establece clusterdisksonly no.

Archivo de opciones:

```
CLUSTERNODE YES
CLUSTERDISKSONLY NO
DOMAIN f: g:
EXCLUDE f:\...\file.txt
```

Caso 3: Realizar la copia de seguridad de un nodo que gestiona las unidades de clúster en un grupo de recursos de clúster, utilizando los puntos de montaje de volúmenes como recursos de clúster

En este caso, se presupone que el nodo es responsable de la copia de seguridad de un grupo de recursos de clúster que tiene dos unidades, f: y f:\mnt. No hay unidades de clúster que aparezcan como puntos de montaje de volúmenes (sistemas operativos Windows Server). Compruebe que define el proceso incremental de dominio tiene únicamente los volúmenes en un grupo de recursos de clústeres. Si dispone de varios grupos de recursos de clúster, asigne un nodo de cliente exclusivo a la gestión de cada grupo de recursos de clúster.


Archivo de opciones

```
CLUSTERNODE YES
CLUSTERDISKSONLY YES
DOMAIN f: f:\mnt
EXCLUDE f:\mnt\...\file.txt
```

La Tabla 1 muestra las combinaciones de clusternode y clusterdisksonly.


Tabla 1. Combinaciones de clusternode y clusterdisksonly

Clus tern ode	Cluste rdisks only	Cuándo utilizarlo
no	sí	Se trata del comportamiento predeterminado si no se especifica ningún valor; puesto que clusterdisksonly se ha establecido en clusterdisksonly yes, se creará el mapa de disco de clúster. Esta combinación se utiliza para realizar una copia de seguridad de las unidades locales.
sí	sí	Este es el método predeterminado de ejecución en un nodo de clúster para hacer la copia de seguridad de discos de clúster, incluyendo los discos que se exponen como puntos de montaje; se creará el mapa de disco de clúster.
sí	no	Para clientes que se ejecutan en sistemas operativos Windows Server, sólo debe especificar clusterdisksonly no si desea omitir la enumeración de volúmenes de clúster por motivos de rendimiento.

 Sistemas operativos Windows

## Clusternode

La opción clusternode especifica el modo en que el cliente de copia de seguridad y archivado gestiona las unidades de clúster.

 Sistemas operativos Windows El cliente de copia de seguridad y archivado gestiona las unidades de clúster en los siguientes entornos:

- Microsoft Cluster Server (MSCS)
- Failover Clustering en sistemas Windows Server

- VERITAS Cluster Server (VCS)

Cuando se establece clusternode yes, solo las unidades compartidas del clúster están disponibles para los procesos de copia de seguridad y archivado. Cuando establece clusternode no, el nombre de nodo se establece de forma predeterminada en el nombre de clúster.

Sistemas operativos Windows Para realizar la copia de seguridad de las unidades locales o del estado del sistema de Windows Server, debe establecer clusternode no.

**Nota:** Debe establecer clusternode yes para todas las operaciones de clúster gestionadas de IBM Spectrum Protect. El uso desigual de la opción clusternode para un nombre de nodo de clúster de IBM Spectrum Protect determinado puede dar lugar a que se invalide contraseña cifrada del nombre de nodo de clúster y se solicite al usuario que vuelva a especificar la contraseña durante la siguiente invocación del programa IBM Spectrum Protect.

Utilice la opción optfile para llamar correctamente al archivo dsm.opt (clúster) correcto para todos los programas de IBM Spectrum Protect para garantizar la funcionalidad correcta para las operaciones relacionadas con clústeres. Consulte la descripción de opción optfile para obtener más información.

Sistemas operativos Windows

## Cientes soportados

---

Esta operación es válida para los clientes del sistema operativo de Windows Server.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-CLUSTERnode-+-----+-----<<
                .-No-- .
                '-Yes-'
```

## Parámetros

---

Sistemas operativos Windows Yes

Sistemas operativos Windows Especifica que desea que el cliente gestione las unidades de clúster en los siguientes entornos:

- MSCS
- Failover Clustering en sistemas Windows Server
- VCS

No

Especifica que desea realizar la copia de seguridad de los discos locales. Éste es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
cluster no

Línea de mandatos:  
-cluster=yes

Esta opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Collocatebyfilespec






---

Utilice la opción collocatebyfilespec para especificar si el cliente de copia de seguridad y archivado utiliza solamente una sesión de servidor para enviar objetos generados a partir de especificación de archivo.

El establecimiento de la opción collocatebyfilespec en yes dará lugar a que se intente eliminar la entremezcla de archivos de especificaciones de archivo distintas, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).





Consideraciones:


- Utilice la opción `collocatebyfilespec` sólo si la agrupación de almacenamiento va directamente a cinta. Si utiliza esta opción para una agrupación de almacenamiento en disco, ello podría afectar al equilibrio de carga y, por consiguiente, al rendimiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados





---


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-COLlocatebyfilespec--+-No--.  
                        +-----+-----<<  
                        '-Yes-'
```

## Parámetros

---

Yes

Especifica que se desea que el cliente utilice solamente una sesión de servidor para enviar objetos generados desde una especificación de archivo. Por lo tanto, si almacena los datos en cinta, los archivos correspondientes a cada especificación de archivo se almacenan en la misma cinta, a menos que se requiera otra cinta para obtener más capacidad. Como resultado puede aumentar el rendimiento de la restauración.

No

Especifica que el cliente (en función de la dinámica de ejecución y de si la opción `resourceutilization` se ha establecido en 3 o en un valor superior) puede utilizar una o varias sesiones de servidor para enviar los archivos desde una única especificación de archivo. Éste es el valor predeterminado.

A consecuencia de ello, el rendimiento de la copia de seguridad puede aumentar. Si la copia de seguridad de los archivos se realiza en una cinta, los archivos se almacenarán en varias cintas. Por lo general, los archivos especificados en la especificación de archivo serán contiguos.

## Ejemplos

---

Archivo de opciones:

```
collocatebyfilespec yes
```

Línea de mandatos:

```
-collocatebyfilespec=yes
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Commethod

---

La opción `commethod` especifica el método de comunicación que se utiliza para proporcionar conectividad en la comunicación entre cliente y servidor.

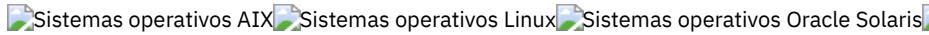
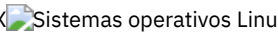
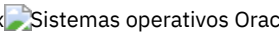
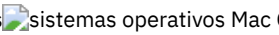
## Clientes soportados


---

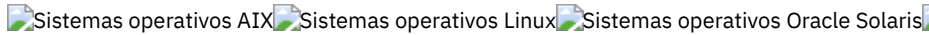
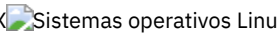
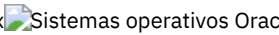
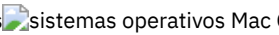
Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha Comunicación del editor de preferencias.


 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Comunicación del editor de preferencias.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Sintaxis

---

```
.-TCPIP-----.  
>>-COMMethod+-----><  
+-SHAREdmem-+  
'-V6TCPIP---'
```

 Sistemas operativos Windows

## Sintaxis

---

```
.-TCPIP-----.  
>>-COMMethod+-----><  
+-SHAREdmem--+  
+-V6TCPIP-----+  
'-NAMedpipes-'
```

## Parámetros


---


### TCPIP

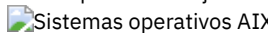
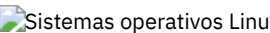
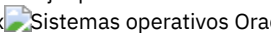
Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP) Éste es el valor predeterminado.



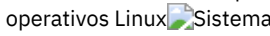
### V6TcPIP



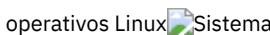
Indica que se debe usar la versión 4 o 6 de TCP/IP, según la configuración del sistema y los resultados de una búsqueda de servicio de nombre de dominio. Debe haber disponible un entorno DNS válido.

 Sistemas operativos Windows **NAMedpipes**

 Sistemas operativos Windows Método de comunicación entre procesos que permite que las corrientes de datos de los mensajes pasen entre un cliente y un servidor. Utilice este método de comunicación con un servidor de IBM Spectrum Protect que se esté ejecutando en la misma estación de trabajo que el cliente.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris **SHAREdmem**

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice el método de comunicación de memoria compartida cuando el cliente y el servidor estén ejecutándose en el mismo sistema. Esto proporciona un mejor rendimiento sobre el protocolo TCP/IP.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Cuando este método de comunicación se especifica en AIX, el cliente puede conectarse como usuario root o como usuario no root, en tanto que el servidor se ejecute como root. Si el servidor no se está ejecutando como root, el ID de usuario que ejecuta el cliente debe coincidir con el que ejecuta el servidor.

**Importante:** Cuando utilice commmethod sharedmem en Linux, es posible que reciba un mensaje de error: ANR8294W Shared Memory Session unable to initialize en el servidor o en la consola del agente de almacenamiento. De forma predeterminada, Linux no se ha configurado con suficientes recursos del sistema para crear las colas de mensajes. Debe aumentar el parámetro del kernel, MSGMNI, a 128 (el valor predeterminado es 16). Puede modificar este parámetro mediante la ejecución del mandato siguiente:

```
echo 128 > /proc/sys/kernel/msgmni
```


Para que este parámetro sea un parámetro permanente después de reiniciar el sistema, puede añadir la siguiente línea al archivo /etc/sysctl.conf y, a continuación, reiniciar el sistema:


```
kernel.msgmni=128
```

Para ver el valor de ipc actual, ejecute este mandato:

```
ipcs -l
```

Compruebe ahora el valor de `max queues system wide`. El valor predeterminado es 16.

 Sistemas operativos WindowsSHAREdmem

 Sistemas operativos WindowsUtilice el método de comunicación de memoria compartida cuando el cliente y el servidor estén ejecutándose en el mismo sistema. Esto proporciona un mejor rendimiento sobre el protocolo TCP/IP.

Nota: para poder utilizar este método de comunicación, el cliente y el servidor deben ejecutarse en la misma cuenta de Windows.

## Ejemplos

---

Archivo de opciones:

Utilice solo TCP/IP V4.

```
commmethod          tcpip
```

Use tanto TCP/IP V4 como V6, según cómo esté configurado el sistema y los resultados de una búsqueda del servicio de nombres de dominio.

```
commmethod V6Tcip
```

Nota: El mandato `dsmc schedule` no puede utilizarse cuando se han especificado tanto `SCHEDMODE prompt` como `commmethod V6Tcip`.

Línea de mandatos:

```
-commm=tcpip
```

```
-commm=V6Tcip
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.





## Commrestartduration

---

La opción `commrestartduration` especifica el número máximo de minutos durante los que el cliente intentará conectarse de nuevo al servidor de IBM Spectrum Protect después de producirse un error de comunicación.

Nota: Un suceso planificado seguirá ejecutándose si el cliente vuelve a conectarse al servidor antes de que haya transcurrido el valor que se ha especificado en `commrestartduration`, aunque haya transcurrido el plazo de tiempo de arranque del suceso.

Puede utilizar la opción `commrestartduration` y `commrestartinterval` en entornos de red con gran actividad o inestables para disminuir los errores de conexión.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows

## Clientes soportados

---


Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha Comunicación, en la sección Opciones comunes del Editor de preferencias.

 Sistemas operativos WindowsEstablezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Comunicación, en la sección Opciones comunes del Editor de preferencias.

## Sintaxis

---

```
>>-COMMRESTARTDuration- minutos-----><
```

## Parámetros

---

`minutos`

Especifica el número máximo de minutos durante los cuales se desea que el cliente intente restablecer conexión con un servidor después de producirse un error de comunicación. El rango de valores es de 0 a 9999, siendo 60 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
commrestartduration 90  
Línea de mandatos:  
No se aplica.






## Commrestartinterval

---

La opción commrestartinterval especifica el número de segundos que deben transcurrir entre los intentos que realiza el cliente para volver a conectarse al servidor de IBM Spectrum Protect después de producirse un error de comunicación.

Nota: utilice esta opción sólo si el valor de commrestartduration es mayor que cero.

Puede utilizar la opción commrestartduration y commrestartinterval en entornos de red con gran actividad o inestables para disminuir los errores de conexión.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha Comunicación, en la sección Opciones comunes del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Comunicación, en la sección Opciones comunes del Editor de preferencias.

## Sintaxis

---

```
>>-COMMRESTARTInterval- segundos-----<<
```

## Parámetros

---

segundos

Especifica el número de segundos que debe transcurrir entre los intentos que realiza un cliente para restablecer la conexión con un servidor después de producirse un error de comunicación. El rango de valores es de 0 a 65535, siendo 15 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
commrestartinterval 30  
Línea de mandatos:  
No se aplica.






## Compressalways

---

La opción compressalways especifica si se debe continuar la compresión si el objeto aumenta de tamaño durante la compresión.

Utilice esta opción con la opción compression y con los mandatos archive, incremental y selective.

La opción compressalways se omite cuando la deduplicación del lado de cliente está habilitada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Cientes soportados

---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

---

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Copia de seguridad, en el recuadro de selección Continuar compresión si el objeto crece del Editor de preferencias.

Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Copia de seguridad, en el recuadro de selección Continuar compresión si el objeto crece del Editor de preferencias.

## Sintaxis

---

```
                .-Yes-.  
>>-COMPRESSAlways--+-----<<  
                '-No--'
```

## Parámetros

---

Yes

La compresión de archivos continúa incluso si el archivo crece como resultado de la compresión. Éste es el valor predeterminado.

No

Los objetos de cliente de copia de seguridad/archivado se envían de nuevo sin comprimir si su tamaño aumenta durante la operación de compresión. El comportamiento de la API depende de la aplicación. Las copias de seguridad de la aplicación puede que no se realicen correctamente.

## Ejemplos

---

Archivo de opciones:  
compressalways yes  
Línea de mandatos:  
-compressa=no

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Compression

---

La opción compression comprime los archivos antes de enviarlos al servidor.

La compresión de archivos reduce el almacenamiento de datos necesario para almacenar versiones de copia de seguridad y copias archivadas de los archivos. Sin embargo, puede afectar al rendimiento de IBM Spectrum Protect. Un procesador rápido en una conexión de red lenta se beneficia de la compresión, pero un procesador lento en una conexión de red rápida, no.

Utilice la opción compression con los mandatos archive, incremental y selective.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris El mandato backup image utiliza el valor de la opción compression que se especifica en el archivo dsm.sys. Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. El servidor también puede definir esta opción, que modifica temporalmente el valor del cliente.











Sistemas operativos Windows El mandato backup image utiliza el valor de la opción compression que se especifica en el archivo dsm.opt. Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. El servidor también puede definir esta opción, que modifica temporalmente el valor del cliente.

El cliente de copia de seguridad y archivado hace copia de seguridad de un archivo esparcido si la compresión del cliente está desactivada. Establezca compression yes para habilitar la compresión de archivos al realizar copias de seguridad de archivos esparcidos con el fin de minimizar el tiempo de transacción de la red y de maximizar el espacio de almacenamiento del servidor.

Si establece compressalways yes, la compresión continuará aunque se incremente el tamaño del archivo. Para detener la compresión si el tamaño del archivo crece y reenviar el archivo sin comprimir, establezca compressalways no.

Si establece compression yes, puede controlar el proceso de compresión de las formas que se indican a continuación:



-  Sistemas operativos Windows Utilice la opción `exclude.compression` en el archivo de opciones del cliente (`dsm.opt`) para excluir archivos o grupos de archivos específicos del proceso de compresión.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice la opción `exclude.compression` en el archivo de opciones del cliente (`dsm.sys`) para excluir archivos o grupos de archivos específicos del proceso de compresión.
-  Sistemas operativos Windows Utilice la opción `include.compression` en el archivo de opciones del cliente (`dsm.opt`) para incluir archivos de un amplio grupo de archivos excluidos en el proceso de compresión.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice la opción `include.compression` en el archivo de opciones del cliente (`dsm.sys`) para incluir archivos de un amplio grupo de archivos excluidos en el proceso de compresión.

Esta opción controla la compresión solo si su administrador especifica que el nodo de cliente pueda comprimir archivos antes de enviarlos al servidor.

El tipo de compresión que utiliza el cliente viene determinado por la combinación de compresión y duplicación de datos del cliente que se utiliza durante proceso de copia de seguridad o archivado. Se utilizan los siguientes tipos de compresión:

#### LZ4

Un método de compresión más rápido y eficiente que el cliente utiliza cuando los datos deduplicados del cliente se envían a una agrupación de almacenamiento de contenedor compatible con LZ4 en el servidor de IBM Spectrum Protect. El servidor debe tener la versión 7.1.5 o posterior y debe utilizar agrupaciones de almacenamiento de contenedor. La compresión LZ4 del cliente solo se utiliza cuando la deduplicación de datos del cliente está habilitada.

#### LZW

Un tipo tradicional de compresión que el cliente utiliza en cualquiera de las situaciones siguientes:

- Los datos deduplicados del cliente se envían a agrupaciones de almacenamiento tradicionales (no de contenedor) del servidor.
- Los datos del cliente no pasan por el proceso de deduplicación de datos. (No se aplica a Data Protection for VMware ni a Data Protection for Microsoft Hyper-V, donde solo se pueden comprimir los datos deduplicados del cliente.)
- Los datos del cliente solo pasan por el proceso de deduplicación de datos tradicional del servidor. (No se aplica a Data Protection for VMware ni a Data Protection for Microsoft Hyper-V, donde solo se pueden comprimir los datos deduplicados del cliente.)

#### Ninguna





El cliente no comprime el objeto. El objeto no se comprime porque la opción `compression` tiene el valor `no` o no se ha especificado durante el proceso de copia de seguridad o archivado. Aunque el cliente no comprime el objeto, es posible que lo comprima el servidor.


No es necesario definir el tipo de compresión. Viene determinado por el cliente de copia de seguridad y archivado en el momento del proceso de la copia de seguridad o archivado.

## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha Copia de seguridad, en la casilla de verificación Comprimir objetos del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Copia de seguridad, en la casilla de verificación Comprimir objetos del Editor de preferencias.

## Sintaxis

```

>>-COMPRESSIon--+-+-----+-----><
                .-No--
                '-Yes-'

```

## Parámetros

#### No

Los archivos no se comprimen antes de enviarlos al servidor. Éste es el valor predeterminado.

Yes

Los archivos se comprimen antes de enviarlos al servidor.

## Ejemplos

Archivo de opciones:  
compression yes  
Línea de mandatos:  
-compressi=no






Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

### Referencia relacionada:

Eliminación de duplicados  
Opciones exclude  
Opciones include


## Console

Utilice la opción console con el mandato query systeminfo para que la información del sistema se visualice en la consola.

- DSMOPTFILE: el contenido del archivo dsm.opt.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
DSMSYSFILE - El contenido del archivo dsm.sys.
- ENV: variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores de IBM Spectrum Protect.
- FILE - Atributos para el nombre de archivo que especifique.
-  Sistemas operativos WindowsFILESNOTTOBACKUP: enumeración de la clave de registro de Windows:










```
HKEY_LOCAL_MACHINE\  
  SYSTEM\  
    CurrentControlSet\  
      BackupRestore\  
        FilesNotToBackup
```

Esta clave especifica los archivos para los que los productos de copia de seguridad no deberían realizar ninguna copia de seguridad. El mandato query inclexcl indicará que el sistema operativo excluirá dichos archivos.




- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
-  Sistemas operativos WindowsKEYSNOTTORESTORE: enumeración de la clave de registro de Windows:

```
HKEY_LOCAL_MACHINE\  
  SYSTEM\  
    ControlSet001\  
      BackupRestore\  
        KeysNotToRestore
```

Esta clave especifica las claves de registro de Windows que los productos de copia de seguridad no deberían restaurar.

-  Sistemas operativos WindowsMSINFO: información del sistema Windows (salida de MSINFO32.EXE).
- OPTIONS - Opciones compiladas.
-  Sistemas operativos WindowsOSINFO - Nombre y versión del sistema operativo cliente
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
OSINFO - Nombre y versión del sistema operativo cliente (incluye información ULIMIT para UNIX y Linux).
- POLICY - Volcado del conjunto de políticas.
-  Sistemas operativos WindowsREGISTRY - Entradas de registro de Windows relacionadas con IBM Spectrum Protect de Windows.
- SCHEDLOG - Contenido de las anotaciones de planificación de IBM Spectrum Protect (por lo general, dsm sched.log).
-  Sistemas operativos WindowsSFP: la lista de archivos protegidos por la característica de protección de archivos del sistema Windows y, para cada archivo, indica si dicho archivo existe. Se hace una copia de seguridad de estos archivos como parte del objeto del sistema SYSFILES.
-  Sistemas operativos WindowsSFP=*filename* - Indica si el archivo especificado (*filename*) se ha protegido mediante la Protección de archivos del sistema de Windows. Por ejemplo:

```
SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
```

-  Sistemas operativos WindowsSYSTEMSTATE: información de estado del sistema de Windows.
-  Sistemas operativos AIXCLUSTER - Información de clústeres de AIX.
-  Sistemas operativos WindowsCLUSTER - Información de clústeres de Windows.

## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Sintaxis

---

```
>>-CONsole-----><
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:

```
query systeminfo dsmoptfile errorlog -console
```

 Sistemas operativos Linux
  Sistemas operativos Windows

## Createnewbase

---

La opción `createnewbase` crea una instantánea base y la utiliza como fuente para ejecutar una copia de seguridad incremental completa.



Algunos archivos pueden no copiarse cuando se ejecuta el mandato de copia de seguridad incremental por diferencia de instantánea. Si los archivos se pasan por alto, puede ejecutar el mandato con la opción `createnewbase` para copiar esos archivos omitidos. Consulte Snapdiff para conocer las razones por las que un archivo puede no copiarse al ejecutar el mandato de copia de seguridad por diferencia de instantánea.

Una razón por la que se puede omitir un archivo durante el proceso de copia de seguridad es porque NetApp Data ONTAP no admite el nombre de archivo. Las versiones 8.0 y las versiones anteriores a 7.3.3 de NetApp Data ONTAP permiten utilizar solo nombres de archivo no pertenecientes al juego de caracteres ASCII de 7 bits. NetApp Data ONTAP versión 7.3.3 y versiones posteriores a 8.0.0 admiten nombres de archivo Unicode. Si ha actualizado NetApp Data ONTAP desde una versión que no admite nombres de archivo Unicode a una versión que sí los admite, ejecute una copia de seguridad incremental con la opción `createnewbase=migrate`.

## Clientes soportados

---

Esta opción es válida para los clientes siguientes:

-  Sistemas operativos Windows Todos los clientes Windows
-  Sistemas operativos Linux Clientes Linux x86\_64

Escriba la opción `createnewbase` en la línea de mandatos. Especifique esta opción con la opción `snapdiff`.

## Sintaxis

---

```
>>-Createnewbase-. -No-----+-----><
                    +-Yes-----+
                    +-IGNore---+
                    '-MIGRate-'
```

## Parámetros

---

No

Especifica que se ejecuta una copia de seguridad incremental por diferencia de instantánea. Si el cliente de copia de seguridad y archivado detecta que el servidor de archivos de NetApp Data ONTAP se ha migrado desde una versión que no permite utilizar nombres de archivo Unicode a un servidor de archivos que sí lo permite, se anota un mensaje de aviso en el registro cronológico

de errores y en el registro de actividad del servidor de IBM Spectrum Protect. El mensaje de aviso indica que debe ejecutar una copia de seguridad incremental completa y anota un código de retorno 8 aunque la operación se completara satisfactoriamente. Este parámetro es el valor predeterminado.

Yes

Especifica que se ejecuta una copia de seguridad incremental completa mediante la creación de una nueva instantánea base, la cual se utiliza para ejecutar una copia de seguridad incremental basada en la exploración de diferencias. Utilice esta opción para copiar cambios de archivo que puedan no haber sido detectados por la API de diferencia de instantánea.

Si la operación se completa satisfactoriamente, el mandato finaliza con un código de retorno de 0.

No especifique `createnevbase=yes` para ninguna planificación en la que se ejecute una copia diaria por diferencia de instantánea. En lugar de ello, cree una planificación mensual separada donde se utilice la opción `createnevbase=yes`.

IGNore

Especifica que se ejecuta una copia de seguridad incremental por diferencia de instantánea cuando el cliente de copia de seguridad y archivado detecta que el servidor de archivos NetApp Data ONTAP se ha actualizado para permitir la utilización de nombres de archivo Unicode.

La opción `ignore` se diferencia del parámetro no en que la opción `ignore` suprime el mensaje de aviso. En lugar de ello, se anota un mensaje informativo en el registro cronológico de errores y en el registro de actividad de IBM Spectrum Protect para indicarle que ejecute una copia de seguridad incremental completa.

Si el mandato finaliza satisfactoriamente, devuelve el código de retorno 0.

Utilice la opción `ignore` si ha actualizado el servidor de archivos NetApp Data ONTAP para que soporte Unicode pero aún no ha ejecutado una copia de seguridad incremental completa. Esta opción se utiliza solamente cuando el cliente de copia de seguridad y archivado detecta que el servidor de archivos se ha migrado y todavía no se ha ejecutado una copia de seguridad incremental completa. Esta opción no se tiene en cuenta en todos los demás casos.

MIGRate

Especifica que si el servidor de archivos NetApp Data ONTAP se ha actualizado a una versión que soporta nombres de archivo Unicode, se crea una instantánea base y se ejecuta una copia de seguridad incremental basada en la exploración de diferencias. La opción `migrate` es distinta de la opción `yes` porque la opción `migrate` crea una instantánea base solo cuando el cliente detecta que se ha actualizado la versión del servidor de archivos NetApp Data ONTAP. La opción `yes` crea una instantánea base cada vez que se ejecuta el mandato.

Tras completarse la copia de seguridad incremental, no se registran más mensajes relacionados con migración en el registro cronológico de errores ni en el registro de actividad del servidor de IBM Spectrum Protect. Cuando la operación se completa correctamente, el mandato finaliza con un código de retorno de 0.

Utilice la opción `migrate` si ha actualizado el servidor de archivos NetApp Data ONTAP para que soporte Unicode pero aún no ha ejecutado una copia de seguridad incremental completa. La opción `migrate` se ignora si no se ha actualizado el servidor de archivos NetApp Data ONTAP.

## Ejemplos

---

Línea de mandatos:

```
dsmc incremental -snapdiff -createnevbase=yes /net/home1
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Datacenter

---


Especifica la ubicación de destino del centro de datos que contendrá los datos de la máquina restaurada.

Utilice esta opción en mandatos `restore vm`.

Si las carpetas se utilizan dentro del centro virtual para organizar centros de datos, el nombre de la carpeta debe incluirse en la especificación del centro de datos, separado por una barra inclinada.

Si está restaurando utilizando un servidor de ESX en lugar de un centro virtual, debe utilizarse la opción `-datacenter=ha-datacenter`.

La ubicación de destino predeterminada es el centro de datos donde se ha almacenado la máquina virtual en el momento de la copia de seguridad.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Ejemplos

---

Restaurar una máquina virtual en un centro de datos USEast organizado bajo un nombre de carpeta llamada Producción en el centro virtual.

```
dsmc restore vm my_vm -datacenter=Production/USEast
```

Restaurar una copia de seguridad de máquina virtual realizada por un centro virtual, pero utilizando un servidor de ESX en el momento de la restauración.

```
restore vm my_vm -datacenter=ha-datacenter
```

Restaurar una máquina virtual en el centro de datos USWest.


```
restore vm my_vm -datacenter=USWEST
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Datstore

---

Especifica el destino del almacén de datos que utilizar durante la operación de restauración de VMware.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Ejemplo

---


Restaurar la máquina virtual en un almacén de datos llamado ds8k\_prod1:






```
restore vm my_vm -datastore=ds8k_prod1
```

## Dateformat

---

La opción dateformat especifica el formato que desea utilizar para visualizar o especificar fechas.
















 Sistemas operativos Windows Utilice esta opción si desea cambiar el formato de fecha predeterminado y establecerlo en el idioma del repositorio de mensajes que utiliza.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen la información de formato de la definición del entorno regional que esté en vigor en el momento en que se inicia el cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno regional.

Nota:

1. La opción dateformat no afecta al cliente web. El cliente web utiliza el formato de fecha para el entorno regional en el que se está ejecutando el navegador. Si un navegador no se está ejecutando en un entorno regional que admite el entorno local, el cliente web utiliza el formato de fecha para inglés de Estados Unidos.
2. si el formato de fecha se modifica y se utiliza la opción schedlogretention para eliminar las anotaciones de planificación, el cliente elimina todas las entradas de las anotaciones de planificación cuyo formato de fecha sea diferente al eliminar las anotaciones. Si el formato de fecha se modifica y se utiliza la opción errorlogretention para eliminar el registro de errores, el cliente elimina todas las entradas del registro de errores cuya fecha sea diferente al eliminar las anotaciones. Cuando modifique el formato de fecha, copie las anotaciones de planificación y de errores si desea conservar las entradas de anotaciones cuyo formato de fecha sea diferente.

Puede utilizar la opción dateformat con los mandatos siguientes.

- delete archive
- delete backup
- expire
- query archive
-  Sistemas operativos Windows query asr
- query backup
- query filespace
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris query image
-  Sistemas operativos Windows query image
-  Sistemas operativos Windows query systemstate
- restore
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris restore image
-  Sistemas operativos Windows restore image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X restore nas
-  Sistemas operativos Windows restore nas

- retrieve
-  Sistemas operativos Windows restore registry
- set event

Si se incluye la opción dateformat con un mandato, ésta debe anteponerse a las opciones fromdate, pitdate y todate.





## Cientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Configuración regional, en la lista desplegable Formato de fecha del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Configuración regional, en la lista desplegable Formato de fecha del Editor de preferencias.

## Sintaxis

---







```
>>-DATEformat-- --número_formato-----><
```



## Parámetros

---

número\_formato



Muestra la fecha en uno de los siguientes formatos. Seleccione el número que se corresponda con el formato de fecha que desee utilizar:





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris 0  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice el formato de fecha que especifica el entorno regional (no se aplica a Mac OS X).





 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Para AIX y Solaris: es el valor predeterminado si el formato de fecha que especifica el entorno local consta de dígitos y de caracteres de separación.

1

MM/DD/AAAA

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Para AIX y Solaris: es el valor predeterminado si el formato de fecha que especifica el entorno local consta de cualquier carácter a excepción de dígitos y caracteres de separación.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Éste es el valor predeterminado para las siguientes traducciones disponibles:





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

- Inglés de Estados Unidos
- Chino (tradicional)
- Coreano

2

DD-MM-AAAA

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Éste es el valor predeterminado para las siguientes traducciones disponibles:

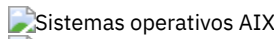
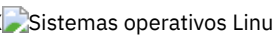
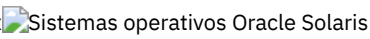
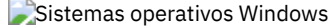
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

- Portugués de Brasil
- Italiano

3

AAAA-MM-DD

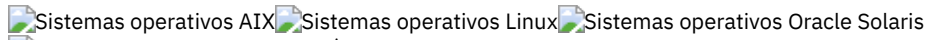
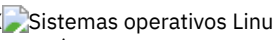
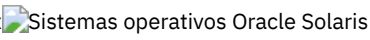
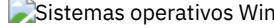
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Éste es el valor predeterminado para las siguientes traducciones disponibles:

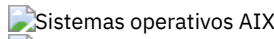
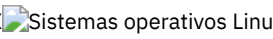
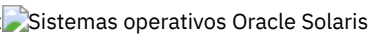

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

- Japonés
- Chino (simplificado)
- Polaco

4

DD.MM.AAAA

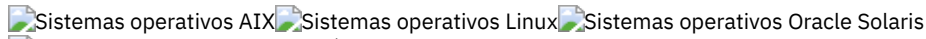
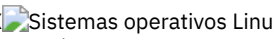
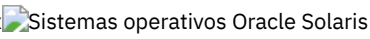
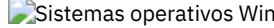
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Éste es el valor predeterminado para las siguientes traducciones disponibles:

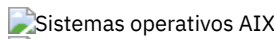
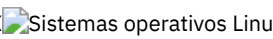
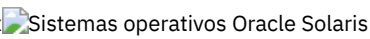
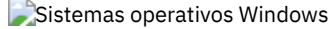
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

- Alemán
- Francés
- Español
- Checo
- Ruso

5

AAAA.MM.DD

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Éste es el valor predeterminado para las siguientes traducciones disponibles:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

- Húngaro

6

AAAA/MM/DD

7

DD/MM/AAAA

## Ejemplos

---

Archivo de opciones:

dateformat 3

Línea de mandatos:

-date=3





Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

## Consideraciones adicionales para especificar los formatos de fecha y hora

---

El formato de fecha y hora que especifique con esta opción debe utilizarse en las opciones que acepten una entrada de fecha y hora. Por ejemplo: totime, fromtime, todate, fromdate y pittime.

Por ejemplo, si especifica la opción timeformat como `TIMEFORMAT 4`, el valor que proporciona en la opción fromtime o totime debe especificarse como una hora, por ejemplo, 12:24:00pm. Si especifica 13:24:00, no será válido porque `TIMEFORMAT 4` necesita un entero de hora menor o igual a 12. Si desea especificar valores de hasta 24 horas en una opción y utilizar comas como separadores, debe especificar `TIMEFORMAT 2`.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Configuración de los formatos de fecha y hora en el archivo de configuración del entorno regional del sistema

Puede especificar formatos de fecha y hora configurándolos en el archivo de entorno regional del sistema. Si especifica formatos de fecha y hora en el archivo del entorno regional, deben definirse utilizando un subconjunto de especificadores de formato de producción de números soportados por la función `strftime()` del lenguaje C. Puede utilizar los siguientes especificadores para establecer los formatos de fecha y hora en los valores de configuración del entorno regional.

### Especificadores de fecha

- `%Y` - el año, en cuatro dígitos. Por ejemplo, 2011.
- `%y` - el año, solo con los dos últimos dígitos. Por ejemplo, 11; no 2011.
- `%m` - el mes, como un número decimal (1-12).
- `%d` - el día del mes (1-31).

En los especificadores de fecha, sólo puede especificar un especificador de año. No especifique `%Y` ni `%y`. El modificador E (un E en mayúsculas) puede preceder los especificadores de fecha para crear la forma alternativa del entorno local para el año, mes o día. Si no existe ningún formato alternativo, el modificador E se ignora. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,), los puntos (.), (.), guiones (-) o barras diagonales (/). No utilice caracteres de varios bytes como separadores.

### Especificadores de hora

- `%H` - la hora, en formato de 24 horas (00-23).
- `%I` - la hora, en formato de 12 horas (00-12).
- `%M` - minutos después de la hora (00-59).
- `%S` - segundos después del minuto (00-59).
- `%p` - añade el indicador AM (antes de mediodía) o PM (después de mediodía).

En los especificadores de hora, sólo puede especificar un especificador de hora. No especifique `%I` y `%H` a la vez.

El modificador O (una O mayúscula) puede ir antes que los especificadores de hora para producir el formato alternativo del entorno regional para la hora, los minutos o los segundos. El modificador O no puede ir antes que el especificador `%p`. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,) o los puntos (.). No utilice caracteres de varios bytes como separadores. No especifique un separador entre el especificador `%p` y el separador que le precede o le sigue.

### Ejemplos de formato de hora, configurados en los valores de entorno regional





 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Para establecer un formato de hora en particular, edite el archivo de configuración del entorno regional que utiliza y modifique la línea `t_fmt` en función de sus necesidades. Sea cual sea el formato de hora seleccionado, se aplica tanto a la salida como a la entrada. Una vez editado el archivo de configuración del entorno regional, debe ejecutarse el mandato `localedef` para crear el archivo del entorno regional final.

Tabla 1. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea `t_fmt`)

Ejemplo	Resultado
"%H:%M:%S"	Muestra la hora en el formato <code>hh:mm:ss</code> , siendo valores válidos para <code>hh</code> el rango de 0 a 23.
"%H,%M,%S"	Muestra la hora en el formato <code>hh,mm,ss</code> , siendo valores válidos para <code>hh</code> el rango de 0 a 23.
"%I,%M,13p"	Muestra la hora en el formato <code>hh,mm,ssA/P</code> , donde <code>hh</code> puede estar entre 1 y 12, y donde <code>A/P</code> es la abreviatura local de antemeridiano (AM en inglés) o postmeridiano (PM en inglés).

### Ejemplos de formato de fecha, configurados en los valores de entorno regional





 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Para establecer un formato de fecha en particular, edite el archivo de configuración y modifique la línea `d_fmt` en función de sus necesidades. Sea cual sea el formato de fecha seleccionado, se aplica tanto a la salida como a la entrada.

Tabla 2. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea `d_fmt`)

Ejemplo	Resultado
---------	-----------



Ejemplo	Resultado
"%m/%d/%y"	Visualiza la fecha con el formato MM/DD/AA.
"%d.%m.%Y"	Visualiza la fecha con el formato DD.MM.AAAA.

## Dedupcachepath





Utilice la opción `dedupcachepath` para especificar la ubicación donde se creó la base de datos de la memoria caché de eliminación de duplicados de datos del lado del cliente.


Esta opción se pasa por alto si la opción `enableddedupcache=no` se establece durante el proceso de copia de seguridad o archivado.

### Clientes soportados

Esta opción es válida para todos los clientes. Esta opción también es válida para la API de IBM Spectrum Protect.

### Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Coloque esta opción en el archivo de opciones del sistema (`dsm.sys`). Puede establecer esta opción en el campo Deduplication Cache Location del Editor de preferencias. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el cuadro de texto Deduplicación > Ubicación de la memoria caché de deduplicación del Editor de preferencias. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.


### Sintaxis

```
>>-DEDUPCACHEPath--path-----<<
```

### Parámetros






`path`

Especifica la ubicación en la que se creará la base de datos de caché en disco si `enableddedupcache` se ha establecido en `yes`. La ubicación predeterminada es para crear el archivo de caché de la eliminación de duplicados de datos del directorio de instalación del cliente de copia de seguridad y archivado o de la API.

 Sistemas operativos Windows En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$: `\\computer7\D$\stgmgr\dedupecache`.

### Ejemplos

Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris `dedupcachepath /volumes/temp`  
 Sistemas operativos Windows `dedupcachepath c:\logs\dedup\`

Línea de mandatos:

No se aplica.

**Referencia relacionada:**

`enableddedupcache`

## Dedupcachesize





Utilice la opción `dedupcachesize` para determinar el tamaño máximo del archivo de la caché de la eliminación de duplicados de datos. Cuando el archivo de la caché alcanza su tamaño máximo, se elimina el contenido de la caché y se añaden las entradas nuevas.


### Clientes soportados

Esta opción es válida para todos los clientes. Esta opción también es válida para la API de IBM Spectrum Protect.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones del sistema (dsm.sys). Puede establecer esta opción en el campo Eliminación de duplicados > Memoria caché de la eliminación de duplicados > Tamaño máximo en el editor Preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el campo Eliminación de duplicados > Memoria caché de la eliminación de duplicados > Tamaño máximo en el editor Preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-DEDUPCACHESize--dedupcachesize-----<<
```

## Parámetros

---

dedupcachesize

Especifica el tamaño máximo, en megabytes, del archivo de la caché de la eliminación de duplicados de datos. El rango de valores es de 1 a 2048, siendo 256 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
dedupcachesize 1024
```

Línea de mandatos:

No se aplica.

**Referencia relacionada:**

Eliminación de duplicados

## Eliminación de duplicados

---

Utilice la opción deduplication para especificar si habilita la eliminación de datos redundantes por parte del cliente cuando se transfieren los datos al servidor IBM Spectrum Protect durante el proceso de copia de seguridad y archivado.

La eliminación de datos duplicados se inhabilita si se define la opción enablelanfree. Se excluyen los archivos cifrados del cliente de copia de seguridad y archivado de la eliminación de duplicados de datos por parte del cliente. También se excluyen los archivos de los sistemas de archivos cifrados.

Para dar soporte a la eliminación de duplicados de datos por parte del cliente, se deben cumplir los siguientes criterios:

- La eliminación de duplicados de datos del lado de cliente está habilitada en el servidor.
- El destino de la agrupación de almacenamiento para los datos debe ser una agrupación de almacenamiento habilitada para la eliminación de duplicados de datos. La agrupación de almacenamiento debe tener el tipo de dispositivo "file".
- Los archivos pueden excluir del proceso de eliminación de duplicados de datos del lado del cliente (todos los archivos están incluidos de forma predeterminada).
- El servidor puede limitar el tamaño máximo de transacción para optimización de almacenamiento de datos definiendo la opción CLIENTDEDUPTXNLIMIT en el servidor. Para obtener más información sobre esta opción, consulte la documentación del servidor de IBM Spectrum Protect.
- El archivo debe tener un tamaño superior a 2 KB.





## Clientes soportados

---


Esta opción es válida para todos los clientes; también se puede utilizar en la API de IBM Spectrum Protect.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema (dsm.sys) en una stanza de servidor. Puede establecer esta opción

seleccionando la casilla de verificación Eliminación de duplicados > Habilitar eliminación de duplicados en el editor Preferencias. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción seleccionando la casilla de verificación Eliminación de duplicados > Habilitar eliminación de duplicados en el editor Preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-DEDUPLICATION--+-No-->>
                    |-----|
                    '-Yes-'<<
```

## Parámetros

---

No

Especifica que no desea habilitar la eliminación de duplicados de datos por parte del cliente para el proceso de copia de seguridad y archivado. No es el valor predeterminado.

Yes

Especifica que desea habilitar la eliminación de duplicados de datos por parte del cliente para el proceso de copia de seguridad y archivado.

## Ejemplos





---

Archivo de opciones:  
deduplication yes  
Línea de mandatos:  
-deduplication=yes

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

### Referencia relacionada:

Opciones include  
Opciones exclude

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Defaultserver

---

Utilice la opción defaultserver para especificar el nombre del servidor de IBM Spectrum Protect a contactar para los servicios de copia de seguridad/archivado si se ha definido más de un servidor en el archivo dsm.sys.

De forma predeterminada, el cliente de copia de seguridad y archivado establecerá contacto con el servidor que se ha definido mediante la primera stanza del archivo dsm.sys. Esta opción sólo se utiliza si no se especifica la opción servername en el archivo de opciones del usuario cliente (dsm.opt).

Si se tiene instalado el cliente de HSM en la estación de trabajo y no se especifica un servidor de migración con la opción migrateserver, utilice esta opción para especificar el servidor donde desea migrar los archivos. Para obtener más información, consulte la documentación de producto de IBM Spectrum Protect for Space Management en el IBM Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SSERBH/welcome>.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX.

## Archivo de opciones

---

Establezca esta opción *al principio* del archivo dsm.sys *delante* de cualquier stanza de servidor.

## Sintaxis

---

```
>>-DEFAULTServer-- --servername----->>
```

## Parámetros

---

servername

Especifica el nombre del servidor predeterminado en el que desea almacenar las copias de seguridad o las copias archivadas. El servidor donde se migran los archivos de los sistemas de archivos locales también puede especificarse con esta opción.

## Ejemplos





---

Archivo de opciones:  
defaults server\_a  
Línea de mandatos:  
No se aplica.

## Deletefiles

---

Utilice la opción deletefiles con el mandato archive para suprimir archivos de la estación de trabajo después de haber realizado el archivado de éstos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows También puede utilizar esta opción con el mandato restore image y la opción incremental para suprimir archivos de la imagen restaurada si éstos se han suprimido después de haber creado la imagen. La supresión de archivos se realizará correctamente si el grupo de copia de seguridad del servidor de IBM Spectrum Protect cuenta con suficientes versiones para los archivos existentes y suprimidos.

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-DELetefiles-----<<
```

## Parámetros


---

No hay parámetros para esta opción.




## Ejemplos

---

Línea de mandatos:

 sistemas operativos Mac OS X

```
dsmc archive "/Users/dgordon/Documents/*.c" -deletefiles
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
dsmc archive "/home/foo/*.c" -deletefiles  
dsmc restore image /local/data -incremental -deletefiles
```




 Sistemas operativos Windows


```
dsmc archive c:\foo\*.c -deletefiles  
dsmc rest image c: -inre -deletefiles
```

## Descripción

---

La opción description asigna o especifica una descripción para los archivos cuando se efectúan operaciones de archivado, supresión de archivado, recuperación, consulta de archivado o consulta de juego de copias de seguridad.

Por ejemplo, si desea archivar un archivo denominado budget.jan y asignarlo a la descripción "Presupuesto de 2002 para proy. 1", especificaría lo siguiente:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 sistemas operativos Mac OS X

```
dsmc archive -des="Presupuesto de 2003 para proy. 1" /home/plan/  
proj1/budget.jan
```

## Sistemas operativos Windows






```
dsmc archive -des="Presupuesto de 2003 para proy. 1" c:\plan\proj1\
budget.jan
```

Nota:

1. La longitud máxima de una descripción es de 254 caracteres.
2. Si el valor de la opción que entre contiene un espacio en blanco, especifique el valor entre comillas ( " ").

Utilice la opción `description` con los mandatos siguientes:

- `archive`
- `delete archive`
- `query archive`
- `query backupset`
- `retrieve`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-DEscription = - --description-----<<
```

## Parámetros

---

`description`




Asigna una descripción al archivo que se está archivando. Si no especifica una descripción con el mandato `archive`, el valor predeterminado es `Archive Date:x`, donde `x` es la fecha del sistema actual. Tenga en cuenta que la fecha siempre consta de 10 caracteres. Si en su formato de fecha el año se indica con dos dígitos, habrá dos espacios en blanco al final de la fecha. Por ejemplo, una descripción predeterminada en la que el año se indique con cuatro dígitos puede ser `"Archive Date: 2002/05/03"`, y la misma descripción predeterminada en la que el año se indique con dos dígitos sería `"Archive Date: 02/05/03 "` (observe que hay dos espacios al final). Al recuperar archivos utilizando la descripción de año con dos dígitos, puede especificar la opción `-description` de cualquiera de estas maneras:

```
-description="ArchiveDate: 02/05/03  "
o bien
-description="ArchiveDate: 02/05/03*"
```

Si se utiliza el mandato `archive` para archivar más de un archivo, la descripción que especifique se aplica a cada archivo. Por ejemplo, para archivar un grupo de archivos y asignar la misma descripción, *Proyecto X*, a cada archivo, escribiría:

 sistemas operativos Mac OS X

```
dsmc archive -description="Proyecto X" "/Users/van/Documents/*.x"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc archive -description="Project X" "/home/allproj/*"
```

 Sistemas operativos Windows

```
dsmc archive -description="Project X" c:\allproj\*.x
```

Posteriormente podrá utilizarse la descripción para recuperar todos los archivos.





## Ejemplos

---


Línea de mandatos:

 sistemas operativos Mac OS X

```
dsmc archive "/Users/van/Documents/*.prj" -des="Presupuesto de
2003 para proy. 1"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc archive "/home/foo/*.prj" -des="2003 Budget for Proj 1"  
dsmc query backupset -loc=server -descr="Mi portátil"
```

 Sistemas operativos Windows






```
dsmc archive -des="2003 Budget for Proj 1" c:\foo\ *.prj
```

## Detail

---


Utilice la opción detail para ver información sobre la clase de gestión, el espacio de archivos, las copias de seguridad, las copias archivadas y otra información adicional en función del mandato con el que se utilice.


Utilice la opción detail con el mandato query mgmtclass para visualizar información detallada acerca de cada clase de gestión del juego de políticas activo. Si no utiliza la opción detail, sólo se mostrará el nombre de la clase de gestión y una breve descripción. Si especifica la opción detail, se mostrará información sobre los atributos de cada grupo de copia que contiene cada clase de gestión. Una clase de gestión puede contener un grupo de copia de seguridad, un grupo de copia archivada, ambos grupos o ninguno.



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Puede que un espacio de archivos activado para Unicode no se visualice correctamente si el servidor no puede visualizar el nombre en Unicode. En este caso, utilice el fsID (identificador de espacio de archivos) del espacio de archivos para identificar estos espacios de archivos en el servidor. Utilice la opción detail con los mandatos delete filespace y query filespace para determinar el ID de espacio de archivos de un espacio de archivos. El ID de espacio de archivos también aparece en el diálogo de información de archivos de las GUI del cliente de copia de seguridad/archivado y del cliente web.

Utilice la opción detail con los mandatos query backup y query archive para que se visualicen los atributos del archivo que ha especificado:

- Fecha de última modificación
- Fecha de último acceso
- Compresión
- Tipo de cifrado
- Deduplicación de datos del lado del cliente
- Indica si el cliente HSM ha migrado o premigrado el archivo

 Sistemas operativos Windows Utilice la opción detail con el mandato query adobjects para visualizar información detallada acerca de los objetos de Active Directory, incluidos todos sus atributos.


 Sistemas operativos Windows Utilice la opción detail con el mandato query adobjects para visualizar información detallada acerca de los objetos de Active Directory, incluidos todos sus atributos.




 Sistemas operativos Linux  Sistemas operativos Windows Utilice el mandato detail con el mandato query VM para visualizar las estadísticas siguientes:






- El número medio de objetos de IBM Spectrum Protect necesarios para describir un único megabloque, entre todos los megabloques de una copia de seguridad.
- El número medio de objetos de IBM Spectrum Protect necesarios para describir un único megabloque, para todos los megabloques de un espacio de archivos.
- La proporción de la cantidad de datos, de los que informa Change Block Tracking, frente a la cantidad de datos de los que realmente se ha realizado una copia de seguridad, en una copia de seguridad determinada.
- La proporción de la cantidad de datos, de los que informa Change Block Tracking, frente a la cantidad de datos de los que realmente se ha realizado una copia de seguridad, para todas las copias de seguridad de este espacio de archivos.
- El número de copias de seguridad que se han creado desde que se ha realizado la última copia de seguridad completa a partir de los discos de producción.

Los valores devueltos en query vm pueden ayudarle a ajustar el heurística (consulte las opciones Mbojrefreshthresh y Mbpctrefreshthresh) para ajustar el desencadenante de los valores para renovaciones megablock.

Utilice la opción detail con los mandatos siguientes:

- delete filespace
- incremental
-  Sistemas operativos Windows query adobjects
- query archive
- query backup
- query filespace
- query inclexcl

- query mgmtclass
-  Sistemas operativos Windowsquery systemstate
-  Sistemas operativos Linux Sistemas operativos Windowsquery vm

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. Esta opción no está establecida en el archivo de opciones del cliente; se utiliza mediante la adición a la línea de mandatos cuando se especifique alguno de los mandatos que lo admiten. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-DEtail----->>
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:

```
dsmc query mgmtclass -detail
```

```
dsmc query filespace -detail
```

```
dsmc query backup file1 -detail
```

 Sistemas operativos Windows

```
dsmc query systemstate -detail
```

 Sistemas operativos Linux  Sistemas operativos Windows

```
dsmc query vm -detail
```

 Sistemas operativos Linux  Sistemas operativos Windows


## Diffsnapshot


---

La opción `diffsnapshot` controla si cliente de copia de seguridad y archivado debe crear la instantánea diferencial al ejecutar una copia de seguridad incremental por diferencia de instantánea.

Si el cliente no crea la instantánea diferencial, se utilizará la instantánea más reciente que se encuentre en el volumen como la instantánea diferencial y como el origen de la operación de copia de seguridad.


El valor predeterminado es crear la instantánea diferencial. Esta opción se omite la primera vez que se utiliza la opción `snapdiff`. La primera vez que se utiliza la opción `snapdiff` en un volumen, se debe crear una instantánea y utilizarla como origen de una copia de seguridad incremental completa. El cliente suprime las instantáneas creadas por cliente de copia de seguridad y archivado después de finalizar la siguiente copia de seguridad incremental por diferencia de instantánea.


 Sistemas operativos Linux Las instantáneas se pueden crear con la herramienta Network Appliance FilerView. Utilice el parámetro `latest` si desea que el cliente utilice la instantánea más reciente que se haya creado con éste o con otro método. El cliente no suprime nunca las instantáneas que se han creado con métodos que no son de IBM Spectrum Protect.

 Sistemas operativos Windows Las instantáneas se pueden crear con la herramienta Network Appliance FilerView. Utilice el parámetro `latest` si desea que el cliente utilice la instantánea más reciente que se ha creado. Sea cual sea el método que utilice para crear las instantáneas con nombre, los nombres de las instantáneas que difieran únicamente en las mayúsculas o minúsculas no funcionarán correctamente con la opción `snapdiff`. Las instantáneas creadas por el cliente no tendrán el problema de las mayúsculas y minúsculas. El cliente no suprime nunca las instantáneas que se han creado con métodos que no son de IBM Spectrum Protect.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

## Sintaxis

---

```
    .-create-.  
>>-DIFFSNAPSHOT-----<<  
    '-latest-'
```

## Parámetros

---

create


Especifique que desea crear una nueva instantánea permanente para que se utilice como instantánea origen. Este es el valor predeterminado.


latest


Especifica que se desea utilizar la instantánea más reciente encontrada en el servidor de archivos como instantánea origen.

## Ejemplos

---


 Sistemas operativos Linux Línea de mandatos:


 Sistemas operativos Linux Realice una copia de seguridad incremental por diferencia de instantánea de un sistema de archivos montado en NFS /vol/vol1 que reside en el servidor de archivos homestore.example.com, donde /net/home1 es el punto de montaje de /vol/vol1.


 Sistemas operativos Linux `incremental -snapdiff -diffsnapshot=latest /net/home1`


El valor latest de la opción -diffsnapshot significa que la operación utilizará la instantánea más reciente (la instantánea activa).

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Realice una copia de seguridad incremental snapdiff a partir de una instantánea tomada de un recurso de red compartido //homestore.example.com/vol/vol1 montado en la unidad H:, donde homestore.example.com es un servidor de archivos.

 Sistemas operativos Windows `incremental -snapdiff H:`

 Sistemas operativos Windows Realice una copia de seguridad incremental snapdiff a partir de una instantánea tomada de un recurso de red compartido //homestore.example.com/vol/vol1 montado en la unidad H:, donde homestore.example.com es un servidor de archivos. El valor de opción de -diffsnapshot de LATEST significa que la operación se producirá utilizando la instantánea más reciente (la instantánea activa) para el volumen H:.

 Sistemas operativos Windows `incremental -snapdiff H: -diffsnapshot=latest`

 Sistemas operativos Linux  Sistemas operativos Windows

## Diffsnapshotname


---

La opción diffsnapshotname permite especificar qué instantánea diferencial, en el volumen de archivador de destino, debe utilizarse durante una copia de seguridad diferencial de instantáneas. Esta opción sólo se especifica si también se especifica diffsnapshot=latest.

Si no se especifica esta opción, diffsnapshot=latest selecciona la instantánea existente más reciente en el volumen del archivador y la utiliza como instantánea diferencial.

## Clientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Esta opción puede especificarse en el archivo de opciones del cliente o bien en la línea de mandatos.

## Sintaxis

---

```
>>-DIFFSNAPSHOTName-- --snapshot_name-----<<
```



## Parámetros

---

### *snapshot\_name*

Especifica el nombre de una instantánea existente que utilizar como instantánea diferencial.

También puede utilizar un patrón con caracteres comodín para seleccionar una instantánea. Los comodines pueden ser cualquiera de los caracteres siguientes:

\*

Un asterisco (\*) coincide con cualquier carácter.

?

El signo de interrogación (?) coincide con un solo carácter.

La instantánea más reciente que coincide con el patrón comodín se selecciona como la instantánea diferencial.

## Ejemplos

---

Archivo de opciones:

```
diffsnapshotname volume_base_snap
```

```
diffsnapshotname nightly.?
```

Línea de mandatos:

```
dsmc incr \\DRfiler\UserDataVol_Mirror_Share -snapdiff  
-useexistingbase -basenameshotname="nightly.?"  
-diffsnapshot=latest -diffsnapshotname="nightly.?"
```

### Referencia relacionada:

Useexistingbase

Basesnapshotname

## Dirmc

---






La opción `dirmc` especifica la clase de gestión que desea utilizar para los directorios.

Si no se especifica esta opción para asociar una clase de gestión con directorios, el programa cliente utiliza la clase de gestión del conjunto de políticas activo del dominio de políticas cuyo período de retención sea más largo. Seleccione una clase de gestión para directorios individuales que retenga los directorios durante, como mínimo, el tiempo que retiene los archivos que se asocian a éstos.

Si especifica una clase de gestión mediante esta opción, todos los directorios especificados en la operación de copia de seguridad están vinculados a dicha clase de gestión.

La opción `dirmc` especifica la clase de gestión de los directorios de los que hace copia de seguridad y no afecta a los directorios archivados. Utilice la opción `archmc` con el mandato `archive` para especificar la clase de gestión disponible para el dominio de políticas al que desea vincular los archivos y los directorios archivados. Si no utiliza la opción `archmc`, el servidor vincula los directorios archivados a la clase de gestión. Si la clase de gestión predeterminada no tiene grupo de copias archivadas, el servidor vincula los directorios archivados a la clase de gestión con el período de retención más reducido.

Importante: Sólo se almacenan los atributos ampliados y los ACLs en las agrupaciones de almacenamiento. La información del directorio, distinta a los atributos ampliados y a los ACLs, permanece en la base de datos. En sistemas Windows, los directorios ocupan espacio de agrupación de almacenamiento.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows





## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha Copia de seguridad, en la sección Clase de gestión de directorios del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Copia de seguridad, en la sección Clase de gestión de directorios del Editor de preferencias.

## Sintaxis

---

```
>>-DIRMc-- --mgmtclassname-----<<
```

## Parámetros

---

mgmtclassname

Especifica el nombre de la clase de gestión que se desea asociar con los directorios. El cliente utiliza el nombre de clase de gestión especificado para todos los directorios de los que realiza copia de seguridad. Si no especifica esta opción, el cliente asocia la clase de gestión al mayor período de retención con directorios.

## Ejemplos

---

Archivo de opciones:

dirmanagdir

Línea de mandatos

No se aplica.

## Dirsonly

---

La opción dirsonly *sólo* procesa directorios. El cliente no procesa archivos.

La opción dirsonly puede utilizarse con los mandatos siguientes:

- archive
- incremental
- query archive
- query backup
- restore
- restore backupset
- retrieve
- selective

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-Dirsonly-----<<
```

## Parámetros


---





No hay parámetros para esta opción.





## Ejemplos


---


 sistemas operativos Mac OS XLínea de mandatos:

 sistemas operativos Mac OS X `dsmc query backup -dirsonly "/Users/*"`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `dsmc query backup -dirsonly "*"`

 Sistemas operativos WindowsLínea de mandatos:

 Sistemas operativos Windows `dsmc query backup -dirsonly c:*`

## Disablenqr

---

La opción disablenqr especifica si el cliente de archivado y copia de seguridad puede usar el método de restauración sin consulta para restaurar archivos y directorios del servidor.

Si establece la opción `disablenqr` en no (el valor predeterminado), el cliente podrá usar el proceso de restauración sin consulta.

Si establece la opción `disablenqr` en yes, el cliente sólo puede utilizar el proceso de restauración estándar (también denominada "restauración clásica").

Nota: No existe ninguna opción ni valor para especificar que el cliente sólo puede utilizar el método de restauración sin consulta.

## Cientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

Coloque esta opción en el archivo `dsm.opt`.

## Sintaxis

---

```
. -No-- .  
>>-DISABLENQR-----+-----+-----><  
' -Yes- '
```

## Parámetros

---

No

Especifica que el cliente puede usar el método de restauración sin consulta. Éste es el valor predeterminado.

Yes

Especifica que el cliente sólo utiliza el método de restauración estándar. No se permite el método de restauración sin consulta.

## Ejemplos

---

Archivo de opciones:

`disablenqr yes`


Línea de mandatos





`-disablenqr=yes`

## Diskbuffsize






---

La opción `diskbuffsize` especifica el tamaño máximo de memoria intermedia de E/S de disco (en kilobytes) que el cliente puede utilizar al leer archivos. La opción `diskbuffsize` sustituye a la opción `largecommbuffers`.

 **Sistemas operativos Windows** Por lo general, puede obtenerse un rendimiento óptimo del cliente de migración de copia de seguridad y de archivado si el valor de esta opción es igual o menor que la cantidad de lectura anticipada del archivo que proporciona el sistema de archivos del cliente. Un almacenamiento intermedio de mayor tamaño precisará más memoria y es posible que no mejore el rendimiento.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Por lo general, puede obtenerse un rendimiento óptimo del cliente de migración de copia de seguridad, archivado o HSM si el valor de esta opción es igual o menor que la cantidad de lectura anticipada del archivo que proporciona el sistema de archivos del cliente. Un almacenamiento intermedio de mayor tamaño precisará más memoria y es posible que no mejore el rendimiento.

Importante: Utilice el valor predeterminado, a menos que el personal de soporte de IBM® le indique algo distinto.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **sistemas operativos Mac OS X**  **Sistemas operativos Oracle Solaris**  
 **Sistemas operativos Windows**

## Cientes soportados





---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 **Sistemas operativos Windows** Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

    Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.



## Sintaxis





---

```
>>-DISKBufsize-- --size-----><
```

## Parámetros

---

  Especifica el tamaño máximo de almacenamiento intermedio de E/S del disco (en kilobytes) que el cliente puede utilizar al leer archivos. El rango de valores es de 16 a 1023; el valor predeterminado es 32.

    Especifica el tamaño máximo de almacenamiento intermedio de E/S del disco (en kilobytes) que el cliente puede utilizar al leer archivos. El rango de valores es de 16 a 1023; el valor predeterminado es 32. Para AIX: si se define la opción enablelanfree no, el valor predeterminado de diskbufsize es 256.

## Ejemplos

---

Archivo de opciones:  
diskbufsize 64  
Línea de mandatos:  
No se aplica.

## Diskcachelocation

---





La opción diskcachelocation especifica la ubicación en la que se crea la base de datos de memoria caché de disco si la opción memoryefficientbackup=diskcachemethod se especifica durante una copia de seguridad incremental.


Puede especificar la opción diskcachelocation en el archivo de opciones o con la opción include.fs. Si la opción diskcachelocation aparece en el archivo de opciones, el valor de ésta se utilizará para todos los espacios de archivos no representados mediante una opción include.fs que contenga el parámetro diskcachelocation.

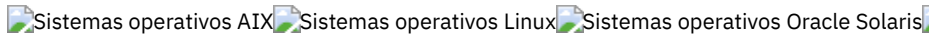

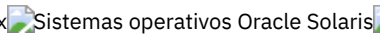

La caché de disco es un archivo temporal que se suprime después de ejecutar el mandato incremental. Esta opción puede utilizarse para seleccionar:

1. Una ubicación que cuenta con más espacio libre en el disco si, al utilizar memoryefficientbackup=diskcachemethod, recibe el mensaje en el que se le indica que el archivo de caché en disco no puede crearse porque no dispone de suficiente espacio de disco.
2. Una ubicación en un volumen físico diferente para reducir la contención para el mecanismo de acceso al disco y mejorar con ello el rendimiento.

Importante: Por razones de rendimiento, no utilice una unidad remota para diskcachelocation.

    La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de los archivos y directorios de los que se hace copia de seguridad. Para UNIX, Linux, calcule 1 byte por carácter en el nombre de vía de acceso. Para Mac OS X, calcule 4 bytes por carácter en el nombre de vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 200 MB en los clientes UNIX y Linux y 800 MB en los clientes Mac OS X. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

 La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de los archivos y directorios de los que se hace copia de seguridad. Calcule 2 bytes por carácter en el nombre de la vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 400 MB. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Al realizar copia de seguridad de un sistema de archivos gestionados HSM, se crea un segundo archivo de caché de disco para la lista de archivos migrados. Los archivos de caché de disco combinados, creados por copias de seguridad incrementales de caché de disco y copias de seguridad del sistema de archivos gestionados HSM, pueden necesitar más de 400 MB de espacio de disco para cada millón de archivos de los que se realice copia de seguridad. El archivo de la memoria caché de disco puede ser muy grande. El soporte de archivos grandes debe estar habilitado en el sistema de archivos que se está utilizando para el archivo de memoria caché de disco.

## Clientes soportados

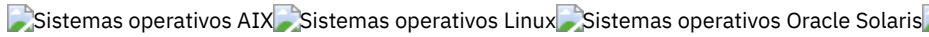

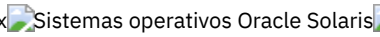

---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones de cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor.

## Sintaxis

---

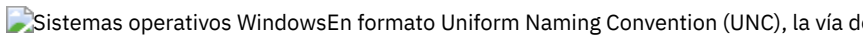
```
>>-DISKCACHELocation-- --vía de acceso-----<<
```

## Parámetros

---

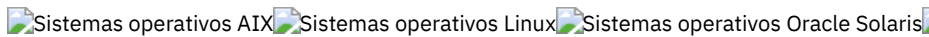

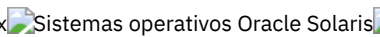

vía de acceso





Especifica la ubicación en la que se creará la base de datos de caché en disco si `memoryefficientbackup=diskcachemethod`. La ubicación predeterminada es para crear el archivo de caché del disco en la raíz del espacio de archivo que se está procesando.

 Sistemas operativos Windows En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$:  
\\computer7\D\$\temp\diskcache.

## Ejemplos


---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
diskcachelocation /home  
diskcachelocation /Volumes/hfs2
```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows

```
diskcachelocation c:\temp  
diskcachelocation c:\tivoli\data
```

Línea de mandatos:



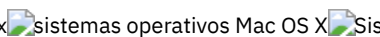

No se aplica.

## Domain

---


La opción `domain` especifica lo que desea incluir en la copia de seguridad incremental.

Solo se realiza copia de seguridad de los objetos de dominio si inicia el mandato incremental sin una especificación de archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris El cliente de copia de seguridad y archivado utiliza el valor `domain` en las situaciones siguientes para determinar qué sistemas de archivos se han de procesar durante una copia de seguridad incremental:

- Cuando se ejecuta una copia de seguridad incremental utilizando el mandato incremental y no especifica qué sistemas de archivos se han de procesar.
- Cuando el administrador de IBM Spectrum Protect define una planificación para ejecutar una copia de seguridad incremental para el usuario, pero no especifica los sistemas de archivos que deben procesarse.

- Cuando selecciona la acción Copia de seguridad de dominio en la GUI del cliente de copia de seguridad y archivado.

 Sistemas operativos Windows El cliente de copia de seguridad y archivado utiliza el valor domain en las situaciones siguientes para determinar qué unidades se han de procesar durante una copia de seguridad incremental:

- Cuando se ejecuta una copia de seguridad incremental con el mandato incremental y no se especifica qué unidades deben procesarse.
- Cuando el administrador de IBM Spectrum Protect define una planificación para ejecutar una copia de seguridad incremental para el usuario, pero no especifica las unidades que deben procesarse.
- Cuando selecciona la acción Copia de seguridad de dominio en la GUI del cliente de copia de seguridad y archivado.





Puede definir la opción domain en las ubicaciones siguientes:

- En un archivo de opciones.
- En la línea de mandatos, cuando se ha especificado con un mandato del cliente.
- En un conjunto de opciones de cliente, que se haya definido en el servidor con el mandato define clientopt.
- Como una opción en un mandato planificado, que se haya definido en el servidor con el mandato define schedule.

Si alguno de estos orígenes contiene una definición de dominio, el cliente realizará copia de seguridad de ese dominio. Si más de un origen especifica un dominio, el cliente realizará copia de seguridad de todos los dominios especificados. Se puede definir el mismo objeto de dominio más de una vez, pero el efecto es el mismo que si lo define sólo una vez. Si no especifica un dominio, el cliente realiza copia de seguridad del dominio predeterminado, como se describe en el parámetro all-local.

Puede excluir objetos del dominio mediante la especificación del operador de exclusión (-) delante del objeto. Si alguna definición de dominio excluye un objeto, ese objeto se excluye del dominio, incluso si otra definición incluye el objeto. No puede utilizar el operador de exclusión de dominio (-) delante de ninguna palabra clave de dominio que empiece por all-.

Si una sentencia de dominio excluye uno o más objetos y ninguna sentencia de dominio incluye objetos, el resultado es un dominio vacío (no se realiza copia de seguridad de nada). Debe especificar los objetos que se incluirán en el dominio si alguna sentencia de dominio excluye objetos.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Ejemplo 1: Este ejemplo utiliza una sentencia de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para /fs1:


```
domain all-local -/fs1
```

Ejemplo 2: Este ejemplo utiliza varias sentencias de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para /fs1:

```
domain all-local domain -/fs1
```

Ejemplo 3: Este ejemplo excluye /fs1 en una operación de copia de seguridad. Si no se utiliza ninguna otra sentencia de dominio, el resultado es un dominio vacío. No se realiza copia de seguridad de nada.

```
domain -/fs1
```

 Sistemas operativos Windows Ejemplo 1: Este ejemplo utiliza una sentencia de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para el estado del sistema:

```
domain all-local -systemstate
```





Ejemplo 2: Este ejemplo utiliza varias sentencias de dominio para realizar copia de seguridad de todos los sistemas de archivos locales excepto para el estado del sistema:



```
domain all-local domain -systemstate
```

Ejemplo 3: Este ejemplo excluye el estado del sistema en una operación de copia de seguridad. Si no se utiliza ninguna otra sentencia de dominio, el resultado es un dominio vacío. No se realiza copia de seguridad de nada.



```
domain -systemstate
```





Si inicia el mandato incremental con una especificación de archivo, el cliente pasa por alto las definiciones de dominio y realiza una copia de seguridad de la especificación de archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Puede incluir un punto de montaje virtual en el dominio del cliente.

 Sistemas operativos AIX  Sistemas operativos Linux Importante: Si está ejecutando GPFS para AIX o GPFS para Linux x86\_64 en un clúster de varios nodos, y todos los nodos comparten un sistema de archivos GPFS montado, el cliente procesa este sistema de

archivos como un sistema de archivos local. El cliente realiza copias de seguridad del sistema de archivos en cada nodo durante una copia de seguridad incremental. Para evitar esta situación, puede realizar una de las siguientes tareas:

- Configure explícitamente la sentencia domain en el archivo de opciones de usuario de cliente (dsm.opt) para enumerar los sistemas de archivos de los que desea que dicho nodo realice una copia de seguridad.
-  Sistemas operativos AIX  Sistemas operativos Linux Establezca la opción exclude.fs en el archivo de opciones del sistema del cliente para excluir el sistema de archivos GPFS de los servicios de copia de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Sistemas de archivos montados automáticamente






Al realizar una copia de seguridad con la opción domain establecida en all-local, no se hace copia de seguridad de los archivos gestionados por el montador automático y los sistemas de archivo de bucle de retorno.


Si realiza copias de seguridad de un sistema de archivos con la opción domain establecida en all-local, se excluyen los subdirectorios que sean puntos de montaje de un sistema de archivos automontado (AutoFS) en una operación de copia de seguridad. Todos los archivos existentes en el servidor para el subdirectorio de montaje automático han caducado.

Si se realiza una copia de seguridad con la opción domain establecida en all-lofs, se hace copia de seguridad de todos los sistemas de archivos de bucle de retorno (LOFS) explícitos y se excluyen todos los sistemas de archivos automontados. Para dispositivos de bucle y sistemas de archivos locales gestionados por el montador automático, establezca la opción domain en all-auto-lofs.

Utilice la opción automount con los parámetros del dominio all-auto-nfs y all-auto-lofs para especificar uno o varios sistemas de archivos de montaje automático que se van a montar y a añadir al dominio. Si especifica la opción automount, los sistemas de archivos automontados se vuelven a montar si se han desactivado durante la ejecución del mandato incremental.

Los puntos de montaje virtual no pueden utilizarse con sistemas de archivos montados automáticamente.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Linux Importante: En algunas distribuciones Linux, es posible que las asignaciones o puntos de montaje del sistema de archivos automontado de tipo de sistema de archivos (AutoFS) no aparezcan en la tabla de montaje actual. A consecuencia de ello, los sistemas de archivos automontados, que se desmontan durante el proceso de archivado o copia de seguridad, podrían procesarse de manera incorrecta y almacenarse como parte del dominio equivocado (por ejemplo, como parte del dominio all-local, all-nfs o all-lofs, según el tipo de sistema de archivos real). Por lo tanto, en este tipo de entornos de distribución de Linux, tiene que especificar el valor correcto para la opción automount, a fin de procesar adecuadamente el valor de opción de dominio en cualquier momento específico.






 sistemas operativos Mac OS X Para Mac OS X, los sistemas de archivos automontados no se admiten. Si un sistema de archivos automontado forma parte de una sentencia de dominio, la copia de seguridad falla y no se procesan archivos en el sistema de archivos automontado. Haga una copia de seguridad del sistema de archivos automontado del sistema host y restáurela. No haga una copia de seguridad del sistema de archivos automontado ni la restaure sobre una conexión de red.





## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones, dsm.opt. Puede establecer esta opción en la ficha Copia de seguridad, en la sección Dominio para copia de seguridad del Editor de preferencias.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones, dsm.opt o dsm.sys. En el archivo dsm.sys, debe colocar esta opción dentro de una stanza de servidor. Puede establecer esta opción en la ficha Copia de seguridad, en la sección Dominio para copia de seguridad del Editor de preferencias.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

## Sintaxis

```
.-----  
v .-all-local----. |  
>>-DOMain-----+----->>  
+-domain-----+
```





object


Especifica los objetos del dominio que se han de incluir en el dominio.


Un nombre de objeto debe incluirse entre comillas si el nombre contiene espacios.


-object


Especifica los objetos del dominio que se han de excluir del dominio.

Un nombre de objeto debe incluirse entre comillas si el nombre contiene espacios.

 Sistemas operativos Windows systemstate

 Sistemas operativos Windows Realiza una copia de seguridad del estado del sistema Windows. El dominio systemstate se incluye en el dominio all-local.

 Sistemas operativos Windows -systemstate


 Sistemas operativos Windows Excluye el estado del sistema del proceso de copia de seguridad.

## Ejemplos




---

Archivo de opciones:


Un archivo de opciones puede contener más de una sentencia domain. Sin embargo, todas las sentencias domain son un ejemplo de una sentencia única en un archivo de opciones.

 sistemas operativos Mac OS X

```
domain all-local
domain all-local -/Volumes/volume2
domain all-local '-/Volumes/Macintosh HD'
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
domain /tst /datasave /joe
"domain all-local"
domain ALL-LOCAL -/home
domain ALL-NFS -/mount/nfs1
```

 Sistemas operativos Windows

```
domain c: d: e:
domain c: systemstate
domain ALL-LOCAL -systemstate
domain ALL-LOCAL -c:
domain ALL-LOCAL -\\florence\e$
```

Una única sentencia de dominio puede listar uno o más objetos para el dominio. Puede utilizar más de una sentencia de dominio. Los dos ejemplos siguientes de dos archivos de opciones proporcionan los mismos resultados de dominio:

Ejemplo 1

```
...
domain fs1
domain all-local
domain -fs3
...
```





Ejemplo 2

```
...
domain all-local fs1 -fs3
...
```

Línea de mandatos:

 sistemas operativos Mac OS X

```
-domain="/ /Volumes/volume2"
-domain="all-local -/Volumes/volume2"
```


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
-domain="/fs1 /fs2"
-domain=/tmp
-domain="ALL-LOCAL -/home"
```

 Sistemas operativos Windows

```
-domain="c: d:"
-domain="ALL-LOCAL -c: -systemstate"
```

## Interacción de las definiciones de dominio

 El dominio se puede definir en distintos orígenes y el resultado es una suma de todas las definiciones de dominio. Como ejemplo de la interacción de las definiciones de dominio, tenga en cuenta cómo las definiciones de dominio de distintos orígenes proporcionan distintos resultados de copia de seguridad. En la tabla, *FS* seguido por un número (por ejemplo, FS1) es un sistema de archivos. En esta tabla se muestran solo los mandatos especificados en la línea de mandatos. En el caso de mandatos planificados, la columna "línea de mandatos" no es pertinente y se deben considerar las opciones del mandato planificado.


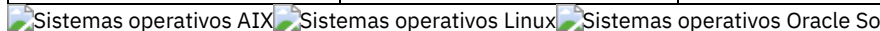
 El dominio se puede definir en distintos orígenes y el resultado es una suma de todas las definiciones de dominio. Como ejemplo de la interacción de las definiciones de dominio, tenga en cuenta cómo las definiciones de dominio de distintos orígenes proporcionan distintos resultados de copia de seguridad. En la tabla, *FS* seguido de un número (por ejemplo FS1) es una unidad. En esta tabla se muestran solo los mandatos especificados en la línea de mandatos. En el caso de mandatos planificados, la columna "línea de mandatos" no es pertinente y se deben considerar las opciones del mandato planificado.

Tabla 1. Interacción de definiciones de dominio de distintos orígenes

Archivo de opciones	Línea de mandatos	Conjunto de opciones de cliente	Objetos de los que se ha realizado copia de seguridad mediante el mandato incremental
domain FS1	incremental -domain=FS2	domain FS3	FS1 FS2 FS3
domain FS1	incremental	domain FS3	FS1 FS3
	incremental -domain=FS2		FS2
	incremental -domain=FS2	domain FS3	FS2 FS3
	incremental	domain FS3	FS3
	incremental		all-local
domain all-local	incremental	domain FS3	all-local + FS3
domain all-local domain -FS1	incremental		all-local, pero no FS1
domain -FS1	incremental		ninguno
domain FS1 FS3	incremental	domain -FS3	FS1
domain all-local	incremental	domain -FS3	all-local, pero no FS3
	incremental FS1 - domain=all-local		FS1
	incremental FS1	domain all-local	FS1
domain -FS1	incremental FS1		FS1

 El dominio se puede definir en distintos orígenes y el resultado es una suma de todas las definiciones de dominio. Como ejemplo de la interacción de las definiciones de dominio, tenga en cuenta cómo las definiciones de dominio de distintos orígenes proporcionan distintos resultados de copia de seguridad. En la tabla, *FS* seguido de un número (por ejemplo FS1) es una unidad. En esta tabla se muestran solo los mandatos especificados en la línea de mandatos. En el caso de mandatos planificados, la columna "línea de mandatos" no es pertinente y se deben considerar las opciones del mandato planificado.

## Domain.image

La opción `domain.image` especifica lo que desea incluir en el dominio de cliente para una copia de seguridad de imágenes.


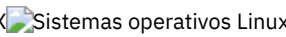
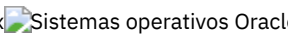
 Debe indicarse explícitamente el nombre de los volúmenes lógicos RAW.

Si no especifica un sistema de archivos con el mandato `backup image` se realizará la copia de seguridad de los sistemas de archivos que especifique en la opción `domain.image`.

Cuando especifica un sistema de archivos con el mandato `backup image`, la opción `domain.image` se pasa por alto.


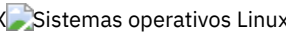
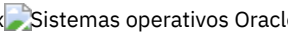
Si no utiliza la opción `domain.image` para especificar sistemas de archivos en el archivo de opciones del cliente y no especifica un sistema de archivos con el mandato `backup image`, se emitirá un mensaje y no se realizará ninguna copia de seguridad.

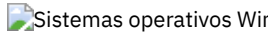
## Clientes soportados

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para AIX, Linux x86\_64, Linux on POWER y Solaris. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

Esta opción es válida para todos los clientes Windows soportados. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el recuadro Copia de seguridad > Dominio para copia de seguridad en el Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el recuadro Copia de seguridad > Dominio para copia de seguridad en el Editor de preferencias.

## Sintaxis

```
-----  
v          |  
>>-DOMAIN . IImage-----<<  
      '-domain-'
```

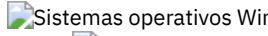

## Parámetros

domain

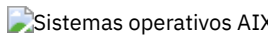

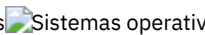
Define los sistemas de archivos o volúmenes lógicos RAW que deben incluirse en el dominio de imagen de cliente predeterminado.

## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris domain.image /fs1 /fs2

 Sistemas operativos Windows Archivo de opciones:  
 Sistemas operativos Windows domain.image d: e: f: domain.image f:\mnt\raw\rawmnt1 f:\mnt\fs\fsmnt1

Línea de mandatos:  
No se aplica.

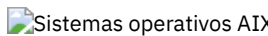
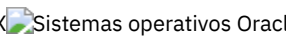
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

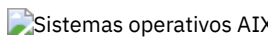
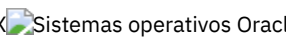
## Domain.nas

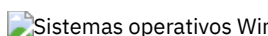
La opción domain.nas especifica los volúmenes que deben incluirse en las copias de seguridad de imagen de NAS.


Puede especificar all-nas para incluir todos los sistemas de archivos montados en el servidor de archivos NAS a excepción de los sistemas de archivos que excluya con la opción exclude.fs.nas.


El cliente de copia de seguridad y archivado utiliza su dominio para copia de seguridad de imágenes NAS cuando ejecuta un mandato backup nas y no especifica los volúmenes que deben procesarse.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Cuando utiliza esta opción en el archivo de opciones del sistema cliente (dsm.sys), la opción domain.nas define el dominio predeterminado para las copias de seguridad de imágenes NAS. Cuando realiza una copia de seguridad de imágenes del sistema de archivos NAS con el mandato backup nas, el cliente añadirá los volúmenes que se especifiquen en la línea de mandatos a los volúmenes definidos en el archivo dsm.sys. Por ejemplo, si especifica domain.nas nas1/vol/vol0 nas1/vol/vol1 en el archivo dsm.sys y especifica dsms backup nas -nasnodename=nas1 /vol/vol2 en la línea de mandatos, el cliente realizará la copia de seguridad de los volúmenes vol/vol0, vol/vol1 y vol/vol2 en el nodo nas1.



 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Si establece la opción domain.nas en all-nas en el archivo dsm.opt, el cliente realizará la copia de seguridad de todos los volúmenes montados en el servidor de archivos NAS. Cuando realiza una copia de seguridad, si utiliza una especificación de archivo y establece la opción domain.nas en all-nas en el archivo dsm.sys, all-nas tendrá prioridad.


 Sistemas operativos Windows Cuando utiliza esta opción en el archivo de opciones del sistema cliente (dsm.opt), la opción domain.nas define el dominio predeterminado para las copias de seguridad de imagen NAS.

 Sistemas operativos Windows Cuando realiza una copia de seguridad de imagen del sistema de archivos NAS mediante la utilización del mandato `backup nas`, el cliente añade los volúmenes que especifica en la línea de mandatos a los volúmenes que se han definido en el archivo `dsm.opt`. Por ejemplo, si especifica `domain.nas nas1/vol/vol0 nas1/vol/vol1` en el archivo `dsm.opt` y especifica `dsmc backup nas -nasnodename=nas1 /vol/vol2` en la línea de mandatos, el cliente realizará la copia de seguridad de los volúmenes `vol/vol0`, `vol/vol1` y `vol/vol2` en el nodo `nas1`.



 Sistemas operativos Windows Si establece la opción `domain.nas` en `all-nas` en el archivo `dsm.opt`, el cliente realizará la copia de seguridad de todos los volúmenes montados en el servidor de archivos NAS. Cuando realiza una copia de seguridad, si utiliza una especificación de archivo y establece la opción `domain.nas` en `all-nas` en el archivo `dsm.opt`, `all-nas` tendrá prioridad.

## Clientes soportados

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción solo es válida para los clientes AIX y Solaris. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

```
.- -----  
V .-all-nas- |  
>>-DOMAIN.Nas-----<<  
      '-domain--'
```

## Parámetros

`domain`

Define los volúmenes que desea procesar. No es posible excluir volúmenes especificando el operador del guión (-).

`all-nas`

Procesa todos los volúmenes montados en el servidor de archivos NAS, excepto aquellos que se excluyan con la opción `exclude.fs.nas`. Éste es el valor predeterminado. Si no existe ninguna sentencia `domain.nas` en el archivo `dsm.opt` y no se ha especificado ningún volumen en la línea de mandatos, el cliente realizará la copia de seguridad de todos los volúmenes montados en el servidor NAS.

## Ejemplos

Archivo de opciones:

```
domain.nas nas1/vol/vol0 nas1/vol/vol1  
domain.nas all-nas
```


Línea de mandatos:

No se aplica.

 Sistemas operativos Linux  Sistemas operativos Windows

## Domain.vmfull

La opción `domain.vmfull` especifica las máquinas virtuales (VM) a incluir en las operaciones de copia de seguridad de imagen de máquina virtual completa.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

Esta opción se aplica a discos de máquina virtual Microsoft Hyper-V y VMware.

 Sistemas operativos Linux  Sistemas operativos Windows

## Domain.vmfull para máquinas virtuales VMware

Para copias de seguridad de máquinas virtuales VMware, la opción domain.vmfull funciona con la opción vmchost. La opción vmchost identifica el servidor vCenter o ESX que contiene las máquinas virtuales que desea proteger. Los parámetros de domain.vmfull se utilizan para centrarse en una operación en un subconjunto de máquinas virtuales que se ejecuten en el sistema identificado por vmchost.


Puede especificar qué máquinas virtuales se procesarán con alguna de las técnicas siguientes:


- Utilice la opción VM= y especifique el nombre de una máquina virtual.
- Proporcione una lista separada por comas de nombres de máquinas virtuales.
- Utilice la sintaxis de comodín para procesar las máquinas virtuales que coinciden con el patrón de nombre.
- Utilice uno de los siguientes parámetros de dominio-nivel:
  - all-vm
  - all-windows
  - schedule-tag
  - vmhost
  - vmfolder
  - vmhostcluster
  - vmdatstore
  - vmresourcepool
  - vmhostfolder
  - vmdatacenter

Al utilizar parámetros de dominio-nivel, las máquinas creadas en el dominio se incluyen automáticamente cuando se produce la siguiente copia de seguridad. Por ejemplo, si utiliza el parámetro vmfolder para realizar una copia de seguridad de todas las máquinas virtuales incluidos en una carpeta, las máquinas virtuales nuevas añadidas a dicha carpeta se incluirán en la siguiente copia de seguridad. Esto también se aplica a los nombres de patrón coincidente que se incluyen en una coincidencia comodín.

Las máquinas virtuales especificadas en la opción domain.vmfull se procesan sólo cuando el mandato backup vm se emite sin especificar una máquina virtual o una lista de máquinas virtuales en la línea de mandatos.

## Clientes soportados

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

El servidor también puede definir esta opción.

## Archivo de opciones

Establezca esta opción en las opciones del cliente, utilizando la línea de mandatos, o mediante el separador Copia de seguridad de máquina virtual del editor de preferencias.

Restricción: No puede establecerse los parámetros siguientes en el Editor de preferencias. Incluya este valor en el archivo de opciones, o en la línea de mandatos al ejecutar un mandato backup vm:

- *nombre\_máquina\_virtual:vmrk=etiqueta\_vmrk*
- schedule-tag
- vmresourcepool
- vmhostfolder
- vmdatacenter

## Sintaxis para máquinas virtuales VMware

```
.-;-----  
V .-vmname1,vmname2-----  
>>-DOMAIN.VMFull-----+-----+>>  
+-VM=vmname1,vmname2-----+  
+- -VM=vmname1,vmname2-----+  
+-ALL-VM-----+  
+-ALL-WINDOWS-----+  
+-SCHEDULE-TAG-----+  
+-VMHost=srv1,srv2-----+  
+-VMFolder=foldername1, foldername2-----+  
+-VMHOSTCLUSTER=cluster1,cluster2-----+  
+-VMDATASTORE=datastore1,datastore2-----+
```

```

+-VMRESOURCEPOOL=resourcepool1,resourcepool2-+
+-VMHOSTFOLDER=hostfolder1,hostfolder2-----+
'-VMDATACENTER=datacenter1,datacenter2-----'

```

Normas de sintaxis: Varias palabras clave deben estar separadas por punto y coma. No incluya espacios detrás de los signos de punto y coma. Si hay varios nombres de máquina virtual o dominio deben ir separados por comas, sin caracteres de espacio. Por ejemplo, consulte `vm=vmname`. La regla sobre varios nombres de dominio o máquina virtual no se aplica si se utiliza la palabra clave "Schedule-Tag".

## Parámetros

### *nombre\_máquina\_virtual*

Especifica el nombre de máquina virtual que se quiere procesar. Nombre en pantalla de la máquina virtual. Puede especificar una lista de nombres de host de máquinas virtuales separando los nombres con comas (`vm1, vm2, vm5`).

### *vm=nombre\_máquina\_virtual*

La palabra clave `vm=` especifica que el siguiente conjunto de valores es una lista de nombres de máquina virtual. La palabra clave `vm=` es el valor predeterminado y no es obligatorio.

En este ejemplo, `vm=` no está especificado y las comas se utilizan para separar los nombres de máquina.

```
domain.vmfull my_vm1,my_vm2
```

Si especifica varias palabras clave, como por ejemplo, `vm=` y `vmfolder=`, los valores a los que hagan referencia deberán separarse por puntos y comas, sin caracteres de espacio:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull vm=my_vm1;vmfolder=folder1;vmfolder=folder2
```

Se pueden utilizar caracteres comodín para seleccionar nombres de máquina virtual que coincidan con un patrón. Un asterisco (\*) coincide con cualquier secuencia de caracteres. El signo de interrogación (?) coincide con cualquier carácter único, por ejemplo:

- Excluir todos los archivos que tengan "test" en el nombre de host: `-vm=*test*`
- Incluir todas las máquinas virtuales con nombres como: "test20", "test25", "test29", "test2A": `vm=test2?`

Puede excluir una máquina virtual de una operación de copia de seguridad especificando el operador `excluye (-)` antes de la palabra clave `vm=`. Por ejemplo, `-vm` se utiliza para excluir una máquina o varias máquinas determinadas, desde una copia de seguridad de nivel de dominio como, por ejemplo, ALL-Windows, ALL-VM y VMFolder. Si "vm1" es el nombre de una máquina virtual en una carpeta denominada "accountingDept", podrá realizar copia de seguridad de todas las máquinas virtuales de la carpeta pero impedir que se realice copia de seguridad de la máquina virtual "vm1". Establezca la siguiente opción:

```
domain.vmfull VMFolder=accountingDept;-vm=vm1
```

No podrá usar el operador `excluye (-)` para excluir un dominio como, por ejemplo, ALL-VM, ALL-Windows o VMFolder. El operador `excluye` funciona sólo en el nivel de nombre de máquina virtual.

### *nombre\_máquina\_virtual:vmdk=etiqueta\_vmdk*

La palabra clave `:vmdk=` sólo se aplica a máquinas virtuales VMware y su uso requiere una licencia para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción suele utilizarse para excluir discos (consulte la sintaxis `:vmdk`) de realizar copia de seguridad. También puede incluir discos de máquina virtual mediante la utilización de la opción `INCLUDE.VMDISK` o excluir discos de máquina virtual mediante la utilización de la opción `EXCLUDE.VMDISK`.

Los discos virtuales dentro de una máquina virtual tienen etiquetas de disco que identifican de forma exclusiva cada disco virtual. Utilice la palabra clave `:vmdk=` para especificar las etiquetas de los discos virtuales que desea incluir en la operación Backup VM. Si no especifica `:vmdk=` y una etiqueta de disco, se realizará una copia de seguridad de todos los discos virtuales en la máquina virtual.

Supongamos que hay una máquina virtual denominada "mi\_ejemplo\_de\_máquina\_virtual". Esta máquina virtual tiene cuatro discos (con la etiqueta `Hard Disk 1`, `Hard Disk 2`, `Hard Disk 3`, `Hard Disk 4`). Para incluir solo el disco duro 2 y el disco duro 3 en una copia de seguridad, añada la palabra clave `:vmdk=` y la etiqueta de disco para esos discos. Las comillas son necesarias alrededor de los parámetros porque las etiquetas de disco contienen caracteres de espacio. Por ejemplo:

```
domain.vmfull "my_vm_example:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

El ejemplo siguiente realiza una copia de seguridad del disco duro 1 y el disco duro 2 en VM1, y del disco duro 3 y el disco duro 4 en VM2. Se utiliza una coma para separar la información de la máquina virtual.

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2",
"vm2:vmdk=Hard Disk 3:vmdk=Hard Disk 4"
```

Al igual que con la palabra clave `-vm=`, también puede usar el operador de exclusión (`-`) con `:vmdk=` para excluir discos de una operación de copia de seguridad.

Para realizar una copia de seguridad de una máquina virtual (vm1) y excluir los discos 3 y 4, utilice la sintaxis siguiente:

```
domain.vmfull "vm1:-vmdk=Hard Disk 3:-vmdk=Hard Disk 4"
```

Para realizar una copia de seguridad dos máquinas virtuales, vm1 y vm2, y excluir a los dos primeros discos en cada máquina, utilice la sintaxis siguiente:

```
domain.vmfull "vm1 :-vmdk=Hard Disk 1:-vmdk=Hard Disk 2",  
"vm2:-vmdk=Hard Disk 1:-vmdk=Hard Disk 2"
```

Puede incluir uno o más discos en una sentencia `domain.vmfull`. Puede excluir uno o más discos en una sentencia `domain.vmfull`. Puede combinar discos de inclusión y exclusión en la misma sentencia. Por ejemplo, la siguiente sentencia es válida:

```
domain.vmfull  
"vm1:vmdk=Hard Disk 1:-vmdk=Hard Disk 2:vmdk=Hard Disk 3:vmdk:Hard Disk 4"
```

Si está presente una sentencia de inclusión, el resto de los discos de la máquina virtual se excluyen de una operación de copia de seguridad, a menos que el resto de los discos también se especifiquen en una sentencia de inclusión. Por ejemplo, la sentencia siguiente excluye todos los discos duros en vm1, excepto para el disco duro 1:

```
domain.vmfull "vm1:vmdk=Hard Disk 1"
```

Los dos siguientes excluyen el disco duro 4 de una copia de seguridad de vm1:

```
domain.vmfull "vm1:vmdk=Hard Disk 1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"  
domain.vmfull "vm1:-vmdk=Hard Disk 4"
```

#### all-vm

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmchost`.

#### all-windows

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmchost`. Las máquinas virtuales también deben tener un tipo de sistema operativo invitado de Windows.

#### schedule-tag

Para copias de seguridad planificadas de máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción `vmchost`.

El administrador del servidor de IBM Spectrum Protect puede añadir esta opción a una definición de planificación para indicar que la planificación es compatible con el código y la categoría `Schedule` (IBM Spectrum Protect). La copia de seguridad de las máquinas virtuales en objetos de VMware a las que se haya asignado el código `Schedule` se ejecutará siguiendo la planificación.

Requisito: Para posibilitar la compatibilidad con los códigos, la opción `-domain.vmfull` no puede contener ningún parámetro adicional a nivel de dominio, aparte del parámetro `Schedule-Tag` de la definición de planificación. En caso contrario, se omite el código `Schedule` (IBM Spectrum Protect). La opción no distingue entre mayúsculas y minúsculas y no puede contener espacios. El entrecomillado del parámetro `Schedule-Tag` es opcional. No se efectúan copias de seguridad de las máquinas virtuales en contenedores de VMware que se han codificado con planificaciones incompatibles.

Si desea más información sobre el código `Planificar`, consulte "Códigos de protección de datos soportados".

#### vmhost=*hostname*

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmchost`. El nombre de host que especifique debe coincidir con el nombre completo de host o dirección IP, ya que se especifica en la vista Hosts y clústeres del servidor vCenter.

Todas las máquinas virtuales que se añaden a este host se incluyen automáticamente en el proceso de copia de seguridad y de restauración. Para hacer una inclusión, las máquinas virtuales también deben estar ejecutándose en el servidor ESX especificado por el nombre de host; no se pueden desconectar.

Este parámetro puede incluir varios servidores ESX que están separados por comas. Cuando el Centro virtual contiene varios servidores ESX, esta opción no determina el servidor ESX a partir del que se toma una instantánea. El servidor ESX a partir del cual se toma una instantánea está determinado por el servicio Web de VMware VirtualCenter.

Cuando se conecta directamente a un host ESX o ESXi, la opción `vmchost` solo se aplica si el `vmhost` es el servidor al que se conecta. De no serlo, se emite un mensaje de advertencia en la consola y este se registra en el archivo `dsmerror.log`; también se registrará como mensaje de suceso del servidor.

Si la opción `vmenabletemplatebackups` se establece en `yes` y las plantillas de VM son parte del dominio, están incluidos en la copia de seguridad.

Restricción: No se puede realizar copia de seguridad de las plantillas de VMware para máquinas virtuales cuando están en un host ESX o ESXi porque los hosts ESX y ESXi no soportan plantillas.

`vmfolder=foldername`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmhost`. Las máquinas virtuales también deben existir en la carpeta VMware especificada por el nombre de la carpeta. El nombre de carpeta puede incluir varias carpetas de VMware que estén separadas por comas.

`vmhostcluster=hostclustername`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmhost`. Las máquinas virtuales también deben estar ejecutándose en el servidor ESX especificado por el nombre de clúster del host. Para incluir más de un nombre de clúster de host, separe los nombres de clúster con comas: `VMHOSTCLUSTER=cluster1,cluster2`.

Si la opción `vmenabletemplatebackups` se establece en `yes` y las plantillas de VM son parte del dominio, están incluidos en la copia de seguridad. Un clúster del host de VMware no está disponible si se conecta directamente a un host ESX o ESXi. Si se conecta directamente a un host ESXi/ESX y se procesa un dominio que incluye un clúster de host, se emite un mensaje de nivel de aviso en la consola y dicho mensaje se registra en el archivo `dsmerror.log`; también se registra como un mensaje de suceso de servidor.

`vmdatastore=datastorename`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el Virtual Center o el servidor ESX especificadas en la opción `vmhost`. La ubicación del almacén de datos configurado de una máquina virtual debe coincidir con el nombre del almacén de datos especificado por `datastorename`. El nombre de almacén de datos puede incluir varios almacenes de datos separados por comas: `VMDATASTORE=datastore1,datastore2`

Las máquinas virtuales pueden tener su disco (archivos `vmdk`) en más de un almacén de datos; pero sólo existe una ubicación de almacén de datos predeterminada. Esta ubicación de almacén de datos predeterminada está definida en la configuración de máquina virtual y es siempre la ubicación del archivo de configuración de máquina virtual (archivo `.vmx`). Cuando una máquina se selecciona para la copia de seguridad utilizando una palabra clave de dominio, el archivo de configuración de máquina virtual, y todos los discos de la máquina virtual se incluyen en la copia de seguridad, también los discos que estén en un almacén de datos diferente al especificado como el dominio.

`vmresourcepool=resourcepoolname`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción `vmhost`. Las máquinas virtuales también deben existir en la agrupación de recursos de VMware especificada por el nombre de la agrupación de recursos. El nombre de la agrupación de recursos puede incluir varias agrupaciones de recursos separadas por comas, por ejemplo: `VMRESOURCEPOOL=resourcepool1,resourcepool2`

`vmhostfolder=hostfoldername`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción `vmhost`. Las máquinas virtuales también deben existir en la carpeta de host de VMware que especifica el nombre de la carpeta de host. El nombre de carpeta de host puede incluir varias carpetas de host de VMware separadas con comas, por ejemplo: `VMHOSTFOLDER=hostfolder1,hostfolder2`

`vmdatacenter=datacentername`

Para máquinas virtuales VMware. Esta opción procesa todas las máquinas virtuales definidas para el servidor de Virtual Center especificado en la opción `vmhost`. Las máquinas virtuales también deben existir en el centro de datos de VMware especificado por el nombre del centro de datos. El nombre del centro de datos puede incluir varios centros de datos separados con comas, por ejemplo: `VMDATACENTER=datacenter1,datacenter2`

Consejo: Si especifica más de un tipo de contenedor, por ejemplo, `vmfolder=folder1` y `vmhostcluster=cluster2`, se protegerán todas las máquinas virtuales que estén contenidas en `folder1` y `cluster2`. Las máquinas virtuales no tienen que estar ubicadas tanto en `folder1` como en `cluster2`.

Puede especificar las máquinas virtuales como se muestra en este ejemplo:

```
domain.vmfull=vmfolder=folder1;vmhostcluster=cluster2
```

## Ejemplos para máquinas virtuales VMware

---

Archivo de opciones:

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull all-vm
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, excepto las que tengan el sufijo `_test` en el nombre.

```
domain.vmfull all-vm;-vm=*_test
```



Incluir todas las máquinas virtuales que tienen Windows como sistema operativo, en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull all-windows
```

Incluir todas las máquinas virtuales en servidores de clúster 1, 2 y 3 en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhostcluster=cluster1,cluster2,cluster3
```

Incluir todos los datos de máquina virtual en `datastore1` en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmdatastore=datastore1
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, pero excluir las máquinas virtuales `testvm1` y `testvm2`.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Incluir las máquinas virtuales que se definen en las carpetas de máquina virtual que se denominan `lab1` y `lab2` en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmfolder=lab1,lab2
```

Incluir todas las máquinas virtuales en los hosts ESX denominados "brovar", "doomzoo", y "kepler" en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhost=brovar.example.com,
doomzoo.example.com,kepler.example.com
```

Incluya las máquinas virtuales en las agrupaciones de recursos VMware `resourcepool_A` y `resourcepool_B` en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmresourcepool=resourcepool_A,resroucepool_B
```

Incluya las máquinas virtuales que están definidas en las carpetas de host de VMware llamadas `hostfolder1` y `hostfolder2` en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmhostfolder=hostfolder1,hostfolder2
```

Incluya todas las máquinas virtuales en el centro de datos VMware `dc1` en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull vmdatacenter=dc1
```



Sistemas operativos Windows

## Domain.vmfull para máquinas virtuales de Microsoft Hyper-V

Para copias de seguridad de máquina virtual Hyper-V, utilice la opción `domain.vmfull` para especificar qué máquinas virtuales Hyper-V se procesan cuando se ejecuta un mandato `backup vm`, sin especificar ningún nombre de máquina virtual Hyper-V.

Puede especificar qué máquinas virtuales se deben procesar utilizando cualquiera de las técnicas siguientes:

- Utilice la opción `VM=` y especifique el nombre de una máquina virtual.
- Proporcione una lista separada por comas de nombres de máquinas virtuales.
- Utilice la sintaxis de comodín para procesar las máquinas virtuales que coinciden con el patrón de nombre.
- Utilice la opción `nombremv:vhdX=` para especificar el disco duro de máquina virtual (VHDX) a incluir o excluir durante la operación de copia de seguridad de Hyper-V RCT de una máquina virtual.
- Utilice el parámetro de nivel de dominio `all-vm`. También puede incluir una o más máquinas virtuales utilizando la palabra clave `VM=` o excluir máquinas virtuales utilizando la sintaxis `-VM=`.

Las máquinas virtuales especificadas en la opción `domain.vmfull` se procesan sólo cuando el mandato `backup vm` se emite sin especificar una máquina virtual o una lista de máquinas virtuales en la línea de mandatos.

Atención: Para operaciones Microsoft Hyper-V, el único parámetro de nivel de dominio válido para la opción `domain.vmfull` es `all-vm`. También puede incluir una o más máquinas virtuales utilizando la palabra clave `VM=`, o excluir máquinas virtuales con la sintaxis `-VM=`.

## Clientes soportados

Esta opción puede utilizarse con clientes Windows soportados. Esta opción también puede definirse en el servidor.

## Archivo de opciones

Establezca esta opción en las opciones del cliente, utilizando la línea de mandatos, o mediante el separador Copia de seguridad de máquina virtual del editor de preferencias.

Restricción: El parámetro `vmname:vhdX=vhdX_location` no puede establecerse en el editor de preferencias. Incluya este valor en el archivo de opciones, o en la línea de mandatos al ejecutar un mandato backup vm:

## Sintaxis para máquinas virtuales Microsoft Hyper-V

```
.-;-----.
V .-vmname1,vmname2-----|
>>-DOMAIN.VMFull-----+----->>
+-VM=vmname1,vmname2-----+
+- -VM=vmname1,vmname2-----+
+-vmname:vhdX=disk_location---+
+- -vmname:vhdX=disk_location+
'-ALL-VM-----'
```

Normas de sintaxis: Varias palabras clave deben estar separadas por punto y coma. No puede haber espacios después de puntos y comas. Si hay varios nombres de máquina o dominio deben ir separados por comas, sin caracteres de espacio. Para obtener ejemplos, consulte `vm=vmname`.

## Parámetros

### *nombre\_máquina\_virtual*

Define el nombre de máquina virtual que se desea procesar. Puede proporcionar una lista de nombres de host de máquinas virtuales separando los nombres con comas (`vm1, VM2, Vm5`). Los nombres son sensibles a las mayúsculas y minúsculas y deben coincidir con las mayúsculas y minúsculas que se muestran en el host Hyper-V en la vista Hyper-V Manager > Máquinas virtuales.

### *vm=nombre\_máquina\_virtual*

La palabra clave `vm=` especifica que el siguiente conjunto de valores es una lista de nombres de máquina virtual. La palabra clave `vm=` es el valor predeterminado y no es obligatorio.

En este ejemplo, `vm=` no está especificado y las comas se utilizan para separar los nombres de máquina.

```
domain.vmfull my_vm1,my_vm2
```

Si especifica varias palabras clave, por ejemplo `vm=` y `-vm=`, los valores a los que hacen referencia las palabras clave deben estar separados por un punto y coma, sin caracteres de espacio intercalado:

```
domain.vmfull vm=my_vm1;vm=my_vm2
domain.vmfull -vm=my_vm3;-vm=my_vm4
```

Se pueden utilizar caracteres comodín para seleccionar nombres de máquina virtual que coincidan con un patrón. Un asterisco (\*) coincide con cualquier secuencia de caracteres. El signo de interrogación (?) coincide con cualquier carácter único, por ejemplo:

- Excluir todos los archivos que tengan "test" en el nombre de host: `-vm=*test*`
- Incluir todas las máquinas virtuales con nombres como: "test20", "test25", "test29", "test2A":

```
vm=test2?
```

Puede excluir una máquina virtual de una operación de copia de seguridad especificando el operador `excluye (-)` antes de la palabra clave `vm=`. Por ejemplo, se utiliza `-vm` para excluir una determinada máquina o máquinas, desde una copia de seguridad de nivel de dominio, como por ejemplo, `ALL-VM`. Si "vm1" es el nombre de una máquina virtual, podrá realizar copia de seguridad de todas las máquinas virtuales del dominio, pero impedir que se realice copia de seguridad de la máquina virtual "vm1".

Establezca la siguiente opción:

```
domain.vmfull all-vm;-vm=vm1
```

No puede utilizar el operador de exclusión (-) para excluir un dominio, como por ejemplo `ALL-VM`. El operador `excluye` funciona sólo en el nivel de nombre de máquina virtual.

### *nombre\_máquina\_virtual:vhdX=ubicación\_vhdX*

Esta opción especifica la ubicación del disco duro de máquina virtual (VHDX) a incluir en las operaciones de copia de seguridad de máquina virtual Hyper-V RCT en el sistema operativo Windows Server 2016.

La variable *nombre\_máquina\_virtual* especifica el nombre de la máquina virtual de la que debe hacerse copia de seguridad. Se pueden utilizar caracteres comodín para seleccionar nombres de máquina virtual que coincidan con un patrón. Un asterisco (\*) coincide con cualquier secuencia de caracteres. El signo de interrogación (?) sustituye a cualquier carácter separado.

La palabra clave `:vhdx=ubicación_disco` especifica la ubicación del disco de máquina virtual que debe incluirse en la operación de copia de seguridad. La ubicación de disco especificada por la variable `ubicación_disco` debe empezar por "SCSI" o "IDE" seguido del número de controlador y el número de ubicación de dispositivo. Por ejemplo:

```
domain.vmfull "vm1:VHDX=IDE 1 0"  
domain.vmfull "vm*:VHDX=SCSI 0 1"  
domain.vmfull "vm?:VHDX=SCSI 0 1"
```

Puede excluir una máquina virtual de las operaciones de copia de seguridad especificando el operador de exclusión (-) antes de la palabra clave `vhdx=`. Por ejemplo, utilice `-vhdx=` para excluir un disco de VM de una operación de copia de seguridad de una máquina virtual. Por ejemplo:

```
domain.vmfull "vm1:-VHDX=IDE 1 0"
```

Si especifica varios discos de máquina virtual para incluir o excluir, la palabra clave `vhdx=` o `-vhdx=` y los valores asociados deben separarse con signos de dos puntos sin caracteres de espacio. Por ejemplo:

```
domain.vmfull "vm1:vhdx=IDE 1 0:vhdx=SCSI 0 1"
```

Si especifica varios nombres y discos de máquina virtual, el nombre de la VM y los valores asociados deben separarse con signos de punto y coma sin caracteres de espacio. Por ejemplo:

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"  
domain.vmfull "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

#### all-vm

Esta opción especifica que una operación `backup vm` procesa todas las máquinas virtuales Hyper-V que conoce el host Hyper-V.

## Ejemplos de máquinas virtuales Microsoft Hyper-V

---

#### Archivo de opciones:

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa.

```
domain.vmfull all-vm
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, excepto las que tengan el sufijo `_test` en el nombre.

```
domain.vmfull all-vm;-vm=*_test
```

Incluir todas las máquinas virtuales en operaciones de copia de seguridad de máquina virtual completa, pero excluir las máquinas virtuales `testvm1` y `testvm2`.

```
domain.vmfull all-vm;-VM=testvm1,testvm2
```

Incluir los discos IDE (con el controlador 1 y la ubicación de disco 0) y los discos SCSI (con el controlador 0 y la ubicación de disco 1) en las operaciones de copia de seguridad de Hyper-V RCT de las máquinas virtuales `vm1` y `vm2`.

```
domain.vmfull "vm1:VHDX=IDE 1 0:VHDX=SCSI 0 1;vm2:VHDX=IDE 1 0:VHDX=SCSI 0 1"
```

Restricción: No puede utilizar la opción `all-vm` junto con la opción `nombremv:-vhdx=` en el archivo de opciones o en la línea de mandatos.



Sistemas operativos Linux

## Dontload

---

Los clientes Linux `x86_64` pueden utilizar la opción `dontload` para evitar que se carguen las bibliotecas de plug-in específicas cuando se inicia el cliente de copia de seguridad-archivado.

El paquete `TIVsm_BAhdw.x86_64` incluido en distribuciones Linux `x86_64` contiene software necesario para dar soporte a las copias de seguridad incrementales de instantáneas para servidores de archivos NetAPP y N-Series. Si este paquete está instalado en un sistema Linux `x86_64` que se utiliza para ejecutar operaciones de transportador de datos para una máquina virtual, los archivos de este paquete hacen que fallen todas las operaciones de seguridad de VMware. Cuando se producen estos errores, aparece el siguiente mensaje:

```
ANS8811E
```

No pueden ejecutarse operaciones VMware cuando el producto de plug-in de hardware `TIVsm-BAhdw` está instalado y cargado. Desinstale el producto de hardware `TIVsm-BAhdw` o establezca la opción `DONTLOAD PIHDW` en el archivo de opciones para evitar que se cargue el plug-in de hardware.

Utilice esta opción para evitar que la biblioteca de plugins se cargue en la RAM cuando se inicie el cliente. Como alternativa, puede desinstalar el paquete TIVsm\_BAhdw si no es necesario para operaciones de instantánea.

## Clientes soportados

---

Esta opción sólo es válida para clientes de Linux x86\_64.

## Archivo de opciones

---

Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

## Sintaxis

---

```
>>-DONTLoad----PIHDW-----<<
```

## Parámetros

---

### PIHDW

Especifica que el plug-in de hardware (TIVsm-BAhdw) no está cargado en la RAM cuando se inicia el cliente. Utilice esta opción en clientes de copia de seguridad-archivado que tengan el plug-in de hardware instalado para evitar que el plug-in provoque anomalías al realizar operaciones de copia de seguridad-archivado en máquinas virtuales de VMware. No existe un valor predeterminado para la opción dontload.

Para determinar si está instalado el plug-in, escriba el siguiente mandato y examine el resultado.

```
rpm -q -a | grep TIV
```

Si el resultado contiene un paquete que empieza por "TIVsm-BAhdw" (seguido por una serie de versión), el paquete de plug-in de hardware está instalado.

## Ejemplos

---

Archivo de opciones:

```
DONTLoad PIHDW
```




Línea de mandatos:

No se aplica. No utilice esta opción en la línea de mandatos.

### Referencia relacionada:

[Backup VM](#)

[Restore VM](#)

 [Sistemas operativos AIX](#)  [Sistemas operativos Linux](#)  [Sistemas operativos Oracle Solaris](#)

## Dynamicimage

---

Utilice la opción dynamicimage con el mandato backup image o la opción include.image para especificar que desea realizar una copia de seguridad de imagen dinámica.

## Clientes soportados

---

Esta opción es válida para los clientes AIX, Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Establezca la sentencia include.image que contiene el valor dynamicimage en la sección del servidor en el archivo de opciones del sistema, dsm.sys. También puede establecer esta opción mediante el editor de preferencias.

## Sintaxis

---

```
>>-DYNAMICImage-- --value-----<<
```

## Parámetros

---

value

Especifique uno de los valores siguientes:

sí

Utilice esta opción sólo si el volumen no puede desmontarse y volverse a montar en modo de sólo lectura. El cliente realiza una copia de seguridad del volumen tal cual, sin volver a montarlo en modalidad de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones escriben datos en el volumen mientras se está realizando la copia de seguridad. En tal caso, ejecute fsck después de una restauración y monte manualmente el sistema de archivos para volver a obtener acceso al volumen. Esta opción es válida para los clientes AIX, Solaris y todos los de Linux.

Nota: Esta opción es válida para los sistemas de archivos JFS2 de AIX.

no

Utilice esta opción si no desea realizar una copia de seguridad de imagen dinámica. Éste es el valor predeterminado. El comportamiento predeterminado depende del tipo del sistema de archivos y la plataforma. En el caso de plataformas y sistemas de archivos que admitan instantáneas, es decir los sistemas de archivos JFS2 de AIX y los sistemas de archivos LVM de LINUX, el valor predeterminado es la copia de seguridad basada en instantánea. Para las demás plataformas y los demás sistemas de archivos UNIX, el valor predeterminado es la copia de seguridad de imágenes estática.

## Ejemplos


---

Archivo de opciones:

```
include.image /kalafsl dynamicimage=yes
```

Línea de mandatos en la imagen de copia de seguridad:

```
dynamicimage=yes
```

 Sistemas operativos AIX

## Efsdecrypt

---

La opción `efsdecrypt` permite controlar si los archivos cifrados mediante un sistema de archivos cifrados (EFS) de AIX se leen con formato cifrado o descifrado.

El valor predeterminado de la opción `efsdecrypt` es `no`, lo cual significa que se ha de hacer la copia de seguridad de los datos cifrados o RAW. Si especifica `yes`, se hace copia de seguridad de los archivos como texto legible, lo que significa que se hace la copia de seguridad como archivos normales, como si los archivos existieran en formato no cifrado en el sistema de archivos.

**Importante:** siempre que ejecute una copia de seguridad que incluya archivos cifrados en un EFS, debe asegurarse de que utiliza la especificación correcta de la opción `efsdecrypt`. Si el valor de la opción `efsdecrypt` cambia entre las dos copias de seguridad incrementales, se volverá a realizar una copia de seguridad de todos los archivos cifrados de los sistemas de archivos EFS, incluso si no se han modificado desde la última copia de seguridad. Por ejemplo, si ejecuta una copia de seguridad incremental de archivos cifrados de los que anteriormente había hecho una copia de seguridad como "raw", debe asegurarse de que `efsdecrypt` se ha especificado como `no`. Si cambia el valor de `efsdecrypt` a `yes`, se volverá a realizar una copia de seguridad de todos los archivos en texto legible incluso si no se han modificado, así que asegúrese de utilizar esta opción cuidadosamente.

Nota: Ésta es una opción global que se aplica a toda la copia de seguridad. Se exigen dos invocaciones independientes del cliente para hacer copia de seguridad de los archivos cifrados como datos raw y de los otros como texto legible.

## Clientes soportados

---

Esta opción es válida para los clientes AIX.

## Archivo de opciones

---

Establezca esta opción en el archivo `dsm.sys` o el archivo de opciones del usuario cliente (`dsm.opt`). En el archivo `dsm.sys`, debe colocar esta opción dentro de una stanza de servidor.

## Sintaxis

---

```
>>-EFSDecrypt--+-No-->
                  |-----|-----><
                  '-Yes-'
```

## Parámetros

---



nombre corto no se ha podido establecer. Si el archivo debe restaurarse con su nombre corto original, tendrá que resolver el conflicto con el archivo existente y, a continuación, volver a intentar la restauración.

Importante: Este parámetro puede ocasionar resultados inesperados en algunos casos. Por ejemplo, si el nombre corto de un archivo se modifica entre la última vez en que se ha realizado una copia de seguridad del archivo y el momento en que se ha restaurado y existe un enlace o entrada de registro que hace referencia al nombre corto más reciente, la restauración del archivo con el nombre corto anterior invalidará la referencia al nombre corto más reciente.

## Ejemplos

---

Archivo de opciones:

```
enable8dot3namesupport yes
```

Línea de mandatos:

```
-enable8dot3namesupport=yes
```

## Enablearchiveretentionprotection

---

La opción `enablearchiveretentionprotection` permite al cliente conectarse al servidor de IBM Spectrum Protect for Data Retention. Esto garantiza que los objetos de archivado no se eliminarán del servidor mientras no se cumplan los requisitos de retención basados en políticas de dicho objeto.

Esta opción se ignora si el cliente conecta con un servidor que no está activado para protección de retención. Si la opción es no (valor predeterminado) y se realiza un intento de conexión con un servidor de retención de datos, la conexión se rechazará.

El servidor de retención de datos está especialmente configurado para esta tarea, por lo tanto el servidor rechaza el proceso de copia de seguridad o restauración normal. Cuando el cliente conecta con un servidor de retención de datos, los mandatos siguientes no estarán disponibles. Si intenta utilizar estos mandatos, se mostrará un mensaje que indicará que no son válidos con este servidor.

- incremental
- backup (todos los submandatos)
- selective
- restore (todos los submandatos excepto `restore backupset -location=file` o `-location=tape`)  
Nota: `restore backupset -location=file` o `-location=tape` no conecta con ningún servidor (excepto el virtual) y, por lo tanto, no se bloqueará en ninguna circunstancia.
- restart restore
- delete backup
- delete group
- expire
- Todos los mandatos query, *excepto*:
  - query access
  - query archive
  - query filespace
  - query inclexcl
  - query managementclass
  - query node
  - query options
  - query schedule
  - query session
  - query systeminfo
  - query tracestatus


## Clientes soportados





---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos Windows Esta opción sólo es válida en el archivo de opciones del cliente (`dsm.opt`) y no es válida en un conjunto de opciones del cliente del servidor. No es válida en ninguna línea de mandatos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción sólo es válida en el archivo `dsm.sys`, dentro de una stanza de servidor, y no es válida en un conjunto de opciones del cliente del servidor. No es válida en ninguna línea de mandatos.

## Sintaxis

---

```
..-No--.
>>-ENABLEARCHIVERETENTIONProtection--+-----+-----><
'-Yes-'
```

## Parámetros

---

- No  
Se rechaza el servidor de retención de datos. Éste es el valor predeterminado.
- Yes  
El cliente conecta con un servidor de retención de datos.

## Enablededupcache

---

Utilice la opción `enablededupcache` para especificar si desea utilizar una memoria caché durante la eliminación de duplicados de datos por parte del cliente. El uso de una memoria caché local puede reducir el tráfico de red entre el servidor y el cliente de IBM Spectrum Protect.

Si realiza una copia de seguridad o archivado con la memoria caché de eliminación de duplicados de datos habilitada, la especificación de las extensiones de datos de las que se ha realizado una copia de seguridad o archivado se guarda en la base de datos de la memoria caché. La próxima vez que ejecute una copia de seguridad o archivado, el cliente consultará la memoria caché de la eliminación de duplicados de datos e identificará las extensiones de datos que se han guardado previamente en el servidor. Las extensiones de datos que sean idénticas a las extensiones de datos del servidor no se vuelven a enviar al servidor.

Si el servidor y la memoria caché no están sincronizados, la memoria caché se elimina y se crea una nueva.

Sólo un proceso puede acceder a la memoria caché de la eliminación de duplicados de datos distribuida a la vez. Instancias de copia de seguridad simultáneas en una estación de trabajo, que utiliza el mismo servidor y la misma agrupación de almacenamiento, deben utilizar nombres de nodo únicos o especificaciones de caché únicas. De esta forma, se puede utilizar todas las instancias en una caché local y optimizar la eliminación de duplicados de datos por parte del cliente.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect también soporta esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor. Puede establecer esta opción en la casilla de verificación **Eliminación de duplicados > Habilitar memoria caché para eliminación de duplicados** del editor **Preferencias**. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows  
Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la casilla de verificación **Eliminación de duplicados > Habilitar memoria caché para eliminación de duplicados** del editor **Preferencias**. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
..-Yes*-.
>>-ENABLEDEDUPCache--+-----+-----><
'-No---'
```

## Parámetros

---

- Yes  
Especifica que desea habilitar la memoria caché de eliminación de duplicados de datos. Si no está habilitada la eliminación de duplicados de datos, este valor no es válido. Yes es el valor predeterminado para el cliente de copia de seguridad y archivado. No es el valor predeterminado para la API de IBM Spectrum Protect.
- No  
Especifica que no desea habilitar la memoria caché de eliminación de duplicados de datos.

## Ejemplos

---



Archivo de opciones:  
enablededupcache no  
Línea de mandatos:  
-enablededupcache=no

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

**Referencia relacionada:**

Eliminación de duplicados  
Dedupcachepath  
Dedupcachesize

## Enableinstrumentation

---

De forma predeterminada, el cliente de copia de seguridad y archivado y la API de IBM Spectrum Protect recopilan automáticamente datos de instrumentación para identificar los cuellos de botella de rendimiento durante el proceso de copia de seguridad y restauración. Para inhabilitar o habilitar más tarde la instrumentación, utilice la opción `enableinstrumentation`.

Con esta opción habilitada, no tiene que esperar que representante de atención al cliente se dirija a usted para que recopile datos de rendimiento cuando se produzca un problema. En su lugar, se pueden recopilar datos cada vez que se ejecute una operación de copia de seguridad o restauración. Esta característica pueden ser útil porque no tiene que reproducir el problema para recopilar datos de rendimiento. El cliente ya recopila dicha información.

Esta opción sustituye las opciones `-TESTFLAG=instrument:detail`, `-TESTFLAG=instrument:API` y `-TESTFLAG=instrument:detail/API` utilizadas en las versiones anteriores del cliente y de la API.

Para cada proceso, se recopilan los siguientes tipos de datos de instrumentación de rendimiento:

- Los nombres de actividad de cada hebra (por ejemplo, `File I/O`, `Data Verb`, `Compression` y `Transaction`), el tiempo medio transcurrido por actividad y la frecuencia de la actividad.
- El tiempo total de actividad correspondiente a cada hebra.
- El mandato que se ha emitido y las opciones que se han utilizado.
- El resumen del mandato de copia de seguridad, restauración o consulta.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (`dsminstr.log`) en el directorio que se especifica mediante la variable de entorno `DSM_LOG` (o la variable de entorno `DSMI_LOG` para los productos que dependen de la API como IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server y IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server). Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato `dsmc`).

Si lo desea, puede cambiar el nombre y la ubicación del archivo de registro de instrumentación mediante la opción `instrlogname`. También puede controlar el tamaño del archivo de registro especificando la opción `instrlogmax`.

No se recopilan datos de rendimiento para la GUI de cliente de copia de seguridad y archivado ni para la GUI de cliente web.

Se recopilan datos de rendimiento para cada uno de los siguientes productos cuando se especifica la opción `enableinstrumentation` en el archivo de opciones del cliente:

- Operaciones de copia de seguridad planificadas a nivel de archivo con el cliente de archivado y copia de seguridad
- Copias de seguridad de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware
- Copias de seguridad de IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V
- Copias de seguridad de IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server
- Copias de seguridad de IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server

También se recopilan datos de rendimiento durante el proceso de archivado y recuperación.





## Clientes soportados


---

Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Coloque esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

Consejo: Esta opción está habilitada de forma predeterminada, de forma que, generalmente, no es necesario que coloque esta opción en el archivo de opciones del cliente, a no ser que tenga que inhabilitar la opción.

## Sintaxis

---

```
..-Yes-  
>>-ENABLEINSTRUMENTATION-----<<  
'-No--'
```

## Parámetros

---

### Yes

Especifica que desea recopilar datos de rendimiento durante las operaciones de copia de seguridad y restauración. El valor predeterminado es Yes, lo que significa que se recopilan datos de rendimiento incluso si no especifica esta opción.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (dsminstr.log) en el directorio que se especifica mediante la variable de entorno DSM\_LOG. Si no ha establecido la variable de entorno DSM\_LOG, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato dsmc). Si el archivo no existe, el cliente lo crea y agrega al mismo datos de rendimiento.

### No

Especifica que no desea recopilar datos de rendimiento durante las operaciones de copia de seguridad y restauración. Si el registro de instrumentación ya existe, no se agregan más datos al archivo.





## Ejemplos

---

Archivo de opciones:

```
enableinstrumentation yes
```

Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes
```

 Sistemas operativos Windows

```
dsmc sel c:\mydir\* -subdir=yes -enableinstrumentation=yes
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

### Tareas relacionadas:

Recopilación de datos de instrumentación del cliente

Recopilación de datos de instrumentación de la API

### Referencia relacionada:

Instrlogmax

Instrlogname

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Enablelanfree

---

La opción enablelanfree especifica si debe activarse una vía de acceso disponible sin LAN a un dispositivo de almacenamiento conectado a una red de área de almacenamiento (SAN).

Una vía de acceso sin LAN permite realizar copias de seguridad, restaurar, archivar y recuperar procesos entre el cliente de copia de seguridad y archivado y el dispositivo de almacenamiento conectado a la SAN.

Para admitir el movimiento de datos sin LAN, debe instalar y configurar el IBM Spectrum Protect para el agente de almacenamiento SAN en la estación de trabajo de cliente.




Nota:


1. Si especifica la opción enablelanfree en el archivo de opciones del cliente (dsm.opt), pero se transfirieron cero (0) bytes a través de la SAN durante la operación, no olvide vincular los datos a una clase de gestión que sea sin LAN.
2. Para restaurar los conjuntos de copias de seguridad en un entorno SAN, consulte para obtener información.

3. Cuando una vía de acceso fuera de la LAN está habilitada, los valores SAN Storage Agent sustituyen las opciones del cliente `tcpserveraddress`, `tcpport` y `ssl`. Esta acción de sustitución se produce para garantizar que tanto el cliente como el agente de almacenamiento utilizan las opciones de comunicación del mismo servidor.

## Cientes soportados




---


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción solo es válida para clientes de AIX, Linux x86\_64, Linux on POWER y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. También puede establecer esta opción seleccionando el recuadro de selección **Habilitar fuera de la LAN** en el separador **General** del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). También puede definir esta opción seleccionando la casilla de verificación **Habilitar fuera de la LAN** en el separador **General** del Editor de preferencias.

## Sintaxis

---

```
>>-ENABLELanfree-----><
      .-No--
      +-----+
      '-Yes-'
```

## Parámetros

---

Yes

Especifica que se desea activar una vía de acceso disponible fuera de la LAN a un dispositivo de almacenamiento conectado a una SAN.

No

Especifica que no se desea activar una vía de acceso disponible fuera de la LAN a un dispositivo de almacenamiento conectado a una SAN. Éste es el valor predeterminado.






## Ejemplos

---

Archivo de opciones:  
`enablelanfree yes`

Línea de mandatos:  
`-enablelanfree=yes`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.






 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Encryptiontype

---

Utilice la opción `encryptiontype` para especificar el algoritmo para el cifrado de datos.

La opción `encryptiontype` sólo afecta las operaciones de archivado y copia de seguridad. Los datos que incluya se almacenarán en formato cifrado, y el cifrado no afectará a la cantidad de datos enviados o recibidos. Durante las operaciones de restauración y recuperación, los datos cifrados se descifrarán utilizando el algoritmo de cifrado correcto independientemente del valor de esta opción.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows





## Cientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. También puede establecer esta opción en la ficha Authorization del editor de preferencias.. El servidor puede modificar esto.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). También puede establecer esta opción en la ficha Authorization del editor de preferencias. El servidor puede modificar esto.

## Sintaxis

---

```
. -AES128- .  
>>-ENCRYPTIONType-----+-----<<  
' -AES256- '
```

## Parámetros

---

### AES128

Cifrado de datos AES de 128 bits. El valor predeterminado es AES de 128 bits.

### AES256

Cifrado de datos AES de 256 bits. El cifrado de datos AES de 256 bits proporciona el nivel más alto de cifrado de datos disponible en operaciones de copia de seguridad y archivado.

## Ejemplos

---

Archivo de opciones:

```
encryptiontype aes128
```

Línea de mandatos:


No se aplica.





## Encryptkey

---

El cliente de copia de seguridad y archivado admite la opción que permite cifrar los archivos cuya copia de seguridad o archivado se realiza en el servidor de IBM Spectrum Protect. Esta opción se activa con la opción include.encrypt.

Todos los archivos que coinciden con el patrón de la especificación include.encrypt se cifrarán antes de que los datos se envíen al servidor. Hay tres opciones para gestionar la clave utilizada para cifrar los archivos (solicitar, guardar y generar). Las tres opciones pueden utilizarse con el cliente de copia de seguridad/archivado o con la API de IBM Spectrum Protect.

 Sistemas operativos Windows La contraseña de clave de cifrado es sensible a las mayúsculas, puede tener hasta 63 caracteres de longitud e incluir los caracteres siguientes:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris La contraseña de clave de cifrado distingue entre mayúsculas y minúsculas y puede tener un máximo de 64 caracteres de longitud e incluir los caracteres siguientes:

A-Z

Cualquier letra, de A hasta Z, mayúsculas o minúsculas. No puede especificarlos caracteres de idioma nacional.

0-9

Cualquier número, del 0 al 9

+

Signo más

.

Punto

-

Subrayado

-

Guión

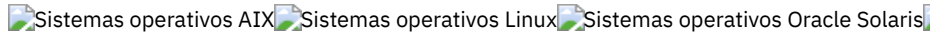



&


Símbolo &

Nota:

1. La API dispone de un modo alternativo de especificar encryptkey=generate; la opción enableclientencryptkey=yes anterior también puede especificarse para solicitar el proceso de generación de cifrado.

2. La opción de la API `enableclientencryptkey=yes` sigue recibiendo soporte, por lo tanto, es una opción posible cuando la API se utiliza para especificar dos opciones en conflicto. Por ejemplo, `enableclientencryptkey=yes` y `encryptkey=prompt` o `encryptkey=save`.
3. Cuando se especifican los valores en conflicto, la API devolverá un mensaje de error.

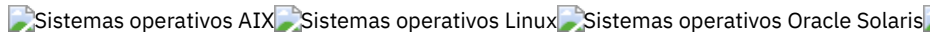



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Atención: Si se utiliza la opción `prompt`, la clave de cifrado no se guarda en el archivo de contraseñas de IBM Spectrum Protect en UNIX. Si olvida la clave, no se podrán recuperar los datos.


 Sistemas operativos Windows Atención: Si se utiliza la opción `prompt`, la clave de cifrado no se guarda en el registro de Windows. Si olvida la clave, no se podrán recuperar los datos.

## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha Autorización, en la sección Contraseña de clave de cifrado del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Autorización, en la sección Contraseña de clave de cifrado del Editor de preferencias.

## Sintaxis

```


      .-save-----
>>-ENCRYPTKey-+-----+-----<
      +-prompt---+
      '-generate-'





```

## Parámetros

### save

La contraseña de clave de cifrado se guarda en el archivo de contraseña del cliente de copia de seguridad y archivado. Se emite una solicitud para una contraseña de clave de cifrado inicial y después de la solicitud inicial, la contraseña de clave de cifrado guardada en el archivo de contraseña se usa para las copias de seguridad y el archivado de los archivos que coinciden con la especificación de `include.encrypt`. La clave se recupera desde el archivo de contraseña en las operaciones de restauración y recuperación.

 Sistemas operativos Windows La contraseña puede tener una longitud máxima de 63 bytes.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris La contraseña puede tener una longitud máxima de 64 bytes.

Cuando se especifica la opción `save` para una aplicación de la API, la contraseña de clave inicial debe proporcionarla la aplicación mediante la utilización de la API en la llamada de función `dsmInitEx`. La API no emite una solicitud para el usuario sino que se basa en la aplicación para solicitar al usuario cuando sea necesario.

Este parámetro es el predeterminado.





Nota: Deben tenerse en cuenta las restricciones siguientes:

- Esta opción sólo se puede usar si también se especifica `passwordaccess generate`.
- El usuario `root` o un usuario autorizado debe especificar la contraseña de clave de cifrado inicial.

### prompt

La gestión de la contraseña de clave de cifrado la proporciona el usuario. Al usuario se le solicita la contraseña de clave de cifrado cuando el cliente inicia una operación de copia de seguridad o de archivado. Se emite una solicitud para la misma contraseña cuando se restaura o se recupera el archivo cifrado.

 Sistemas operativos Windows Esta contraseña puede tener una longitud máxima de 63 bytes.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Esta contraseña puede tener una longitud máxima de 64 bytes.

Cuando se especifica la opción `prompt` para una aplicación de la API, la contraseña de clave debe proporcionarla la aplicación mediante la utilización de la API en la llamada de función `dsmInitEx`. La API no emite una solicitud para el usuario sino que se basa en la aplicación para solicitar al usuario cuando sea necesario.

#### generate

Una contraseña de clave de cifrado se genera dinámicamente cuando el cliente inicia una operación de copia de seguridad o de archivado. Esta clave generada se utiliza para las copias de seguridad de archivos que coinciden con la especificación `include.encrypt`. La contraseña de clave generada, en formato cifrado, se conserva en el servidor de IBM Spectrum Protect. La contraseña de clave se devuelve al cliente para que el archivo pueda descifrarse en las operaciones de restauración y de recuperación.

## Ejemplos

---

Archivo de opciones:

```
encryptkey prompt
```

Línea de mandatos:

No se aplica.

## Errorlogmax

---

La opción `errorlogmax` especifica el tamaño máximo del registro de errores, en megabytes. El nombre predeterminado para el registro de errores es `dsmerror.log`.

El ajuste de registro se controla con la opción `errorlogmax`. Si `errorlogmax` se establece en cero (0), el tamaño del registro es ilimitado; las entradas registradas no se "ajustan" y comienzan a sobrescribirse las entradas registradas anteriores. Si `errorlogmax` no está establecida en cero, las entradas de registro más recientes sobrescriben las entradas más antiguas del registro cuando el registro alcanza su tamaño máximo.

La eliminación de registros se controla con la opción `errorlogretention`. Los registros eliminados no se ajustan. En su lugar, las entradas de registro más antiguas que el número de días especificado por la opción `errorlogretention` se eliminan del archivo de registro.

Si cambia de ajuste de anotación (opción `errorlogmax`) a eliminación de anotación (opción `errorlogretention`), todas las entradas de las anotaciones existentes se guardan y la anotación se depura mediante el nuevo criterio `errorlogretention`. Las entradas de anotaciones eliminadas se guardan en un archivo llamado `dsmerlog.pru`.

Si cambia de eliminación de registros (opción `errorlogretention`) a ajuste de registros (opción `errorlogmax`), todos los registros del registro existente se copian en el archivo de registro `dsmerlog.pru`, se vacía el registro existente y el registro comienza a utilizar el nuevo criterio de ajuste de registro.

Si simplemente cambia el valor de la opción `errorlogmax`, los registros existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.






Si no se especifica `errorlogmax` ni `errorlogretention`, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogretention`, la anotación se elimina mediante el valor de retención especificado. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `errorlogmax`, la anotación existente se trata como si fuera una anotación eliminada. Es decir, el contenido del archivo `dsmerror.log` se copia en un archivo denominado `dsmerlog.pru`, se crean nuevas entradas de registro en `dsmerror.log` y el registro se ajusta cuando alcanza su tamaño máximo.

Nota: Si especifica un valor distinto de cero para `errorlogmax` (que permite la acomodación de anotaciones), no puede utilizar la opción `errorlogretention` para crear registros eliminados. Los registros se pueden eliminar o ajustar, pero no ambas cosas.

Los registros creados con la opción `errorlogmax` contienen un registro de cabecera de registro que contiene información similar a este registro de ejemplo:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0 Fri Dec 9 06:46:53 2011
```

Tenga en cuenta que las fechas y las indicaciones de la hora del texto `LOGHEADERREC` no se convierten o formatean utilizando los valores especificados en las opciones `dateformat` o `timeformat`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

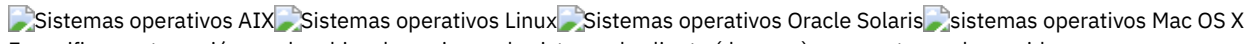
## Clientes soportados

---

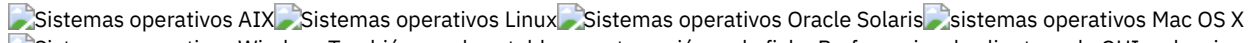
Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

 Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 También puede establecer esta opción en la ficha Preferencias de cliente en la GUI, seleccionando Habilitar ajuste de archivo de registro de errores y especificando un valor distinto de cero para el tamaño máximo para el archivo de anotaciones cronológicas. Para impedir el ajuste del archivo de anotaciones, establezca el valor de tamaño máximo a cero. Cuando el ajuste máximo se establece en cero, borrar o establecer la opción Habilitar ajuste de archivo de registro de errores no tiene ningún efecto; el ajuste de anotaciones no se produce si el tamaño máximo se establece en cero.

## Sintaxis

---

```
>>-ERRORLOGMAX-- --size-----<<
```

## Parámetros

---

size

Especifica el tamaño máximo, en megabytes, del archivo de anotaciones. El rango de valores es de 0 a 2047; el valor predeterminado es 0, que desactiva la acomodación del archivo de registro y deja que el archivo crezca indefinidamente.

## Ejemplos

---

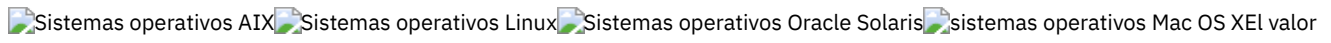
Archivo de opciones:  
errorlogmax 2000  
Línea de mandatos:  
-errorlogmax=2000


Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Errorlogname

---


Esta opción especifica la vía de acceso totalmente calificada y el nombre de archivo en el que se deben guardar los mensajes de error.

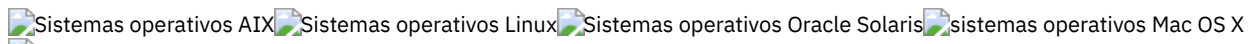

 El valor de esta opción modifica temporalmente la variable de entorno DSM\_LOG. Los archivos dsmwebc1.log y dsmsched.log se crean en el mismo directorio que el archivo de registro de errores que especifica con la opción errorlogname.

 Para Mac OS X, la ubicación predeterminada es una de las siguientes:

```
~/Library/Logs/tivoli/tsm/  
/Library/Logs/tivoli/tsm/
```

 Para Mac OS X, dsmerror.log puede ser un enlace simbólico.

 El valor de esta opción modifica temporalmente la variable de entorno DSM\_LOG. Los archivos dsmwebc1.log y dsmsched.log se crean en el mismo directorio que el archivo de registro de errores que especifica con la opción errorlogname.

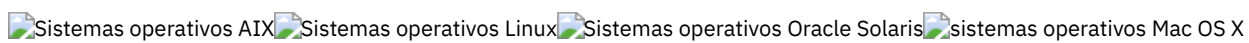
## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha General, en el botón Seleccionar anotaciones de errores del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha General, en el botón Seleccionar anotaciones de errores del Editor de preferencias.

## Sintaxis

---





```
>>-ERRORLOGName-- --filespec-----><
```

## Parámetros

---





### filespec





La vía de acceso completamente calificada y el nombre del archivo donde se debe almacenar la información de anotaciones de errores. Si no existe ninguna parte de la vía de acceso que especifica, el cliente intenta crearla.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X El archivo dsmerror.log no puede ser un enlace simbólico.


## Ejemplos





---





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones:


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
errorlogname /tmp/tsmerror.log


 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows errorlogname c:\temp\dsmerror.log


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X -  
errorlogname=/tmp/tsmerror.log

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows -errorlogname=c:\temp\dsmerror.log

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos Windows La ubicación del archivo de registro especificada con el programa de utilidad de configuración de servicios de cliente o el asistente de configuración del cliente altera temporalmente la ubicación especificada en el archivo de opciones del cliente (dsm.opt).

## Errorlogretention

---

La opción errorlogretention especifica durante cuántos días van a conservarse las entradas de las anotaciones de errores antes de eliminarlas y si se van a guardar las entradas eliminadas en otros archivos.

El registro de errores se elimina cuando se graba el primer error en el registro después de iniciar una sesión de cliente. Si la única sesión ejecutada es el planificador cliente y está en ejecución las veinticuatro horas del día, puede que las anotaciones de errores no se eliminen según las expectativas. Detenga la sesión y vuelva a iniciarla para que el planificador pueda eliminar las anotaciones de error.

Si cambia de eliminación de anotación (opción errorlogretention) a ajuste de anotación (opción errorlogmax), todos los registros de las anotaciones existentes se copian en el archivo de anotación dsmerlog.pru, la anotación existente se vacía y el registro empieza según los nuevos criterios de ajuste de anotaciones.

Si cambia de ajuste de anotación (opción errorlogmax) a eliminación de anotación (opción errorlogretention), todas las entradas de las anotaciones existentes se guardan y la anotación se depura mediante el nuevo criterio errorlogretention. Las entradas de anotaciones eliminadas se guardan en un archivo llamado dsmerlog.pru.

Si no se especifica errorlogmax ni errorlogretention, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción errorlogretention, la anotación se elimina mediante el valor de retención especificado. Cuando la anotación se ha creado sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción errorlogmax, la anotación existente se trata como si fuera una anotación eliminada. Es decir, el contenido del archivo dsmerror.log se copia en un archivo llamado dsmerlog.pru, se crean nuevas entradas de registro en dsmerror.log y la anotación se ajusta cuando llega a su tamaño máximo.

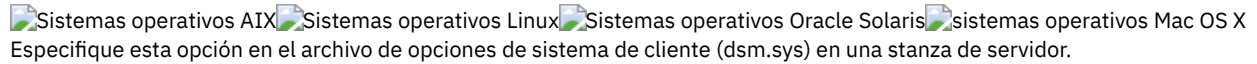
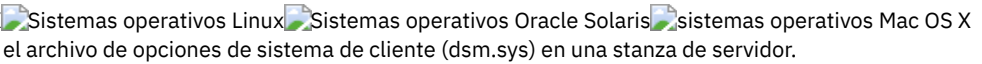
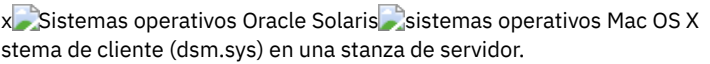
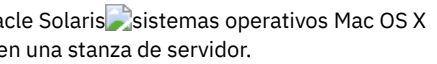
Nota: Si especifica la opción errorlogretention para crear anotaciones eliminadas, no podrá especificar la opción errorlogmax. Los registros pueden ser eliminados o ajustados, pero no las dos cosas.




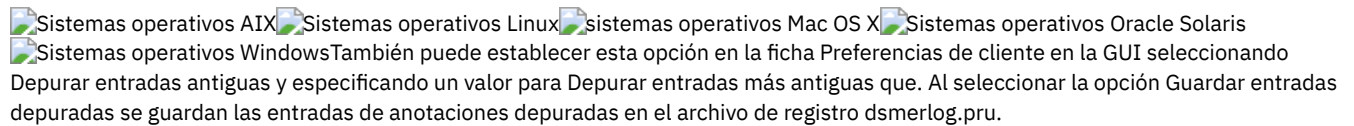
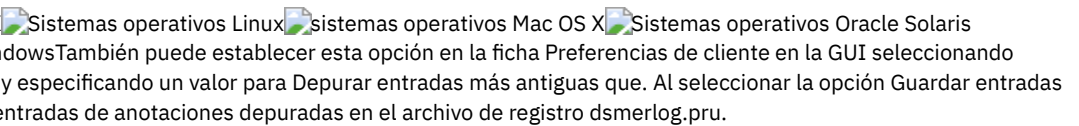
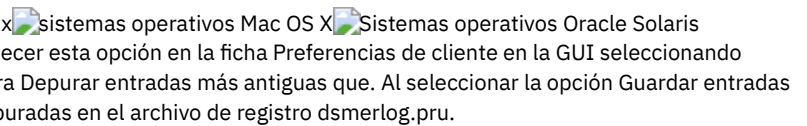
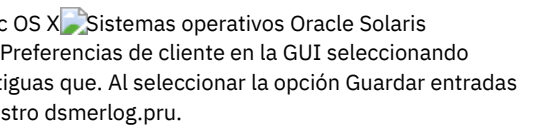
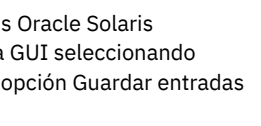
## Cientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones


 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 Sistemas operativos Oracle Solaris
 
 sistemas operativos Mac OS X  
 Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.


 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).


 Sistemas operativos AIX
 
 Sistemas operativos Linux
 
 sistemas operativos Mac OS X
 
 Sistemas operativos Oracle Solaris
 
 Sistemas operativos Windows  
 También puede establecer esta opción en la ficha Preferencias de cliente en la GUI seleccionando Depurar entradas antiguas y especificando un valor para Depurar entradas más antiguas que. Al seleccionar la opción Guardar entradas depuradas se guardan las entradas de anotaciones depuradas en el archivo de registro dsmerlog.pru.

## Sintaxis

```

      .-N---.  .-D-.
>>-ERRORLOGRetention--+-----+--+-----+-----><
      '-días-'  '-S-'
  
```

## Parámetros

N o days

Especifica cuánto tiempo se debe esperar antes de eliminar las anotaciones de errores.

N

No se eliminan el registro de errores. Esto hace que las anotaciones de errores crezcan indefinidamente. Éste es el valor predeterminado.

days

El número de días que se deben conservar las entradas del archivo de anotaciones antes de eliminar las anotaciones. El rango de valores oscila entre 0 y 9999.

D o S

Especifica si se deben guardar las entradas eliminadas. Utilice un espacio o una coma para separar este parámetro del anterior.

D

Elimina las entradas del registro de errores al eliminarlas. Éste es el valor predeterminado.

S

Guarda las entradas de las anotaciones de errores al eliminarlas.

Las entradas depuradas se copian desde el registro de errores al archivo dsmerlog.pru que está situado en el mismo directorio que el archivo dsmerlog.log.

## Ejemplos

Archivo de opciones:

Eliminar entradas de anotaciones desde el archivo dsmerlog.log que tengan más de 365 días y guardar las entradas eliminadas en dsmerlog.pru.

```
errorlogretention 365 S
```

Línea de mandatos:

```
-errorlogr=365,S
```

Archivo de opciones:


Eliminar entradas de anotaciones desde el archivo dsmerlog.log que tengan más de 365 días y no guardar las entradas eliminadas.

```
errorlogretention 365 D
```





Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Opciones exclude

Utilice las opciones `exclude` para excluir objetos de la imagen de copia de seguridad o de los servicios de archivado.


 Sistemas operativos Windows Por ejemplo, puede que desee excluir este tipo de información:

- Todos los archivos temporales
- Todas las memorias caché locales de archivos de red
- Todos los archivos que contienen código objeto compilado que se pueda reproducir fácilmente utilizando otros métodos
- Los archivos del sistema operativo








 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Por ejemplo, puede que desee excluir este tipo de información:





- Todos los archivos temporales
- Todas las memorias caché locales de archivos de red
- Todos los archivos que contienen código objeto compilado que se pueda reproducir fácilmente utilizando otros métodos
- Los archivos del sistema operativo





Puede excluir archivos específicos del proceso de cifrado durante una copia de seguridad.


 Sistemas operativos Windows Se pueden excluir los archivos de acceso remoto especificando nombres UNC (convenio de denominación universal) en la sentencia de exclusión.





Nota:

1.  Sistemas operativos Windows Cuando excluya un archivo que anteriormente se había incluido, las versiones de copia de seguridad existentes se desactivarán durante la siguiente copia de seguridad incremental.
2.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excepción de `exclude.fs`, cuando excluya un archivo que anteriormente se había incluido, las versiones de copia de seguridad existentes se desactivarán durante la siguiente copia de seguridad incremental.
3.  Sistemas operativos Windows Las sentencias `exclude` no son sensibles a mayúsculas y minúsculas.
4. El servidor puede definir opciones de exclusión con la opción `inlexcl`.
5.  Sistemas operativos Windows Como sucede con otras sentencias de inclusión/exclusión, puede utilizar la opción `inlexcl` para especificar un archivo que puede tener formato Unicode y que contenga sentencias de exclusión con nombres de archivos en formato Unicode.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Excluya cualquier archivo de sistemas o imagen que pueda dañar el sistema operativo al recuperarse. También debe excluir el directorio que contiene los archivos de cliente de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Para excluir un directorio completo denominado `/any/test`, especifique lo siguiente:


 Sistemas operativos Windows Para excluir un directorio completo denominado `any\test`, especifique lo siguiente:





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X





```
exclude.dir /any/test
```

 Sistemas operativos Windows

```
exclude.dir c:\any\test
```

 Sistemas operativos Windows Para excluir los subdirectorios que empiezan por `test` y que se encuentran en el directorio `any`, especifique lo siguiente:


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Para excluir los subdirectorios que empiezan por `test` y que se encuentran en el directorio `/any`, especifique lo siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
exclude.dir /any/test*
```

 Sistemas operativos Windows





```
exclude.dir c:\any\test*
```


 Sistemas operativos Windows Nota: si define una sentencia de exclusión sin letra de unidad, como por ejemplo `exclude.dir code`, se excluirá del proceso el directorio `code` de todas las unidades.

## Clientes soportados

Esta opción es válida para todos los clientes.



## Archivo de opciones





 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer estas opciones en la ficha Incluir/excluir, en la sección Definir opciones de inclusión/exclusión del Editor de preferencias.





 Sistemas operativos Windows  
 Coloque estas opciones en el archivo de opciones del cliente (dsm.opt). Puede establecer estas opciones en la ficha Incluir/excluir, en la sección Definir opciones de inclusión/exclusión del Editor de preferencias.

## Sintaxis

```
>>-opciones-- --patrón-----><
```





 Sistemas operativos Windows  
 exclude, exclude.backup, exclude.file, exclude.file.backup  
 Sistemas operativos Windows  
 Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad.





 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 exclude, exclude.backup, exclude.file, exclude.file.backup


 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 Utilice estas opciones para excluir un archivo o un grupo de archivos de los servicios de copia de seguridad y de los servicios de gestión de espacio (si el cliente de HSM está instalado). La opción exclude.backup sólo excluye archivos de la copia de seguridad normal, no de HSM.

exclude.archive

Excluye sólo de los servicios de archivado el archivo o grupo de archivos que coincidan con el patrón.





 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 exclude.attribute.symlink


 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 Excluye un archivo o un grupo de archivos que son enlaces simbólicos o alias (los alias se aplican a Mac OS X) sólo del proceso de copia de seguridad.





 sistemas operativos Mac OS X Nota: Para Mac OS X, se excluyen los alias.


exclude.compression

Excluye archivos del proceso de compresión si la opción compression se ha establecido en yes. Esta opción se aplica a copias de seguridad y copias archivadas.







 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X

 Sistemas operativos Windows  
 exclude.dedup





 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X





 Sistemas operativos Windows  
 Excluye archivos para la eliminación de duplicados de datos por parte del cliente. Para controlar una operación de eliminación de duplicados de datos por parte del cliente, especifique ieobjtype como valor de la opción exclude.dedup.

Los parámetros ieobjtype válidos son:

- Archivo
-  Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 Imagen
-  Sistemas operativos Windows  
 SYSTEMState
-  Sistemas operativos Windows  
 Asr


El valor predeterminado es File.


 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 exclude.dir

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X  
 Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia `exclude.dir /test/dan/data1` excluye el directorio `/test/dan/data1`, sus archivos y todos sus subdirectorios y sus archivos.

Si excluye un directorio que anteriormente se había incluido, el servidor dará caducidad a las versiones de copia de seguridad existentes de los archivos y directorios que se encuentran debajo de éste durante la siguiente copia incremental. Utilice esta opción para excluir una parte de los datos que no tenga archivos subyacentes de los que deba realizarse una copia de seguridad.

Nota: Evite realizar una copia de seguridad selectiva, o una copia de seguridad parcial incremental, de un archivo individual de un directorio excluido. La próxima vez que realice una copia de seguridad incremental, se dará caducidad a los archivos cuya copia de seguridad se ha realizado de esta forma.

 Sistemas operativos Windows `exclude.dir`

 Sistemas operativos Windows Excluye un directorio, sus archivos y todos sus subdirectorios y sus archivos del proceso de copia de seguridad. Por ejemplo, la sentencia `exclude.dir c:\test\dan\data1` excluye el directorio `c:\test\dan\data1`, sus archivos y todos sus subdirectorios y sus archivos.





Si excluye un directorio que anteriormente se había incluido, el servidor dará caducidad a las versiones de copia de seguridad existentes de los archivos y directorios que se encuentran debajo de éste durante la siguiente copia incremental. Utilice esta opción para excluir una parte de los datos que no tenga archivos subyacentes de los que deba realizarse una copia de seguridad.





Nota: Evite realizar una copia de seguridad selectiva, o una copia de seguridad parcial incremental, de un archivo individual de un directorio excluido. La próxima vez que realice una copia de seguridad incremental, se dará caducidad a los archivos cuya copia de seguridad se ha realizado de esta forma.





Nota: si define una sentencia de exclusión sin letra de unidad, como por ejemplo `exclude.dir code`, se excluirá del proceso el directorio `code` de todas las unidades.




`exclude.encrypt`



Excluye los archivos especificados del proceso de cifrado. Esta opción no afecta a la exclusión de los archivos del proceso de copia de seguridad o archivado, sólo afecta a la exclusión de los archivos del proceso de cifrado.



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `exclude.fs`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Excluye los sistemas de archivos que coinciden con el patrón especificado de las operaciones de copia de seguridad, copia de seguridad de imágenes incremental y operaciones de archivado. Si en algún momento se realizó una copia de seguridad de los archivos de los sistemas de archivos excluidos, no se llevará a cabo la operación de volver a vincular con clase de gestión ni caducarán los archivos suprimidos. No obstante, las versiones de copia de seguridad existentes permanecerán en el servidor según los valores de clases de gestión asociadas. Los archivos previamente archivados del sistema de archivos excluido permanecen en el servidor como copias de archivo.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X La opción `exclude.fs` NO impide la copia de seguridad o archivado de ningún punto de montaje virtual que son los subdirectorios del sistema de archivos excluido.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice `exclude.image` para excluir sistemas de archivos de operaciones de copia de seguridad de imágenes.




 Sistemas operativos AIX  Sistemas operativos Oracle Solaris `exclude.fs.nas`

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato `backup nas`. El nombre de nodo NAS debe estar prefijado al nombre del sistema de archivos, por ejemplo: `netappsj1/vol/vol11`. Para aplicar esta exclusión a todos los nodos NAS sustituya el nombre de nodo NAS con un comodín, por ejemplo: `*/vol/vol11`. El mandato `backup nas` pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias `exclude.fs` y `exclude.dir`. Esta opción *sólo* es válida para los clientes AIX y Solaris.

 Sistemas operativos Windows `exclude.fs.nas`

 Sistemas operativos Windows Excluye sistemas de archivos del servidor de archivos NAS del proceso de copias de seguridad de imágenes cuando se utiliza con el mandato `backup nas`. El nombre de nodo NAS debe estar prefijado al nombre del sistema de archivos, por ejemplo: `netappsj1/vol/vol11`. Para aplicar esta exclusión a todos los nodos NAS sustituya el nombre de nodo NAS con un comodín, por ejemplo: `*/vol/vol11`. El mandato `backup nas` pasa por alto todas las demás sentencias de exclusión, incluidas las sentencias `exclude.dir`. Esta opción es válida para todos los clientes Windows.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `exclude.image`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Excluye sistemas de archivos montados y volúmenes lógicos RAW que coincidan con el patrón especificado de las operaciones de copia de seguridad de imágenes completas. Esta opción es válida únicamente para AIX, todos los clientes Linux y Solaris. Utilice `exclude.fs` para excluir sistemas de archivos de operaciones de copia de seguridad de imágenes incremental.

Restricción: Esta opción no se aplica a Mac OS X.

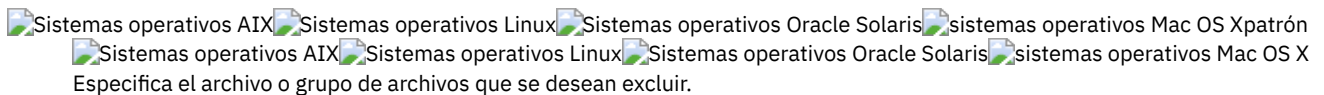
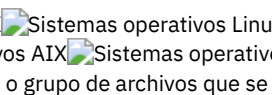
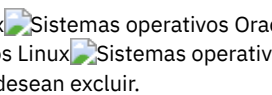
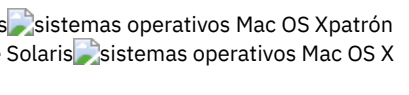
 Sistemas operativos Windows

Tabla 1. Componentes de servicios del sistema y palabras clave correspondientes

Componente	Palabra clave
------------	---------------

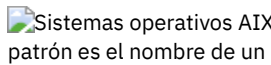
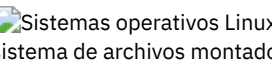
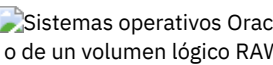
Componente	Palabra clave
Background Intelligent Transfer Service	BITS
Anotaciones de sucesos	EVENTLOG
Removable Storage Management	RSM
Base de datos de clústeres	CLUSTERDB
Servicio de almacenamiento remoto	RSS
Licencias de Terminal Server	TLS
Windows Management Instrumentation	WMI
Base de metadatos de Internet Information Services (IIS)	IIS
Base de datos DHCP	DHCP
Base de datos Wins	WINSDB


## Parámetros

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica el archivo o grupo de archivos que se desean excluir.

Nota: En sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de exclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (dsm.sys) o en la línea de mandatos.

Si el patrón comienza con comillas dobles o simples, contiene espacios en blanco intercalados o signos de igual, debe incluir el valor entre comillas simples (') o comillas dobles ("). Los signos que se utilicen para la apertura y el cierre deben ser del mismo tipo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris En la opción exclude.image, el patrón es el nombre de un sistema de archivos montado o de un volumen lógico RAW.

 Sistemas operativos Windows patrón

 Sistemas operativos Windows Especifica el archivo o grupo de archivos que se desean excluir.

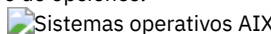



Nota: En sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de exclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

Si el patrón comienza con comillas dobles o simples, contiene espacios en blanco intercalados o signos de igual, debe incluir el valor entre comillas simples (') o comillas dobles ("). Los signos que se utilicen para la apertura y el cierre deben ser del mismo tipo.

- En la opción exclude.image, el patrón es el nombre de un sistema de archivos o de un volumen lógico RAW.

## Ejemplos

Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
exclude /unix/
exclude ../../core
exclude /home/jones/proj1/*
exclude.archive ../../core
exclude.backup /home/jones/proj1/devplan/
exclude.dir /home/jones/tmp
exclude.backup /users/home1/file1
exclude.image /usr/*/*
exclude.encrypt /users/home2/file1
exclude.compression /home/gordon/proj1/*
exclude.fs.nas netappsj/vol/vol0
exclude.attribute.symlink ../../*
exclude.dedup /Users/Administrator/Documents/Important/../../*
```

 Sistemas operativos Windows

```

exclude ?:\...\swapper.dat
exclude "?:\ea data. sf"
exclude ?:\io.sys
exclude ?:\...\spart.par
exclude c:\*\budget.fin
exclude c:\devel\*
exclude.dir c:\home\jodda
exclude.archive c:\home\*.obj
exclude.encrypt c:\system32\mydocs\*
exclude.compression c:\test\file.txt

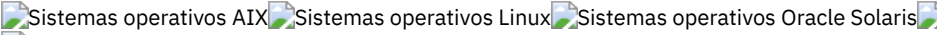
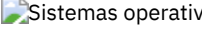
exclude.fs.nas netappsj/vol/vol0
exclude.dedup c:\Users\Administrator\Documents\Important\...\*
exclude.dedup e:\*\* ieobjtype=image
exclude.dedup ALL ieobjtype=systemstate
exclude.dedup ALL ieobjtype=ASR

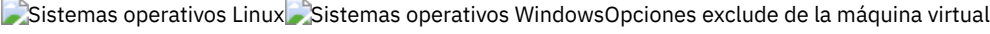
```

Línea de mandatos:

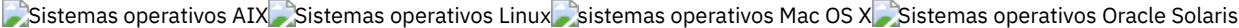
No se aplica.

- 

Control del proceso de enlaces simbólicos y alias  
El cliente de copia de seguridad y archivado trata los vínculos simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. Sin embargo, no se realiza la copia de seguridad del archivo al que hace referencia el enlace simbólico. En algunos casos, los enlaces simbólicos pueden volver a crearse fácilmente y no es necesario realizar una copia de seguridad de los mismos.
- Control del proceso de compresión  
En este tema se indican diversos aspectos que han de tenerse en cuenta si desea excluir archivos o grupos de archivos específicos del proceso de compresión durante una operación de copia de seguridad o archivado.
- 


Proceso de sistemas de archivos NAS  
Utilice la opción `exclude.fs.nas` para excluir sistemas de archivos del proceso de copia de seguridad de imágenes NAS.
- 

Opciones `exclude` de la máquina virtual  
Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.



## Control del proceso de enlaces simbólicos y alias

El cliente de copia de seguridad y archivado trata los vínculos simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. Sin embargo, no se realiza la copia de seguridad del archivo al que hace referencia el enlace simbólico. En algunos casos, los enlaces simbólicos pueden volver a crearse fácilmente y no es necesario realizar una copia de seguridad de los mismos.

Además, realizar una copia de seguridad de estos enlaces simbólicos puede incrementar el tiempo de proceso de la copia de seguridad y puede ocupar un volumen de espacio notable en el servidor de IBM Spectrum Protect. Para excluir un archivo o un grupo de archivos que sean enlaces simbólicos del proceso de copia de seguridad puede utilizar la opción `exclude.attribute.symlink`. Si es necesario, puede utilizar la opción `include.attribute.symlink` para incluir enlaces simbólicos en un grupo amplio de archivos excluidos para el proceso de copia de seguridad.

Por ejemplo, para excluir todos los enlaces simbólicos del proceso de copia de seguridad, excepto los que existen en el directorio `/home/spike`, especifique estas sentencias en el archivo `dsm.sys`:

```

exclude.attribute.symlink /.../*
include.attribute.symlink /home/spike/.../*





```

**Referencia relacionada:**

Opciones `include`


## Control del proceso de compresión

En este tema se indican diversos aspectos que han de tenerse en cuenta si desea excluir archivos o grupos de archivos específicos del proceso de compresión durante una operación de copia de seguridad o archivado.

- Recuerde que el cliente de copia de seguridad y archivado compara los archivos que procesa con los patrones especificados en las sentencias de inclusión y exclusión leyéndolas de abajo arriba en el archivo de opciones.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X El cliente procesará `exclude.fs`, `exclude.dir`, y otras sentencias de inclusión/exclusión en primer lugar. A continuación, el cliente considerará las sentencias `exclude.compression`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:

```
exclude /home/jones/proj1/*.*
exclude.compression /home/jones/proj1/file.txt
include /home/jones/proj1/file.txt
```

El cliente examina las sentencias (realiza una lectura desde el final hasta el principio) y determina que el archivo `/home/jones/proj1/file.txt` es candidato para la copia de seguridad, pero no es candidato para el proceso de compresión.

-  Sistemas operativos Windows El cliente procesa en primer lugar `exclude.dir` y otras sentencias de inclusión/exclusión. A continuación, el cliente considerará las sentencias `exclude.compression`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:






```
exclude c:\test\*.*
exclude.compression c:\test\file.txt
include c:\test\file.txt
```

El cliente examina las sentencias (realiza una lectura desde el final hasta el principio) y determina que el archivo `c:\test\file.txt` es candidato para la copia de seguridad, pero no es candidato para el proceso de compresión.

- El proceso de compresión de inclusión-exclusión es válido únicamente para procesos de copias de seguridad y archivado. La opción `exclude.compression` no afecta a la exclusión de los archivos del proceso de copia de seguridad o archivado, sólo afecta a la exclusión del proceso de compresión.



#### Referencia relacionada:

Compression

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Proceso de sistemas de archivos NAS

Utilice la opción `exclude.fs.nas` para excluir sistemas de archivos del proceso de copia de seguridad de imágenes NAS.

 Sistemas operativos Linux  Sistemas operativos Windows Nota: La opción `exclude.fs.nas` no es válida para una copia de seguridad incremental por diferencia de instantánea.

Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Los nodos NAS representan un tipo de nodo exclusivo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en el cliente de copia de seguridad y archivado. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de exclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado se aplica a todos los servidores de archivos NAS.
- Con independencia de la plataforma del cliente utilizada, las especificaciones de sistema de archivos NAS utilizan la barra inclinada (/) como separador, tal como se muestra en el siguiente ejemplo: `/vol/vol10`.


Por ejemplo, para excluir `/vol/vol1` de los servicios de copia de seguridad en todos los nodos NAS, especifique la sentencia de exclusión siguiente:



```
exclude.fs.nas */vol/vol1
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Opciones exclude de la máquina virtual

Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

-  Sistemas operativos Linux  Sistemas operativos Windows Exclude.vmdisk  
La opción EXCLUDE.VMDISK excluye un disco de máquina virtual de las operaciones de copia de seguridad.

**Referencia relacionada:**

Exclude.vmdisk

 Sistemas operativos Linux  Sistemas operativos Windows

## Fbbranch


---


Utilice la opción fbbranch con los mandatos backup fastback o archive fastback.

La opción fbbranch especifica el ID de la ramificación del servidor de FastBack remoto cuya copia de seguridad o archivado se va a ejecutar. La opción fbbranch solo es necesaria si el cliente de archivado y copia de seguridad está instalado en el FastBack Disaster Recovery Hub o si hay un proxy dedicado conectado a un repositorio de FastBack Disaster Recovery Hub replicado. No especifique la opción fbbranch si el cliente de archivado y copia de seguridad está instalado en el servidor de FastBack.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos Linux Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
>>-FBBranch=--ID_ramificación-----<<
```

## Parámetros

---

ID\_ramificación

Especifica el ID de ramificación del servidor de FastBack. El valor forma parte de la configuración de recuperación tras desastre del servidor de FastBack.

## Ejemplos

---

Línea de mandatos:

```
-FBBranch=oracle
```

En un cliente de archivado y copia de seguridad instalado en el FastBack Disaster Recovery Hub:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=myFbServer  
-fbbranch=oracle
```

Línea de mandatos:

En un cliente de archivado y copia de seguridad conectado a un repositorio en un FastBack Disaster Recovery Hub remoto:

```
dsmc backup fastback -fbpolicyname=policy1 -fbserver=server1  
-Fbreposlocation=\myDrHub.company.com\REP  
-fbbranch=oracle
```

Si se ha especificado la opción fbbranch en una estación de trabajo del cliente de archivado y copia de seguridad que está instalado en el servidor de FastBack, se omite la opción fbbranch.

 Sistemas operativos Linux  Sistemas operativos Windows

## Fbclientname

---



Utilice la opción fbclientname con los mandatos backup fastback o archive fastback.


La opción fbclientname es el nombre de uno o varios clientes de FastBack separados por comas de los que se va a efectuar una copia de seguridad o archivado desde el proxy de copia de seguridad. Los valores para la opción fbclientname no son válidos si se especifica más de una política en la opción fbpolycyname.


No puede incluir espacios en los valores de opción fbclientname.

Si no especifica los valores de la opción fbvolumename, se realizará una copia de seguridad de todos los volúmenes de los clientes de FastBack de la política especificada. Si especifica varios clientes de FastBack en la opción fbclientname, no podrá especificar valores para la opción fbvolumename.

## Cientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos Linux Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
      .-,-----  
      v          |  
>>-FBclientname----client_name+-----<<
```

## Parámetros

---

nombre\_cliente

Especifica el nombre de uno o varios clientes de FastBack. Puede especificar hasta 10 nombres de cliente de FastBack.


Importante:


Al especificar el mandato archive fastback o backup fastback:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar siempre la opción FBReposLocation para Linux.

## Ejemplos

---


 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux

```
dsmc backup fastback -fbpolycyname=Policy1  
-fbclientname=fbclient1,fbclient2  
-fbserver=myFbServer  
-fbreposlocation=/mnt/FBLocation
```

Realiza copias de seguridad de todos los volúmenes para los clientes fbclient1 y fbclient2 de FastBack que se encuentran en la política Policy1.


 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
dsmc backup fastback -fbpolicyname=Policy1
-fbclientname=fbclient1,fbclient2
-fbserver=myFbServer
-fbreposlocation=\myFbServer.company.com\REP
```


Realiza copias de seguridad de todos los volúmenes para los clientes fbclient1 y fbclient2 de FastBack que se encuentran en la política Policy1.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
dsmc backup fastback -fbpolicyname=Policy1
-fbclientname=fbclient1
-fbvolumename=c:,f: -fbserver=myFbServer
-fbreposlocation=\myFbServer.company.com\REP
```

Realiza copias de seguridad de los volúmenes C:\ y F:\ para el cliente fbclient1 de FastBack que se encuentra en la política Policy1.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
dsmc backup fastback -fbpolicyname=Policy1
-fbclientname=fbWindowsClient,fbLinuxClient
-fbserver=myFbServer
-fbreposlocation=\myFbServer.company.com\REP
```

Realiza copias de seguridad de todos los volúmenes para el cliente fbWindowsClient de FastBack que se encuentra en la política Policy1.

No se efectuarán copias de seguridad de los volúmenes del cliente fbLinuxClient de FastBack de Linux desde el cliente de archivado y copia de seguridad de Windows. Para ejecutar un proceso de copia de seguridad o archivado en los volúmenes desde un cliente FastBack de Linux, utilice el cliente de archivado y copia de seguridad de Linux.

 Sistemas operativos Linux  Sistemas operativos Windows

## Fbpolicyname


---


Utilice la opción fbpolicyname con los mandatos backup fastback o archive fastback.

La opción fbpolicyname es el nombre de una o varias políticas de FastBack separadas por comas de las que se va a efectuar una copia de seguridad o archivado desde el proxy de copia de seguridad. Debe especificar, como mínimo, un nombre de política. Especifique varios nombres de políticas utilizando una lista de políticas delimitadas por comas. No hay ningún valor predeterminado.

Si uno o más nombres de políticas FB contiene espacios, debe especificarlos dentro de las comillas. A continuación se muestra un ejemplo: "FB Policy NAME1, FBPolicy Name 2".

Si no se especifica ningún valor para las opciones fbclientname y fbvolumename, se realiza copia de seguridad de todos los volúmenes de todos los clientes de FastBack de la política que se especifiquen. Si especifica varias políticas en la opción fbpolicyname, no puede especificar valores para las opciones fbclientname y fbvolumename.


 Sistemas operativos Windows Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará copia de seguridad o se archivarán los volúmenes de Windows en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Windows.


 Sistemas operativos Linux Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.

Debe existir al menos una instantánea en el repositorio de FastBack para las políticas de FastBack que se han archivado, o de las cuales se han realizado copias de seguridad, antes de emitir el mandato dsmc

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos Linux Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
      .-,-,-----  
      |          |  
>>-FBPolicyname---policy_name+-----<<
```

## Parámetros

---

nombre\_política

Especifica el nombre de las políticas de FastBack. Puede especificar hasta 10 nombres de política de FastBack.

Importante:

Al especificar el mandato archive fastback o backup fastback:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName. se puede tener especificado un único FBPolicy y un único FBClientName. Debe especificar exactamente un FBClientName. No se puede omitir.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar siempre la opción FBReposLocation para Linux.

## Ejemplos

---

Línea de mandatos:

```
dsmc backup fastback -fbpolicyname=Policy1,Policy2,Policy3  
-fbserver=myFbServer  
-fbreposlocation=\\myFbServer.company.com\REP
```

Realiza una copia de seguridad de todos los volúmenes de los clientes de FastBack que se encuentran en las políticas Policy1, Policy2 y Policy3.

Para explicar políticas con espacios, inclúyalas entre comillas dobles, por ejemplo:

```
-fbpolicyname="Policy 1,Policy2,Policy3"
```


 Sistemas operativos Linux  Sistemas operativos Windows


## Fbreposlocation


---

Utilice la opción fbreposlocation con los mandatos backup fastback o archive fastback.

La opción fbreposlocation especifica la ubicación del repositorio de Tivoli Storage Manager FastBack para que el proxy del cliente de archivado y copia de seguridad se conecte para emitir los mandatos de shell de Tivoli Storage Manager FastBack necesarios para montar las instantáneas apropiadas.

 Sistemas operativos Linux Esta opción es necesaria para sistemas Linux. No existe una ubicación predeterminada.


 Sistemas operativos Linux Si especifica la opción fbreposlocation para una instantánea en el servidor de FastBack, utilice el formato nombre\_servidor@GRUPO\_TRABAJO.


 Sistemas operativos Linux Existen dos maneras de especificar la ubicación de repositorio de FastBack en el FastBack Disaster Recovery Hub:


- Especifique la ubicación completa del repositorio mediante la opción -fbreposlocation=\\DR\_Hub\rep\_server. Cuando se utiliza este formato, DR\_Hub es el nombre de máquina de FastBack Disaster Recovery Hub y rep\_server es el nombre del

repositorio de servidor de FastBack replicado en el DR Hub.

- Especifique la ubicación del repositorio utilizando una combinación de las opciones `-fbreposlocation=` y `-fbbranch`. Al utilizar este formato, especifique la ubicación del repositorio del DR Hub mediante la opción `-fbreposlocation=DR_Hub@WORKGROUP`, y especifique el nombre del repositorio del servidor de FastBack replicado en el DR Hub utilizando la opción `-fbbranch`.


 **Sistemas operativos Windows** En los sistemas de Windows, no tiene que especificar la opción `fbreposlocation` cuando el cliente de copia de seguridad y archivado esté instalado en un servidor DR Hub o en una estación de trabajo del servidor de FastBack. Si el cliente de copia de seguridad y archivado está instalado en un proxy del cliente dedicado, se necesita la opción `fbreposlocation` de la ubicación de repositorio.


 **Sistemas operativos Windows** Si especifica la opción `fbreposlocation` para el FastBack Disaster Recovery Hub, especifique solo el directorio base del repositorio de DR Hub con esta opción. Después, utilice la opción `fbbranch` para indicar el ID de ramificación del servidor al que se va a hacer copia de seguridad. Si especifica la opción `fbreposlocation` para el servidor de FastBack, utilice el formato `\\<fbserver>\REP`. En este caso, no utilice la opción `fbbranch`.

 **Sistemas operativos Linux** Si utiliza el formato `-fbr=\\<fbserver>\REP`, especifique dos barras inclinadas invertidas antes de `<fbserver>` y una barra inclinada invertida antes de `REP` al utilizar el cliente de archivado y copia de seguridad en modalidad interactiva. Si utiliza este formato como un mandato de Linux `dsmc backup fastback -fbr=\\<servidor_fb>\REP`, debe especificar cuatro barras inclinadas invertidas antes de `<servidor_fb>` y dos barras inclinadas invertidas antes de `REP`. Esto se debe a que el shell de Linux interpreta una barra inclinada invertida como un carácter de escape; la primera barra inclinada se trata como un carácter de escape para la siguiente barra inclinada invertida.

## Clientes soportados

---

 **Sistemas operativos Linux** Esta opción es válida para clientes de Linux x86\_64.

 **Sistemas operativos Windows** Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
>>-FBReposlocation--ubicación_repositorio-----><
```

## Parámetros


---


ubicación\_repositorio

Especifica la ubicación de repositorio de Tivoli Storage Manager FastBack.

## Ejemplos


---


 **Sistemas operativos Linux** Línea de mandatos:

 **Sistemas operativos Linux**

```
dsmc backup fastback -fbpolicyname=Policy1
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub
-fbreposlocation=\\myFbDrHub\rep_myFbServer
```


Nota: Dado que Linux solo se admite como una configuración de proxy dedicado, siempre es necesaria una ubicación de repositorio en proxy Linux.


 **Sistemas operativos Linux** Línea de mandatos:

 **Sistemas operativos Linux**

```
dsmc backup fastback -fbpolicyname=Policy1
-fbclientname=fbclient1,fbclient2 -fbserver=myFbDrHub
-fbreposlocation=myFbDrHub -fbbranch=rep_myFbServer
```

Nota: Dado que Linux solo se admite como una configuración de proxy dedicado, siempre es necesaria una ubicación de repositorio en proxy Linux.

 **Sistemas operativos Windows** Línea de mandatos:

 **Sistemas operativos Windows**

La opción `fbreposlocation` sólo es necesaria en una máquina de proxy dedicada. Si se ha especificado la opción `fbreposlocation` en una máquina donde se han instalado el servidor de FastBack o FastBack Disaster Recovery Hub, se pasa por alto.

Utilice este mandato si el cliente proxy dedicado de IBM Spectrum Protect está conectado a un repositorio de servidor de Tivoli Storage Manager FastBack remoto:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\\myFbServer.company.com\REP
```

La ubicación del repositorio es necesaria.

myFbServer es el nombre de host abreviado de la máquina donde está instalado el servidor de FastBack.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

Utilice este mandato cuando el cliente proxy dedicado de IBM Spectrum Protect se esté conectando a un repositorio remoto en el FastBack Disaster Recovery Hub:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\\myfbdrhub.company.com\REP  
-fbbranch=aFbServerBranch
```

La ubicación del repositorio es necesaria.

El parámetro myFbServer especifica el nombre de host abreviado del servidor de FastBack cuya rama de FastBack se especifica utilizando la opción FBBranch.

La opción fbbranch especifica el ID de la ramificación del servidor FastBack en el concentrador de recuperación tras desastre.

 Sistemas operativos Linux  Sistemas operativos Windows

## Fbserver

---


Utilice la opción fbserver con los mandatos backup fastback o archive fastback.


La opción fbserver especifica el nombre de host abreviado de la estación de trabajo de servidor de Tivoli Storage Manager FastBack propietaria del repositorio especificado por la opción fbreposlocation. Para un DR Hub, la opción fbserver especifica el nombre corto de la estación de trabajo del servidor FastBack a cuyo repositorio de ramificaciones está conectado el cliente de copia de seguridad y archivado.

La opción fbserver es la clave para recuperar las credenciales de usuario necesarias para conectarse al repositorio del servidor de FastBack o el repositorio del servidor del concentrador DR para el proceso de montaje.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos Linux Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
>>- -FBServer-- --server_name-----><
```

## Parámetros

---


nombre\_servidor

Especifica el nombre de host abreviado de la máquina en la que está instalado el servidor de FastBack.

## Ejemplos

---


 Sistemas operativos Linux Línea de mandatos:


 Sistemas operativos Linux El cliente de archivado y copia de seguridad está instalado en una máquina de cliente proxy de Linux. Utilice este mandato para archivar todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para policy1 de FastBack:

```
dsmc archive fastback -fbpolicyname=Policy1  
-fbserver=myfbserver  
-fbreposlocation=myfbserver@WORKGROUP
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se producirá un error en el mandato.

El nombre del servidor de FastBack, -myfbserver, es el nombre de host abreviado del servidor de FastBack donde se encuentra el repositorio.

 Sistemas operativos Linux Línea de mandatos:


 Sistemas operativos Linux El repositorio, rep\_server1, se encuentra en el FastBack Disaster Recovery Hub, myFbDrHub.


```
dsmc archive fastback -fbpolicyname="Policy 1"  
-fbserver=myFbDrHub  
-fbreposlocation=\\myFbDrHub\rep_server1
```

El nombre del servidor de FastBack, -myFbDrHub es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio

El parámetro -fbreposlocation especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no se proporciona la ubicación del repositorio, el mandato falla.


-fbserver debería apuntar al nombre de host abreviado del FastBack DR Hub en este caso.

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux Archivar todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:


```
dsmc archive fastback -Fbpolicyname=policy1  
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"  
-fbreposlocation=basil@WORKGROUP
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad de IBM Spectrum Protect se está ejecutando en la máquina del servidor de FastBack cuyo nombre abreviado es myFbServer:


```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServer
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad de IBM Spectrum Protect se está ejecutando en la máquina de FastBack Disaster Recovery Hub y se conecta al repositorio de ramificaciones del servidor branch1 de FastBack. El nombre de host abreviado del servidor de FastBack es myFbServer:


```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServer  
-fbbranch=branch1
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad se ejecuta en una máquina de proxy dedicado y está conectado al repositorio del servidor de FastBack remoto. El servidor de FastBack está instalado en una máquina cuyo nombre abreviado es myFbServerMachine:

```
dsmc archive fastback -fbpolicyname=Policy1 -fbserver=myFbServerMachine  
-fbreposlocation=\\myFbServerMachine.company.com\Rep
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad se está ejecutando en una máquina de proxy dedicado y está conectado a un repositorio del FastBack remoto en el FastBack DR Hub. El servidor de FastBack con ID de ramificación branch1 está instalado en una máquina cuyo nombre abreviado es myFbServer.

```
dsmc backup fastback -fbpolicyname=Policy1 -fbserver=myFbServer  
-fbreposlocation=\\myDrHubMachine.company.com\Rep  
-fbbranch=branch1
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Fbvolumename

---


Utilice la opción fbvolumename con los mandatos backup fastback o archive fastback.


La opción fbvolumename es el nombre de uno o varios volúmenes de Tivoli Storage Manager FastBack separados por comas de los que se va a efectuar una copia de seguridad o archivado desde el proxy de copia de seguridad. Los valores de la opción fbvolumename no son válidos si se especifica más de un cliente de FastBack en la opción fbclientname.

Si especifica varios clientes de FastBack en la opción fbclientname, no podrá especificar valores para la opción fbvolumename.

## Cientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos Linux Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos. El servidor también puede definir o sustituir esta opción.

## Sintaxis

---

```
      .-,-----  
      v          |  
>>-FBVolumename---volume_name+-----<<
```

## Parámetros


---

nombre\_volumen

Especifica el nombre de los volúmenes de Tivoli Storage Manager FastBack. Puede especificar hasta 10 nombres de volumen de FastBack.

Importante:


Al especificar el mandato archive fastback o backup fastback:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName. se puede tener especificado un único FBPolicy y un único FBClientName. Debe especificar exactamente un FBClientName. No se puede omitir.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7.  Sistemas operativos Linux Debe especificar la opción FBReposLocation.

## Ejemplos

---


 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1  
-fbvolumename=data1,data2 -fbserver=myFbDrHub  
-fbreposlocation=\myFbDrHub\rep_server1
```

Realiza una copia de seguridad de los volúmenes data1 y data2 desde el cliente client1 de FastBack que se encuentra en la política Policy1.


 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
dsmc backup fastback -fbpolicyname=Policy1 -fbclientname=client1  
-fbvolumename=c:,f: -fbserver=myFbServer  
-fbreposlocation=\myFbServer.company.com\REP
```

Realiza una copia de seguridad de los volúmenes C:\ y F:\ desde el cliente Client1 de FastBack que se encuentra en la política Policy1.

 Sistemas operativos Windows

 Sistemas operativos Windows

```
dsmc archive fastback -fbpolicyname=Policy1 -fbclientname=client1
-fbvolumename=c:,f: -fbserver=myFbServer
-fbreposlocation=\\myFbServer.company.com\REP
```






Archiva los volúmenes C: y F: del cliente Client1 de FastBack que se encuentra en la política Policy1.

## Filelist

---



Utilice la opción filelist para procesar una lista de archivos.

Puede utilizar la opción filelist con los mandatos siguientes:

- archive
-  Sistemas operativos Windows backup group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X backup group
- delete archive
- delete backup
- expire
- incremental
- query archive
- query backup
- restore
- retrieve
- selective

El cliente de copia de seguridad y archivado abre el archivo que especifique con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico. A excepción de los mandatos restore y retrieve, cuando utiliza la opción filelist, el cliente pasa por alto todas las demás especificaciones de archivo de la línea de mandatos.

Los archivos (entradas) que contenga filelist deben seguir las siguientes reglas:

- Cada entrada debe ser una vía de acceso completa o relativa de un archivo o directorio. Tenga en cuenta que si incluye un directorio en una entrada de lista de archivo, se realizará una copia de seguridad del directorio, pero no de sus contenidos.
- Cada vía de acceso debe especificarse en una única línea. Cada línea sólo puede contener una única vía de acceso.
- Las vías de acceso no deben contener caracteres de control, como 0x18 (CTRL-X), 0x19 (CTRL-Y) o 0x0A (nueva línea).
- De forma predeterminada, las vías de acceso no debe contener caracteres comodín. No incluya asterisco (\*) o interrogaciones (?) en una vía de acceso. Esta restricción se puede alterar temporalmente si habilita la opción denominada wildcardsareliteral. Para obtener más información sobre esta opción, consulte Wildcardsareliteral.
-  sistemas operativos Mac OS X  Sistemas operativos Windows Filelist puede ser un archivo MBCS o un archivo Unicode con todas las entradas Unicode. En Mac OS X, la lista de archivos se puede codificar en el lenguaje del sistema operativo actual o UTF-16.
- Si se ha establecido, la opción del cliente denominada quotessareliteral permite que se interpreten literalmente comillas en una especificación de archivo, como comillas y no como delimitadores. Para obtener más información sobre esta opción, consulte Quotessareliteral. Si no se establecen quotessareliteral ni wildcardsareliteral, las comillas dobles y el proceso de comodín funciona tal como se describe en la lista siguiente:
  - Si una vía de acceso o un nombre de archivo contiene un espacio, encierre la vía de acceso completamente entre comillas (") o apóstrofes ('). Por ejemplo "C:\Mis Documentos\spreadsheet.xls" o 'C:\Mis documentos\spreadsheet.xls'.
  - Si una vía de acceso contiene uno o más apóstrofes ('), encierre la entrada completamente entre comillas ("). Si una vía de acceso contiene una o más comillas dobles, encierre la vía de acceso completamente entre apóstrofes. El proceso de lista de archivos no da soporte a vías de acceso con una mezcla de comillas y apóstrofes.

Los ejemplos siguientes ilustran el uso correcto e incorrecto de comillas dobles y de apóstrofes en las vías de acceso.

Esta vía de acceso de ejemplo contiene un apóstrofo, por lo que debe estar encerrada entre comillas:

```
"/home/gatzby/mydir/gatzby's_report.out"
```

Esta vía de acceso de ejemplo contiene un apóstrofo, por lo que debe estar encerrada entre apóstrofes:

```
'/home/gatzby/mydir/"top10".out'
```



Este ejemplo de vía de acceso contiene un carácter de espacio, por lo que debe encerrarse entre apóstrofes o comillas:

```
"/home/gatzby/mydir/top 10.out"
```

o bien

```
'/home/gatzby/mydir/top 10.out'
```

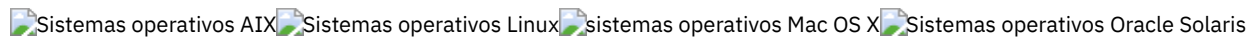
Esta vía de acceso de ejemplo no está soportada para ser procesada como lista de archivos porque contiene delimitadores no equilibrados (" y '):

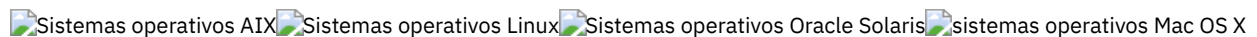
```
/home/gatzby/mydir/andy's_"top 10" report.out
```

Estas vías de acceso no están soportadas para el proceso de lista de archivos porque contiene caracteres comodín:

```
/home/gatzby*  
/home/*/20??.txt
```

- Cualquier entrada de lista de archivos de IBM Spectrum Protect que no cumpla con estas reglas será ignorada.

 Sistemas operativos AIX, Sistemas operativos Linux, sistemas operativos Mac OS X, Sistemas operativos Oracle Solaris, Sistemas operativos Windows. Los siguientes son ejemplos de vías de acceso válidas en una lista de archivos:

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X

```
/home/dir/file1  
/usr/tivoli/file2  
/usr/avi/dir1  
/fs1/dir2/file3  
"/fs2/Ha Ha Ha/file.txt"  
"/fs3/file.txt"
```

 Sistemas operativos Windows

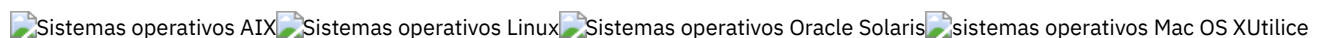
```
c:\myfiles\directory\file1  
c:\tivoli\mydir\yourfile.doc  
..\notes\avi\dir1  
..\fs1\dir2\file3  
"d:\fs2\Ha Ha Ha/file.txt"  
"d:\fs3\file.txt"
```

Para alterar temporalmente el proceso estándar de caracteres de comillas y comodín, consulte `Quotesareliteral` y `Wildcardsareliteral`.

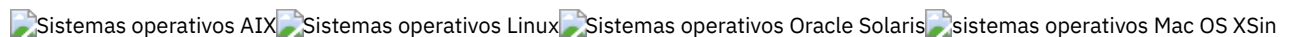
Puede utilizar la opción `filelist` durante una operación de soporte de archivos abiertos. En tal caso, el cliente procesa las entradas en la lista de archivos del volumen virtual en lugar de en el volumen real.

Si una entrada de `filelist` se refiere a un directorio, sólo se procesará dicho directorio, y no los archivos que contenga ese directorio.


Si el nombre de archivo (la `filelistspec`) que especifica con la opción `filelist` no existe, el mandato no se ejecuta correctamente. El cliente pasa por alto todas las entradas en `filelist` que no sean archivos o directorios válidos. El cliente registra los errores y el proceso pasa a la siguiente entrada.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X. Utilice especificaciones de archivo con los mandatos `restore` y `retrieve` para indicar el destino de las entradas restauradas de `filelist`. Por ejemplo, en el siguiente mandato `restore`, la especificación de archivo `/user/record/` representa el destino de la restauración de todas las entradas de `filelist`.

```
restore -filelist=/home/dir/file3 /usr/record/
```

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X. Sin embargo, en el siguiente mandato `selective`, la especificación de archivo `/usr/record/` se pasa por alto.

```
selective -filelist=/home/dir/file3 /usr/record/
```

 Sistemas operativos Windows. Utilice especificaciones de archivo con los mandatos `restore` y `retrieve` para indicar el destino de las entradas restauradas de `filelist`. Por ejemplo, en el siguiente mandato `restore`, `d:\dir\` representa el destino de la restauración de todas las entradas de `filelist`.

```
restore -filelist=c:\filelist.txt d:\dir\
```

 Sistemas operativos Windows. Sin embargo, en el siguiente mandato `selective`, la especificación de archivo `d:\dir\` se pasa por alto.

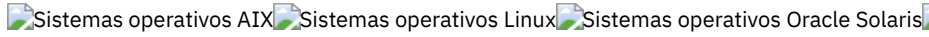
```
selective -filelist=c:\filelist.txt d:\dir\
```


Si especifica un directorio en una lista de archivos para el mandato delete archive o delete backup, el directorio no se suprime. Las listas de archivos que utilice con el mandato delete archive o delete backup no deben incluir directorios.

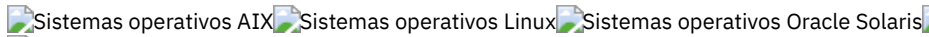

Las entradas de la lista se procesan en el orden en que aparecen en filelist. Para obtener un rendimiento óptimo del proceso, clasifique previamente filelist por nombre de espacio de archivos y por vía de acceso.

Nota: El cliente puede hacer una copia de seguridad de un directorio dos veces si se producen las condiciones siguientes:

- Filelist contiene una entrada para el directorio
- Filelist contiene una o varias entradas para los archivos de dicho directorio
- No existe ninguna copia de seguridad del directorio

 Por ejemplo, la lista de archivos incluye las entradas /home/dir/file1 y /home/dir. Si el directorio /dir no existe en el servidor, el directorio /home/dir se envían al servidor por segunda vez.

 Por ejemplo, filelist incluye las entradas c:\dir0\myfile y c:\dir0. Si el directorio \dir0 no existe en el servidor, el directorio c:\dir0 se envía al servidor por segunda vez.

## Cientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

```
>>-FILEList = - --filelistspec-----<<
```

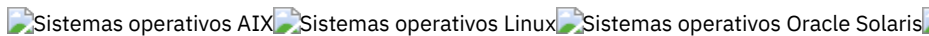
## Parámetros

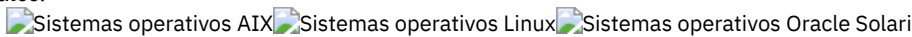
especificación lista archivos


Especifica la ubicación y el nombre del archivo que contiene la lista de archivos que deben procesarse con el mandato.


Nota: cuando especifique la opción filelist en la línea de mandatos, la opción subdir se pasa por alto.

## Ejemplos

 Línea de mandatos:

 sel -filelist=/home/avi/filelist.txt

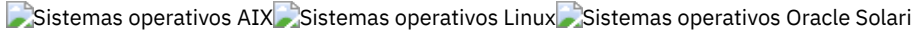
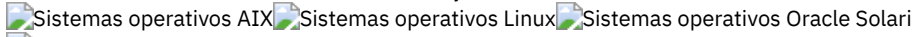

 Línea de mandatos:

 sel -filelist=c:\avi\filelist.txt

## Filename


Utilice la opción filename con el mandato query systeminfo para especificar un nombre de archivo en el que almacenar la información.

Puede almacenar la información recopilada de uno o varios de los elementos siguientes:

- DSMOPTFILE: el contenido del archivo dsm.opt.
-  DSMSYSFILE - El contenido del archivo dsm.sys.
-  ENV - Variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores de IBM Spectrum Protect.
- FILE - Atributos para el nombre de archivo que especifique.
-  FILESNOTTOBACKUP: enumeración de la clave de registro de Windows:










```
HKEY_LOCAL_MACHINE\  
SYSTEM\  
CurrentControlSet\  
BackupRestore\  
FilesNotToBackup
```

Esta clave especifica los archivos para los que los productos de copia de seguridad no deberían realizar ninguna copia de seguridad. El mandato query inclexcl indicará que el sistema operativo excluirá dichos archivos.




- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
-  Sistemas operativos WindowsKEYSNOTTORESTORE: enumeración de la clave de registro de Windows:

```
HKEY_LOCAL_MACHINE\  
  SYSTEM\  
    ControlSet001\  
      BackupRestore\  
        KeysNotToRestore
```






Esta clave especifica las claves de registro de Windows que los productos de copia de seguridad no deberían restaurar.

-  Sistemas operativos WindowsMSINFO: información del sistema Windows (salida de MSINFO32.EXE).
- OPTIONS - Opciones compiladas.
-  Sistemas operativos WindowsOSINFO - Nombre y versión del sistema operativo cliente.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X OSINFO - Nombre y versión del sistema operativo cliente (incluye información ULIMIT para UNIX y Linux).
- POLICY - Volcado del conjunto de políticas.
-  Sistemas operativos WindowsREGISTRY - Entradas de registro de Windows relacionadas con IBM Spectrum Protect.
- SCHEDLOG - Contenido del registro de planificación (por lo general, dsmsched.log).
-  Sistemas operativos WindowsSFP: la lista de archivos protegidos por la característica de protección de archivos del sistema Windows y, para cada archivo, indica si dicho archivo existe. Se hace una copia de seguridad de estos archivos como parte del objeto del sistema SYSFILES.
-  Sistemas operativos WindowsSFP=*filename* - Indica si el archivo especificado (*filename*) se ha protegido mediante la Protección de archivos del sistema de Windows. Por ejemplo:

```
SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
```

-  Sistemas operativos WindowsSYSTEMSTATE: información de estado del sistema de Windows.
-  Sistemas operativos AIXCLUSTER - Información de clústeres de AIX.
-  Sistemas operativos WindowsCLUSTER - Información de clústeres de Windows.

Nota: La principal finalidad del mandato query systeminfo es ayudar al soporte de IBM® en el diagnóstico de problemas, aunque los usuarios que estén familiarizados con los conceptos relacionados con esta información también podrían encontrarlo de utilidad. Si utiliza la opción console, no se realiza ningún formato especial de la salida para ajustarla a la altura o anchura de la pantalla. Por consiguiente, es posible que la salida de la consola sea difícil de leer debido a la longitud y a la acomodación de líneas. En este caso, se recomienda utilizar la opción filename con el mandato query systeminfo para que la salida se grabe en un archivo que, posteriormente, podrá enviarse al soporte de IBM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Sintaxis

---

```
>>-FILENAME = - --outputfilename-----<<
```

## Parámetros

---

nombearchivosalida

Especifica un nombre de archivo en el que ha de almacenarse la información. Si no especifica un nombre de archivo, la información se almacenará, de forma predeterminada, en el archivo dsminfo.txt.

## Ejemplos

---

Línea de mandatos:

```
query systeminfo dsmpoptfile errorlog -filename=tsminfo.txt
```

## Filesonly






---

La opción filesonly restringe los procesos de copia de seguridad, restauración, recuperación o consulta a *sólo* los archivos.

No puede restaurar o recuperar directorios del servidor de IBM Spectrum Protect cuando utiliza la opción `filesonly` con los mandatos `restore` o `retrieve`. Sin embargo, se crean directorios con atributos predeterminados, si es necesario, como marcadores de posición para los archivos que restaure o recupere.

También puede utilizar la opción `filesonly` con los mandatos siguientes:

- `archive`
- `incremental`
- `query archive`
- `query backup`
- `restore`
- `restore backupset`
- `restore group`
- `retrieve`
- `selective`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-FILESOnly-----><
```











## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows Línea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows `dsmc incremental -filesonly`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Followsymbolic

---

Durante una operación de copia de seguridad, la opción `followsymbolic` especifica si desea utilizar un enlace simbólico como punto de montaje virtual. Durante una operación de restauración o recuperación, la opción `followsymbolic` especifica cómo el cliente de copia de seguridad y archivado restaura un directorio cuyo nombre coincide con un enlace simbólico en el sistema de archivos de destino de restauración.

Para operaciones de copia de seguridad, la opción `followsymbolic` puede influenciar el valor de la opción `virtualmountpoint`. Si utiliza la opción `virtualmountpoint` para especificar un enlace simbólico como punto de montaje virtual, debe establecer también la opción `followsymbolic`.

Durante las operaciones de restauración y recuperación, `followsymbolic` puede influenciar cómo el cliente maneja un enlace simbólico en el sistema de archivos. Establezca la opción `followsymbolic` sólo cuando el cliente intente restaurar un directorio cuyo nombre coincida con un enlace simbólico en el sistema de archivos de destino de la restauración.

Si especifica `followsymbolic=no` (valor predeterminado), el cliente no restaurará el contenido del directorio, sino que devolverá el siguiente mensaje de error:

```
ANS4029E Error al procesar 'nombre de espacio de archivos nombre de vía de acceso
nombre de archivo':
no se pudo crear una vía de acceso de directorio; ya existe
un archivo con el mismo nombre
que un directorio.
```

Si especifica `followsymbolic=yes`, el cliente restaura el contenido del directorio en el destino del enlace simbólico.

Por ejemplo, imaginemos que el cliente ha realizado copia de seguridad de un archivo con esta vía de acceso: /fs1/dir1/subdir1/file1. Imaginemos también que existe en el sistema de archivos de destino de la restauración un enlace simbólico /fs1/dir1, que está vinculado con /fs88/dir88/subdir88. Restaure el archivo con el mandato:

```
restore /fs1/dir1/subdir1/file1
```

Si especifica `followsymbolic=no`, el cliente no restaura el archivo, sino que devuelve el mensaje de error precedente. Si especifica `followsymbolic=yes`, el cliente restaura file1 en /fs88/dir88/subdir88/subdir1/file1.

Si restaura un enlace simbólico (no un directorio) cuyo nombre coincide con un enlace simbólico en el sistema de archivos de destino de la restauración, el cliente restaura el enlace simbólico.

Si se utiliza un enlace simbólico como punto de montaje virtual, la vía de acceso al destino del enlace deberá especificarse utilizando una vía de acceso de archivo absoluta.

Utilice esta opción con los mandatos `restore` y `retrieve`, o en el archivo de opciones de usuario del cliente (`dsm.opt`).

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX, a excepción de Mac OS X.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones de cliente (`dsm.opt`).

## Sintaxis

---

```
.-No--.  
>>-FOLlowsymbolic-----+-----<<  
'-Yes-'
```

## Parámetros

---

No

No realiza copia de seguridad de un punto de montaje que es un enlace simbólico. No restaura un directorio si el sistema de archivos de destino de la restauración contiene un enlace simbólico con un nombre coincidente. Éste es el valor predeterminado.

Yes

Restaura el contenido de un directorio en el destino de un enlace simbólico.

## Ejemplos

---

Archivo de opciones:

```
followsymbolic Yes
```

Línea de mandatos:

```
-fol=Yes
```

## Forcefailover

---

La opción `forcefailover` permite al cliente migrar tras error inmediatamente al servidor secundario.

Puede utilizar la opción `forcefailover` para conectar inmediatamente con el servidor secundario, aunque el servidor primario continúe en línea. Por ejemplo, puede utilizar esta opción para verificar que el cliente de archivado de copia de seguridad está migrando tras error en el servidor secundario esperado.

No edite esta opción durante las operaciones normales.





## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones



---









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Coloque esta opción en el archivo de opciones del sistema cliente (`dsm.sys`).





Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.

## Ejemplos

 sistemas operativos Mac OS X Línea de mandatos:  
 sistemas operativos Mac OS X `dsmc query backup -fromdate=12/11/2003 "/Users/van/Documents/*"`









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `dsmc query backup -fromdate=12/11/2003 /home/dilbert/*`






 Sistemas operativos Windows Línea de mandatos:  
 Sistemas operativos Windows `dsmc query backup -fromdate=12/11/2003 c:\Windows\Program Files\*.exe`

## Fromnode

La opción `fromnode` permite que un nodo realice mandatos para otro nodo. Un usuario de otro nodo debe utilizar el mandato `set access` para permitirle consultar, restaurar o recuperar archivos para el otro nodo.

La opción `fromnode` puede utilizarse con los mandatos siguientes:

- `query archive`
- `query backup`
- `query filespace`
-  Sistemas operativos Windows `query group`
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `query image`
- `query mgmtclass`
- `restore`
- `restore group`
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `restore image`
- `retrieve`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

Esta opción es válida para todos los clientes.

## Sintaxis



```
>>>-FROMNode = - --nodo-----><
```









## Parámetros



`nodo`


Especifica el nombre de nodo en una estación de trabajo o un servidor de archivos a cuyas copias de seguridad o copias archivadas se quiere acceder.

## Ejemplos





 sistemas operativos Mac OS X Línea de mandatos:  
 sistemas operativos Mac OS X `dsmc query archive -fromnode=bob -subdir=yes "/Users/van/Documents/*"`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `dsmc query archive -fromnode=bob -subdir=yes "/home/jones/*"`

 Sistemas operativos Windows Línea de mandatos:  
 Sistemas operativos Windows `dsmc query archive -fromnode=bob -subdir=yes d:\`

 Sistemas operativos Windows Nota: El cliente de copia de seguridad y archivado puede utilizar la información de espacio de archivos al restaurar archivos. La información de espacio de archivos puede contener el nombre del sistema desde el que se ha realizado la copia de seguridad de los archivos. Si realiza la restauración desde otro nodo cliente de copia de seguridad y archivado y no especifica un

destino para los archivos restaurados, el cliente utilizará la información de espacio de archivos para restaurar los archivos. En este caso, el cliente intentará restaurar los archivos en el sistema de archivos del sistema original. Si el sistema de la restauración dispone de acceso al sistema de archivos del sistema original, puede restaurar archivos en el sistema de archivos original. Si el sistema de archivos de la restauración no dispone de acceso a la unidad del sistema original, el cliente puede devolver un mensaje de error de red. Si desea restaurar la estructura de directorios original pero en un sistema distinto, especifique sólo el sistema de archivos de destino cuando realice la restauración. Esto es cierto cuando se restauran archivos de otro nodo y cuando se recuperan archivos de otro nodo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X


## Fromowner

---

La opción `fromowner` especifica un propietario alternativo del que restaurar versiones de copia de seguridad o copias archivadas o imágenes. El propietario debe otorgar acceso a otro usuario para que éste utilice los archivos o imágenes.

Por ejemplo, para restaurar archivos del directorio `/home/devel/proja` que pertenece al usuario `usermike` del sistema **puma**, y colocar los archivos restaurados en un directorio de su propiedad denominado `/home/id/proja`, introduzca el mandato siguiente:

```
dsmc restore -fromowner=usermike -fromnode=puma /home/devel/proja/  
/home/id/proja/
```

 sistemas operativos Mac OS X Nota: El archivado de las restauraciones de imágenes no se aplica a los sistemas operativos Mac OS X.

Los usuarios que no sean `root` pueden especificar `-fromowner=root` para acceder a los archivos propiedad del usuario `root`, si éste les ha otorgado acceso a los archivos.

**Nota:** si se especifica la opción `fromowner` sin la opción `fromnode`, el usuario activo debe estar en el mismo nodo que el usuario `fromowner`.

La opción `fromowner` puede utilizarse con los mandatos siguientes:

- `query archive`
- `query backup`
- `query group`
- `query image`
- `restore`
- `restore image`
- `restore group`
- `retrieve`

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux.

## Sintaxis

---

```
>>-FROMowner = - --propietario-----<<
```

## Parámetros

---

propietario  
Nombre de un propietario alternativo.

## Ejemplos

---

Línea de mandatos:  
`dsmc query archive "/home/id/proja/*" -fromowner=mark`

## Fromtime

---






Utilice la opción `fromtime` con la opción `fromdate` para especificar una fecha a partir de las cuales desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

El cliente de copia de seguridad y archivado pasa por alto esta opción si no especifica la opción `fromdate`.

La opción `fromtime` puede utilizarse con los mandatos siguientes:



- delete backup
- query archive
- query backup
- restore
- restore group
- retrieve

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-FROMTime = - --hora-----<<
```

## Parámetros

---





hora





Especifica una hora de inicio en una fecha específica a partir de la cual desea buscar copias de seguridad o copias archivadas. Si no especifica una hora, se utiliza el valor predeterminado 00:00:00. Especifique la hora en el formato seleccionado con la opción timeformat.

Si incluye la opción timeformat en un mandato, ésta deberá preceder a las opciones fromtime, pittime y totime.


## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 dsmsc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM -tod=06/30/2003 /home/\*





 Sistemas operativos Windows  
 Línea de mandatos:

 Sistemas operativos Windows  
 dsmsc q b -timeformat=4 -fromt=11:59AM -fromd=06/30/2003 -tot=11:59PM -tod=06/30/2003 c:\\*

## Groupname




---


Utilice la opción groupname con el mandato backup group para especificar el nombre de un grupo. Sólo podrá realizar operaciones en grupos nuevos o en la versión actualmente activa del grupo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

 Sistemas operativos Windows  
 Esta opción es válida para todos los clientes Windows.

## Sintaxis

---

```
>>-GROUPName = - --nombre-----<<
```

## Parámetros

---




nombre

Especifica el nombre del grupo que contendrá los archivos de los que se ha realizado una copia de seguridad utilizando la opción filelist. No se permite el uso de delimitadores de directorio en el nombre de grupo, ya que no se trata de una especificación de archivo sino de un campo de nombre.

## Ejemplos

---

Línea de mandatos:

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```



```
backup group -filelist=c:\dir1\filelist1 -groupname=group1  
-virtualfsname=\virtfs -mode=full
```

## Grupos (obsoleto)

---

Esta opción está obsoleta.


 

## Host

---

El host especifica la ubicación del servidor ESX de destino donde se crea la máquina virtual durante una operación de restauración de VMware.

Utilice esta opción en mandatos restore vm para especificar el servidor de host ESX en el que se deben restaurar los datos.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Ejemplo

---






Restaura la máquina virtual en el servidor de ESX denominado vmesxbld1.

```
restore vm -host=vmesxbld1.us.acme.com
```

## Httpport

---

La opción httpport especifica una dirección de puerto TCP/IP para el cliente web.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

     
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador Cliente web, en el campo Puerto HTTP del editor de preferencias.

 Especifique esta opción en el archivo de opciones del sistema cliente (dsm.opt). Puede establecer esta opción en el separador Cliente web, en el campo Puerto HTTP del editor de preferencias.

## Sintaxis

---

```
>>-HTTPport-- --port_address-----><
```

## Parámetros

---

port\_address

Especifica la dirección de puerto TCP/IP que se utiliza para la comunicación con el cliente web. El rango de valores es de 1000 a 32767, siendo 1581 el valor predeterminado.

## Ejemplos

---





Archivo de opciones:





```
httpport 1502
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
-httpport=1502
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X No se aplica.

## Hsmreparsetag

---

La opción hsmreparsetag especifica un código de reanálisis exclusivo que crea un producto HSM instalado en el sistema.

Muchos productos HSM utilizan puntos de reanálisis para recuperar archivos migrados. Tras migrar un archivo, en el sistema de archivos se deja un pequeño archivo de resguardo con el mismo nombre que el archivo original. El archivo de resguardo es un punto de reanálisis que desencadena una recuperación del archivo original cuando un usuario o una aplicación accede al archivo de resguardo. El punto de reanálisis incluye un identificador exclusivo llamado *código de reanálisis* para identificar el producto HSM que migró el archivo.

Si el cliente de archivado y copia de seguridad de IBM Spectrum Protect no reconoce el código de reanálisis en un archivo de resguardo, dicho cliente de archivado y copia de seguridad hace que el producto HSM recupere el archivo original. Puede impedir que los archivos se recuperen si especifica el código de reanálisis con la opción hsmreparsetag.

El cliente de archivado y copia de seguridad reconoce el código de reanálisis de los productos HSM de las siguientes empresas:

- International Business Machines Corp.
- Wisdata System Co. Ltd.
- BridgeHead Software Ltd.
- CommVault Systems, Inc.
- Data Storage Group, Inc.
- Enigma Data Solutions, Ltd.
- Enterprise Data Solutions, Inc.
- Global 360
- GRAU DATA AG
- Hermes Software GmbH
- Hewlett Packard Company
- International Communication Products Engineering GmbH
- KOM Networks
- Memory-Tech Corporation
- Moonwalk Universal
- Pointsoft Australia Pty. Ltd.
- Symantec Corporation

Si el producto HSM que utiliza no está en la lista anterior, utilice la opción hsmreparsetag para especificar el código de reanálisis. Pregunte al proveedor de su producto HSM por el código de reanálisis que utiliza el producto.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>---HSMREPARSETAG---valor_código_reanálisis-----<<
```

## Parámetros

---

valor\_código\_reanálisis

Un valor en base decimal (base 10) o hexadecimal (base 16) que especifica el código de reanálisis.

## Ejemplos

---

Archivo de opciones:

Especifique un código de reanálisis de HSM en formato decimal:

```
hsmreparsetag 22
```

Especifique un código de reanálisis de HSM en formato hexadecimal:

```
hsmreparsetag 0x16
```

Línea de mandatos:

No se aplica.

## Ieobjtype

---

Utilice la opción ieobjtype para especificar un tipo de objeto para la operación de eliminación de duplicación de datos por parte del cliente dentro de las sentencias de inclusión/exclusión.

La opción ieobjtype es un parámetro adicional a las opciones include.dedup o exclude.dedup.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect también soporta esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones del sistema (dsm.sys). Puede establecer esta opción en la ficha Incluir/excluir del editor de preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Incluir/excluir del editor de preferencias. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
.-File-----.  
>>-IEObjtype--+-Image-----+-----<<  
+-SYSTEMState-+  
'-Asr-----'
```

## Parámetros


---


File


Especifica que desea incluir archivos para, o excluir archivos desde, el proceso de eliminación de duplicación de datos por parte del cliente. File es el valor predeterminado.


Image

Especifica que desea incluir imágenes para, o excluir imágenes desde, el proceso de eliminación de duplicación de datos por parte del cliente.

 Sistemas operativos Windows System State

 Sistemas operativos Windows Especifica que desea incluir el estado del sistema para, o excluir el estado del sistema desde, el proceso de eliminación de duplicación de datos por parte del cliente.

 Sistemas operativos Windows Asr

 Sistemas operativos Windows Especifica que desea incluir objetos de recuperación del sistema automáticos para, o excluir objetos de recuperación del sistema automáticos desde, el proceso de eliminación de duplicación de datos por parte del cliente.

## Ejemplos

---

Archivo de opciones:

```
exclde.dedup e:\*\* ieobjtype=image
exclde.dedup /home/*/* ieobjtype=image
```

Línea de mandatos:

No se aplica.

### Referencia relacionada:

Opciones exclude  
Opciones include

## Ifnewer

---

La opción ifnewer sustituye un archivo existente por la última versión de copia de seguridad si ésta es más reciente que el archivo existente.

Únicamente se tienen en cuenta las copias de seguridad activas, a menos que se utilicen además las opciones inactive o latest.

**Nota:** las entradas de directorio se sustituyen por la última versión de copia de seguridad, independientemente de si la versión de copia de seguridad es más antigua o más nueva que la versión existente.

La opción ifnewer puede utilizarse con los mandatos siguientes:

- restore
- restore backupset
- restore group
- retrieve

Nota: esta opción se pasa por alto si la opción replace está establecida en No.

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-IFNewer-----<<
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:

```
dsmc restore "/Users/grover/Documents/*" -sub=y -rep=y -ifnewer
dsmc restore "/home/grover/*" -sub=y -rep=y -ifnewer
```

Línea de mandatos:

```
dsmc restore -ifnewer d:\logs\*.log
```

## Imagegapsize

---

Utilice la opción imagegapsize con el mandato backup image, en el archivo de opciones, o con la opción include.image para especificar el tamaño mínimo de las regiones vacías de un volumen que desea pasar por alto durante la realización de la copia de seguridad de imágenes.



Utilice esta opción para la copia de seguridad de imagen basada en LAN y sin LAN.


Por ejemplo, si especifica un tamaño de intervalo de 10, significa que no se hará copia de seguridad de una región vacía del disco que tenga más de 10 KB. Se hará copia de seguridad de los intervalos que tengan un tamaño exacto de 10 KB. Se hará una copia de seguridad de las regiones vacías que tienen exactamente 10 KB y menos de 10 KB, aunque no contengan datos. Sin embargo, se hará copia de seguridad de una región vacía que tenga menos de 10 KB, aunque no contenga datos. Un tamaño de intervalo de imagen más pequeño significa que es necesario transferir menos datos, aunque puede reducirse el rendimiento. Un tamaño de intervalo de imagen más grande implica que se transfieren más datos, aunque puede obtenerse un mayor rendimiento.

 Sistemas operativos Windows Establezca la sentencia `include.image` que contiene el valor `imagegapsize` en el archivo `dsm.opt`.

## Cientes soportados


---


 Sistemas operativos AIX  Sistemas operativos Linux Esta opción sólo es válida para clientes AIX, Linux y JFS2. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX Especifique esta opción en la stanza de servidor del archivo de opciones del sistema cliente (`dsm.sys`) o en la sentencia `include.image` del archivo `dsm.sys`.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis


---


```
>>-IMAGEgapsize-- --size-----><
```


## Parámetros

---

 Sistemas operativos AIX `size`

 Sistemas operativos AIX Especifica el tamaño mínimo de las regiones vacías de un sistema de archivos JFS2 de AIX que debe pasarse por alto durante una copia de seguridad de imágenes. Puede especificar los calificadores `k` (kilobytes) `m` (megabytes) o `g` (gigabytes) con el valor. Si no se especifica ningún calificador, el valor se interpreta en kilobytes. Los valores válidos van de 0 a 4294967295 KB. Si especifica 0, se realizará copia de seguridad de todos los bloques, incluidos los bloques no utilizados del final del volumen. Si especifica un valor distinto de 0, no se realizará copia de seguridad de los bloques no utilizados del final del volumen. Para la copia de seguridad de imágenes basada en red de área local y fuera de la red de área local, el valor predeterminado es 32 KB. Esta opción se aplica tanto a la copia de seguridad estática como a la basada en instantánea.  
Nota: Esta opción es válida para los sistemas de archivos JFS2 de AIX. Si especifica un valor de `imagegapsize` mayor que 0 para un sistema de archivos que no sea AIX JFS2, recibirá un mensaje de aviso.


 Sistemas operativos Windows `ssize`

 Sistemas operativos Windows Especifica el tamaño mínimo de las regiones vacías en un volumen lógico con formato que debe omitirse durante una copia de seguridad de imágenes. Puede especificar los calificadores `k` (kilobytes) `m` (megabytes) o `g` (gigabytes) con el valor. Si no se especifica ningún calificador, el valor se interpreta en KB. Los valores válidos van de 0 a 4294967295 KB. Si especifica 0, se realizará copia de seguridad de todos los bloques, incluidos los bloques no utilizados del final del volumen. Si especifica un valor distinto de 0, no se realizará copia de seguridad de los bloques no utilizados del final del volumen. Para la copia de seguridad de imágenes basada en red de área local y fuera de la red de área local, el valor predeterminado es 32 KB.  
Nota: Debido a las limitaciones del sistema operativo, utilice esta opción solo para sistemas de archivos NTFS. Si especifica un valor de `imagegapsize` mayor que 0 para un sistema de archivos que no sea NTFS, recibirá un mensaje de aviso.

## Ejemplos


---

 Sistemas operativos AIX Archivo de opciones:

 Sistemas operativos AIX Añada lo siguiente a la stanza de servidor del archivo `dsm.sys`: `imagegapsize 1m`





Ejemplo de lista de inclusión/exclusión: `include.image /kalafs1 imagegapsize=-128k`

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows `imagegapsize 1m`

Ejemplo de lista de inclusión/exclusión: `include.image h: MYMC imagegapsize=1m`

Línea de mandatos:  
-imagegapsize=64k


   




## Imagetofile

---

Utilice la opción `imagemetofile` con el mandato `restore image` para especificar que desea restaurar la imagen de origen en un archivo.

Puede que tenga que restaurar la imagen de un archivo si existen sectores defectuosos en el volumen de destino o si desea manipular los datos de la imagen. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

 Linux admite el montaje de un archivo de imagen como volumen lógico, por lo tanto, puede obtener acceso a los datos del archivo dentro de la imagen. A continuación se muestran algunos ejemplos:




  

- El cliente de archivado y copia de seguridad ha realizado una copia de seguridad del sistema de archivos `/usr`. El siguiente mandato restaurará la imagen del sistema de archivos en el archivo `/home/usr.img`:

```
# dsmc restore image /usr /home/usr.img -imagemetofile
```




- Para montar el archivo de imagen en el directorio `/mnt/usr`, puede ejecutarse el mandato de montaje siguiente:


```
# mount /home/usr.img /mnt/usr -o loop=/dev/loop0
```

   Ahora, el contenido de la imagen está disponible desde `/mnt/usr`, como si en ese directorio se hubiera montado un sistema de archivos normal.

## Clientes soportados

---

   Esta opción solo es válida para clientes de AIX, Oracle Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

 Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-IMAGETOfile-----<<
```







## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

   Línea de mandatos:  
    
`dsmc restore image /usr /home/usr.img -imagemetofile`






 Línea de mandatos:  
  
`dsmc restore image d: e:\diskD.img -imagemetofile`

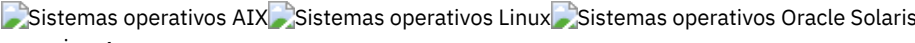



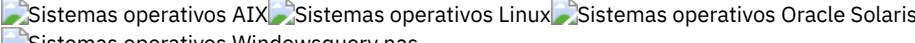






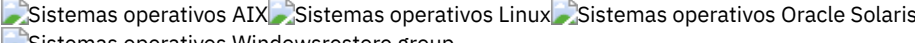




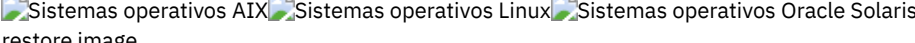



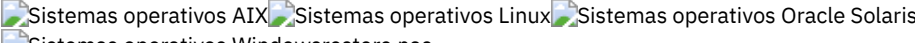





## Inactive





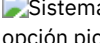
---

Utilice la opción `inactive` para que se visualicen los objetos activos e inactivos.

Puede utilizar la opción `inactive` con los mandatos siguientes:

- `delete group`
-  `query asr`
- `query backup`
-     `query group`

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows query image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsquery nas
-  Sistemas operativos Windowsquery systemstate
-  Sistemas operativos Windowsquery vm (vmbackuptype=fullvm and vmbackuptype=hypervfull)
- restore
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsrestore group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows restore image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsrestore nas
-  Sistemas operativos Windowsrestore vm (vmbackuptype=fullvm and vmbackuptype=hypervfull)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos WindowsImportante: Cuando utilice la opción inactive durante una operación de restauración, utilice también la opción pick u otra opción de filtro porque, a diferencia de la opción latest, todas las versiones se restaurarán en un orden indeterminado. Esta opción es implícita cuando se utiliza pitdate.

## Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.



## Sintaxis

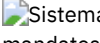







```
>>-INActive-----<<
```



## Parámetros

No hay parámetros para esta opción.

## Ejemplos

 sistemas operativos Mac OS XLínea de mandatos:  
 sistemas operativos Mac OS Xdsmc restore "/Users/zoe/Documents/\*" -inactive -pick

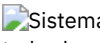
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
dsmc restore "/home/zoe/\*" -inactive -pick

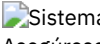



 Sistemas operativos WindowsLínea de mandatos:  
 Sistemas operativos Windowsdsmc restore -inactive c:\id\projecta\ -pick

## Incl excl





La opción incl excl especifica la vía de acceso y el nombre de archivo de un archivo de opciones de inclusión/exclusión.

Se permiten varias sentencias incl excl. Sin embargo, debe especificar esta opción para cada archivo de inclusión/exclusión.

 Sistemas operativos WindowsAsegúrese de almacenar el archivo de opciones de inclusión/exclusión en un directorio para el que todos los usuarios dispongan de acceso de lectura.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Asegúrese de almacenar el archivo de opciones de inclusión/exclusión en un directorio para el que todos los usuarios dispongan de acceso de lectura, como /etc.

Durante el proceso, las sentencias de inclusión/exclusión del archivo de inclusión/exclusión se colocan en la posición de lista ocupada por la opción incl excl, en el mismo orden, y se procesan en consecuencia.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XSi tiene el cliente de HSM instalado en la estación de trabajo, puede utilizarse un archivo de opciones de inclusión/exclusión para excluir archivos de la copia de seguridad y de la gestión de espacio o para excluir sólo de una de ambas operaciones.







## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Incluya esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha Incluir/excluir del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Incluir/excluir del editor de preferencias.

## Sintaxis

---

```
>>-INCLExcl-- --filespec-----><
```

## Parámetros

---

filespec

Especifica la vía de acceso y el nombre de archivo de un archivo de opciones de inclusión/exclusión.



## Ejemplos

---

Archivo de opciones:

 sistemas operativos Mac OS X

```
INCLExcl /Users/user1/Documents/backup.excl
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
incl excl /usr/dsm/backup.excl  
incl excl /etc/incl excl.def
```

 Sistemas operativos Windows

```
incl excl c:\dsm\backup.excl
```

Línea de mandatos:

No se aplica.






- Consideraciones sobre los clientes habilitados para Unicode  
Un archivo de inclusión/exclusión puede tener formato Unicode o que no sea Unicode.

## Opciones include

---


Las opciones include especifican los objetos que desea incluir para los servicios de copia de seguridad y archivado.

Las opciones de inclusión especifican cualquiera de los elementos siguientes:

-  sistemas operativos Mac OS X Objetos de un amplio grupo de objetos excluidos que desea incluir para los servicios de copia de seguridad y archivado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Objetos de un amplio grupo de objetos excluidos que desea incluir para los servicios de copia de seguridad, archivado, imagen y gestión de espacio.
-  Sistemas operativos Windows Objetos de un amplio grupo de objetos excluidos que desea incluir para los servicios de copia de seguridad, archivado e imagen.
- Archivos que se incluyen para el proceso de copia de seguridad o archivado que también desea incluir para el proceso de cifrado.
- Archivos que se incluyen para el proceso de copia de seguridad o archivado que desea incluir en el proceso de compresión.
- Objetos a los que se desea asignar una clase de gestión específica.
- Una clase de gestión para asignar a todos los objetos a los que no se asigna una clase de gestión de forma explícita.
- Espacios de archivos a que se desea asignar un proceso de copia de seguridad de memoria eficiente







- Espacios de archivo para los que desea utilizar la opción diskcachelocation con el fin de que sistemas de archivos específicos utilicen ubicaciones específicas distintas para la caché en disco de éstos.

Si no se asigna una clase de gestión específica a los objetos, se utiliza la clase de gestión predeterminada del conjunto de políticas activo del dominio de políticas. Utilice el mandato query mgmtclass para visualizar información sobre las clases de gestión disponibles en el conjunto de políticas activo.

 Sistemas operativos Windows Para incluir archivos a los que se accede de forma remota, especifique nombres UNC (Universal Naming Convention) en la sentencia include.

Recuerde: El cliente de copia de seguridad y archivado compara los archivos que procesa con los patrones especificados en las sentencias de inclusión y exclusión leyéndolas de abajo arriba en el archivo de opciones.





Nota:


1.  Sistemas operativos Windows La sentencia exclude.dir modifica temporalmente todas las sentencias de inclusión que coinciden con el patrón.
2.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Las sentencias exclude.fs y exclude.dir modifican temporalmente todas las sentencias de inclusión que coinciden con el patrón.
3.  Sistemas operativos Windows Las sentencias de include no son sensibles a las mayúsculas y minúsculas.
4. El servidor también puede definir estas opciones con la opción inclexcl.

## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir la opción include.fs.nas.

## Archivo de opciones




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer estas opciones en el separador Incluir/excluir del editor de preferencias.

 Sistemas operativos Windows Coloque estas opciones en el archivo de opciones del cliente (dsm.opt). Puede establecer estas opciones en el separador Incluir/excluir del editor de preferencias.

## Sintaxis

```
>>-opciones-- --patrón-- --+-----+-----<<
      '- --parámetro_opcional-'
```

include, include.backup, include.file

Utilice estas opciones para incluir archivos o asignar clases de gestión para el proceso de copias de seguridad. La opción include afecta al proceso de archivado y copia de seguridad. Si desea asignar distintas clases de gestión para proceso de archivado y copia de seguridad, especifique siempre include.archive e include.backup con sus propias clases de gestión. En el ejemplo siguiente, la clase de gestión archmc se asigna cuando se realiza una operación de archivado. La clase de gestión se asigna cuando se realiza una operación de archivado, puesto que include.backup utiliza solo para el proceso de copias de seguridad; no se utiliza para el proceso de archivado.  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X






```
include.archive /home/test/* archmc
include.backup /home/test/*
```

 Sistemas operativos Windows

```
include.archive c:\test\*\ archmc
include.backup c:\test\*
```


include.archive

Incluye archivos o asigna clases de gestión para los procesos de archivado.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X include.attribute.symlink





 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Incluye un archivo o un grupo de archivos que son enlaces simbólicos o alias en un grupo amplio de archivos excluidos del proceso de copia de seguridad únicamente.





 sistemas operativos Mac OS XNota: Para Mac OS X, se incluyen los alias.


#### include.compression

Incluye archivos para el proceso de compresión si establece la opción compression en yes. Esta opción se aplica a copias de seguridad y copias archivadas.



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windowsinclude.dedup

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos WindowsIncluye archivos para la eliminación de duplicados de datos por parte del cliente. Para controlar una operación de eliminación de duplicados de datos por parte del cliente, especifique ieobjtype como valor de la opción include.dedup. De forma predeterminada, todos objetos elegibles por eliminación de duplicación de datos se incluyen en la eliminación de duplicación de datos por parte del cliente.

Los parámetros ieobjtype válidos son:

- Archivo
- Imagen
-  Sistemas operativos WindowsSYSTEMState
-  Sistemas operativos WindowsAsr


El valor predeterminado es File.




#### include.encrypt


Incluye los archivos especificados para el proceso de cifrado. De forma predeterminada, el cliente no realiza el proceso de cifrado.

Notas:

1. El cifrado solo puede habilitarse en el cliente de copia de seguridad/archivado mediante la opción include.encrypt. Si no se utiliza ninguna sentencia include.encrypt, no se realizará el cifrado.
2. El cifrado no es compatible con la deduplicación del lado del cliente. Los archivos que se incluyen para el cifrado no se deduplican mediante la deduplicación del lado del cliente.
3. El cifrado no es compatible con las copias de seguridad de máquina virtual VMware que utilizan las modalidades de copia de seguridad siempre incremental (MODE=IFIncremental y MODE=IFFull). Si el cliente se configura para el cifrado, no se puede utilizar la copia de seguridad siempre incremental.
4. El cifrado no es compatible con IBM Spectrum Protect for Virtual Environments Data Protection for VMware Recovery Agent. Si el cliente se configura para cifrado, puede utilizar el cliente para restaurar las copias de seguridad que se hayan creado con las modalidades de copia de seguridad completa o incremental (MODE=Full y MODE=Incremental). Sin embargo, no puede utilizar Recovery Agent para restaurar las copias de seguridad cifradas. Las copias de seguridad creadas con la modalidad completa o incremental se han creado con el cliente de la versión 7.1 o anterior.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solarisinclude.fs

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 Sistemas operativos AIXPara los sistemas de archivos JFS2 de AIX: utilice la opción snapshotcachesize en el archivo dsm.sys o con la opción include.fs para especificar un tamaño de instantánea adecuado que permita que todos los bloques de datos antiguos puedan almacenarse mientras tiene lugar la operación de archivado o de copia de seguridad de archivos basada en instantánea.


Para controlar la forma en que el cliente ha de procesar el espacio de archivos para la copia de seguridad incremental, puede especificar estas opciones adicionales en el archivo dsm.sys, como valores de la opción include.fs: diskcachelocation y memoryefficientbackup.

Cada una de las opciones include.fs, memoryefficientbackup y diskcachelocation debe estar en la misma línea en el archivo de opciones.

```
include.fs /home
    memoryefficientbackup=diskcachemethod
    diskcachelocation=/usr
include.fs /usr
    memoryefficientbackup=diskcachemethod
    diskcachelocation=/home
include.fs /Volumes/hfs3
    memoryefficientbackup=diskcachemethod
    diskcachelocation=/Volumes/hfs2
AIX JFS2 filesystems only: include.fs
    /kalafs1 snapshotproviderfs=JFS2
```

Si estas opciones aparecen en el archivo de opciones y una opción include.fs, los valores de include.fs se utilizarán para el espacio del archivo especificado en lugar de los valores de un archivo de opciones o de la línea de mandatos.



 Sistemas operativos Windowsinclude.fs



 Sistemas operativos Windows Si se ha configurado el soporte de archivos abiertos, el cliente realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones tienen bloqueados (o en uso). La instantánea permite que la copia de seguridad pueda realizarse a partir de una copia de instante específico que coincida con el sistema de archivos en el momento de tomarse la instantánea. Los cambios que posteriormente se realicen en el sistema de archivos no se incluirán en la copia de seguridad. Puede establecer el parámetro `snapshotproviderfs` de la opción `include.fs` en `none` para especificar qué unidades no utilizan el soporte de archivos abiertos.

Para controlar la forma en que el cliente procesa el espacio de archivos para la copia de seguridad incremental, puede especificar estas opciones adicionales en el archivo `dsm.opt` como valores de la opción `include.fs`: `diskcachelocation` y `memoryefficientbackup`.


```
include.fs d: memoryefficientbackup=diskcachem
diskcachelocation=e:\temp
include.fs e: memoryefficientbackup=diskcachem
diskcachelocation=c:\temp
```




Si estas opciones aparecen en el archivo de opciones y una opción `include.fs`, los valores de `include.fs` se utilizarán para el espacio del archivo especificado en lugar de los valores de un archivo de opciones o de la línea de mandatos.




 Sistemas operativos AIX  Sistemas operativos Oracle Solaris `include.fs.nas`


 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Utilice la opción `include.fs.nas` para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, mediante la utilización de la opción `toc` con la opción `include.fs.nas` en el archivo `dsm.sys`. Esta opción solo es válida para los clientes AIX y Solaris.

 Sistemas operativos Windows `include.fs.nas`

 Sistemas operativos Windows Utilice la opción `include.fs.nas` para vincular una clase de gestión a sistemas de archivos de almacenamiento conectado a red (NAS). También puede especificar si el cliente ha de guardar la información de la Tabla de contenido (TOC) durante una copia de seguridad de imágenes del sistema de archivos NAS, mediante la utilización de la opción `toc` con la opción `include.fs.nas` en el archivo de opciones del cliente (`dsm.opt`).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris `include.image`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión si se utiliza con el mandato `backup image`. El mandato `backup image` ignora todas las demás opciones de inclusión.

 Sistemas operativos Linux Para los clientes Linux `x86_64`: Utilice la opción `snapshotcachesize` en las siguientes situaciones:

- Con el mandato `backup image`
- En el archivo `dsm.sys`
- Con la opción `include.image`




Utilizar la opción `snapshotcachesize` en estas situaciones le permite especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen.

Un tamaño de instantánea del 100% asegurará que la instantánea sea válida.


 Sistemas operativos AIX Para los clientes AIX `JFS2_systems`: Utilice la opción `snapshotcachesize` en las siguientes situaciones:

- Con el mandato `backup image`
- En el archivo `dsm.sys`
- Con la opción `include.image`

Utilizar la opción `snapshotcachesize` en estas situaciones le permite especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

 Sistemas operativos Windows `include.image`

 Sistemas operativos Windows Incluye un espacio de archivos o un volumen lógico o asigna una clase de gestión si se utiliza con el mandato `backup image`. El mandato `backup image` ignora todas las demás opciones de inclusión.

De forma predeterminada, el cliente realiza una copia de seguridad de imágenes fuera de línea. Para habilitar y controlar una operación de imagen en línea, puede especificar estas opciones en el archivo `dsm.opt`, como valores de la opción `include.image`: `snapshotproviderimage`, `presnapshotcmd`, `postsnapshotcmd`.

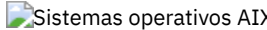

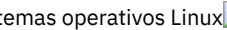
 Sistemas operativos Windows `include.systemstate`


 Sistemas operativos Windows Esta opción vincula copias de seguridad de estado del sistema a la clase de gestión especificada. Si especifica esta opción, especifíquela siempre como el patrón. Si no especifica esta opción, las copias de

seguridad de estado del sistema están vinculadas a la clase de gestión predeterminada.



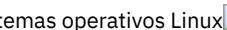
## Parámetros


### pattern

Especifica los objetos para incluir en el proceso de copia de seguridad o archivado o para asignar una clase de gestión específica.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Nota: en sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (dsm.sys) o en la línea de mandatos.

 Sistemas operativos Windows Nota: en sistemas de archivos NAS, debe añadir un prefijo de nombre de nodo NAS a la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos identificado hará referencia al nombre de nodo NAS que se ha especificado en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

Si el patrón comienza con comillas dobles o simples, contiene espacios en blanco intercalados o signos de igual, debe incluir el valor entre comillas simples (') o comillas dobles ("). Los signos que se utilicen para la apertura y el cierre deben ser del mismo tipo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Para la opción include.image, el patrón es el nombre de un sistema de archivos montado o de un volumen lógico RAW.

 Sistemas operativos Windows Para la opción include.image, el patrón es el nombre de un sistema de archivos o de un volumen lógico RAW.

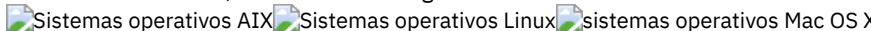

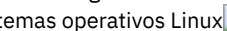

 Sistemas operativos Windows

Nota: Cuando especifica include.systemstate, el único patrón válido es all.

## parámetro opcional

### mgmtclassname

Especifica el nombre de la clase de gestión que se desea asignar a los objetos. Si no especifica ninguna clase de gestión, se utiliza la clase de gestión predeterminada. Para asociar una clase de gestión con un grupo de copia de seguridad en una sentencia de inclusión, utilice la sintaxis siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
include virtual_filespace_name\group_name management_class_name
```

 Sistemas operativos Windows

```
include virtual_filespace_name/group_name management_class_name
```

donde:

#### *virtual\_filespace\_name*

Especifica el nombre del espacio de archivos virtual del servidor de IBM Spectrum Protect que ha asociado con el grupo, en el mandato Backup Group.

#### *group\_name*


Es el nombre del grupo que ha creado al ejecutar el mandato Backup Group.

#### *management\_class\_name*

Es el nombre de la clase de gestión a asociar con los archivos del grupo.

Por ejemplo, un grupo denominado MyGroup se almacena en un espacio de archivos virtual denominado MyVirtualFileSpace. Para asociar una clase de gestión, denominada TEST, con el grupo, utilice la sintaxis siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X

 Sistemas operativos Oracle Solaris

```
include MyVirtualFileSpace/MyGroup TEST
```

 Sistemas operativos Windows

```
include MyVirtualFileSpace\MyGroup TEST
```

Tabla 1. Otros parámetros opcionales

parámetro opcional	Utilizar con la opción
ieobdtype	include.dedup

parámetro_opcional	Utilizar con la opción
memoryefficientbackup	include.fs
diskcachelocation	include.fs
Sistemas operativos Linux dynamicimage	Sistemas operativos Linux include.image
Sistemas operativos Linux postsnapshotcmd	Sistemas operativos Linux include.image
Sistemas operativos Linux presnapshotcmd	Sistemas operativos Linux include.image
Sistemas operativos Linux snapshotcachesize	Sistemas operativos Linux include.image
Sistemas operativos Windows snapshotproviderfs	Sistemas operativos Windows include.image
Sistemas operativos Linux snapshotproviderimage	Sistemas operativos Linux include.image

## Ejemplos

Archivo de opciones:

```
include /home/proj/text/devel.*
include /home/proj/text/* textfiles
include * managall
include /WAS_ND_NDNODE mgmtclass
include /WAS_APPNODE mgmtclass
include.image /home
include.archive /home/proj/text/
  * myarchiveclass
include.backup /home/proj/text/
  * mybackupclass
include.compression /home/proj/text/
  devel.*
include.encrypt /home/proj/gordon/*
include.fs.nas netappsj/vol/vol0
  homemgmtclass
```

```
include.dedup /Users/Administrator/Documents/Important/.../*
```

AIX only:

```
include.image /home
  MGMTCLASSNAME
  snapshotproviderimage=JFS2
  snapshotcachesize=40
include.image /home
  snapshotproviderimage=NONE
include.fs /kalafs1
  snapshotproviderfs=JFS2
```

LINUX only:

```
include.image /home
  snapshotproviderimage=LINUX_LVM
include.image /myfs1 dynamicimage=yes
```

```
include.image /home MGMTCLASSNAME
  snapshotproviderimage=NONE
include.image /myfs1 dynamicimage=yes
include.attribute.symlink /home/spike/.../*
include.fs /usr
  memoryefficientbackup=diskcachemethod
```

#### Sistemas operativos Windows

Sólo Windows:

```
include c:\proj\text\devel.*
include c:\proj\text\* textfiles
include ?:\* managall
include WAS_ND_NDNODE mgmtclass
include WAS_APPNODE mgmtclass
include.backup c:\win98\system\* mybackupclass
include.archive c:\win98\system\* myarchiveclass
include.encrypt c:\win98\proj\gordon\*
include.compress c:\test\file.txt

include.image h: MGMTCLASSNAME
  snapshotproviderimage=vss

include.image x:
  snapshotproviderimage=none
include.image y:
  snapshotproviderimage=vss
include.image z: MGMTCLASSNAME
  snapshotproviderimage=none
include.fs c:
  snapshotproviderfs=vss
















include.systemstate ALL mgmtc3
include.dedup c:\Users\Administrator\Documents\Important\...\*
include.dedup e:\*\* ieobjtype=image
include.dedup ALL ieobjtype=systemstate
include.dedup ALL ieobjtype=ASR
```

#### Sistemas operativos WindowsPara encriptar todos los archivos de todas las unidades:

```
include.encrypt ?:\...\*
```

Línea de mandatos:


No se aplica.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Control del proceso de enlaces simbólicos y alias  
IBM Spectrum Protect trata los enlaces simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. No obstante, no se realiza una copia de seguridad del archivo al que hace referencia el vínculo simbólico.
-  Sistemas operativos WindowsProceso de compresión y cifrado  
Tenga en cuenta la información siguiente si quiere incluir archivos o grupos de archivos específicos en la compresión y el cifrado durante una operación de copia de seguridad o archivado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle SolarisProceso de compresión y cifrado de copia de seguridad  
En este tema se indican diversos aspectos que han de tenerse en cuenta si desea incluir archivos o grupos de archivos específicos para el proceso de compresión y cifrado durante una operación de copia de seguridad o archivado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos WindowsProceso de sistemas de archivos NAS  
Utilice la opción include.fs.nas para asociar una clase de gestión a sistemas de archivos NAS y para controlar si la información de la tabla de contenido se guarda para la copia de seguridad del sistema de archivos.
-  Sistemas operativos Linux  Sistemas operativos WindowsOpciones include de la máquina virtual  
Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.





**Conceptos relacionados:**





 Sistemas operativos WindowsExcluir archivos con nombres UNC

**Tareas relacionadas:**

 Sistemas operativos Windows Configuración del soporte de archivos abiertos




**Referencia relacionada:**




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Snapshotcachesize





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XToc

**Información relacionada:**

 Sistemas operativos AIX  Sistemas operativos Linux  Mandato mmbackup: Requisitos de IBM Spectrum Protect

 Sistemas operativos AIX  Sistemas operativos Linux  Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect

 Sistemas operativos AIX  Sistemas operativos Linux  Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Control del proceso de enlaces simbólicos y alias

---

IBM Spectrum Protect trata los enlaces simbólicos y los alias (los alias se aplican sólo a Mac OS X) como archivos reales y realiza una copia de seguridad de los mismos. No obstante, no se realiza una copia de seguridad del archivo al que hace referencia el vínculo simbólico.

En algunos casos, los enlaces simbólicos y los alias pueden volver a crearse fácilmente y no es necesario realizar una copia de seguridad de los mismos. Además, realizar una copia de seguridad de estos enlaces simbólicos o alias puede incrementar el tiempo de proceso de la copia de seguridad y puede ocupar un volumen de espacio notable en el servidor de IBM Spectrum Protect.

Para excluir un archivo o un grupo de archivos que sean enlaces simbólicos o alias del proceso de copia de seguridad puede utilizar la opción `exclude.attribute.symlink`. Si es necesario, puede utilizar la opción `include.attribute.symlink` para incluir enlaces simbólicos o alias en un grupo amplio de archivos excluidos para el proceso de copia de seguridad. Por ejemplo, para excluir todos los enlaces simbólicos o alias del proceso de copia de seguridad, excepto los que existen en el directorio `/home/spike`, especifique estas sentencias en el archivo `dsm.sys`:

```
exclude.attribute.symlink /.../*
include.attribute.symlink /home/spike/.../*
```

**Referencia relacionada:**

Opciones exclude

 Sistemas operativos Windows

## Proceso de compresión y cifrado

---

Tenga en cuenta la información siguiente si quiere incluir archivos o grupos de archivos específicos en la compresión y el cifrado durante una operación de copia de seguridad o archivado.

- Debe establecer la opción `compression` en *yes* para activar el proceso de compresión. Si no especifica la opción `compression` o si establece la opción `compression` en *no*, el cliente de copia de seguridad y archivado no realizará el proceso de compresión.
- El cliente procesa en primer lugar `exclude.dir` y otras sentencias de inclusión/exclusión. A continuación, el cliente considerará las sentencias `include.compression` e `include.encrypt`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:




```
exclude c:\test\file.txt
include.compression c:\test\file.txt
include.encrypt c:\test\file.txt
```

El cliente examina primero la sentencia `exclude c:\test\file.txt` y determina que `c:\test\file.txt` se ha excluido del proceso de copia de seguridad, por lo que no es candidato al proceso de compresión o cifrado.

- El proceso de compresión de inclusión/exclusión y de cifrado es válido *sólo* para procesos de copias de seguridad/archivado.
- Como sucede con otras sentencias de inclusión/exclusión, puede utilizar la opción `inlexcl` para especificar un archivo en formato Unicode, que contiene sentencias `include.compression` e `include.encrypt` que especifican archivos Unicode. Consulte `Inlexcl` para obtener más información.

**Referencia relacionada:**

Compression

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Proceso de compresión y cifrado de copia de seguridad

---



En este tema se indican diversos aspectos que han de tenerse en cuenta si desea incluir archivos o grupos de archivos específicos para el proceso de compresión y cifrado durante una operación de copia de seguridad o archivado.

- Debe establecer la opción `compression` en `yes` para activar el proceso de compresión. Si no especifica la opción `compression` o si establece la opción `compression` en `no`, el cliente de copia de seguridad y archivado no realizará el proceso de compresión.
- El cliente procesará `exclude.fs`, `exclude.dir`, y otras sentencias de inclusión/exclusión en primer lugar. A continuación, el cliente considerará las sentencias `include.compression` e `include.encrypt`. Por ejemplo, considerando la siguiente lista de inclusión/exclusión:






```
exclude /home/jones/proj1/file.txt
include.compression /home/jones/proj1/file.txt
include.encrypt /home/jones/proj1/file.txt
```

El cliente examinará en primer lugar la sentencia `exclude /home/jones/proj1/file.txt` y determinará que `/home/jones/proj1/file.txt` ha de excluirse del proceso de copia de seguridad y que, por lo tanto, no es candidato para el proceso de compresión y cifrado.

- El proceso de compresión de inclusión/exclusión y de cifrado es válido *sólo* para procesos de copias de seguridad/archivado.

#### Referencia relacionada:



Compresion

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows


## Proceso de sistemas de archivos NAS

---

Utilice la opción `include.fs.nas` para asociar una clase de gestión a sistemas de archivos NAS y para controlar si la información de la tabla de contenido se guarda para la copia de seguridad del sistema de archivos.

 Sistemas operativos Linux  Sistemas operativos Windows Nota: La opción `include.fs.nas` no es válida para una copia de seguridad incremental por diferencia de instantánea.

Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Los nodos NAS representan un nuevo tipo de nodo. El nombre de nodo NAS identifica de forma exclusiva un servidor de archivos NAS y sus datos en el cliente de copia de seguridad y archivado. Puede añadir un prefijo de nombre de nodo NAS en la especificación de archivo para indicar el servidor de archivos al que se aplica la sentencia de inclusión. Si no especifica un nombre de nodo NAS, el sistema de archivos que especifique se aplica a todos los servidores de archivos NAS.
- Con independencia del sistema operativo de cliente utilizado, las especificaciones de sistema de archivos NAS utilizan la barra inclinada (/) como separador, tal como se muestra en el siguiente ejemplo: `/vol/vol0`.
-  Sistemas operativos Windows Las designaciones del sistema de archivos NAS que se especifican en la línea de mandatos requieren delimitadores de llave ({ y }) en los nombres de sistemas de archivos, como: `{/vol/vol0}`. No utilice delimitadores de llave si especifica esta opción en el archivo de opciones.

Utilice esta sintaxis:

```
>>-patrón-- mgmtclassname- toc=valor-----<<
```

Donde:

patrón

Especifica los objetos para incluir en los servicios de copia de seguridad, para asignar una clase de gestión específica o para controlar la creación de TOC. Puede utilizar caracteres comodín en el patrón.

mgmtclassname

Especifica el nombre de la clase de gestión que se desea asignar a los objetos. Si no especifica ninguna clase de gestión, se utiliza la clase de gestión predeterminada.

toc=valor

Para obtener más información, consulte Toc.

Ejemplo 1: para asignar una clase de gestión al sistema de archivos `/vol/vol1` de un nodo NAS denominado `netappsj`, especifique la sentencia de inclusión siguiente:

```
include.fs.nas netappsj/vol/vol1 nasMgmtClass toc=yes
```

Ejemplo 2: para asignar la misma clase de gestión a todas las vías de acceso que están subordinadas al sistema de archivos `/vol/` en un nodo NAS denominado `netappsj` (por ejemplo, `/vol/vol1`, `/vol/vol2`, y `/vol/vol3`), especifique la siguiente sentencia de inclusión:


include.fs.nas netappsj/vol/\* nasMgmtClass toc=yes









 Sistemas operativos Linux  Sistemas operativos Windows

## Opciones include de la máquina virtual

---

Las opciones de inclusión y exclusión de la máquina virtual influyen en el comportamiento de las operaciones de copia de seguridad y restauración de máquinas virtuales. Estas opciones se procesan antes de procesar cualquier opción de línea de mandatos, por lo que las opciones en la línea de mandatos pueden alterar temporalmente las opciones especificadas en cualquiera de las opciones de inclusión o de exclusión de la máquina virtual. Consulte las descripciones de opciones individuales para obtener información sobre las opciones.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

-  Sistemas operativos Linux  Sistemas operativos Windows `Include.vm`  
En operaciones de máquina virtual, esta opción altera temporalmente la clase de gestión que se especifica en la opción `vmmc`.
-  Sistemas operativos Linux  Sistemas operativos Windows `Include.vmdisk`  
La opción `INCLUDE.VMDISK` incluye un disco de máquina virtual (VM) en las operaciones de copia de seguridad. Si no especifica una o más etiquetas de disco, se hace copia de seguridad de todos los discos de la máquina virtual.
-  Sistemas operativos Linux  Sistemas operativos Windows `INCLUDE.VMSNAPSHOTATTEMPTS`  
Utilice la opción `INCLUDE.VMSNAPSHOTATTEMPTS` para determinar el número total de intentos de instantánea a probar para una operación de seguridad de máquina virtual (VM) que falla debido a un error de instantánea.
-  Sistemas operativos Linux  Sistemas operativos Windows `INCLUDE.VMTSMVSS`  
La opción `INCLUDE.VMTSMVSS` notifica a las aplicaciones de máquina virtual que está a punto de producirse una copia de seguridad. Esta opción permite a la aplicación truncar registros de transacciones y confirmar transacciones, de forma que la aplicación se pueda reanudar de un estado coherente cuando haya finalizado la copia de seguridad. Se puede especificar un parámetro opcional para suprimir el recorte de los registros de transacciones. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

### Referencia relacionada:

`Include.vmdisk`

`INCLUDE.VMTSMVSS`


`INCLUDE.VMSNAPSHOTATTEMPTS`

 Sistemas operativos Linux  Sistemas operativos Windows

## Include.vm

---

En operaciones de máquina virtual, esta opción altera temporalmente la clase de gestión que se especifica en la opción `vmmc`.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.


La clase de gestión especificado en la opción `vmmc` se aplica a todas las copias de seguridad VMware.


La clase de gestión especificado en la opción `vmmc` se aplica a todas las copias de seguridad Hyper-V.


Puede utilizar la opción `include.vm` para alterar temporalmente dicha clase de gestión, para una o varias máquinas virtuales. La opción `include.vm >` no modifica ni afecta a la clase de gestión que especifica la opción `vmctlmc`. La opción `vmctlmc` vincula los archivos de control de la máquina virtual con máquina virtual a una clase de gestión específica.

## Clientes soportados

---

 Sistemas operativos Linux Esta opción se puede utilizar con clientes Linux soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción se puede utilizar con clientes Windows soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción se puede utilizar con clientes Windows soportados configurados para hacer copias de seguridad de máquinas virtuales Hyper-V.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente.

## Sintaxis

---

```
>>-INCLUDE.VM-- --vmname-- --+-----+-----><
                          '-mgmtclassname-'
```

## Parámetros

---

### vmname

Parámetro obligatorio. Especifica el nombre de una máquina virtual que desea vincular a la clase de gestión especificada. Nombre en pantalla de la máquina virtual. Sólo se puede especificar una máquina virtual en cada sentencia `include.vm`. Sin embargo, pueden especificarse tantas sentencias `include.vm` como desee para vincular cada máquina virtual a una clase de gestión específica.

Puede incluir caracteres comodín en el nombre de la máquina virtual. Un asterisco (\*) coincide con cualquier serie de caracteres. El signo de interrogación (?) coincide con un solo carácter. Si el nombre de la máquina virtual contiene un carácter de espacio, escriba el nombre entre comillas dobles (").

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, escriba el carácter comodín signo de interrogación en lugar de los caracteres especiales cuando especifique el nombre de la máquina virtual.

### mgmtclassname

Parámetro opcional. Especifica la clase de gestión que se debe utilizar cuando se realice la copia de seguridad de la máquina virtual. Si este parámetro no se especifica, la clase de gestión predeterminada para la clase de gestión de la máquina virtual se especifica mediante la opción `vmmc`.

## Ejemplos

---

Supongamos que las siguientes clases de gestión existen y están activas en el servidor de IBM Spectrum Protect:

- MCFORTESTVMS
- MCFORPRODVMS
- MCUNIQUEVM

### Ejemplo 1

La siguiente sentencia `include.vm` en el archivo de opciones del cliente vincula todas las máquinas virtuales con nombres que comienzan por `VMTEST` a la clase de gestión denominada `MCFORTESTVMS`:

```
include.vm vmtest* MCFORTESTVMS
```

### Ejemplo 2

La siguiente sentencia `include.vm` del archivo de opciones del cliente vincula una máquina virtual denominada `WHOPPER VM1 [PRODUCTION]` con la clase de gestión denominada `MCFORPRODVMS`:

```
include.vm "WHOPPER VM1 ?PRODUCTION?" MCFORPRODVMS
```

El nombre de la máquina virtual debe especificarse entre comillas porque contiene caracteres de espacio. Además, se utiliza el carácter comodín signo de interrogación para que coincida con los caracteres especiales en el nombre de la máquina virtual.

### Ejemplo 3

La siguiente sentencia `include.vm` del archivo de opciones del cliente vincula una máquina virtual denominada `VM1` a la clase de gestión `MCUNIQUEVM`:

```
include.vm VM1 MCUNIQUEVM
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Include.vmdisk

---

La opción `INCLUDE.VMDISK` incluye un disco de máquina virtual (VM) en las operaciones de copia de seguridad. Si no especifica una o más etiquetas de disco, se hace copia de seguridad de todos los discos de la máquina virtual.

Esta opción solo está disponible si está utilizando el producto con licencia IBM Spectrum Protect for Virtual Environments. Para obtener más información sobre esta opción, consulte la documentación de producto de IBM Spectrum Protect for Virtual Environments en el Knowledge Center de IBM® en <http://www.ibm.com/support/knowledgecenter/SSERB6/welcome>.

La opción `INCLUDE.VMDISK` especifica la etiqueta de un disco de máquina virtual que debe incluirse en una operación `backup vm`. Si incluye un disco en el mandato `backup vm`, los parámetros de línea de mandatos alteran temporalmente las sentencias

INCLUDE.VMDISK en el archivo de opciones.

Esta opción se aplica a discos de máquina virtual Microsoft Hyper-V y VMware.

 Sistemas operativos Linux  Sistemas operativos Windows


## INCLUDE.VMDISK para máquinas virtuales VMware


---

Utilice la opción INCLUDE.VMDISK para incluir una máquina virtual de VMware en las operaciones de copia de seguridad.

### Clientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

### Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente. Los parámetros de línea de mandatos alteran temporalmente las sentencias en el archivo de opciones.

### Sintaxis para máquinas virtuales VMware

---

```
>>-INCLUDE.VMDISK--vmname-- -vmdk_label-----><
```

### Parámetros

---

#### *nombre\_máquina\_virtual*

Especifica el nombre de la máquina virtual que contiene un disco que desea incluir en una operación Backup VM. Nombre en pantalla de la máquina virtual. Solo puede especificar un nombre de máquina virtual en cada sentencia INCLUDE.VMDISK.

Especifique sentencias INCLUDE.VMDISK adicionales para cada disco de máquina virtual a incluir.

El nombre de la máquina virtual puede contener un asterisco (\*) para que coincida con cualquier serie de caracteres y el signo de interrogación (?) para que coincida con cualquier carácter. Entrecomille el nombre de máquina (" ") si el nombre de máquina contiene caracteres de espacio.

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([ o ]), puede ser que el nombre de la máquina virtual no coincida correctamente. Si un nombre de máquina virtual utiliza caracteres especiales en el nombre, puede que necesite utilizar el carácter de interrogación (?) para que coincida con los caracteres especiales en el nombre de la máquina virtual.

Por ejemplo, para incluir `Hard Disk 1` en la copia de seguridad de una máquina virtual denominada "Windows VM3 [2012R2]", utilice esta sintaxis en el archivo de opciones: `INCLUDE.VMDISK "Windows VM3 ?2012R2?" "Hard Disk 1"`

#### *vmdk\_label*

Especifica la etiqueta de disco del disco que desea incluir. Los caracteres comodín no están permitidos. Utilice el mandato Backup VM con la opción `-preview` para determinar las etiquetas de disco de una máquina virtual determinada.

Consulte el tema "Copia de seguridad de VM" para conocer la sintaxis.

### Ejemplos

---

#### Archivo de opciones

Suponga que una máquina virtual denominada `vm1` contiene cuatro discos, etiquetados como Disco duro 1, Disco duro 2, Disco duro 3 y Disco duro 4. Para incluir solo el Disco 2 en una operación Backup VM, especifique lo siguiente en el archivo de opciones:

```
INCLUDE.VMDISK "vm1" "Hard Disk 2"
```

Incluir los discos 2 y 3 en operaciones Backup VM:

```
INCLUDE.VMDISK "vm1" "Hard Disk 2"  
INCLUDE.VMDISK "vm1" "Hard Disk 3"
```

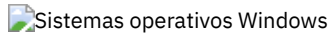
#### Línea de mandatos

Incluir un único disco cuando se realiza una copia de seguridad de `vm1`:

```
dsmc backup vm "vm1:vmdk=Hard Disk 1"
```

Incluir el disco duro 2 y el disco duro 3 en vm1:

```
dsmc backup vm "vm1:vmdk=Disco duro 2:vmdk=Disco duro 3"
```



Sistemas operativos Windows

## INCLUDE.VMDISK para máquinas virtuales Microsoft Hyper-V

---

Utilice la opción INCLUDE.VMDISK para incluir un disco de máquina virtual de las operaciones de copia de seguridad Hyper-V RCT en sistemas operativos Windows Server 2016 o posteriores.

### Clientes soportados

---

Esta opción puede utilizarse con clientes Windows Server 2016 y posteriores.

### Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente. Los parámetros de línea de mandatos alteran temporalmente las sentencias en el archivo de opciones.

### Sintaxis para máquinas virtuales Microsoft Hyper-V

---

```
>>-INCLUDE.VMDISK--nombre_máquina_virtual-- -ubicación_disco---><
```

### Parámetros

---

#### *nombre\_máquina\_virtual*

Especifica el nombre de la máquina virtual que contiene un disco que desea incluir en una operación backup vm. Nombre en pantalla de la máquina virtual. Puede especificar sólo un nombre de máquina virtual en cada sentencia INCLUDE.VMDISK.

Especifique sentencias INCLUDE.VMDISK adicionales para cada disco de máquina virtual a incluir.

El nombre de máquina virtual puede contener un asterisco (\*) para que coincida con cualquier serie de caracteres y un signo de interrogación (?) para que coincida con cualquier carácter. Si el nombre de máquina virtual contiene caracteres de espacio, escriba el nombre de máquina virtual entre comillas (" ").

Consejo: Si el nombre de máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([ ]), es posible que el nombre de máquina virtual no se pueda hacer coincidir correctamente. Si un nombre de máquina virtual incluye caracteres especiales, utilice un signo de interrogación (?) para representar los caracteres especiales.

Por ejemplo, para incluir un disco de máquina virtual SCSI en la copia de seguridad de una máquina virtual denominada "Windows VM3 [2012R2]", utilice esta sintaxis en el archivo de opciones:

```
INCLUDE.VMDISK "Windows VM3 ?2012R2?" "SCSI 0 1"
```

#### *ubicación\_disco*

Especifique la ubicación del disco de máquina virtual a incluir en una operación de copia de seguridad de Hyper-V RCT. La etiqueta de la ubicación de disco debe empezar por "SCSI" o "IDE" seguido del número de controlador y el número de ubicación de dispositivo. Los caracteres comodín no están permitidos.

Consejo: Utilice el mandato backup vm con la opción -preview para determinar la ubicación de los discos en una máquina virtual determinada. Consulte el tema "Copia de seguridad de VM" para conocer la sintaxis.

### Ejemplos

---

#### Archivo de opciones

La máquina virtual `vm1` contiene un disco de máquina virtual IDE (VHDX) en el número de controlador 1 y la ubicación de dispositivo 0. Para incluir este VHDX en las operaciones backup vm, especifique la sentencia siguiente en el archivo de opciones:

```
INCLUDE.VMDISK vm1 "IDE 1 0"
```

La máquina virtual `vm2` contiene un disco de máquina virtual SCSI en el número de controlador 0 y la ubicación de dispositivo 1. Incluya este VHDX en las operaciones de copia de seguridad especificando la sentencia siguiente en el archivo de opciones:

```
INCLUDE.VMDISK vm2 "SCSI 0 1"
```

#### Línea de mandatos

Incluir un solo disco de IDE (en el número de controlador 1 y la ubicación de dispositivo 0) al realizar la copia de seguridad de la máquina virtual `vm1`:

```
dsmc backup vm "vm1:vhdX=IDE 1 0"
```

Incluir un disco SCSI (en el número de controlador 0 y la ubicación de dispositivo 1) en la operación de copia de seguridad de la máquina virtual `vm2`:

```
dsmc backup vm "vm2:vhdX=SCSI 0 1"
```

#### Referencia relacionada:

Backup VM

Restore VM

Domain.vmfull

Exclude.vmdisk

 Sistemas operativos Linux  Sistemas operativos Windows


## INCLUDE.VMSNAPSHOTATTEMPTS


---


Utilice la opción `INCLUDE.VMSNAPSHOTATTEMPTS` para determinar el número total de instantánea a probar para una operación de seguridad de máquina virtual (VM) que falla debido a un error de instantánea.


### Clientes soportados

---

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

 Sistemas operativos Linux Esta opción se puede utilizar con clientes Linux soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción se puede utilizar con clientes Windows soportados configurados para hacer copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados que estén configurados para hacer copia de seguridad de máquinas virtuales en hosts Hyper-V que se ejecutan en sistemas operativos Windows Server 2016.

### Archivo de opciones

---

Esta opción es válida en el archivo de opciones del cliente (`dsm.opt`). También puede incluirse en el servidor en un conjunto de opciones del cliente. No es válida en la línea de mandatos.

### Sintaxis

---

```
>>-INCLUDE.VMSNAPSHOTATTEMPTS--nombremv--núm_con_detención----->  
>--núm_sin_detención-----<
```

### Parámetros

---

`vmname`

Parámetro posicional obligatorio que especifica el nombre de la máquina virtual para intentar el número total de instantáneas, si un intento de copia de seguridad falla debido a un error de instantánea. Nombre en pantalla de la máquina virtual.

Sólo se puede especificar una máquina virtual en cada sentencia `INCLUDE.VMSNAPSHOTATTEMPTS`. Sin embargo, para configurar los intentos de instantáneas totales para otras máquinas virtuales, puede utilizar los métodos siguientes:

- Para cada máquina virtual a la que desee que se aplique esta opción, especifique tantas sentencias `INCLUDE.VMSNAPSHOTATTEMPTS` como sean necesarias para reintentar las instantáneas que han fallado.
- Utilice caracteres comodín para el valor de parámetro `vmname` para especificar nombres de máquina virtual que coincidan con el patrón de comodín. Un asterisco (\*) coincide con cualquier serie de caracteres. El signo de interrogación (?) coincide con un solo carácter. Si el nombre de la máquina virtual contiene un carácter de espacio, escriba el nombre entre comillas dobles (").

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, escriba el carácter de comodín de signo de interrogación (?) en lugar de los caracteres especiales cuando especifique el nombre de la máquina virtual.

`núm_con_detención`

Parámetro posicional que especifica la siguiente acción:

Para operaciones de copia de seguridad de VMware:

- Para máquinas virtuales Windows con la protección de aplicaciones de IBM Spectrum Protect habilitada, *num\_with\_quiescing* especifica el número de veces para intentar la instantánea con detención de IBM Spectrum Protect VSS y detención VSS del proveedor del sistema Microsoft Windows. La detención de VSS solo se aplica a máquinas virtuales Windows.

Dependiendo del número especificado, el primer intento de instantánea siempre se realiza con detención VSS de IBM Spectrum Protect. Los intentos de instantánea subsiguientes se realizan con detención VSS del proveedor del sistema Windows.

- Para máquinas virtuales Windows sin la protección de aplicaciones de IBM Spectrum Protect habilitada y para máquinas virtuales Linux, *num\_with\_quiescing* especifica el número de veces para intentar la instantánea con detención de sistema de archivos de herramientas de VMware.

El valor máximo que puede especificar es diez (10). El valor predeterminado es dos (2). El valor mínimo que puede especificar es cero (0).

Para operaciones de copia de seguridad de Hyper-V RCT:

El parámetro *num\_with\_quiescing* especifica el número de veces que se intentará realizar las instantáneas con inmovilización para crear copias de seguridad coherentes con la aplicación.

Puede especificar un valor comprendido entre 0 y 10. El valor predeterminado es 2.

núm\_sin\_detención

Para operaciones de copia de seguridad de VMware:

Parámetro posicional que especifica el número de veces para intentar la instantánea con la detención del sistema de archivos de herramientas de VMware Tools y la detención de aplicaciones (VSS) inhabilitadas, una vez completado el número especificado de intentos con detención de VSS (*num\_with\_quiescing*). Por ejemplo, puede especificar este parámetro para una máquina virtual que ya está protegida por un agente IBM® Data Protection instalado en una máquina virtual huésped.

El valor máximo que puede especificar es diez (10). El valor mínimo que puede especificar es cero (0), que es el valor predeterminado.

Importante: Cuando este parámetro se aplica a una copia de seguridad de máquina virtual, la copia de seguridad no resulta afectada si se detiene el sistema. Como resultado, no se garantiza la coherencia de sistema operativo, sistema de archivos y aplicación. Un entrada `include.vmsnapshotattempts 0 0` no es válida. Las operaciones de copia de seguridad requieren como mínimo una instantánea.

Para operaciones de copia de seguridad de Hyper-V RCT:

La opción *num\_without\_quiescing* especifica el número de veces que se deben intentar instantáneas sin detenerse después de que se haya completado el número especificado de intentos en la opción *num\_with\_quiescing*.

Puede especificar un valor comprendido entre 0 y 10. El valor predeterminado es 0.

Importante: Cuando este parámetro se aplica a una copia de seguridad de VM, la copia de seguridad se considera coherente con respecto a bloqueos. Como resultado, no se garantiza la coherencia de sistema operativo, sistema de archivos y aplicación. Un entrada `include.vmsnapshotattempts 0 0` no es válida. Las operaciones de copia de seguridad requieren como mínimo una instantánea.

## Ejemplos

---

Ejemplos de VMware:

### Ejemplo 1

La siguiente sentencia `INCLUDE.VMSNAPSHOTATTEMPTS` del archivo de opciones de cliente realiza dos intentos de instantánea total (con detención de VSS) para la máquina virtual `VM_a`:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM_a 2 0
```

### Ejemplo 2

La siguiente sentencia `INCLUDE.VMSNAPSHOTATTEMPTS` del archivo de opciones de cliente realiza tres intentos de instantánea total para las máquinas virtuales de Windows que coinciden con la serie `vmServer_Dept*`:

- El primer intento se realiza con detención VSS de IBM Spectrum Protect.
- El segundo intento se realiza con la detención de VSS del proveedor de sistema de Windows.
- El tercer intento de instantánea se realiza sin detención de VSS.

```
INCLUDE.VMSNAPSHOTATTEMPTS vmServer_Dept* 2 1
```

### Ejemplo 3

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza un intento de instantánea total (con detención de VSS) para las máquinas virtuales que coincidan con la serie vmDB\_Dept\*:

```
INCLUDE.VMSNAPSHOTATTEMPTS vmDB_Dept* 1 0
```

### Ejemplo 4

La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza dos intentos de instantánea total (con detención de VSS) para todas las máquinas virtuales.

- El primer intento se realiza con detención VSS de IBM Spectrum Protect.
- El segundo intento se realiza con la detención de VSS del proveedor de sistema de Windows.

```
INCLUDE.VMSNAPSHOTATTEMPTS * 2 0
```

### Ejemplo 5

En este ejemplo, la máquina virtual DB15 tiene un agente IBM Data Protection instalado en la máquina virtual huésped y no necesita una instantánea coherente con la aplicación. La siguiente sentencia INCLUDE.VMSNAPSHOTATTEMPTS del archivo de opciones de cliente realiza un intento de instantánea total (con detención de VSS) para la máquina virtual DB15:

```
INCLUDE.VMSNAPSHOTATTEMPTS DB15 0 1
```

### Ejemplos de Hyper-V:

#### Ejemplo 1


Especifique la siguiente sentencia en el archivo de opciones de cliente para realizar dos intentos de instantánea total en copias de seguridad coherentes respecto a bloqueos para todas las máquinas virtuales Hyper-V que empiezan por LinuxVM:

```
INCLUDE.VMSNAPSHOTATTEMPTS LinuxVM* 0 2
```

#### Ejemplo 2

Especifique la siguiente sentencia en el archivo de opciones de cliente para realizar tres intentos de instantánea para la máquina virtual VM1: dos intentos de instantánea coherente con aplicación y, si fallan, para realizar un intento de instantánea coherente respecto a bloqueos:

```
INCLUDE.VMSNAPSHOTATTEMPTS VM1 2 1
```

 Sistemas operativos Windows Si está restaurando copias de seguridad de protección de aplicaciones, consulte Consideraciones sobre la duplicación para la restauración de una copia de seguridad de protección de aplicaciones desde el transportador de datos.

#### Referencia relacionada:

INCLUDE.VMTSMVSS

 Sistemas operativos Linux  Sistemas operativos Windows

## INCLUDE.VMTSMVSS

---


La opción INCLUDE.VMTSMVSS notifica a las aplicaciones de máquina virtual que está a punto de producirse una copia de seguridad. Esta opción permite a la aplicación truncar registros de transacciones y confirmar transacciones, de forma que la aplicación se pueda reanudar de un estado coherente cuando haya finalizado la copia de seguridad. Se puede especificar un parámetro opcional para suprimir el recorte de los registros de transacciones. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.


Cuando esta opción incluye una máquina virtual, IBM Spectrum Protect proporciona protección de aplicaciones. Es decir, el cliente se congela y desbloquea los grabadores VSS y, opcionalmente, trunca los registros de la aplicación. Si una máquina virtual no está protegida por esta opción, VMware proporciona protección de aplicaciones y bloquea y desbloquea los grabadores VSS, pero los registros de aplicación no se truncan.

Importante: Antes de iniciar las copias de seguridad de protección de aplicaciones, asegúrese de que la base de datos de la aplicación, como por ejemplo la base de datos de Microsoft SQL Server o la base de datos de Microsoft Exchange Server, se encuentre en una unidad que no sea la unidad de arranque, en caso de que se requiera una operación diskshadow revert durante la restauración.

## Clientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.



## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente. Esta opción no se puede establecer mediante el editor de preferencias o en la línea de mandatos.

## Sintaxis

---

```
>>-INCLUDE.VMTSMVSS----nombre_máquina_virtual---- --OPTions=KEEPSqllog-><
```

## Parámetros

---

### *nombre\_máquina\_virtual*

Especifica el nombre de la máquina virtual que contiene las aplicaciones que desea proteger. Nombre en pantalla de la máquina virtual. Especifique una máquina virtual por sentencia INCLUDE.VMTSMVSS. Por ejemplo, para incluir una máquina virtual denominada Windows VM3 [2012R2], utilice esta sintaxis en el archivo de opciones: INCLUDE.VMTSMVSS "Windows VM3 [2012R2]".

Para proteger todas las máquinas virtuales con esta opción, utilice un asterisco como un comodín (INCLUDE.VMTSMVSS \*). También puede utilizar signos de interrogación para hacer coincidir cualquier carácter único. Por ejemplo, INCLUDE.VMTSMVSS vm?? protege todas las máquinas virtuales que tienen nombres que empiezan por vm y que están seguidas por dos caracteres cualquiera (vm10, vm11, vm17, etc.).

Consejo: Si el nombre de la máquina virtual contiene caracteres especiales, como por ejemplo corchetes ([ o ]), puede ser que el nombre de la máquina virtual no coincida correctamente. Si un nombre de máquina virtual utiliza caracteres especiales en el nombre, puede utilizar el carácter de interrogación (?) para que coincida con los caracteres especiales en el nombre de la máquina virtual.

No existe ningún valor predeterminado para este parámetro. Para habilitar la protección de aplicaciones, debe incluir máquinas virtuales para protegerlas en una o más sentencias INCLUDE.VMTSMVSS. Asegúrese de que no excluye un disco en una máquina virtual (utilizando la opción EXCLUDE.VMDISK) si el disco contiene datos de aplicación que quiera proteger.

### OPTions=KEEPSqllog

Si se ha especificado el parámetro OPTions KEEPSqllog en una sentencia INCLUDE.VMTSMVSS, dicho parámetro impide que se trunquen los registros del servidor de SQL cuando un cliente de archivado de copia de seguridad que se instala en un nodo de transportador de datos realiza una copia de seguridad de una máquina virtual que está ejecutando un servidor SQL. La especificación de este parámetro permite al administrador del servidor de SQL gestionar de forma manual (realizar copia de seguridad y, posiblemente, truncar) los registros del servidor de SQL, para que se puedan conservar y se puedan utilizar para restaurar las transacciones de SQL a un determinado punto de comprobación, una vez que se restaure la máquina virtual. Cuando se especifica esta opción, no se truncará el registro SQL y se visualiza el siguiente mensaje y se registra en el servidor:

```
La protección de aplicaciones ANS4179I IBM Spectrum Protect  
no ha truncado los registros de Microsoft SQL Server en la máquina virtual 'VM'.
```

Elimine la opción OPTIONS=KEEPSQLLOG para habilitar el truncamiento de los registros SQL al completarse una copia de seguridad.

Nota: El cliente no realiza la copia de seguridad de los archivos de registro de SQL. El administrador de SQL debe realizar una copia de seguridad de los archivos de registro para que se puedan aplicar una vez que se restaure la base de datos.

## Ejemplos

---

### Archivo de opciones

Configurar la protección de aplicaciones para una máquina virtual que se denomina vm\_example:

```
INCLUDE.VMTSMVSS vm_example
```


Configurar la protección de aplicaciones para vm11, vm12 y vm15:

```
INCLUDE.VMTSMVSS vm11  
INCLUDE.VMTSMVSS vm12  
INCLUDE.VMTSMVSS vm15 options=keepsqlllog
```

### Línea de mandatos

No aplicable; esta opción no puede especificarse en la línea de mandatos.

### Conceptos relacionados:

 Sistemas operativos Windows Consideraciones sobre la duplicación para la restauración de una copia de seguridad de protección de aplicaciones desde el transportador de datos

**Referencia relacionada:**

Vmtimeout

Exclude.vmdisk

Include.vmdisk

INCLUDE.VMSNAPSHOTATTEMPTS





## Incrbydate

---


Utilice la opción `incrbydate` con el mandato incremental para realizar la copia de seguridad de los archivos nuevos y cambiados que tienen una fecha de modificación posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que excluya el archivo de la copia de seguridad.




Importante: Archivos que se han modificado o creado después de que el cliente de copia de seguridad y archivado procesara sus respectivos directorios, pero antes de que se completara la copia de seguridad incremental por fecha, y tampoco se realizará la copia de seguridad en futuras copias de seguridad incrementales por fecha, a menos que los archivos hayan vuelto a modificarse. Por este motivo se debe ejecutar periódicamente una copia de seguridad incremental, sin especificar la opción `incrbydate`.






La copia incremental por fecha actualiza la fecha y la hora de la última copia incremental en el servidor. Si se ejecuta una copia incremental por fecha sólo en parte de un sistema de archivos, no se actualizará la fecha de la última copia incremental completa, y la próxima copia incremental por fecha volverá a efectuar copia de seguridad de estos archivos.











 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris






Importante:

 sistemas operativos Mac OS X la hora de la última copia de seguridad incremental hace referencia a la hora del servidor y la hora de modificación de archivo hace referencia a la hora del cliente. Si las horas del servidor y del cliente no están sincronizadas, o el cliente y el servidor están en distintos husos horarios, esto afectará a la copia de seguridad incremental por fecha y a la copia de seguridad de imágenes con `mode=incremental`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris la hora de la última copia de seguridad incremental hace referencia a la hora del servidor y la hora de modificación de archivo hace referencia a la hora del cliente. Si las horas del servidor y del cliente no están sincronizadas, o el cliente y el servidor están en distintos husos horarios, esto afectará a la copia de seguridad incremental por fecha y a la copia de seguridad de imágenes con `mode=incremental`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Tanto las copias de seguridad incrementales como las copias de seguridad incrementales por fecha hacen copia de seguridad de los archivos nuevos y modificados. Una copia incremental por fecha tarda menos tiempo en procesarse que una copia incremental completa y requiere menos memoria. Sin embargo, a diferencia de una copia de seguridad incremental completa, una copia de seguridad incremental por fecha no conserva el almacenamiento del servidor actual de todos los archivos de la estación de trabajo por los motivos siguientes:

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows No da caducidad a las versiones de copia de seguridad de los archivos que se han suprimido de la estación de trabajo.
- No revincula versiones de copia de seguridad con una nueva clase de gestión si ésta ha cambiado.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X No realiza la copia de seguridad de los archivos cuyos atributos han cambiado, como los datos de la lista de control de acceso (ACL), a menos que las fechas y las horas de modificación también hayan cambiado.
-  Sistemas operativos Windows No realiza la copia de seguridad de los archivos cuyos atributos han cambiado, como la información de seguridad de NTFS, a menos que las fechas y las horas de modificación también hayan cambiado.
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Consejo: Si se dispone de un tiempo limitado durante la semana para efectuar copias de seguridad pero se dispone de tiempo extra durante los fines de semana, puede mantener el almacenamiento de servidor actual de los archivos de la estación de trabajo si realiza una copia de seguridad incremental con la opción `incrbydate` durante la semana y una copia de seguridad incremental completa los fines de semana.

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

>>-INCRbydate----->>

## Parámetros

---





No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:

```
dsmc incremental -incrbydate
```




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows





## Incremental

---

Utilice la opción incremental con el mandato restore image para asegurarse de que los cambios que se han realizado en la imagen base también se aplicarán a la imagen restaurada.




Si también utiliza la opción deletefiles, los cambios incluyen la supresión de los archivos y directorios que se encontraban en la imagen original pero que posteriormente se han suprimido de la estación de trabajo.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Nota: La utilización de la opción incremental con el mandato restore image para realizar una copia de seguridad de imágenes dinámica no recibe soporte.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción solo es válida para AIX, Linux x86\_64, Linux on POWER y Solaris. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---


>>-INCRemental----->>

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Línea de mandatos:

```
res i  
"/home/devel/projecta/*" -incremental
```

 Sistemas operativos Windows Línea de mandatos:

```
res i d: -incremental
```

 Sistemas operativos Windows

## Incrthreshold

---

La opción incrthreshold especifica el valor de umbral para el número de directorios de cualquier espacio de archivos con registro por diario que pueda tener objetos activos en el servidor, pero no objetos equivalentes en la estación de trabajo.

Cuando un cliente de Windows suprime un archivo o un directorio que tiene un nombre largo, a veces informa de ello mediante la utilización del nombre comprimido. Después de haberse suprimido el objeto, el nombre comprimido puede volver a utilizarse y el aviso de supresión ya no podrá identificar a un objeto exclusivo. Durante la realización de una copia de seguridad incremental con diario de un espacio de archivos, esto puede dar como resultado que la respuesta *ninguna versión activa* del servidor dé lugar a una caducidad incorrecta para un objeto.

La opción incrthreshold permite especificar la acción que debe realizar cuando surge esta opción:

- Si establece la opción incrthreshold en 0 (el valor predeterminado), no se realizará ninguna acción. La principal consecuencia es que, en una operación de restauración de uno de dichos directorios, es posible que tales objetos se restauren de forma

inadvertida. Cuando se ejecute la siguiente copia de seguridad incremental sin diario en este directorio, el servidor de IBM Spectrum Protect establecerá que caduquen todos los objetos del directorio que existan en el servidor, pero no los que existan en la estación de trabajo.

- Si se especifica un valor mayor que cero, el cliente guarda el nombre del directorio del objeto en el diario durante las copias de seguridad de diario. Durante una copia de seguridad incremental completa con diario del espacio de archivos, si el número de directorios en el espacio de archivos es mayor que o igual a este valor, se efectúa una copia de seguridad incremental completa de cada directorio. Esto tiene lugar automáticamente una vez finalizada la copia de seguridad con registro por diario y no es necesario realizar ningún mandato.
- Si establece la opción `incrthreshold` en 1, el cliente realizará una copia de seguridad incremental completa de estos directorios siempre que se reciba una respuesta *versión no activa* durante la realización de una copia de seguridad incremental completa con diario del espacio de archivos.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el campo Backup > Threshold for non-journal incremental backup del Editor de preferencias.

## Sintaxis

---

```
>>-INCRThreshhold--número_directorios----->>
```

## Parámetros

---

### *número\_directorios*

Especifica el valor de umbral del número de directorios en un espacio de archivos que pueden contener archivos activos que deberían haber caducado. Cuando se alcanza dicho umbral en una copia de seguridad incremental de espacios de archivos de diario completa, el cliente inicia una copia de seguridad incremental en cada uno de dichos directorios una vez finalizada la copia de seguridad con registro por diario. El rango de valores es de 0 a 2.000.000.000, siendo 0 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
incrthreshold 1
```

Línea de mandatos:

```
-increthreshold=1
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Instrlogmax

---

La opción `instrlogmax` especifica el tamaño máximo del registro de instrumentación (`dsminstr.log`) en MB. Los datos de rendimiento del cliente se recopilan en el archivo `dsminstr.log` durante el proceso de copia de seguridad o restauración cuando la opción `enableinstrumentation` tiene el valor *yes*.

Si cambia el valor de la opción `instrlogmax`, las anotaciones existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.





## Clientes soportados

---


Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-INSTRLOGMAX-- --tamaño-----><
```

## Parámetros

---

### tamaño

Especifica el tamaño máximo, en MB, del archivo de registro de instrumentación. El rango de valores es el comprendido entre 0 y 2047. El valor predeterminado es 25.

Cuando el tamaño del archivo dsminstr.log supera el tamaño máximo, se cambia el nombre del archivo de registro por dsminstr.log.bak. Los siguientes datos de instrumentación se siguen guardando en el archivo dsminstr.log.

Si especifica 0, el archivo de registro crece indefinidamente.






## Ejemplos

---

Archivo de opciones:

```
instrlogmax 100
```

Línea de mandatos:

```
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
dsmc sel /home/mydir/* -subdir=yes -enableinstrumentation=yes -instrlogmax=100  
 Sistemas operativos Windows dsmc sel c:\mydir\* -subdir=yes -enableinstrumentation=yes -  
instrlogmax=100
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

### Referencia relacionada:

Enableinstrumentation

Instrlogname

## Instrlogname

---

La opción instrlogname especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información que recopila el cliente de copia de seguridad y archivado.

Cuando se utiliza la opción enableinstrumentation yes para recopilar datos de rendimiento durante operaciones de copia de seguridad y restauración, el cliente almacena automáticamente la información en un archivo de registro.

De forma predeterminada, los datos de rendimiento se almacenan en el archivo de registro de instrumentación (dsminstr.log) en el directorio que se especifica mediante la variable de entorno DSM\_LOG (o la variable de entorno DSMI\_LOG para los productos que dependen de la API IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server y IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server). Si no ha establecido la variable de entorno DSM\_LOG, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato dsmc).

Utilice esta opción sólo cuando desee cambiar el nombre del archivo y la ubicación del registro de instrumentación.

Si desea controlar el tamaño del archivo de registro, utilice la opción instrlogmax.





## Clientes soportados


---





Esta opción es válida para todos los clientes y la API de IBM Spectrum Protect.


## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Esta opción se puede definir en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Importante: Establezca la variable de entorno `DSM_LOG` en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente. El directorio raíz no es un valor válido para `DSM_LOG`.

 Sistemas operativos Windows

Importante: Establezca la variable de entorno `DSM_LOG` en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente.

## Sintaxis

---


```
>>-INSTRLOGNAME-- --filespec-----><
```




## Parámetros


---

### filespec

Especifica la vía de acceso y el nombre de archivo donde desea almacenar la información de rendimiento durante el proceso de copia de seguridad o restauración. Si no existe ninguna parte de la vía de acceso que especifica, el cliente intenta crearla.

 Sistemas operativos Windows Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio especificado por la variable de entorno `DSM_LOG`. Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato `dsmc`).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio especificado por la variable de entorno `DSM_LOG`. Si no ha establecido la variable de entorno `DSM_LOG`, el archivo de registro de instrumentación se almacena en el directorio actual (el directorio en el que se ha emitido el mandato `dsmc`). El archivo de registro de instrumentación no puede ser un enlace simbólico.

 sistemas operativos Mac OS X En Mac OS X, si sólo especifica un nombre de archivo, el archivo se almacenará en la carpeta predeterminada. Los directorios predeterminados son:




```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

Este nombre de archivo de registro de instrumentación sustituye el nombre de archivo de registro de instrumentación anterior `dsminstr.report.pXXX` que se ha creado con la opción `TESTFLAG=instrument:detail` o `instrument:API`.


## Ejemplos

---

### Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Para clientes AIX, Linux y Oracle Solaris:

```
instrlogname /home/user1/mydir/mydsminstr.log
```




 sistemas operativos Mac OS X Para clientes Mac OS X:

```
instrlogname /Users/user1/Library/Logs/mydsminstr.log
```


 Sistemas operativos Windows Para clientes Windows:

```
instrlogname c:\mydir\mydsminstr.log
```

### Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Para clientes AIX, Linux y Oracle Solaris:

```
dsmc sel /home/user1/mydir/* -subdir=yes -instrlogname=/usr/log/mydsminstr.log
```

 sistemas operativos Mac OS X Para clientes Mac OS X:

```
dsmc sel /Users/user1/mydir/* -subdir=yes -instrlogname=/Users/user1/Library/Logs/mydsminstr.log
```

 Sistemas operativos Windows Para clientes Windows:


```
dsmc sel c:\mydir\* -subdir=yes -instrlogname=c:\temp\mydsminstr.log
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

**Referencia relacionada:**

Enableinstrumentation

Instrlogmax

 Sistemas operativos Windows

## Journalpipe

---

La opción journalpipe especifica el nombre de pipe de un gestor de sesión de daemon de registro por diario al que se adjuntarán los clientes de copia de seguridad.

### Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

### Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

```
JournalPipe \\.\pipe\jnlSessionMgr1
```

### Sintaxis

---

```
>>-JOURNALPipe--nombre_conducto-----<<
```

### Parámetros

---

nombre\_conducto

Especifique el nombre del conducto al que el cliente se conecta al realizar una copia de seguridad basada en el diario. El nombre predeterminado del conducto es \\.\pipe\jnlSessionMgr.

### Ejemplos





---

Archivo de opciones:

```
JOURNALPipe \\.\pipe\jnlSessionMgr
```

Línea de mandatos:




Esta opción no se puede establecer en la línea de mandatos.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows




## Lanfreecommmethod


---

La opción lanfreecommmethod especifica el protocolo de comunicaciones entre el cliente y el agente de almacenamiento de IBM Spectrum Protect. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si utiliza la recuperación de errores de LAN, debe tener lanfreecommmethod en el archivo dsm.sys dentro de una stanza de servidor.




 Sistemas operativos Windows Si utiliza la recuperación de errores de LAN, lanfreecommmethod TCPip deberá especificarse en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Para AIX, Linux y Solaris, utilice la opción lanfreshmport para especificar el número de puerto de la memoria compartida en el que el agente de almacenamiento está a la escucha.

 Sistemas operativos Windows Para Windows, utilice la opción lanfreshmport para identificar de forma exclusiva el agente de almacenamiento con el que el cliente intenta conectarse.

### Clientes soportados




---


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---







```
>>-LANFREECCommmethod-- --commethod-----><
```

## Parámetros



---

método comunicación

Especifica el protocolo admitido para el cliente de copia de seguridad y archivado:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris TCPip  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP)



Utilice la opción lanfreecppport para especificar el número de puerto TCP/IP en el que está conectado el agente de almacenamiento. El método de comunicación TCP/IP es el valor predeterminado para los usuarios no root en todas las plataformas admitidas.



 Sistemas operativos Windows TCPip  
 Sistemas operativos Windows Protocolo de control de transmisiones/Protocolo de Internet (TCP/IP)







Utilice la opción lanfreecppport para especificar el número de puerto TCP/IP en el que está conectado el agente de almacenamiento.

V6Tcip

Indica que se debe usar la versión 4 o 6 de TCP/IP, según la configuración del sistema y el resultado de una búsqueda de servicio de nombre de dominio. La única situación en la que esto no se aplica es cuando se utiliza dsmc schedule y se solicita schedmode. Debe haber disponible un entorno DNS válido.

 Sistemas operativos Windows NAMedpipes  
 Sistemas operativos Windows Método de comunicación entre procesos que permite que las corrientes de datos de los mensajes pasen entre un cliente y un servidor. Éste es el valor predeterminado. No especifique la opción lanfreecppport si desea utilizar el método de comunicación NAMedpipes para la comunicación fuera de la LAN.

 Sistemas operativos Windows SHAREdmem  
 Sistemas operativos Windows Utilice el método de comunicación de memoria compartida cuando el cliente y el agente de almacenamiento estén ejecutándose en el mismo sistema. El método de memoria compartida proporciona mejor rendimiento que el protocolo TCP/IP. El cliente de archivado y copia de seguridad debe tener permisos de administrador local.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris SHAREdmem  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice el método de comunicación de memoria compartida cuando el cliente y el agente de almacenamiento estén ejecutándose en el mismo sistema. La memoria compartida proporciona mejor rendimiento que el protocolo TCP/IP. Este es el método de comunicación predeterminado para los usuarios root de AIX, Linux y Solaris. Cuando este método de comunicación se especifica en AIX, el usuario del cliente de copia de seguridad/archivado puede haber iniciado la sesión como usuario root o como usuario no root, siempre que el agente de almacenamiento se ejecute como root. Si el Agente de almacenamiento no se está ejecutando como root, el ID de usuario que ejecuta el cliente de copia de seguridad/archivado debe coincidir con el que ejecuta el Agente de almacenamiento.

## Ejemplos

---

Archivo de opciones:

```
lanfreecommmethod tcp
```

Utilice únicamente TCP/IP v4

```
lanfreecommmethod V6Tcip
```

Use TCP/IP v4 o v6, en función de cómo esté configurado el sistema y del resultado de una búsqueda del servicio de nombres de dominio.

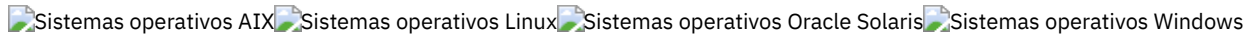





Línea de mandatos:

```
-lanfreec=tcp
```

```
-lanfreec=V6Tcpip
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows




## Lanfreshmport


---

Utilice la opción lanfreshmport cuando se haya especificado `lanfreecommmethod=SHAREdmem` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento. Esta opción activa el proceso entre el cliente y el dispositivo de almacenamiento conectado a la SAN.

### Clientes soportados




---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

### Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Coloque esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones de cliente (`dsm.opt`).

### Sintaxis

---

```
>>-LANFREESHmport-- --port_address-----><
```

### Parámetros

---

port\_address

Especifica el número que se utiliza para conectar con el agente de almacenamiento. El rango de valores oscila entre 1 y 32767.

Para los clientes de Windows, el valor predeterminado es 1.

Para el resto de los clientes, excepto los clientes Windows, el valor predeterminado es 1510.

### Ejemplos

---

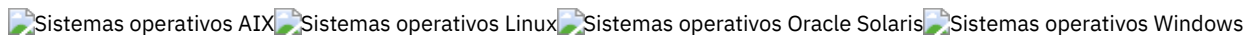



Archivo de opciones:

```
lanfrees 1520
```

Línea de mandatos:

```
-lanfrees=1520
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Lanfreectpport




---


La opción lanfreectpport especifica el número de puerto TCP/IP en el que está escuchando el agente de almacenamiento de IBM Spectrum Protect.

Utilice esta opción cuando haya especificado `lanfreecommmethod=TCPIP` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento. No especifique la opción lanfreectpport si desea utilizar el método de comunicación NAMedpipes para la comunicación sin LAN.

### Clientes soportados




---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción solo es válida para clientes de AIX, Linux x86\_64, Linux on POWER y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Establezca esta opción en el archivo dsm.sys en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-LANFREETCPPort-- --port_address-----<<
```

## Parámetros

---

port\_address

Especifica el número de puerto TCP/IP en el que está conectado el agente de almacenamiento. El rango de valores es de 1 a 32767; siendo 1500 el valor predeterminado.

**Nota:** el valor lanfreetcpport del cliente debe coincidir con el valor tcpport del agente de almacenamiento para las comunicaciones con el agente de almacenamiento (servidor virtual). El valor tcpport del cliente debe coincidir con el valor tcpport del servidor para las comunicaciones con el servidor real.

## Ejemplos

---





Archivo de opciones:

```
lanfreetcpp 1520
```

Línea de mandatos:

```
-lanfreetcpp=1520
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Lanfreesl

---

Utilice la opción lanfreesl para habilitar SSL (Secure Sockets Layer) para proporcionar comunicaciones seguras de cliente y de agente de almacenamiento. Esta opción está en desuso si se conecta a un servidor IBM Spectrum Protect V8.1.2 o posterior.

## Clientes soportados

---

Esta opción se soporta en todos los clientes, a excepción de los clientes Mac OS X.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente. No puede establecer esta opción en la GUI ni en la línea de mandatos.

## Sintaxis

---

```
>>-LANFREESL+-----+-----<<  
.-No--  
!-Yes-
```

## Parámetros

---

No

Especifica que el cliente de copia de seguridad y archivado no utiliza SSL al comunicarse con el agente de almacenamiento. No es el valor predeterminado.

Yes

Especifica que el cliente de copia de seguridad y archivado habilita SSL al comunicarse con el agente de almacenamiento. Para habilitar SSL, especifique `lanfreessl=yes` y cambie el valor de la opción `lanfreetcpport`. Cambie el valor de la opción `lanfreetcpport` si fuera necesario porque el agente de almacenamiento de IBM Spectrum Protect normalmente está configurado para estar a la escucha de las conexiones SSL en un puerto por separado.

## Ejemplos





---

Archivo de opciones:

```
lanfreessl yes
lanfreessl no
```

Línea de mandatos:

No aplicable. No puede establecer esta opción en la línea de mandatos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Lanfreetcpserveraddress

---




La opción `lanfreetcpserveraddress` especifica la dirección TCP/IP del agente de almacenamiento de IBM Spectrum Protect.


Utilice esta opción cuando haya especificado `lanfreecommmethod=TCPip` o `V6Tcipip` para la comunicación entre el cliente de copia de seguridad y archivado y el agente de almacenamiento.

La alteración temporal del valor predeterminado para esta opción es útil cuando se configuran datos sin LAN en un entorno en el que el cliente y el agente de almacenamiento se ejecutan en sistemas distintos. Puede obtener esta dirección de agente de almacenamiento del administrador.

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción solo es válida para clientes de AIX, Linux x86\_64, Linux on POWER y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows soportados.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del sistema del cliente.

## Sintaxis

---

```
>>-LANFREETCPServeraddress-- --stagent_address-----><
```

## Parámetros

---

`dirección_agentealmacenamiento`

Especifica una dirección TCP/IP de 1 a 64 caracteres para un servidor. Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. El valor predeterminado es 127.0.0.1 (localhost).

## Ejemplos

---

Archivo de opciones:

```
LANFREETCPServeraddress stagent.example.com
LANFREETCPServeraddress 192.0.2.1
```

Línea de mandatos:

No se aplica.

 Sistemas operativos Windows

## Idioma

---

La opción language especifica el idioma para la presentación de mensajes del cliente.

Puede utilizar el inglés de Estados Unidos (ENU) en todos los clientes.

El idioma en el que se visualiza la GUI de Java™ del cliente de copia de seguridad y archivado viene determinado por el entorno local de visualización de Windows, no por el entorno local del sistema Windows. Por ejemplo, si el sistema Windows y el entorno local de entrada es el francés, pero el entorno local de visualización es el ruso, la GUI de Java se visualizará en ruso de forma predeterminada, si no se utiliza la opción idioma. Si desea visualizar la GUI de Java en inglés de Estados Unidos o en otro idioma, puede modificar el idioma de visualización predeterminado mediante la opción language.

Consejo: La opción language no afecta al cliente web. El cliente web muestra sus mensajes en el idioma asociado al entorno regional del navegador. Si el navegador se ejecuta en un entorno local no admitido por el cliente, el cliente web se visualizará en inglés de Estados Unidos.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Configuración regional, en la lista desplegable Idioma del Editor de preferencias.

## Sintaxis

---

```
>>-LANGUage-- --language-----><
```

## Parámetros

---

language

Especifica el idioma que se desea utilizar. Los idiomas disponibles son los siguientes:

- ENU (inglés, Estados Unidos).
- PTB (portugués de Brasil)
- CHS (chino, simplificado)
- CHT (chino, tradicional)
- FRA (francés estándar)
- DEU (alemán estándar)
- ITA (italiano estándar)
- JPN (japonés)
- KOR (coreano)
- ESP (español estándar)
- CSY (checo)
- HUN (húngaro)
- PLK (polaco)
- RUS (ruso)

## Ejemplos

---

Archivo de opciones:

```
language enu
```

Línea de mandatos:

No se aplica.

## Latest

---

Utilice la opción latest para restaurar la versión de copia de seguridad más reciente de un archivo, aunque la copia de seguridad no esté activa.

Puede utilizar la opción latest con los mandatos siguientes:

- restore
- restore group

Si va a efectuar una restauración de un instante específico (con la opción pitdate), no es necesario especificar latest porque esta opción es implícita cuando se utiliza pitdate.

## Clientes soportados

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.



## Sintaxis









```
>>-LATest-----<<
```



## Parámetros






No hay parámetros para esta opción.

## Ejemplos

 sistemas operativos Mac OS XLínea de mandatos:  
 dsmc restore "/Users/devel/projecta/\*" -latest

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 dsmc restore "/home/devel/projecta/\*" -latest

 Sistemas operativos WindowsLínea de mandatos:  
 Sistemas operativos Windowsdsmc restore c:\devel\projecta\ -latest

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Localbackupset

La opción localbackupset especifica si la GUI del cliente de copia de seguridad y archivado pasa por alto la conexión inicial con el servidor de IBM Spectrum Protect, para restaurar un juego de copias de seguridad locales en una estación de trabajo independiente.

Si establece la opción localbackupset en yes, la GUI no intentará establecer la conexión inicial con el servidor. En este caso, la GUI sólo activará la función de restauración.





Si establece la opción localbackupset en no (el valor predeterminado), a GUI intentará establecer la conexión inicial con el servidor y activará todas las funciones de la GUI.

Nota: El mandato restore backupset admite la restauración de conjuntos de copias de seguridad locales en una estación de trabajo autónoma sin que se utilice la opción localbackupset.

## Clientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

 Sistemas operativos WindowsEstablezca esta opción en el archivo dsm.opt.

## Sintaxis

```
>>-LOCALbackupset-+-No-- .-No-- .  
                    +-Yes- '-Yes-'
```

## Parámetros

---




- No  
Especifica que la GUI intenta la conexión inicial con el servidor y activa todas las funciones. Éste es el valor predeterminado.
- Yes  
Especifica que la GUI no intenta la conexión inicial con el servidor y activa sólo la función de restauración.

## Ejemplos

---

Archivo de opciones:  
`localbackupset yes`

Esta opción no es válida con el cliente de línea de mandatos dsmd.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Makesparsefile

---

Utilice la opción `makesparsefile` con los mandatos `restore` o `retrieve` para especificar el modo en que los archivos esparcidos se volverán a crear.

Los archivos esparcidos no tienen espacio de disco asignado para cada bloque en todo el espacio de direcciones, lo que provoca la aparición de espacios vacíos en los archivos. El cliente de copia de seguridad y archivado detecta los archivos esparcidos durante una operación de copia de seguridad y los marca como esparcidos en el servidor de IBM Spectrum Protect. Los espacios vacíos se detectan por su contenido, que siempre son ceros.

Si establece la opción `makesparsefile` en `yes` (que es el valor predeterminado), los espacios vacíos del archivo no se graban en disco, por lo que no se asigna espacio de disco adicional durante una restauración.

Si establece la opción `makesparsefile` en `no`, los espacios vacíos no se vuelven a crear, lo que hace que se asignen bloques de disco para todo el espacio de direcciones. Esto puede provocar que se utilice más espacio de disco. Asegúrese de que tiene espacio de disco suficiente para restaurar todos los datos.

En algunos sistemas UNIX y Linux, puede ser necesario hacer una copia de seguridad de archivos específicos del sistema como archivos no esparcidos. Utilice la opción `makesparsefile` para los archivos que precisen la existencia de bloques de disco físicos, como `ufsboot` en Solaris, que se ejecuta en el momento de arrancar el sistema. El cargador de archivos de arranque del sistema operativo accede a los bloques de disco físicos directamente y no admite los archivos esparcidos.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`).

## Sintaxis

---

```
.-Yes-.  
>>-MAKESParsefile-+-----<<  
'-No--'
```

## Parámetros

---

- Yes  
Especifica que los espacios vacíos del archivo no se graban para que no se asigne espacio de disco adicional durante una restauración. Éste es el valor predeterminado.
- No  
Especifica que los espacios vacíos no se vuelven a crear, lo que hace que se asignen bloques de disco para todo el espacio de direcciones.

## Ejemplos

---

Archivo de opciones:  
makesparsefile no  
Línea de mandatos:  
-makesparsefile=no

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Managedservices

---







La opción `managedservices` especifica si el servicio de aceptación de clientes de IBM Spectrum Protect ha de gestionar el planificador, el cliente web o ambos.

Restricción: no puede utilizar `dsmcad` para la planificación cuando establece la opción `sessioninitiation` en `serveronly`. El daemon de aceptación de clientes sirve de temporizador externo para el planificador. Al iniciar el planificador, éste realiza una consulta al servidor para saber si hay otro suceso planificado. El suceso se ejecuta de forma inmediata o el planificador se cierra. El daemon de aceptación de clientes reinicia el planificador cuando es el momento de ejecutar el suceso planificado.





Nota:

1. Si establece la opción `shedmode` en `prompt`, el servidor solicitará información al daemon de aceptación de clientes cuando sea el momento de ejecutar la planificación. El planificador se conectará y desconectará del servidor cuando el daemon de aceptación de clientes se inicie por primera vez.

El mandato `dsmc schedule` no puede utilizarse cuando se han especificado `shedmode prompt` y `commmethod V6Tcip`.

2.  sistemas operativos Mac OS X Para Mac OS X, si no especifica la opción `managedservices`, el daemon de aceptación de clientes gestionará el programa del planificador y el cliente Web de forma predeterminada.
3.  Sistemas operativos Windows Establezca la opción `passwordaccess` en `generate` en el archivo de opciones del cliente (`dsm.opt`) y genere una contraseña para que IBM Spectrum Protect pueda gestionar la contraseña automáticamente.
4.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca la opción `passwordaccess` en `generate` en el archivo `dsm.sys` y genere una contraseña para que IBM Spectrum Protect pueda gestionar la contraseña automáticamente.

La utilización del daemon de aceptación de clientes para gestionar el servicio del planificador puede proporcionar las ventajas siguientes:

- Se resuelven los problemas de retención de memoria que pueden ocurrir con los métodos tradicionales para ejecutar el planificador. La utilización del daemon de aceptación de clientes para gestionar el planificador necesita muy poca memoria entre las operaciones planificadas.
- El daemon de aceptación de clientes puede gestionar el programa del planificador y el cliente web, ambos, con lo que se reduce el número de procesos de fondo de la estación de trabajo.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Para utilizar el cliente web, debe especificar esta opción en el archivo de opciones del sistema cliente.


## Clientes soportados





---






Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Cliente Web del Editor de preferencias.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha Cliente Web del Editor de preferencias.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Sintaxis

---


```
>>-MANAGEDServices--mode-----<<
```


## Parámetros





---




mode


Especifica si el daemon de aceptación de clientes ha de gestionar el planificador, el cliente web o ambos.

 Sistemas operativos Windowswebclient



 Sistemas operativos WindowsEspecifica que el daemon de aceptación de clientes ha de gestionar el cliente web.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X webclient


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 sistemas operativos Mac OS XEspecifica que el daemon de aceptación de clientes ha de gestionar el cliente web. Es el valor predeterminado para UNIX y Linux. webclient y schedule son los valores predeterminados para Mac OS X.

 sistemas operativos Mac OS X  Sistemas operativos Windowschedule


 sistemas operativos Mac OS X  Sistemas operativos WindowsEspecifica que el daemon de aceptación de clientes ha de gestionar el planificador. webclient y schedule son los valores predeterminados para Mac OS X.

 sistemas operativos Mac OS Xnone

 sistemas operativos Mac OS XSólo para Mac OS X, especifica que el daemon de aceptación de clientes no ha de gestionar el cliente web ni planificadores. Establezca managedservices en none para permitir que el mandato dsmc schedule.

## Ejemplos

 Sistemas operativos WindowsArchivo de opciones:

 Sistemas operativos WindowsA continuación se muestran ejemplos de cómo podría especificar la opción managedservices en el archivo de opciones del cliente (dsm.opt).

Tarea

Especificar que el daemon de aceptación de clientes gestiona únicamente el cliente web.

```
managedservices webclient
```

Tarea

Especificar que el daemon de aceptación de clientes gestiona únicamente el planificador.

```
managedservices schedule
```


Tarea

Especificar que el daemon de aceptación de clientes ha de gestionar el cliente web y el planificador, ambos.


```
managedservices schedule webclient
```

Nota: el orden en que se especifiquen estos valores carece de importancia.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 sistemas operativos Mac OS XArchivo de opciones:

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 sistemas operativos Mac OS XA continuación se muestran ejemplos de cómo podría especificar la opción managedservices en el archivo de opciones del cliente (dsm.sys).

Tarea

Especificar que el daemon de aceptación de clientes gestiona únicamente el cliente web.

```
managedservices webclient
```

Tarea

Especificar que el daemon de aceptación de clientes gestiona únicamente el planificador.


```
managedservices schedule
```

Tarea

Especificar que el daemon de aceptación de clientes ha de gestionar el cliente web y el planificador, ambos.

```
managedservices schedule webclient
```

Nota: el orden en que se especifiquen estos valores carece de importancia.

 sistemas operativos Mac OS XTarea

 sistemas operativos Mac OS XEn Mac OS X, para utilizar el mandato dsmc schedule, especifique:

```
managedservices none
```

Línea de mandatos:

No se aplica.



## Maxcmdretries

---

La opción `maxcmdretries` especifica el número máximo de veces que el planificador cliente (en la estación de trabajo del usuario) intenta procesar un mandato planificado que da error.

El reintento de mandato sólo se inicia si el planificador cliente todavía no ha hecho una copia de seguridad de un archivo, nunca ha conectado con el servidor o ha fallado antes de realizar la copia de seguridad de un archivo. Esta opción sólo se utiliza cuando el planificador se está ejecutando.

El administrador de IBM Spectrum Protect también puede utilizar esta opción. Si el administrador especifica un valor para esta opción, ese valor alterará temporalmente la información que se ha especificado en el archivo de opciones de cliente después de que el nodo de cliente haya establecido contacto con el servidor correctamente.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador Planificador, en el campo Número máximo de reintentos de mandatos del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Planificador, en el campo Número máximo de reintentos de mandatos del Editor de preferencias.

## Sintaxis

---

```
>>-MAXCMDRetries-- --maxcmdretries-----><
```

## Parámetros

---

`maxcmdretries`

Especifica el número de veces que el planificador cliente puede intentar procesar un mandato planificado que no se ha conseguido realizar. El rango de valores es de 0 a 9999, siendo 2 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
maxcmdr 4
```

Línea de mandatos:

```
-maxcmdretries=4
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos Linux  Sistemas operativos Windows

## Mbobjrefreshthresh

---

La opción `mbobjrefreshthresh` (umbral de renovación de objeto megablock) es un número que define un umbral. Cuando el número de objetos de IBM Spectrum Protect necesarios para describir cualquier megablock de 128 MB supera este valor, se renueva el megablock completo y caducan los objetos utilizados para representar esta área, en las copias de seguridad anteriores.



Cuando realiza la copia de seguridad de una máquina virtual, los datos se almacenan en el servidor de IBM Spectrum Protect en unidades de 128 MB, denominadas *megabloques*. Si un área del disco de producción cambia y se realiza una nueva copia de seguridad incremental, se crea un megablock nuevo para representar los cambios realizados en los datos de la copia de seguridad anterior. Dado que se puede crear un nuevo megablock con cada copia de seguridad incremental, al final los megabloques pueden afectar negativamente al rendimiento de la base de datos de IBM Spectrum Protect y, por lo tanto, afectar negativamente al rendimiento de la mayor parte de operaciones de IBM Spectrum Protect.


Utilice esta opción cuando calcule los objetos de IBM Spectrum Protect que representan datos de producción para cada copia de seguridad de máquina virtual. Por ejemplo, cuando el número de objetos de IBM Spectrum Protect supera este valor, se renueva el

megabloque. Esta acción significa que el bloque de 128 MB completo se copia en el servidor y se representa como un único objeto de IBM Spectrum Protect. El valor mínimo es 2 y el valor máximo es 8192. El valor predeterminado es 50.

## Clientes soportados

---

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los transportadores de datos que protegen máquinas virtuales VMware. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

 Sistemas operativos Windows Esta opción es válida para los transportadores de datos que protegen máquinas virtuales Microsoft Hyper-V. Debe tener licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

## Archivo de opciones

---

Esta opción es válida en el archivo de opciones del cliente (dsm.opt). También puede incluirse en el servidor en un conjunto de opciones del cliente. No es válida en la línea de mandatos.

## Sintaxis

---

```
>>-MBOBJREFRESHTHRESH .-50----- .
                        +-----+-----><
                        '-entero-'
```

## Parámetros

---

El valor mínimo que puede especificar son 2 megablocks, el mayor valor es 8192 megablocks; el valor predeterminado es de 50 megablocks.

## Ejemplos

---

Seleccione esta opción para desencadenar una renovación de megablock cuando el número de objetos necesarios para representar un megablock actualizado supere los 20 objetos:

```
MBOBJREFRESHTHRESH 20
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Mbpctrefreshthresh

---



La opción `mbpctrefreshthresh` (umbral de renovación de porcentaje de megablock) es un número que define un umbral. Cuando el porcentaje de objetos de IBM Spectrum Protect necesarios para describir que algún megabloque de 128 MB supera este valor, se renueva el megabloque entero y caducan los objetos utilizados para representar esta área, en las copias anteriores.


Cuando realiza una copia de seguridad de una máquina virtual, los datos se almacenan en el servidor de IBM Spectrum Protect en unidades de 128 MB, denominadas *megabloques*. Si un área del disco de producción cambia y se realiza una nueva copia de seguridad incremental, se crea un megablock nuevo para representar los cambios realizados en los datos de la copia de seguridad anterior. Dado que se puede crear un nuevo megabloque con cada copia de seguridad incremental, al final los megabloques pueden afectar negativamente al rendimiento de la base de datos de IBM Spectrum Protect y, por lo tanto, afectar negativamente al rendimiento de la mayor parte de operaciones de IBM Spectrum Protect.

Utilice esta opción cuando calcule la cantidad de datos adicionales de la que se realiza copia de seguridad para cada máquina virtual. Por ejemplo, cuando un bloque de 128-MB de un disco de producción cambia más del porcentaje especificado, todo el bloque 128-MB se copia en el servidor. El bloque se representa como un único objeto de IBM Spectrum Protect.

## Clientes soportados

---

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los clientes que son nodos de movimiento de datos que protegen las máquinas virtuales de VMware. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

 Sistemas operativos Windows Esta opción es válida para los clientes que actúan como nodos de transportador de datos que protegen máquinas virtuales Microsoft Hyper-V. Debe tener licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection

for VMware, o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

## Archivo de opciones

Esta opción es válida en el archivo de opciones del cliente (dsm.opt). También puede incluirse en el servidor en un conjunto de opciones del cliente. No es válida en la línea de mandatos.

## Sintaxis

```
>>-MBPCTREFRESHTHRESH .-50----- .  
-+-----+-----><  
'-entero-'
```

## Parámetros

El valor mínimo que puede especificar son 1 por ciento, el mayor valor es 99 por ciento; el valor predeterminado es 50 por ciento.

## Ejemplos

Seleccione esta opción para desencadenar una renovación megablock el 50 por ciento (o más) de los objetos de una megablock en un disco de producción han cambiado:


```
MBPCTREFRESHTHRESHOLD 50
```





## Memoryefficientbackup






La opción memoryefficientbackup especifica el algoritmo de reserva de memoria que ha de utilizarse para procesar las copias de seguridad de espacio de archivos completas.


Un método hace una copia de seguridad de un directorio a la vez, usando menos memoria. El otro método utiliza mucha menos memoria, pero necesita más espacio de disco.

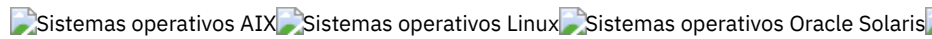
Utilice la opción memoryefficientbackup con el mandato incremental cuando la estación de memoria tenga restricciones de memoria. También puede utilizar esta opción como parámetro para la opción include.fs para seleccionar el algoritmo que el cliente de copia de seguridad y archivado ha de utilizar en función de cada espacio de archivos.

 Sistemas operativos Windows Utilice memoryefficientbackup=diskcachemethod para cualquier espacio de archivos que tenga demasiados archivos como para que el cliente complete la copia de seguridad incremental con el valor predeterminado, memoryefficientbackup=no, o con memoryefficientbackup=yes. El archivo de caché en disco que crea la copia de seguridad incremental de caché en disco inicial puede necesitar hasta 5 GB de espacio de disco por cada millón de archivos o directorios cuya copia de seguridad desea realizarse.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice memoryefficientbackup=diskcachemethod para cualquier espacio de archivos que tenga demasiados archivos como para que el cliente complete la copia de seguridad incremental con el valor predeterminado, memoryefficientbackup=no, o con memoryefficientbackup=yes.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las siguientes copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de vía de acceso de los archivos y directorios de los que se hace copia de seguridad. Para UNIX y Linux, calcule 1 byte por carácter en el nombre de la vía de acceso. Para Mac OS X, calcule 4 bytes por carácter en el nombre de vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 200 MB en los clientes UNIX y Linux y 800 MB en los clientes Mac OS X. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

 Sistemas operativos Windows La cantidad real de espacio en el disco necesaria para el archivo de caché del disco creado por las siguientes copias de seguridad incrementales de la caché del disco depende del número de archivos y directorios incluidos en la copia de seguridad y de la longitud promedio de vía de acceso de los archivos y directorios de los que se hace copia de seguridad. Calcule 2 bytes por carácter en el nombre de la vía de acceso. Por ejemplo, si se va a realizar una copia de seguridad de 1.000.000 de archivos y directorios y la longitud promedio de la vía de acceso es de 200 caracteres, la base de datos ocupará aproximadamente 400 MB. Otra forma de calcular a fin de realizar cierta planificación es multiplicar el número de archivos y directorios por la longitud de la vía de acceso más larga a fin de establecer el tamaño máximo de base de datos.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X Al realizar copia de seguridad de un sistema de archivos gestionados HSM, se crea un segundo archivo de caché de disco para la lista de archivos migrados. Los archivos de caché de disco combinados, creados por copias de seguridad incrementales de caché de disco y copias de seguridad del sistema de archivos gestionados HSM, pueden necesitar más de 400 MB de espacio de disco para cada millón de archivos de los que se realice copia de seguridad. El archivo de la memoria caché de disco puede ser muy grande. La admisión de archivos grandes se puede habilitar en el sistema de archivos que se está utilizando para el archivo de memoria caché de disco.

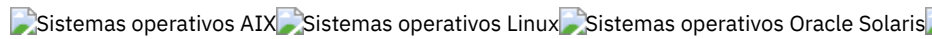
## Cientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X Esta opción se admite tanto en dsm.opt como dentro de una stanza de servidor en dsm.sys, pero el valor de dsm.opt se pasa por alto si también aparece en dsm.sys. También puede incluir esta opción en la línea de mandatos inicial. En la modalidad interactiva, esta opción puede utilizarse con el mandato incremental: También puede definir esta opción en el separador Ajuste del rendimiento del Editor de preferencias y seleccionar el recuadro de selección Utilizar algoritmo de bajo consumo de memoria.

 Sistemas operativos Windows Especifique esta opción en el archivo de opciones del usuario cliente (dsm.opt) o en la línea de mandatos inicial. También puede definir esta opción en el separador Ajuste del rendimiento del Editor de preferencias y seleccionar el recuadro de selección Utilizar algoritmo de bajo consumo de memoria.

## Sintaxis

---

```
.-No-----+
>>-MEMORYEfficientbackup-+-----><
+-Yes-----+
'-DISKCacheMethod-'
```

## Parámetros

---

No

El nodo cliente utiliza el método más rápido y que hace un uso más intensivo de la memoria al procesar copias de seguridad incrementales. Éste es el valor predeterminado.

Yes

El nodo cliente utiliza el método que requiere menos memoria al procesar copias de seguridad incrementales.

Diskcachemethod

El nodo cliente utiliza el método que requiere mucha menos memoria pero más espacio en el disco al procesar copias de seguridad incrementales para sistemas de archivos completos.

## Ejemplos

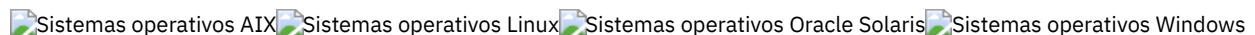
---

Archivo de opciones:

```
memoryefficientbackup yes
memoryefficientbackup diskcachem
```

Línea de mandatos:

```
-memoryef=no
```

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, Sistemas operativos Windows

## Mode

---




Utilice la opción mode para especificar la modalidad de copia de seguridad que desea utilizar al realizar operaciones de copia de seguridad específicas.

La opción mode no tiene ningún efecto al realizar copias de seguridad de un dispositivo lógico RAW.

Puede utilizar la opción mode con los siguientes mandatos de copia de seguridad:

```
backup image
```



Para especificar si ha de realizarse una copia de seguridad de imagen selectiva o incremental de los sistemas de archivos de cliente.


 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows backup nas


Para especificar si ha de realizarse una copia de seguridad de imagen completa o diferencial de los sistemas de archivos NAS.  
backup group

Para especificar si ha de realizarse una copia de seguridad de grupo completa o diferencial que contenga una lista de archivos de uno o más orígenes de espacio de archivos.

backup vm

 Sistemas operativos Linux  Sistemas operativos Windows Para máquinas virtuales VMware, este parámetro especifica si se va a realizar una copia de seguridad completa-constante-incremental o una copia de seguridad incremental-constante-incremental de máquinas virtuales VMware.



 Sistemas operativos Windows Para máquinas virtuales Microsoft Hyper-V, este parámetro especifica si se va a realizar una copia de seguridad completa incremental-constante o una incremental-constante-incremental de máquinas virtuales Hyper-V.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

## Clientes soportados

---

Esta opción es válida en todos los clientes soportados excepto Mac OS. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los transportadores de datos que protegen máquinas virtuales VMware. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

 Sistemas operativos Windows Esta opción es válida para los transportadores de datos que protegen máquinas virtuales Microsoft Hyper-V. Debe tener licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

## Sintaxis

---

Para copias de seguridad de imagen de los sistemas de archivos de cliente

```
>>-MODE = .-Selective---
           +-----+
           'Incremental'
```

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

Para copias de seguridad de imagen de los sistemas de archivos NAS

```
>>-MODE = .-differential-
           +-----+
           'full'
```

Para copias de seguridad de grupo

```
>>-MODE = .-full-----
           +-----+
           'differential'
```

 Sistemas operativos Linux  Sistemas operativos Windows

Para copias de seguridad de máquinas virtuales VMware

```
>>-MODE= .-IFIncremental-
          +-----+
          'IFFull'
```

 Sistemas operativos Windows

Para copias de seguridad de máquinas virtuales Microsoft Hyper-V

```
.-IFIncremental-.  
>>-MODE = +-----+-----<<  
'-IFFull-----'
```

## Parámetros




### Parámetros de copia de seguridad de imagen

#### selective

Especifica que se desea realizar una copia de seguridad de imagen completa (selectiva). Esta es la modalidad predeterminada para copias de seguridad de imagen de sistemas de archivos de cliente.

#### incremental

Especifica que se desea realizar una copia de seguridad sólo de los datos han cambiado desde la última copia de seguridad. Si todavía no se ha creado una copia de seguridad de imagen, entonces la primera copia de seguridad es una copia de seguridad de imagen completa (mode=selective), independientemente de qué opción de modalidad se especifique.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

### Parámetros de copia de seguridad NAS

#### differential

Es el valor predeterminado para los objetos NAS. Especifica que desea realizar una copia de seguridad de NAS de los archivos que han cambiado desde la última copia de seguridad completa. Si no existe ninguna copia de una imagen completa almacenada en el servidor de IBM Spectrum Protect, se realiza una copia de seguridad completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar MODE =differential envía una copia de seguridad de imagen diferencial. Si se envía una imagen completa durante una copia de seguridad diferencial, queda reflejada como una imagen completa mediante el mandato de servidor QUERY NASBACKUP.

Una imagen completa puede ser elegible para caducidad en función del control de versiones o la retención (verexists retextra), pero se seguirá manteniendo en el servidor para permitir la restauración de imágenes diferenciales dependientes. Una imagen completa que sea elegible para caducidad no se puede seleccionar para restauración, por lo que no se visualiza mediante el mandato de servidor QUERY NASBACKUP. Las copias de seguridad de imágenes diferenciales que dependen de una imagen completa "caducada" pueden ser restauradas.

#### full

Especifica que desea realizar una copia de seguridad completa de sistemas de archivos NAS.

### Parámetros de copia de seguridad de grupos

#### full

Especifica que desea realizar una copia de seguridad completa de sistemas de objetos de grupos. Este es el valor predeterminado para las copias de seguridad de grupos.

#### differential

Especifica que desea realizar una copia de seguridad de grupo de los archivos que han cambiado desde la última copia de seguridad completa. Si no existe ninguna copia de una imagen completa almacenada en el servidor de IBM Spectrum Protect, se realiza una copia de seguridad completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar MODE =differential envía una copia de seguridad de imagen diferencial. Si se envía una imagen completa durante una copia de seguridad diferencial, queda reflejada como una imagen completa mediante el mandato de servidor QUERY GROUP.

Una imagen completa puede ser elegible para caducidad en función del control de versiones o la retención (verexists retextra), pero se seguirá manteniendo en el servidor para permitir la restauración de imágenes diferenciales dependientes. Una imagen completa que sea elegible para caducidad no se puede seleccionar para restauración, por lo que no se visualiza mediante el mandato de servidor QUERY GROUP. Las copias de seguridad de imágenes diferenciales que dependen de una imagen completa "caducada" pueden ser restauradas.

 Sistemas operativos Linux  Sistemas operativos Windows

### Parámetros de copias de seguridad de máquina virtual VMware

#### IFFull

Especifica que desea realizar una copia de seguridad completa-constante-incremental de una máquina virtual. Una copia de seguridad completa-constante-incremental realiza una copia de seguridad de todos los bloques utilizados en discos de máquinas virtuales de VMware.

De forma predeterminada, la primera copia de seguridad de una máquina virtual VMware es una copia de seguridad completa-constante-incremental (`mode=iffull`), aunque se especifique `mode=ifincremental` (o se deje el valor predeterminado de la opción `mode`). Las copias de seguridad posteriores tienen el valor predeterminado en `mode=ifincremental`.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

Para obtener una descripción de la estrategia de copia de seguridad incremental constante para máquinas virtuales VMware, consulte Tipos de copia de seguridad y de restauración.

#### IFIncremental

Especifica que desea realizar una copia de seguridad incremental siempre incremental de una máquina virtual. Una copia de seguridad incremental-constante-incremental realiza una copia de seguridad sólo de los bloques de disco que han cambiado desde la última copia de seguridad.

Esta modalidad es la modalidad de copia de seguridad predeterminada de las copias de seguridad de máquina virtual VMware.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

### Sistemas operativos Windows

#### Parámetros de máquina virtual de Hyper-V de Microsoft

##### IFIncremental

Especifica que desea realizar una copia de seguridad incremental siempre incremental de una máquina virtual Hyper-V. Una copia de seguridad incremental-constante-incremental realiza una copia de seguridad sólo de los bloques de disco que han cambiado desde la última copia de seguridad.

Esta modalidad es la modalidad de copia de seguridad predeterminada para copias de seguridad Hyper-V.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

Para obtener una descripción de la estrategia de copia de seguridad constante incremental para máquinas virtuales Hyper-V, consulte Estrategia de copia de seguridad incremental-constante.

##### IFFull

Especifica que desea realizar una copia de seguridad completa-constante-incremental de una máquina virtual Hyper-V. Una copia de seguridad completa-constante-incremental realiza una copia de seguridad de todos los bloques utilizados en discos de máquinas virtuales.



De forma predeterminada, la primera copia de seguridad de una máquina virtual Hyper-V es una copia de seguridad completa-constante-incremental (`mode=iffull`), aunque se especifique `mode=ifincremental` (o se deje el valor predeterminado de la opción `mode`). Las copias de seguridad posteriores tienen el valor predeterminado en `mode=ifincremental`.

No puede utilizar esta modalidad de copia de seguridad para realizar una copia de seguridad de una máquina virtual, si el cliente está configurado para cifrar los datos de copia de seguridad.

## Ejemplos


---

#### Tarea

 Sistemas operativos Linux  Sistemas operativos Windows Realizar una copia de seguridad de una máquina virtual VMware denominada `vm1` utilizando la modalidad incremental siempre incremental para copiar sólo los datos que han cambiado desde la última copia de seguridad.


```
dsmc backup vm vm1 -mode=ifincremental  
-vmbackuptype=full
```

#### Sistemas operativos Windows Tarea



 Sistemas operativos Windows Realizar una copia de seguridad de máquina virtual completa-constante-incremental de una máquina virtual Hyper-V denominada `msvm1`



```
dsmc backup vm msvm1 -mode=iffull
```

#### Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar una copia de seguridad incremental-constante-incremental de una máquina virtual Hyper-V denominada msvm1


```
dsmc backup vm msvm1 -mode=ifincremental
```

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Tarea

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.



```
dsmc backup nas -mode=full -nasnodename=nas1  
/vol/vol0 /vol/vol1
```

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.


```
dsmc backup nas -mode=differential -nasnodename=nas1  
{/vol/vol0} {/vol/vol1}
```

 Sistemas operativos AIX  Sistemas operativos Linux Tarea




 Sistemas operativos AIX  Sistemas operativos Linux Realizar la copia de seguridad del espacio de archivos /home/test utilizando una copia de seguridad de imágenes incremental que realice la copia de seguridad sólo de los archivos nuevos y de los archivos que han cambiado desde la última copia de seguridad de imágenes completa.




```
dsmc backup image /home/test -mode=incremental -snapshotproviderimage=none
```

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar la copia de seguridad de la unidad c: utilizando una copia de seguridad de imágenes incremental que realice la copia de seguridad sólo de los archivos nuevos y de los archivos que han cambiado desde la última copia de seguridad de imágenes completa.


```
dsmc backup image c: -mode=full
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Realizar una copia de seguridad completa de todos los archivos de la lista de archivos /home/dir1/filelist1 en el nombre de espacio de archivos virtual /virtfs que contiene el archivo /home/group1 de líder de grupo.

```
dsmc backup group -filelist=/home/dir1/filelist1  
-groupname=group1 -virtualfsname=/virtfs -mode=full
```

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar una copia de seguridad completa de todos los archivos de la lista de archivos c:\dir1\filelist1 en el nombre de espacio de archivos virtual \virtfs que contiene el archivo c:\group1 de líder de grupo.

```
dsmc backup group -filelist=c:\dir1\filelist1 -groupname=group1  
-virtualfsname=\virtfs -mode=incremental -vmbackuptype=fullvm
```





#### Referencia relacionada:

Backup VM

Backup Group

Backup Image

Backup NAS

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Monitor

---

La opción monitor especifica si se supervisará una copia de seguridad o una restauración de imagen de sistemas de archivos pertenecientes a un servidor de archivos de almacenamiento conectado a red (NAS).

Si especifica monitor=yes, el cliente de copia de seguridad y archivado supervisará la operación actual de copia de seguridad o de restauración de imagen NAS y visualizará la información del proceso en la pantalla. Éste es el valor predeterminado.




Si especifica monitor=no, el cliente no supervisará la operación actual de copia de seguridad o de restauración de imagen NAS y estará disponible para procesar el siguiente mandato.


Utilice esta opción con los mandatos backup nas o restore nas.

## Clientes soportados

---



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción *sólo* es válida para los clientes AIX, HP-UX, Linux y Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Sintaxis

---

```
.-Yes-.
>>-MONitor = -+-----+-----><
               '-No--'
```

## Parámetros

---

Yes

Especifica que se desea supervisar la operación actual de copia de seguridad o de restauración de imagen NAS y ver en pantalla la información de proceso. Éste es el valor predeterminado.




No

Especifica que no se desea supervisar la operación actual de copia de seguridad o de restauración de imagen NAS.


## Ejemplos

---


Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes
/vol/vol0 /vol/vol1
```

 Sistemas operativos Windows

```
backup nas -mode=full -nasnodename=nas1 -monitor=yes
{/vol/vol0} {/vol/vol1}
```

 Sistemas operativos Windows

## Myprimaryserver

---

La opción myprimaryserver especifica el nombre de servidor primario que utiliza el cliente para iniciar la sesión en el servidor secundario en modalidad de migración tras error.

Durante el proceso de inicio de sesión normal (no migración tras error), la opción myprimaryserver se envía al cliente y se guarda en el archivo dsm.opt. No edite esta opción durante las operaciones normales.

Importante: Si cambia el valor para la opción myprimaryserver, la información de autenticación como la contraseña y la clave de cifrado de IBM Spectrum Protect no seguirán funcionando con el nuevo servidor primario. Se le pedirá la contraseña y la clave de cifrado para las operaciones que requieren la autenticación. Por lo tanto, no cambie este valor aunque cambie la información de conexión de servidor secundario.

## Clientes soportados

---

Esta opción sólo es válida para los clientes de Windows.

## Archivo de opciones

---

Esta opción se coloca en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-MYPRIMARYServer----primary_servername-----><
```

## Parámetros

---

primary\_servername

Especifica el nombre del servidor primario que se utilizará para la autenticación durante una migración tras error. El servidor primario es el servidor de IBM Spectrum Protect que utiliza un cliente para la producción normal.

## Ejemplos

---

Archivo de opciones:

```
*** Estas opciones no se deben cambiar manualmente
REPLSERVERNAME      TARGET
REPLTCPSEVERADDRESS 192.0.2.9
REPLTCPSPORT        1501
REPLSERVERGUID      60.4a.c3.e1.85.ba.11.e2.af.ce.00.0c.29.2f.07.d3

MYREPLICATIONServer TARGET
MYPRIMARYSERVERNAME SERVER1
*** end of automatically updated options
```

Línea de mandatos:

No se aplica.

### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

### Tareas relacionadas:

Configuración del cliente de migración automática tras error

## Myreplicationserver

---

La opción myreplicationserver especifica qué stanza de servidor secundario utiliza el cliente durante una migración tras error.

La stanza de servidor secundario se identifica mediante la opción replservername y contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.





## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción se coloca dentro de una stanza del servidor en el archivo dsm.sys.

 Sistemas operativos Windows Esta opción se coloca en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-MYREPLICATIONServer----repl_servername-----<<
```

## Parámetros

---

repl\_servername

Especifica el nombre de la stanza para el servidor secundario que se utilizará durante una migración tras error. Este valor es normalmente el nombre del servidor secundario, no el nombre de host del servidor. Además, el valor del parámetro repl\_servername no distingue entre mayúsculas y minúsculas, pero el debe coincidir con el valor especificado para la opción REPLSERVERName.

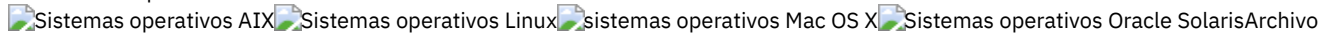
## Ejemplos

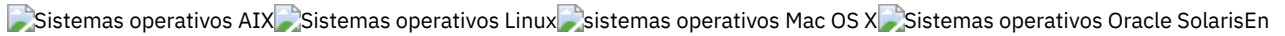
Archivo de opciones:

```
MYREPLICATIONServer TargetReplicationServer1
```

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción `replservername` y el nombre del servidor secundario. La stanza `servername` debe contener la opción `myreplikationserver`, que apunta al servidor secundario que se especifica mediante la stanza `replservername`. Sólo se puede especificar un servidor secundario por stanza `servername`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```


```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SERvername          server_a
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDACCESS      prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SERvername          server_b
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname2.example.com
PASSWORDACCESS      generate
INCLExcl            /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```
SERvername          server_c
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname3.example.com
PASSWORDACCESS      generate
MYREPLICATIONServer TargetReplicationServer1
```

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo `dsm.opt`, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza `REPLSERVERName`. La opción `MYREPLICATIONServer` apunta al nombre de servidor secundario especificado por la stanza `REPLSERVERName`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00
```


```
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDACCESS      prompt
MYREPLICATIONServer TargetReplicationServer1
MYPRIMARYSERVER     Server1
```

### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

### Tareas relacionadas:

Configuración del cliente de migración automática tras error

Sistemas operativos Windows

## Namedpipename

---

La opción namedpipename especifica el nombre de named pipe para las comunicaciones entre un cliente y un servidor en el mismo dominio de servidor de Windows.

### Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

### Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Comunicación del editor de preferencias.

### Sintaxis

---

```
>>-NAMedpipename-- --nombre-----><
```

### Parámetros

---

nombre

Nombre de un named pipe. El valor predeterminado es `\\.\pipe\Server1`.

### Ejemplos

---

Archivo de opciones:

```
namedpipename \\.\pipe\dsmser1
```

Línea de mandatos:

```
-namedpipename=\\.\pipe\dsmser1
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows




## Nasnodename


---


La opción nasnodename especifica el nombre de nodo del servidor de archivos NAS cuando se procesan sistemas de archivos NAS. El cliente le solicita un ID de administrador.

El nombre de nodo identifica el servidor de archivos NAS en el servidor de IBM Spectrum Protect. El servidor debe inscribir el servidor de archivos NAS.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Puede especificar esta opción en la línea de mandatos o en el archivo de opciones del cliente (dsm.sys).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Puede modificar temporalmente el valor predeterminado en el archivo dsm.sys especificando un valor distinto en la línea de mandatos. Si no especifica la opción nasnodename en el archivo dsm.sys, debe especificar esta opción en la línea de mandatos cuando se procesen sistemas de archivos NAS.


 Sistemas operativos Windows Puede especificar esta opción en la línea de mandatos o en el archivo de opciones del cliente (dsm.opt).


 Sistemas operativos Windows Puede modificar temporalmente el valor predeterminado en el archivo dsm.opt especificando un valor distinto en la línea de mandatos. Si no especifica la opción nasnodename en el archivo dsm.opt, debe especificar esta opción en la línea de mandatos cuando se procesen sistemas de archivos NAS.

Puede utilizar la opción nasnodename con los mandatos siguientes:

- backup nas
- delete filespace
- query backup
- query filespace
- restore nas

El mandato delete filesystem se puede utilizar para suprimir interactivamente espacios de archivos NAS del almacenamiento del servidor.

 Utilice la opción `nasnodename` para identificar el nodo del servidor de archivos NAS. Especifique la opción `nasnodename` en el archivo de opciones del sistema cliente (`dsm.sys`). El valor del archivo de opciones del sistema del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos. Si no especifica la opción `nasnodename` en el archivo de opciones del cliente, deberá especificar esta opción en la línea de mandatos cuando procese sistemas de archivos NAS.


 Utilice la opción `nasnodename` para identificar el nodo del servidor de archivos NAS. Especifique la opción `nasnodename` en el archivo de opciones del cliente (`dsm.opt`). El valor del archivo de opciones del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos. Si no especifica la opción `nasnodename` en el archivo de opciones del cliente, deberá especificar esta opción en la línea de mandatos cuando procese sistemas de archivos NAS.


Utilice la opción `class` para especificar la clase del espacio de archivos que se ha de suprimir. Para que se muestre una lista de los espacios de archivos que pertenecen a un nodo NAS y así poder elegir cuál suprimir, utilice la opción `-class=nas`.

Para suprimir espacios de archivos NAS mediante la utilización del cliente web, consulte el tema en el que se explica la realización de la copia de seguridad de los datos.

## Clientes soportados


---


 Esta opción solo es válida para los clientes de AIX, Linux y Solaris. La API de IBM Spectrum Protect no admite esta opción.

 Esta opción es válida para todos los clientes Windows. La API de cliente de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en la ficha General del editor de preferencias.

 Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha General del editor de preferencias.

## Sintaxis

---

```
>>-NASNodename-- --nodename-----><
```

## Parámetros

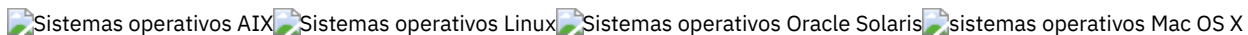
---

`nodename`  
Especifica el nombre de nodo del servidor de archivos NAS.

## Ejemplos

---

Archivo de opciones:  
`nasnodename nas2`  
Línea de mandatos:  
`-nasnodename=nas2`




## Nfstimeout

---

La opción `nfstimeout` especifica el número de segundos que el cliente espera a que se reciba una llamada de sistema de estado en un sistema de archivos NFS antes de que exceda el tiempo de espera.

Puede utilizar esta opción para mitigar el funcionamiento predeterminado de las llamadas de estado en los sistemas de archivos. Por ejemplo, si un sistema de archivos NFS es obsoleto, NFS excederá el tiempo de espera de una llamada de sistema de estado (montaje por software) o colgará el proceso (montaje por hardware).

Si el valor de esta opción se cambia por un valor distinto de cero, una hebra llamadora crea un thread nuevo para emitir la llamada de estado del sistema. La hebra de llamador excede el tiempo de espera de la hebra nueva y la operación puede continuar.

 **Sistemas operativos Oracle Solaris**Nota: En Solaris, la opción `nfstimeout` puede fallar si el montaje de NFS es por hardware. Si se cuelga el proceso, desactive la opción `nfstimeout` y monte el sistema de archivos NFS montado por software de este modo:

```
mount -o soft,timeo=5,retry=5 machine:/filesystem /mountpoint
```

Los parámetros son los siguientes:

`soft`

Genera un montaje por software del sistema de archivos NFS. Si se produce un error, la función `stat()` devuelve un error. Si se ha utilizado la opción `hard`; `stat()` nunca vuelve hasta que el sistema de archivos está disponible.

`timeo=n`

Establece el tiempo de espera para un error de montaje de tipo `soft` en *n* décimas de segundo.

`retry=n`

Establece los reintentos internos y los reintentos de montaje en *n*; el valor predeterminado es 10000.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux. El servidor también puede definir esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo `dsm.sys` dentro de una sección del servidor o el archivo de opciones de cliente (`dsm.opt`).

## Sintaxis

---

```
>>-NFSTIMEout-- --número-----><
```

## Parámetros

---

`number`

Especifica el número de segundos que el cliente espera a que se reciba una llamada de estado del sistema en un sistema de archivos antes de que exceda el tiempo de espera. El rango de valores es de 0 a 120, siendo 0 segundos el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
nfstimeout 10
```

Línea de mandatos:

```
-nfstimeout=10
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.


## Nodename

---

Utilice la opción `nodename` en el archivo de opciones de cliente para identificar la estación de trabajo en el servidor. Puede utilizar nombres de nodo diferentes para identificar varios sistemas operativos en la estación de trabajo.

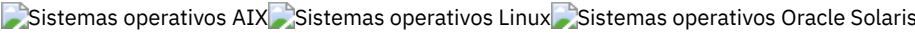



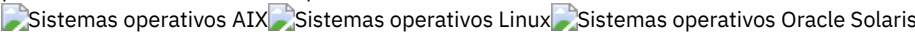
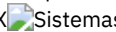


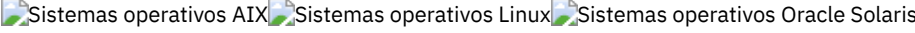



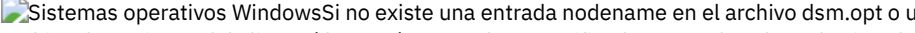
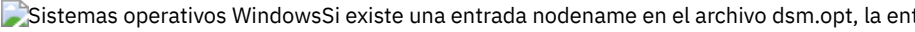
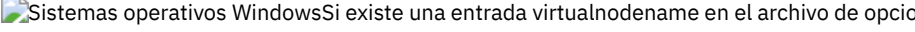
Cuando se utiliza la opción `nodename`, se le solicita la contraseña asignada al nodo que especifique, en caso de que se requiera.

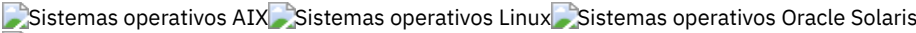

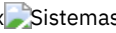


Si desea restaurar o recuperar archivos del servidor mientras trabaja en una estación de trabajo diferente, utilice la opción `virtualnodename`. También puede utilizar la opción `asnodename`, si el administrador la ha configurado.

 **Sistemas operativos Windows**Si trabaja desde una estación de trabajo distinta, podrá utilizar la opción `nodename` aunque la opción `passwordaccess` se haya establecido en `generate..`. Para impedir que esto ocurra, utilice la opción `virtualnodename` en vez de usar `nodename`.

 **Sistemas operativos Windows**El nombre de nodo no es necesariamente el nombre del host TCP/IP.

Al conectarse a un servidor, el cliente debe identificarse ante el servidor. Esta identificación de conexión se determina del modo siguiente:

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si no existe una entrada nodename en el archivo dsm.sys o una entrada virtualnodename en el archivo de opciones del cliente (dsm.opt) o no se ha especificado un nombre de nodo virtual en una línea de mandatos, el identificador de conexión predeterminado es el nombre que devuelve el mandato hostname.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si existe una entrada nodename en el archivo dsm.sys, la entrada nodename modificará temporalmente el nombre que devuelve el mandato hostname.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si existe una entrada virtualnodename en el archivo de opciones del cliente (dsm.sys) o se ha especificado un nombre de nodo virtual en una línea de mandatos, éste no podrá ser igual al nombre que devuelve el mandato hostname. Cuando el servidor acepte el valor de virtualnodename, se solicitará una contraseña (si la autenticación está activada), aunque la opción passwordaccess se haya establecido en generate. Una vez se ha establecido la conexión con el servidor, se permite el acceso a cualquier archivo del que se efectúa copia de seguridad utilizando este identificador de inicio de sesión.
-  Sistemas operativos Windows Si no existe una entrada nodename en el archivo dsm.opt o una entrada virtualnodename en el archivo de opciones del cliente (dsm.opt) o no se ha especificado un nombre de nodo virtual en una línea de mandatos, el identificador de conexión predeterminado es el nombre que devuelve el mandato hostname.
-  Sistemas operativos Windows Si existe una entrada nodename en el archivo dsm.opt, la entrada nodename modificará temporalmente el nombre que devuelve el mandato hostname.
-  Sistemas operativos Windows Si existe una entrada virtualnodename en el archivo de opciones del cliente (dsm.opt) o se ha especificado un nombre de nodo virtual en una línea de mandatos, éste no podrá ser igual al nombre que devuelve el mandato hostname. Cuando el servidor acepte el valor de virtualnodename, se solicitará una contraseña (si la autenticación está activada), aunque la opción passwordaccess se haya establecido en generate. Una vez se ha establecido la conexión con el servidor, se permite el acceso a cualquier archivo del que se efectúa copia de seguridad utilizando este identificador de inicio de sesión.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

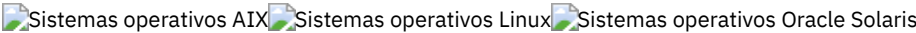



## Cientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor. Puede establecer esta opción en el separador General, en el campo Nombre de nodo del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador General, en el campo Nombre de nodo del editor de preferencias.

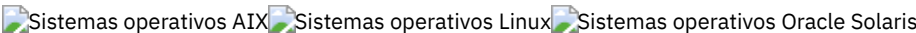

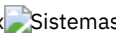

## Sintaxis

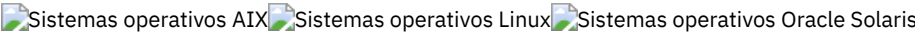



---

```
>>-NODename-- --nodename-----><
```

## Parámetros

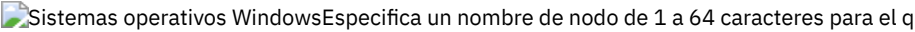
---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
nodename

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifica un nombre de nodo de 1 a 64 caracteres para el que se solicitan servicios de IBM Spectrum Protect. El valor predeterminado es el valor que se devuelve con el mandato hostname.

Si no se especifica un nombre de nodo, el nombre de nodo se establecerá de forma predeterminada en el nombre de sistema principal de la estación de trabajo.

 Sistemas operativos Windows nodename

 Sistemas operativos Windows Especifica un nombre de nodo de 1 a 64 caracteres para el que se solicitan servicios de IBM Spectrum Protect. El valor predeterminado es el valor que se devuelve con el mandato hostname.

Si no se especifica un nombre de nodo, el nombre de nodo se establecerá de forma predeterminada en el nombre de sistema principal de la estación de trabajo.

## Ejemplos


---

Archivo de opciones:

nodename pilar

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows -nodename=cougar

 Sistemas operativos Windows Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos Windows

## Nojournal

---

Utilice la opción nojournal con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario predeterminada.

La copia de seguridad incremental con diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- Las frecuencias de copia no predeterminadas (distintas de 0) no se imponen en el servidor de IBM Spectrum Protect.
- Si se realizan cambios en los atributos de un objeto, es necesario realizar una copia de seguridad del objeto completo.

Por estos motivos, es recomendable utilizar la opción nojournal de forma periódica para realizar una copia de seguridad incremental completa tradicional.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-NOJournal-----<<
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:

```
dsmc incr c: -nojournal
```

 Sistemas operativos AIX  Sistemas operativos Linux

## Nojournal

---

Utilice la opción nojournal con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional, en lugar de la copia de seguridad basada en registro por diario predeterminada.

La copia de seguridad incremental con diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- Las frecuencias de copia no predeterminadas (distintas de 0) no se imponen en el servidor de IBM Spectrum Protect.
- El daemon de registro por diario no detecta los cambios realizados en archivos especiales UNIX y, por lo tanto, no se incluyen en la copia de seguridad.

Por estos motivos, es recomendable utilizar la opción nojournal de forma periódica para realizar una copia de seguridad incremental completa tradicional.

## Clientes soportados

---

Esta opción es válida para el cliente de copia de seguridad-archivado de AIX y Linux.

## Sintaxis

---



>>-NOJournal-----<<

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---





Línea de mandatos:


```
dsmc incr /home -nojournal
```





## Noprompt

---

La opción noprompt suprime la solicitud de confirmación que presentan los mandatos delete group, delete archive, expire, restore image y set event.

- delete archive
- delete backup
- delete group
- expire
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows restore image

 sistemas operativos Mac OS X Nota: El mandato restore image no se aplica a los sistemas operativos Mac OS X.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

>>-NOPrompt-----<<

## Parámetros


---





No hay parámetros para esta opción.





## Ejemplos


---


 sistemas operativos Mac OS XLínea de mandatos:

```
 sistemas operativos Mac OS X dsmc delete archive -noprompt "/Users/van/Documents/*"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

```
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dsmc delete archive -noprompt "/home/project/*"
```

 Sistemas operativos Windows Línea de mandatos:

```
 Sistemas operativos Windows dsmc delete archive -noprompt c:\home\project\*
```

## Nrtablepath

---

La opción nrtablepath especifica la ubicación de la tabla de réplica de nodo en el cliente. El cliente de copia de seguridad y archivado utiliza esta tabla para almacenar la información acerca de cada operación de copia de seguridad o archivado en el servidor de IBM Spectrum Protect.

El servidor en el que hace una copia de seguridad de los datos debe ser de la Versión 7.1 o posterior y debe poder replicar datos del nodo del cliente en el servidor secundario.

Cuando se produce una migración tras error, la información que se encuentra en el servidor secundario es posible que no sea la versión más reciente si la réplica no se ha realizado antes de la migración tras error. El cliente puede comparar la información en la tabla de réplica de nodo en la información que se encuentra en el servidor secundario para determinar si la copia de seguridad del servidor es la versión de copia de seguridad más reciente.

## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Coloque esta opción en el archivo de opciones del sistema cliente (dsm.sys).

Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

Esta opción también se puede configurar en el conjunto de opciones de cliente en el servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-NRTABLEPath---vía de acceso-----<<
```

## Parámetros

---

vía de acceso

Especifica la ubicación en que se crea la base de datos de tabla de réplica de nodo. La ubicación predeterminada es el directorio de instalación del cliente de copia de seguridad y archivado.

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Para usuarios que no sean root, debe especificar una vía de acceso sobre la que el ID de usuario tenga acceso de grabación, por ejemplo un directorio temporal. La mayoría de los usuarios que no son root no tienen acceso al directorio de instalación del cliente.

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Restricción: La tabla de réplica de nodo no se puede crear en el directorio raíz (/). Si decide especificar una ubicación para la tabla de réplica de nodo, no especifique el directorio raíz.

Sistemas operativos Windows Restricción: La tabla de réplica de nodo no se puede crear en el directorio C:\. Si decide especificar una ubicación para la tabla de réplica de nodo, no especifique el directorio C:\.

## Ejemplo

---

Archivo de opciones:

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris  
nrtablepath /Volumes/nrtbl  
 Sistemas operativos Windows nrtablepath C:\nrtbl

Línea de mandatos:

No se aplica.

### Tareas relacionadas:

Determinación del estado los datos replicados del cliente  
Configuración del cliente de migración automática tras error

## Numberformat

---

La opción numberformat especifica el formato que desea utilizar para visualizar los números.

Sistemas operativos Windows Utilice esta opción si desea cambiar el formato de número predeterminado y establecerlo en el idioma del repositorio de mensajes que utiliza.
























Sistemas operativos AIX Sistemas operativos Oracle Solaris Los clientes AIX y Solaris admiten entornos regionales distintos del inglés que describen cada interfaz de usuario que varía en función de la ubicación o el idioma.






Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen

la información de formato de la definición del entorno local que esté en funcionamiento en el momento en que se llama al cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno local.

**Nota:** la opción `numberformat` no afecta al cliente web. El cliente web utiliza el formato de número de la configuración regional con la que se ejecuta el navegador. Si el navegador no se está ejecutando en un entorno local compatible, el cliente web utiliza un formato de números para el inglés estadounidense.

Puede utilizar la opción `numberformat` con los mandatos siguientes:

- `delete archive`
- `delete backup`
- `expire`
- `query archive`
-  `query asr`
- `query backup`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
-  `query image`
- `restore`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
-  `restore image`
- `restore nas`
-  `restore registry`
- `retrieve`
- `set event`






## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

     Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Configuración regional, en el campo Formato numérico del Editor de preferencias.

## Sintaxis

---

```
>>-NUMBERformat-- --number-----<<
```

## Parámetros

---

`number`



Muestra los números utilizando uno de los siguientes formatos. Especifique el número (0–6) que corresponda al formato de número que desee utilizar.






0

Utiliza el formato de fecha especificado por el entorno local. Es el valor predeterminado (no se aplica a Mac OS X).

1

1,000.00

     Éste es el valor predeterminado para las siguientes traducciones disponibles:






- Inglés de Estados Unidos
- Japonés
- Chino (tradicional)
- Chino (simplificado)
- Coreano






2

1,000,00

3

1 000,00

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos Windows Este es el valor predeterminado para las siguientes traducciones disponibles:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos Windows





- Francés
- Checo
- Húngaro
- Polaco
- Ruso






4

1 000.00

5

1.000,00



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos Windows Este es el valor predeterminado para las siguientes traducciones disponibles:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos Windows

- Portugués de Brasil
- Alemán
- Italiano
- Español

6

1'000,00

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris En AIX and Solaris: para definir formatos de número, modifique las líneas siguientes en el archivo de origen del entorno local. Sea cual sea el formato seleccionado se aplica tanto a la salida como a la entrada.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris

punto\_decimal

El carácter que separa el número entero de la parte decimal.

separador\_miles

El carácter que separa las centenas, los millares y los millones.

grouping

El número de dígitos que se incluye en cada grupo se separa con el carácter thousands\_sep.

## Ejemplos

Archivo de opciones:

```
num 4
```

Línea de mandatos:






```
-numberformat=4
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

## Optfile

---

La opción `optfile` especifica el archivo de opciones de cliente que se ha de utilizar cuando inicia una sesión del cliente de copia de seguridad y archivado.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Sintaxis

---





```
>>-OPTFILE = - --file_name-----<<
```

## Parámetros

---

nombre\_archivo

Especifica un archivo de opciones del cliente alternativo, si utiliza el nombre de vía de acceso cualificado al completo. Si sólo especifica el nombre del archivo, el cliente da por supuesto que el nombre de archivo especificado se encuentra en el directorio de trabajo actual. El valor predeterminado es `dsm.opt`.






 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

**Restricción:** especifique la vía de acceso completa cuando utilice esta opción con el daemon de aceptación de clientes (`dsmcad`), pues éste cambia su directorio de trabajo por el directorio raíz ("/") después de la inicialización.


## Ejemplos

---





Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

```
dsmc query session -optfile=myopts.opt
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Daemon de aceptación de clientes:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmcad -optfile=/usr/tivoli/tsm/client/ba/bin/myopts.opt
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Contraseña

---






La opción `password` especifica una contraseña para IBM Spectrum Protect.

Si no se especifica esta opción y el administrador ha establecido la autenticación en `On`, se le solicitará una contraseña al usuario al iniciar una sesión del cliente de copia de seguridad y archivado.

Nota:

1. Si el servidor solicita una contraseña, ésta no se visualizará cuando la escriba. No obstante, si utiliza la opción `password` en la línea de mandatos, la contraseña se visualizará cuando que la escriba.
2. Si el nombre de servidor de IBM Spectrum Protect cambia o si los clientes de copia de seguridad y archivado se dirigen a otro servidor, todos los clientes deberán autenticarse de nuevo con el servidor, porque se debe volver a generar la contraseña cifrada almacenada.

La opción `password` no se tiene en cuenta si el valor de `passwordaccess` es `generate`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Cientes soportados





---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt).

## Sintaxis

---

```
>>-PASsword-- --password-----><
```

## Parámetros

---

### *password*

Especifica la contraseña utilizada para iniciar sesión en el servidor de IBM Spectrum Protect.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de la contraseña varían, dependiendo de donde se almacenan y gestionan las contraseñas, y en función de la versión del servidor al que el cliente se conecta.

Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )  
| { } [ ] : ; < > , ? / ~
```






Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z  
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z  
0 1 2 3 4 5 6 7 8 9  
_ - & + .
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Recuerde:

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.




 Sistemas operativos Windows

En sistemas Windows:

Escriba los parámetros de mandato entre comillas (").

Ejemplo de línea de mandatos:

```
dsmc set password "t67@#$$%^&" "pass2><w0rd"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

En sistemas AIX, Linux y Solaris:

Escriba los parámetros de mandato entre comillas simples (').

Ejemplo de línea de mandatos:

```
dsmc set password -type=vmquest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$$%^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

## Ejemplos


---





Archivo de opciones:

```
password contraseña
```

Línea de mandatos:

```
-password=contraseña
```

 Sistemas operativos Windows-password="secret>shh"

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris-  
password='my>pas\$word'

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Passwordaccess

---






La opción passwordaccess especifica si desea generar la contraseña automáticamente o establecerla mediante una solicitud al usuario.

El administrador puede solicitar una contraseña para su nodo cliente activando la función de autenticación. Consulte al administrador si se requiere una contraseña para el nodo cliente del usuario.

Si necesita una contraseña, puede seleccionar uno de los métodos siguientes:

- Definir la contraseña del nodo cliente y hacer que el cliente la solicite cada vez que usted solicite servicios.
- Hacer que el cliente genere automáticamente una nueva contraseña para el nodo cliente cada vez que caduque, la cifre y la almacene en un archivo y la recupere del archivo cuando se soliciten los servicios. No se solicita al usuario que especifique la contraseña.
- Si el servidor no está configurado para solicitar una contraseña al iniciar sesión, todavía se le puede solicitar que escriba la contraseña de nodo cuando el cliente de archivado y copia de seguridad establece una conexión con el servidor. Este comportamiento se produce si esta opción, passwordaccess, se permite como valor predeterminado o si la establece en indicador de passwordaccess. La contraseña que proporciona en respuesta a la solicitud se utiliza sólo para cifrar la información de inicio de sesión; no se utiliza para iniciar sesión en el servidor. En esta configuración, puede evitar tener que especificar una contraseña estableciendo esta opción en passwordaccess generate. Al establecer passwordaccess generate el cliente crea, almacena y envía la contraseña en su lugar. Cuando se establece passwordaccess generate, se ignora la opción password.

Debe establecer la opción passwordaccess en generate en las situaciones siguientes:

-  Sistemas operativos AIX  Sistemas operativos Linux Cuando se utilice el cliente de HSM.
- Cuando se utilice el cliente web.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Cuando se efectúen operaciones NAS.
- Cuando se utilice IBM Spectrum Protect for Workstations.





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor. Puede establecer esta opción en el separador Autorización, en la sección Acceso con contraseña del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador Autorización, en la sección Acceso con contraseña del editor de preferencias.

## Sintaxis

---

```
>>-PASSWORDAccess--+-prompt---.-----><
                        |-----|
                        |generate-|
```





## Parámetros

---

### prompt

Se le solicitará la contraseña del nodo de cliente cada vez que un cliente se conecte al servidor. Éste es el valor predeterminado.

Para proteger la contraseña del nodo cliente, escriba los mandatos sin la contraseña y espere a que el cliente se la solicite.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Cada usuario debe conocer la contraseña de IBM Spectrum Protect para el nodo cliente. Cualquier usuario que conozca la contraseña del nodo cliente puede obtener acceso a todas las copias de seguridad y todas las copias archivadas que se originan desde el nodo cliente. Por ejemplo: si el usuario especifica el nombre de nodo y la contraseña de un nodo cliente desde otro nodo cliente, el usuario se convierte en un usuario root virtual.

Las aplicaciones API deben proporcionar la contraseña cuando se inicie una sesión. La aplicación es la encargada de obtener la contraseña.





### generate

Cifra y almacena la contraseña de forma local y genera una nueva cuando caduca la anterior. El cliente genera aleatoriamente la nueva contraseña. Las restricciones de la contraseña varían, dependiendo de donde se almacenan y gestionan las contraseñas, y en función de la versión del servidor al que el cliente se conecta. Las contraseñas generadas tienen una longitud de 63 caracteres y contienen al menos dos de los caracteres siguientes :

- mayúsculas
- minúsculas
- caracteres numéricos
- caracteres especiales

Además, el primer carácter y el último de una contraseña generada es un carácter alfabético y pueden ser mayúsculas o minúsculas. Las contraseñas generadas no contienen caracteres repetidos.

Aparecerá una solicitud de contraseña al inscribir una estación de trabajo con un servidor utilizando la inscripción abierta, o bien si el administrador cambia manualmente la contraseña.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Cuando se inicia la sesión localmente, los usuarios no necesitan saber la contraseña del nodo cliente. Sin embargo, si se utiliza la opción nodename en un nodo remoto, los usuarios pueden acceder a los archivos de los que son propietarios y a los archivos a los que otro usuario les conceda acceso.

## Ejemplos





---

Archivo de opciones:

```
passwordaccess generate
```

Línea de mandatos:





No se aplica.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Passworddir





---

La opción passworddir especifica el directorio donde debe almacenarse el archivo de la contraseña cifrada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
El directorio predeterminado para AIX es /etc/security/adsm y para otras plataformas UNIX y Linux es /etc/adsm. El directorio predeterminado para Mac es /Library/Preferences/Tivoli Storage Manager. Independientemente de donde se almacene, el archivo de contraseñas creado por el cliente siempre se denomina TSM.sth. Tres archivos forman un archivo de contraseña. TSM.KDB almacena las contraseñas cifradas. TSM.sth almacena la clave de cifrado aleatoria utilizada para cifrar contraseñas en el archivo TSM.KDB. Este



archivo está protegido por el sistema de archivos. TSM.IDX es un archivo de índices utilizado para realizar el seguimiento de las contraseñas en el archivo TSM.KDB.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X





## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

## Sintaxis

---

```
>>-PASSWORDDIR-- --directoryname-----><
```

## Parámetros












---

directoryname





Especifica la vía de acceso en la que se almacenará el archivo de contraseñas cifradas. El nombre del archivo de contraseñas es TSM.sth. Si cualquier parte de la vía de acceso especificada no existe, IBM Spectrum Protect intenta crearla.

## Ejemplos

---

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X Archivo de opciones:  
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  sistemas operativos Mac OS X

```
passworddir "/Users/user1/Library/Preferences/Tivoli Storage Manager/"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
passworddir /etc/security/tsm
```

Línea de mandatos:





No se aplica.

## Pick






---







La opción pick crea la lista de versiones de copia de seguridad o copias archivadas que coinciden con la especificación de archivo que ha especificado.

En esta lista, puede seleccionar las versiones que se desee procesar. Incluya la opción inactive para ver los objetos activos e inactivos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para las imágenes, si no especifica un espacio de archivos de origen y un espacio de archivos de destino, la lista pick contiene todas las imágenes cuya copia de seguridad se ha realizado. En este caso, las imágenes seleccionadas desde la lista pick se restauran en su ubicación original. Si especifica el espacio de archivos origen y el espacio de archivos destino, puede seleccionar sólo una entrada de la lista pick.

La opción pick puede utilizarse con los mandatos siguientes:

- delete archive
- delete backup
- delete group
- expire
- restore
-  Sistemas operativos Windows restore asr
- restore group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows restore image

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsrestore nas
-  Sistemas operativos Windowsrestore vm
- retrieve

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-PIck-----><
```

## Parámetros


---





No hay parámetros para esta opción.





## Ejemplos


---


 sistemas operativos Mac OS XLínea de mandatos:

```
 sistemas operativos Mac OS X dsmc restore "/Users/van/Documents/*" -pick -inactive
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

```
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
dsmc restore "/home/project/*" -pick -inactive
```

 Sistemas operativos WindowsLínea de mandatos:

```
 Sistemas operativos Windowsdsmc restore c:\project\* -pick -inactive
```
























## Pitdate

---






Utilice la opción pitdate con la opción pittime para establecer un instante específico para visualizar o restaurar la última versión de las copias de seguridad.

Se procesarán los archivos cuya copia de seguridad se ha realizado *en o antes* de la fecha y hora que especifique y que no se han suprimido *antes* de la fecha y la hora que especifique. Las versiones de copia de seguridad que se hayan creado después de esta fecha y hora se pasan por alto.

La opción pitdate puede utilizarse con los mandatos siguientes:

- delete backup
-  Sistemas operativos Windowsquery asr
- query backup
- query group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowsquery image
-  Sistemas operativos Windowsquery nas
-  Sistemas operativos Windowsquery systemstate
-  Sistemas operativos Windowsquery vm (vmbackuptype=fullvm and vmbackuptype=hypervfull)
- restore
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsrestore group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowsrestore image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsrestore nas
-  Sistemas operativos Windowsrestore vm (vmbackuptype=fullvm and vmbackuptype=hypervfull)

Cuando se utiliza pitdate, las opciones inactive y latest son implícitas.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-PITDate = - --date-----<<
```

## Parámetros

---


date


Especifica la fecha apropiada. Escriba la fecha en el formato seleccionado con la opción dateformat.





Si se incluye la opción dateformat con un mandato, ésta debe anteponerse a las opciones fromdate, pitdate y todote.





## Ejemplos


---


 sistemas operativos Mac OS XLínea de mandatos:

```
 sistemas operativos Mac OS Xdsmc restore "/Volumes/proj4/myproj/*" -sub=y -pitdate=08/01/2003 -  
pittime=06:00:00
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

```
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
dsmc restore "/fsl/*" -sub=y -pitdate=08/01/2003 -pittime=06:00:00
```

 Sistemas operativos WindowsLínea de mandatos:

```
 Sistemas operativos Windowsdsmc restore -pitdate=08/01/2003 c:\myfiles\
```



















## Pittime

---


Utilice la opción pittime con la opción pitdate para establecer un instante específico para el cual desea visualizar o restaurar la última versión de las copias de seguridad.

Se procesarán los archivos cuya copia de seguridad se ha realizado *en o antes* de la fecha y hora que especifique y que no se han suprimido *antes* de la fecha y la hora que especifique. Las versiones de copia de seguridad que se hayan creado después de esta fecha y hora se pasan por alto. Esta opción se ignora si no especifica la opción pitdate.

La opción pittime puede utilizarse con los mandatos siguientes:

- delete backup
-  Sistemas operativos Windowsquery asr
- query backup
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows query image
-  Sistemas operativos Windowsquery nas
-  Sistemas operativos Windowsquery systemstate
-  Sistemas operativos Windowsquery vm(vmbackuptype=fullvm and vmbackuptype=hypervfull)
- restore
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows restore image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X
-  Sistemas operativos Windowsrestore nas
-  Sistemas operativos Windowsrestore vm (vmbackuptype=fullvm and vmbackuptype=hypervfull)

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-PITTime = - --hora-----<<
```

## Parámetros

---

hora

Especifica una hora en la fecha indicada. Si no se especifica una hora, se toma el valor predeterminado 23:59:59. Especifique la hora en el formato seleccionado con la opción timeformat.





Cuando incluya la opción timeformat en un mandato, ésta deberá preceder a las opciones fromtime, pittime y tottime.

## Ejemplos


---

 sistemas operativos Mac OS XLínea de mandatos:

```
dsmc query backup -pitt=06:00:00 -pitd=08/01/2003  
"/Volumes/proj5/myproj/*"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

```
dsmc q b "/fs1/*" -pitt=06:00:00 -pitd=08/01/2003
```

 Sistemas operativos WindowsLínea de mandatos:

```
dsmc query backup -pitt=06:00:00 -pitd=08/01/2003 c:\myfiles\
```

## Postschedulecmd/Postnschedulecmd

---

La opción postschedulecmd/postnschedulecmd especifica un mandato que el programa cliente procesa después de ejecutar una planificación.

Si desea que el programa cliente para esperar a que el mandato finalice antes de continuar con otro proceso, utilice la opción postschedulecmd. Si no desea esperar a que el mandato finalice antes de que el cliente continúe con otro proceso, especifique la opción postnschedulecmd.

El comportamiento del manejo de códigos de retorno y de las acciones planificadas depende de la opción especificada y del tipo de operación que se haya planificado:

- Para operaciones planificadas en las que la acción planificada es distinto de COMMAND:

Si el mandato postschedulecmd no se completa con el código de retorno 0 (cero), el código de retorno para el suceso planificado es 8 o el código de suceso para la operación planificada, lo que ocurra antes. Si no desea que esta regla se aplique al mandato postschedulecmd, cree un archivo script o por lotes que inicie el mandato y finalice con el código de retorno 0. A continuación, configure postschedulecmd de modo que inicie el archivo script o por lotes.

- Para operaciones planificadas en las que la acción planificada es COMMAND:

El código de retorno del mandato especificado en la opción postschedulecmd no afecta al código de retorno del que se informa al servidor cuando se completa el suceso planificado. Si desea que los resultados de las operaciones postschedulecmd afecten al código de retorno del suceso planificado, incluya las operaciones postschedulecmd en el script del mandato de acción planificado en lugar de utilizar la opción postschedulecmd.

- Si la acción del planificador no se puede iniciar y el mandato especificado en la opción preschedulecmd se completa con un código de retorno de cero (0), se ejecuta el mandato especificado por la opción postschedulecmd.
- No se realiza el seguimiento de código de retorno de una operación especificada en la opción postnschedulecmd, y no afecta al código de retorno del suceso planificado.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha Planificador, en el recuadro de texto Mandato de planificación del Editor de preferencias. El servidor también puede definir estas opciones.

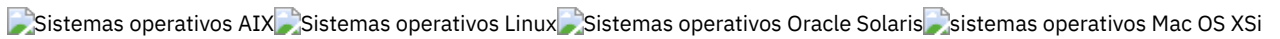
 Sistemas operativos WindowsEstablezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Planificador, en el recuadro de texto Mandato de planificación del Editor de preferencias. El servidor también puede definir estas opciones.

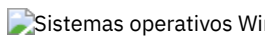
```
>>--+-POSTSchedulecmd--+-+-- --cmdstring-----><
'-POSTNSchedulecmd-'
```

## Parámetros

### cmdstring

Especifica el mandato que se debe procesar. Con esta opción puede entrarse un mandato para que se ejecute después de una planificación. Utilice únicamente una opción `postschedulecmd`.

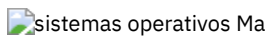
 Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas. Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples.

 Especifique la serie del mandato tal como la escribiría desde el indicador de mandatos del sistema operativo. Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas simples. Por ejemplo:

```
'net stop someservice'
```

Utilice una serie en blanco, o nula, para `cmdstring` si desea impedir que se ejecute cualquier mandato que el administrador del servidor de IBM Spectrum Protect utiliza para `postschedulecmd` o para `preschedulecmd`. Si especifica una serie en blanco o nula en una de las dos opciones, se impedirá que el administrador pueda utilizar un mandato en ambas opciones.

Si el administrador utiliza una serie en blanco o nula en la opción `postschedulecmd`, el usuario no podrá ejecutar un mandato posterior a la planificación (`post-schedule`).

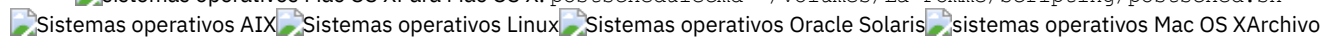
 En el caso de Mac OS X, si el mandato planificado `postschedulecmd` es un AppleScript, tiene que utilizar el mandato `osascript` para ejecutar el script. Por ejemplo, si "Database Script" es un AppleScript, especifique este mandato:

```
postschedulecmd osascript "/Volumes/La Pomme/Scripting/
Database Script"
```

## Ejemplos

 Archivo de opciones:

```
postschedulecmd "/Volumes/La Pomme/Scripting/postsched.sh"
```

 Archivo de opciones:

```
postschedulecmd "restart database"
```

La serie del mandato es un mandato válido para arrancar la base de datos.

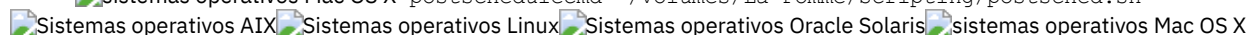
 Archivo de opciones:



```
posts startdb.cmd
posts 'rename c:\myapp\logfile.log logfile.new'
posts 'net start "simple service"'
posts 'rename "c:\myapp\log file.log" "log file.new"'
posts '"C:\Archivos de programa\MyTools\runreport.bat"
log1.in log2.in'
```

 Línea de mandatos:

```
postschedulecmd="/Volumes/La Pomme/Scripting/postsched.sh"
```

 Línea de mandatos:

 Línea de mandatos:

```
postschedulecmd="'restart database'"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

### Conceptos relacionados:


Códigos de retorno del cliente


### Referencia relacionada:


## Postsnapshotcmd



---


La opción `postsnapshotcmd` le permite ejecutar scripts o mandatos de shell del sistema operativo después de que el cliente de copia de seguridad y archivado haya iniciado una instantánea durante una operación de copia de seguridad basada en instantánea.


 **Sistemas operativos Windows** Esta opción se puede utilizar en conjunción con la opción `presnapshotcmd` para que pueda detener una aplicación mientras se crea una instantánea, y después reiniciar esa aplicación después de que se haya iniciado la instantánea. Esta opción solo es válida si se ha configurado OFS o la copia de seguridad de imágenes en línea.

 **Sistemas operativos AIX** **AIX únicamente:** esta opción solo se aplica a la copia de seguridad o archivado del archivo JFS2 basada en instantánea y a la copia de seguridad de imagen basada en instantánea. Para una copia de seguridad de archivos basada en instantánea o archivado, utilice esta opción con el mandato `backup`, con la opción `include.fs` o bien en el archivo `dsm.sys`.


 **Sistemas operativos Linux** **Linux únicamente:** esta opción sólo es válida si LVM está instalado y configurado en el sistema, lo cual permite realizar una copia de seguridad de imágenes basada en instantánea.

 **Sistemas operativos AIX**  **Sistemas operativos Linux** **Solo AIX y Linux:** para una copia de seguridad de imágenes basada en instantánea, utilice esta opción con el mandato `backup image`, con la opción `include.image` o en el archivo `dsm.sys`.

 **Sistemas operativos Windows** Para una copia de seguridad de imágenes en línea, utilice esta opción con el mandato `backup image`, con la opción `include.image` o bien en el archivo `dsm.opt`.

 **Sistemas operativos Windows** Para operaciones de soporte de archivos abiertos, utilice la opción `postsnapshotcmd` en una sentencia `include.fs` o en el archivo de opciones del cliente (`dsm.opt`).

Si `postsnapshotcmd` falla, la operación continúa pero se anotan los avisos que corresponda.



 **Sistemas operativos Windows** **Atención:** Durante operaciones de copia de seguridad de imágenes o de copia de seguridad diferencial de instantánea, si el mandato que incluye en la sentencia `presnapshotcmd` o `postsnapshotcmd` inicia un proceso asíncrono, es posible que el mandato no finalice antes de que termine la operación de copia de seguridad. Si el mandato no finaliza antes de que termine la copia de seguridad, es posible que los archivos temporales se bloqueen, lo que impide que se supriman. Se produce un suceso de base de datos y se registra el siguiente mensaje en el archivo `dsmerror.log`:


```
ANS0361I DIAG: ..\..\common\db\cacheobj.cpp( 777): dbDelete():
  remove('C:\adsm.sys\SystemExcludeCache__24400820.TsmCacheDB'):
  errno 13: "Permiso denegado".
```

El archivo que se especifica en el mensaje (`cacheobj.cpp`) se puede suprimir manualmente después de que finalice el mandato iniciado mediante la opción `presnapshotcmd` o `postsnapshotcmd`.

## Clientes soportados



---


 **Sistemas operativos AIX**  **Sistemas operativos Linux** Esta opción solo es válida para los clientes AIX y los clientes Linux x86\_64. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

 **Sistemas operativos Windows** Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 **Sistemas operativos AIX**  **Sistemas operativos Linux** Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. También puede establecer esta opción en la ficha `Image-Snapshot` del editor de preferencias.

 **Sistemas operativos Windows** Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). También puede establecer esta opción en la ficha `Imagen-Instantánea` del editor de preferencias.

## Sintaxis



---

```
>>---POSTSNAPshotcmd--- --"cmdstring"-----<<
```

## Parámetros

---

 Sistemas operativos AIX  Sistemas operativos Linux "cmdstring"

 Sistemas operativos AIX  Sistemas operativos Linux Especifica el mandato que ha de procesarse.


Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.


Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:

```
"resume database  
myDb"
```

Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:

```
'resume database "myDb"'
```

 Sistemas operativos Windows "cmdstring"

 Sistemas operativos Windows Especifica el mandato de detención que ha de ejecutarse.

Utilice espacios en blanco o una cadena nula en `cmdstring` si se desea evitar que se ejecute cualquier mandato que utilice el administrador para `postsnapshotcmd`. Si especifica un espacio en blanco o una cadena nula impide que el administrador utilice un mandato en esta opción. Si el administrador utiliza un espacio en blanco o una cadena nula en la opción `postsnapshotcmd`, el usuario no puede ejecutar un mandato posterior a la instantánea.

Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.

Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:



```
"resume database  
myDb"
```



Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:

```
'resume database "myDb"'
```

## Ejemplos


---

 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux `postsnapshotcmd "any command"`



La serie del mandato es un mandato válido para reiniciar la aplicación.


 Sistemas operativos Windows Archivo de opciones:


 Sistemas operativos Windows `postsnapshotcmd "restart application"`

La serie del mandato es un mandato válido para reiniciar la aplicación.

 Sistemas operativos AIX  Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux `backup image -postsnapshotcmd="any command"`

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `backup image -postsnapshotcmd="restart application"`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Preschedulecmd/Prenschedulecmd

---

La opción `preschedulecmd` especifica un mandato que el programa cliente procesa antes de ejecutar una planificación.

El programa de cliente espera a que se complete el mandato antes de empezar la planificación. Si no se desea esperar, especifique `prenschedulecmd`.

Nota:

1. La finalización satisfactoria del mandato `preschedulecmd` se considera una condición previa para ejecutar la operación planificada. Si el mandato `preschedulecmd` no finaliza con el código de retorno 0, no se ejecutarán la operación planificada ni los mandatos `postschedulecmd` y `postnschedulecmd`. El cliente notificará que el suceso planificado no se ha ejecutado correctamente y el código de retorno será 12. Si no desea que esta regla se aplique al mandato `preschedulecmd`, cree un archivo script o por lotes que invoque el mandato y finalice con el código de retorno 0. A continuación, configure `preschedulecmd` de modo que invoque el archivo script o por lotes. El código de retorno del mandato `prenschedulecmd` no se registra y no afecta al código de retorno del suceso planificado.

2. El servidor también puede definir la opción preschedulecmd (y la opción preschedulecmd).





## Cientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador Planificador, en el recuadro de diálogo Mandato de planificación del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador Planificador, en el recuadro de diálogo Mandato de planificación del Editor de preferencias.

## Sintaxis

---





```
>>+-PRESchedulecmd-+--- --cmdstring-----<<  
  '-PRENSchedulecmd-'
```


## Parámetros


---

### cmdstring


Especifica el mandato que se debe procesar. Utilice sólo una opción preschedulecmd. Con esta opción puede entrarse un mandato para que se ejecute antes de una planificación.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas. Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples.

 Sistemas operativos Windows  
Especifique la serie del mandato tal como la escribiría desde el indicador de mandatos del sistema operativo; si la serie que especifica necesita comillas para ejecutarla en un indicador de Windows, incluya las comillas como sea necesario. Si la serie del mandato contiene espacios en blanco, especifique la serie del mandato entre comillas simples.

 Sistemas operativos Windows  
En este ejemplo, las comillas simples son necesarias porque la serie de mandato contiene caracteres de espacio:


```
'net stop someservice'
```

 Sistemas operativos Windows  
En este siguiente ejemplo, las comillas dobles son necesarias porque el archivo al que se va a cambiar el nombre y el nombre de archivo nuevo contienen caracteres de espacio. Debido a que la serie de mandato contiene caracteres de espacio, toda la serie debe estar metida entre comillas simples.

```
presc 'rename "c:\myapp\log file.log" "log file.old"'
```

Utilice espacios en blanco o una cadena nula para cmdstring si desea impedir que se ejecuten mandatos que el administrador del servidor de IBM Spectrum Protect utilice para postschedulecmd y preschedulecmd. Si especifica una serie en blanco o nula en una de las dos opciones, se impedirá que el administrador pueda utilizar un mandato en ambas opciones.

Si su administrador utiliza un espacio en blanco o una cadena nula en la opción preschedulecmd, el usuario no puede ejecutar un mandato previo a la planificación.





 Sistemas operativos Mac OS X  
Para Mac OS X, si el mandato de planificación preschedulecmd es un script de Apple, deberá utilizar el mandato osascript para ejecutar el script. Por ejemplo, si ""Database Script"" es un script de Apple, especifique este mandato:

```
preschedulecmd osascript "/Volumes/La Pomme/Scripting/  
Database Script"
```

## Ejemplos

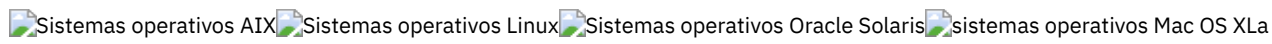
---

Archivo de opciones:

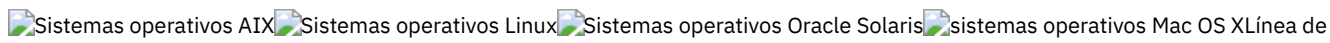
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

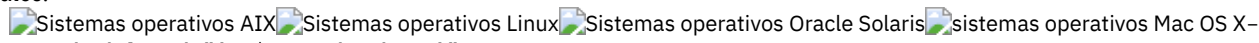


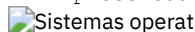
```
preschedulecmd "<mandato de detención del producto de base de datos>  
base de datos"
```

 La serie del mandato es un mandato válido para paralizar la base de datos.

```
 presc stopdb.cmd  
presc 'rename c:\myapp\logfile.log logfile.old'  
presc 'net stop "simple service"  
presc 'rename "c:\myapp\log file.log" "log file.old"  
presc '"C:\Archivos de programa\MyTools\runreport.bat"  
log1.in log2.in'
```

 Línea de mandatos:

```
 preschedulecmd="quiesce database"
```

 Línea de mandatos:

```
 preschedulecmd="quiesce database"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

#### Conceptos relacionados:

Códigos de retorno del cliente

## Preservelastaccessdate

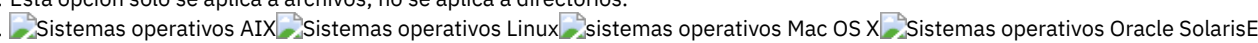
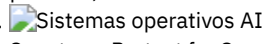
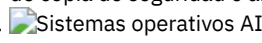
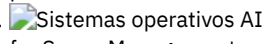
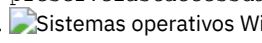
Utilice la opción preservelastaccessdate para especificar si una operación de copia de seguridad o de archivado cambia la última hora de acceso.

Una operación de copia de seguridad o archivado puede cambiar la última hora de acceso de un archivo. Tras una operación, el cliente de copia de seguridad y archivado puede restablecer la última hora de acceso al valor anterior a la operación. En lugar de modificarse, el cliente de copia de seguridad-archivado puede conservar la última hora de acceso. El restablecimiento de la última hora de acceso requiere un proceso adicional para cada archivo del que se haga copia de seguridad o se archive.

Si habilita el soporte de archivos abiertos, la última fecha de acceso de los archivos siempre prevalecerá independientemente de los valores de preservelastaccessdate. Cuando está activado el soporte de archivos abiertos, no utilice la opción preservelastaccessdate.

Utilice esta opción con los mandatos incremental, selective o archive.

Nota:

1. Esta opción sólo se aplica a archivos; no se aplica a directorios.
2.  El restablecimiento de la última fecha de acceso afecta al rendimiento de la copia de seguridad y el archivado.
3. El restablecimiento de la última fecha de acceso puede afectar a aplicaciones que dependan de últimas fechas de acceso precisas, como es el caso de la aplicación de gestión de recursos de almacenamiento (SRM).
4.  En sistemas de archivos que no están gestionados por el cliente IBM Spectrum Protect for Space Management o durante operaciones de copia de seguridad o archivado de usuarios que no sean root, el atributo ctime se restablece. El atributo de última fecha y hora cambiada (ctime) se restablece a la fecha y hora de la operación de copia de seguridad o archivado.
5.  La opción updatectime prevalece sobre la opción preservelastaccessdate. Si ambas opciones están establecidas en yes, la opción preservelastaccessdate se pasa por alto.
6.  En sistemas de archivos que no gestione el cliente IBM Spectrum Protect for Space Management, no utilice preservelastaccessdate yes ni el mandato de GPFS mmbackup. El mandato mmbackup y preservelastaccessdate yes selecciona todos los archivos para cada operación de copia de seguridad.
7.  La última fecha de acceso no se puede conservar en archivos que estén protegidos contra escritura por el atributo de sólo lectura o por un permiso de seguridad de NTFS restrictivo.
8. No se puede restablecer la fecha del último acceso de los archivos de sólo lectura. La opción preservelastaccessdate omite los archivos de sólo lectura y no cambia su fecha.





## Clientes soportados


Esta opción es válida para todos los clientes.

El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Coloque esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en el separador Copia de seguridad del editor de preferencias.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Copia de seguridad del editor de preferencias.

## Sintaxis

---

```
..-No--.  
>>-PRESERVELastaccessdate--+-+-----+-----<<  
'-Yes-'
```

## Parámetros

---

No

Una operación de copia de seguridad o archivado puede cambiar la última fecha de acceso. Este es el valor predeterminado.

Yes





Una operación de copia de seguridad o archivado no cambia la última fecha de acceso.





## Ejemplos

---


Archivo de opciones:

```
preservelastaccessdate yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Línea de mandatos:



```
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Incremental /proj/test/test_file -preservelastaccessdate=yes
```



 Sistemas operativos Windows Línea de mandatos:

```
 Sistemas operativos Windows dsmc incr c: e: f: -preservelastaccessdate=yes
```

**Información relacionada:**

 Sistemas operativos AIX  Sistemas operativos Linux [Mandato mmbackup: Requisitos de IBM Spectrum Protect](#)

 Sistemas operativos AIX  Sistemas operativos Linux [Orientación para integrar IBM Spectrum Scale AFM con IBM Spectrum Protect](#)

 Sistemas operativos AIX  Sistemas operativos Linux [Utilización de las opciones de inclusión y exclusión de IBM Spectrum Protect con el mandato mmbackup de IBM Spectrum Scale](#)

## Preservepath






---

La opción preservepath especifica qué volumen del directorio origen se reproducirá como parte del directorio destino cuando se restauran o recuperan archivos en una ubicación nueva.

Utilice la opción -subdir=yes para incluir el subárbol completo del directorio de origen (los directorios y archivos que se encuentren en el directorio de origen del nivel más bajo) como el origen que debe restaurarse. Si un directorio destino necesario no existe, se crea. Si un archivo destino tiene el mismo nombre que un archivo origen, se graba sobre él. Utilice la opción -replace=prompt para que el cliente le pregunte antes de sobrescribir los archivos.

Utilice la opción preservepath con los mandatos siguientes:

- restore
- restore backupset
- restore group
- retrieve

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Sintaxis

```
.-Subtree--.  
>>-PRESERVEpath = +-----<  
+-Complete+  
+-NOBase----+  
'-NONE-----'
```

## Parámetros

### Subtree

Crea el directorio de origen de más bajo nivel como un subdirectorio del directorio de destino. Los archivos del directorio de origen se almacenan en el nuevo subdirectorio. Éste es el valor predeterminado.

### Complete

Restaura toda la vía de acceso, empezando desde el directorio raíz, en el directorio especificado. La vía de acceso completa incluye todos los directorios excepto el nombre del espacio de archivos.

### NOBase

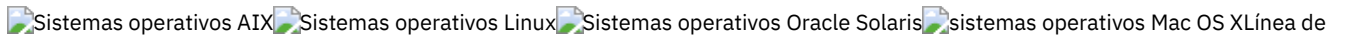
Restaura el contenido del directorio de origen sin directorio de nivel inferior, o base, en el directorio de destino especificado.

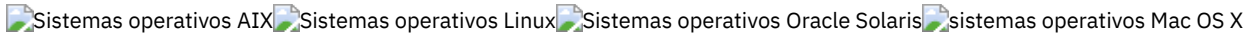
### NONE

Restaura todos los archivos de origen seleccionados en el directorio de destino. Ninguna parte de la vía de acceso de origen al mismo nivel o por encima del directorio de origen se reproduce en el destino.

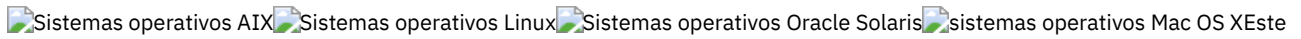
Si se especifica SUBDIR=yes, el cliente restaura todos los archivos de los directorios de origen en el directorio de destino único.

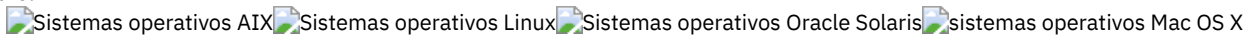
## Ejemplos

 Línea de mandatos:

 Supongamos que el espacio de archivos del servidor contiene las copias de seguridad siguientes:

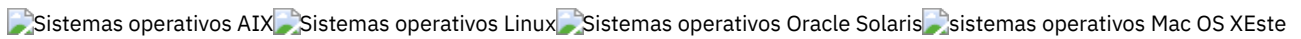
```
/fs/h1/m1/file.a  
/fs/h1/m1/file.b  
/fs/h1/m1/l1/file.x  
/fs/h1/m1/l1/file.y
```

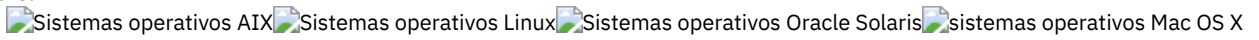
 Este mandato:

  
dsmc res /fs/h1/m1/ /u/ann/ -preser=complete

### Restaura estos directorios y archivos:

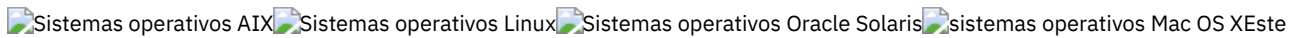
```
/u/ann/h1/m1/file.a  
/u/ann/h1/m1/file.b
```

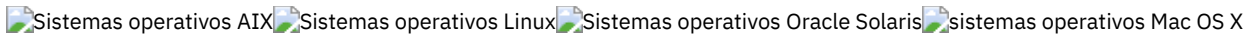
 Este mandato:

  
dsmc res /fs/h1/m1/ /u/ann/ -preser=nobase

### Restaura estos directorios y archivos:

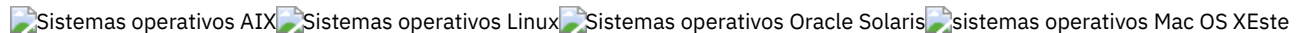
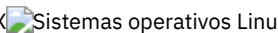
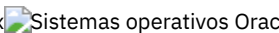

```
/u/ann/file.a  
/u/ann/file.b
```

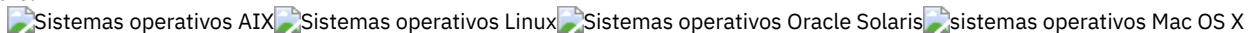
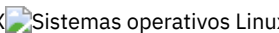


 Este mandato:

  
dsmc res backupset /fs/h1/m1/ /u/ann/ -su=yes  
-preser=nobase -loc=file

**Restaura estos directorios y archivos:**

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/file.x  
/u/ann/file.y
```

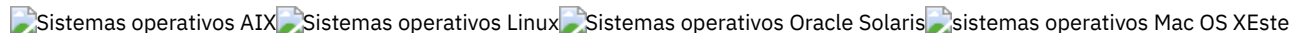
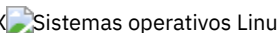
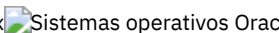

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:

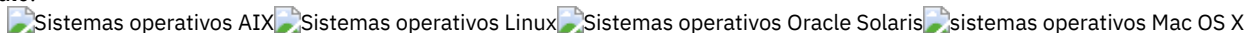
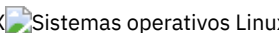


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=subtree
```

**Restaura estos directorios y archivos:**

```
/u/ann/m1/file.a  
/u/ann/m1/file.b
```


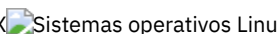


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:


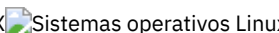


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -preser=none
```

**Restaura estos directorios y archivos:**

```
/u/ann/file.a  
/u/ann/file.b
```


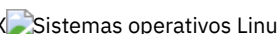


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:


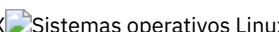


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=complete
```

**Restaura estos directorios y archivos:**

```
/u/ann/h1/m1/file.a  
/u/ann/h1/m1/file.b  
/u/ann/h1/m1/l1/file.x  
/u/ann/h1/m1/l1/file.y
```


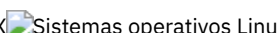
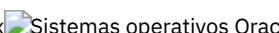

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:


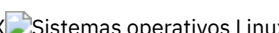
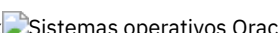

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=nobase
```

**Restaura estos directorios y archivos:**

```
/u/ann/file.a  
/u/ann/file.b  
/u/ann/l1/file.x  
/u/ann/l1/file.y
```


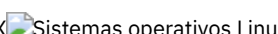
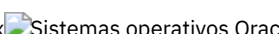

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:

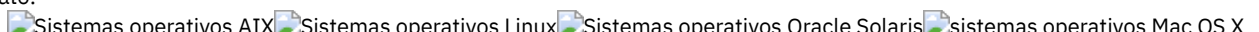
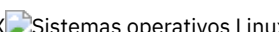
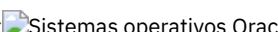

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=subtree
```

**Restaura estos directorios y archivos:**

```
/u/ann/m1/file.a  
/u/ann/m1/file.b  
/u/ann/m1/l1/file.x  
/u/ann/m1/l1/file.y
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc res /fs/h1/m1/ /u/ann/ -su=yes -preser=none
```


**Restaura estos directorios y archivos:**


```
/u/ann/file.a
/u/ann/file.b
/u/ann/file.x
/u/ann/file.y
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Suponga que el espacio de archivos de servidor contiene las copias de seguridad siguientes:


```
c:\h1\m1\file.a
c:\h1\m1\file.b
c:\h1\m1\l1\file.x
c:\h1\m1\l1\file.y
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res backupset my.backupset.file /fs/h1/m1/ /u/ann/ -su=yes` crea un archivo de conjunto de copias de seguridad local llamado "my.backupset.file".

**Restaura estos directorios y archivos:**


```
c:\ann\h1\m1\file.a
c:\ann\h1\m1\file.b
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -preser=nobase.`

**Restaura estos directorios y archivos:**


```
c:\ann\file.a
c:\ann\file.b
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -preser=subtree.`

**Restaura estos directorios y archivos:**


```
c:\ann\m1\file.a
c:\ann\m1\file.b
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -preser=none.`

**Restaura estos directorios y archivos:**

```
c:\ann\file.a
c:\ann\file.b
```


 Sistemas operativos Windows Este mandato:


 Sistemas operativos Windows

```
dsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=
complete
```

**Restaura estos directorios y archivos:**

```
c:\ann\h1\m1\file.a
c:\ann\h1\m1\file.b
c:\ann\h1\m1\l1\file.x
c:\ann\h1\m1\l1\file.y
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=nobase.`

**Restaura estos directorios y archivos:**

```
c:\ann\file.a
c:\ann\file.b
c:\ann\l1\file.x
c:\ann\l1\file.y
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=subtree.`

**Restaura estos directorios y archivos:**

```
c:\ann\m1\file.a
c:\ann\m1\file.b
c:\ann\m1\l1\file.x
c:\ann\m1\l1\file.y
```


 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows `dsmc res c:\h1\m1\ c:\ann\ -su=yes -preser=none.`

**Restaura estos directorios y archivos:**

```
c:\ann\file.a
c:\ann\file.b
c:\ann\file.x
c:\ann\file.y
```




 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows

```
dsmc res backupset c:\h1\m1\ c:\ann\ -su=yes
-preser=nobase -loc=file
```

**Restaura estos directorios y archivos:**

```
c:\ann\file.a
c:\ann\file.b
c:\ann\file.x
c:\ann\file.y
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows


## Presnapshotcmd


---



La opción `presnapshotcmd` le permite ejecutar mandatos del sistema operativo antes de que el cliente de copia de seguridad y archivado inicie una instantánea.


Esto le permite detener una aplicación antes de que el cliente inicie la instantánea durante una operación de copia de seguridad basada en instantánea o archivado.


 Sistemas operativos Windows Esta opción se puede utilizar en conjunción con la opción `postsnapshotcmd` para que pueda detener una aplicación mientras se crea una instantánea, y después reiniciar esa aplicación después de que se haya iniciado la instantánea. Esta opción solo es válida si se ha configurado OFS o la copia de seguridad de imágenes en línea.

 Sistemas operativos AIX Únicamente: esta opción solo se aplica a la copia de seguridad o archivado del archivo JFS2 basada en instantánea y a la copia de seguridad de imagen basada en instantánea. Para una copia de seguridad de archivos basada en instantánea o archivado, utilice esta opción con el mandato `backup`, con la opción `include.fs` o bien en el archivo `dsm.sys`.


 Sistemas operativos Linux Únicamente: esta opción solo es válida si LVM está instalado y configurado en el sistema, lo cual permite realizar una copia de seguridad de imágenes basada en instantánea.

 Sistemas operativos AIX  Sistemas operativos Linux Solo AIX y Linux: para una copia de seguridad de imágenes basada en instantánea, utilice esta opción con el mandato `backup image`, con la opción `include.image` o bien en el archivo `dsm.sys`.

 Sistemas operativos Windows Para una copia de seguridad de imágenes en línea, utilice esta opción con el mandato `backup image`, con la opción `include.image` o bien en el archivo `dsm.opt`.

 Sistemas operativos Windows Para realizar operaciones de soporte de archivos abiertos, utilice la opción `presnapshotcmd` en una sentencia `include.fs` o en el archivo de opciones del cliente (`dsm.opt`).

Si la ejecución de `presnapshotcmd` no se realiza correctamente, se da por supuesto que la aplicación no se encuentra en un estado coherente y el cliente detiene la operación y visualiza el mensaje de error adecuado.



 Sistemas operativos Windows Atención: Durante operaciones de copia de seguridad de imágenes o de copia de seguridad diferencial de instantánea, si el mandato que incluye en la sentencia `presnapshotcmd` o `postsnapshotcmd` inicia un proceso asíncrono, es posible que el mandato no finalice antes de que termine la operación de copia de seguridad. Si el mandato no finaliza antes de que termine la copia de seguridad, es posible que los archivos temporales se bloqueen, lo que impide que se supriman. Se produce un suceso de base de datos y se registra el siguiente mensaje en el archivo `dsmerror.log`:


```
ANS0361I DIAG: ..\..\common\db\cacheobj.cpp( 777): dbDelete():
remove('C:\adsm.sys\SystemExcludeCache__24400820.TsmCacheDB'):
errno 13: "Permiso denegado".
```

El archivo que se especifica en el mensaje (`cacheobj.cpp`) se puede suprimir manualmente después de que finalice el mandato iniciado mediante la opción `presnapshotcmd` o `postsnapshotcmd`.

## Clientes soportados



---


 Sistemas operativos AIX  Sistemas operativos Linux Esta opción solo es válida para los clientes AIX JFS2 y Linux x86\_64. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. También puede establecer esta opción en la ficha **Image-Snapshot** del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). También puede establecer esta opción en la ficha Imagen-Instantánea del editor de preferencias.





## Sintaxis

---

```
>>---PRESNAPshotcmd---- --"cmdstring"-----<<
```

## Parámetros

---

 Sistemas operativos AIX  Sistemas operativos Linux "cmdstring"  
 Sistemas operativos AIX  Sistemas operativos Linux Especifica el mandato que ha de procesarse.



Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.

Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:

```
"quiesce database myDb"
```

Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:

```
'resume database "myDb"'
```

 Sistemas operativos Windows "cmdstring"  
 Sistemas operativos Windows Especifica el mandato de detención que ha de ejecutarse.

Utilice espacios en blanco o una serie nula en `cmdstring` si se desea evitar que se ejecute cualquier mandato que utilice el administrador para `presnapshotcmd`. Si especifica un espacio en blanco o una cadena nula impide que el administrador utilice un mandato en esta opción. Si el administrador utiliza un espacio en blanco o una serie nula en la opción `presnapshotcmd`, el usuario no podrá ejecutar un mandato de previo a la instantánea.

Utilice la opción `srvprepostsnapdisabled` para impedir que el administrador del servidor de IBM Spectrum Protect pueda ejecutar mandatos del sistema operativo en el sistema cliente.

Si la cadena del mandato contiene espacios en blanco, debe especificarse entre comillas:





```
"quiesce database myDb"
```

Si ya ha colocado la serie del mandato entre comillas, especifique toda la serie del mandato entre comillas simples:



```
'resume database "myDb"'
```

## Ejemplos

---





 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones:  
 Sistemas operativos AIX  Sistemas operativos Linux

```
presnapshotcmd "any shell command or script"
```



 Sistemas operativos Windows Archivo de opciones:  
 Sistemas operativos Windows

```
presnapshotcmd "<inserte aquí mandato detención aplicación>  
aplicación"
```

La serie del mandato es un mandato válido para detener la aplicación.

 Sistemas operativos AIX  Sistemas operativos Linux Línea de mandatos:  
 Sistemas operativos AIX  Sistemas operativos Linux

```
backup image -presnapshotcmd="any shell command or script"
```

 Sistemas operativos Windows Línea de mandatos:  
 Sistemas operativos Windows

```
backup image -presnapshotcmd="<inserte aquí el mandato  
de detención de la  
aplicación> aplicación"
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Queryschedperiod

---

La opción `queryschedperiod` especifica el número de horas que se desea que espere el planificador cliente entre los intentos de establecer contacto con el servidor para realizar trabajos planificados.

Esta opción sólo se aplica si el valor de `schedmode` es `polling`. Esta opción sólo se utiliza cuando se está ejecutando el planificador.

El administrador también puede definir esta opción. Si el administrador especifica un valor para esta opción, ese valor altera temporalmente el valor establecido en el archivo de opciones de cliente después de que el nodo de cliente haya establecido contacto correctamente con el servidor.





## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-QUERYSCHeDperiod-- --horas-----<<
```

## Parámetros

---

horas

Especifica el número de horas que el planificador cliente espera entre intentos de establecer contacto con el servidor para realizar trabajos planificados. El rango de valores es de 1 a 9999; el valor predeterminado es 4.

## Ejemplo

---

Archivo de opciones:  
`querysch 6`

## Querysummary


---

La opción `querysummary` proporciona estadísticas sobre los archivos, directorios y objetos que devuelven los mandatos `query backup` o `query archive`.

La opción `querysummary` proporciona las estadísticas siguientes:

- El número añadido de archivos y directorios devueltos por el mandato `query backup` o `query archive`
- El número añadido de datos de los objetos devueltos por el mandato `query backup` o `query archive`
- La estimación de uso de memoria de restauración clásica para restaurar objetos devueltos por el mandato `query backup` o `query archive`
- El número total de volúmenes de servidor únicos donde residen los objetos devueltos por el mandato `query`



 Sistemas operativos Windows Los objetos únicos que se expanden en varios volúmenes sólo incluirán un volumen en las estadísticas de número total de volúmenes. Por ejemplo, si c:\bigfile se expande en dos volúmenes, sólo uno de los volúmenes se contará en el número de volúmenes estimado.

## Cientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-QUERYSUMMARY-----<<
```





## Parámetros

---





No hay parámetros para esta opción.





## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
dsmc q ba '/usr/fs1/\*' -sub=yes -querysummary

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
[root@kaveri:/home/cpark] $ dsmc q ba '/kalafs1/*' -sub=yes -querysummary
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
Versión de cliente 8, release 1, nivel 0.0
Fecha/hora del cliente: 12/09/2016 12:05:35
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.
```

```
Node Name: KAVERI
Sesión establecida con el servidor TEMPLAR: AIX-RS/6000
Versión de servidor 8, release 1, nivel 0.0
Fecha/hora del servidor: 12/09/2016 12:05:35 Último acceso: 12/07/2016 07:48:59
```

Tamaño	Fecha copia	seg.	Clase gest.	Archivo A/I
4,096	B	08/07/08 12:07:30	BASVT2	A /kalafs1/
256	B	08/07/08 12:07:30	BASVT2	A /kalafs1/dir1
10.485.760	B	08/07/08 12:07:30	DEFAULT	A /kalafs1/info1
5.242.880	B	08/07/08 12:07:30	DEFAULT	A /kalafs1/info2
1.044	B	08/07/08 12:07:30	DEFAULT	A /kalafs1/dir1/subfile1
1.044	B	08/07/08 12:07:30	DEFAULT	A /kalafs1/dir1/subfile2

Estadísticas de resumen


Total arch.	Total dir.	Prom. tam. arch.	Total datos	Est. memoria
4	2	3,75 MB	15,00 MB	1,07 KB

Número estimado de volúmenes: 2

```
[root@kaveri:/home/cpark] $
```

 Sistemas operativos Windows

Línea de mandatos:

 Sistemas operativos Windows dsmc query backup k:\.\* -subdir=yes -QUERYSUMMARY

 Sistemas operativos Windows

```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
```

Versión de cliente 8, release 1, nivel 0.0  
 Fecha/hora del cliente: 12/09/2016 12:05:35  
 (c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.

Nombre de nodo: BARKENSTEIN  
 Sesión establecida con el servidor  
 BARKENSTEIN\_SERVER1: Windows  
 Versión de servidor 8, release 1, nivel 0.0  
 Fecha/hora del servidor: 12/09/2016 12:05:35 Último acceso: 12/08/2016 05:46:09

Tamaño		Fecha copia seg.	Clase gest.	Archivo A/I
0	B	04/02/2008 20:21:51	STANDARD	A \\barkenstein\k\$\
0	B	04/02/2008 20:21:51	STANDARD	A \\barkenstein\k\$\jack_test
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\
				Información volúmenes sistema
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Test1
0	B	04/02/2008 20:21:51	STANDARD	A \\barkenstein\k\$\TestTree
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Tree150
0	B	04/02/2008 19:49:20	STANDARD	A \\barkenstein\k\$\Tree150.1
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Tree150.2
0	B	04/02/2008 19:50:51	STANDARD	A \\barkenstein\k\$\Tree150.3
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Tree1500
0	B	04/02/2008 10:41:40	STANDARD	A \\barkenstein\k\$\Tree150_2
0	B	04/02/2008 20:02:31	STANDARD	A \\barkenstein\k\$\tree18
0	B	04/02/2008 20:15:04	STANDARD	A \\barkenstein\k\$\Tree18.test
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Tree30
0	B	04/01/2008 12:37:07	STANDARD	A \\barkenstein\k\$\Tree30.2
0	B	04/02/2008 19:52:30	STANDARD	A \\barkenstein\k\$\tree30.test
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file1
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file10
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file11
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file12
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file13
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file14
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file15
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file16
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file17
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file18
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file19
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file2
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file20
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file21
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file3
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file4
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file5
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file6
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file7
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file8
11,788	B	04/02/2008 19:55:32	DEFAULT	A \\barkenstein\k\$\file9
11,788	B	04/02/2008 13:31:06	DEFAULT	A \\barkenstein\k\$\file910
10,964	B	04/01/2008 12:37:07	DEFAULT	A \\barkenstein\k\$\filea
10,964	B	04/01/2008 12:37:07	DEFAULT	A \\barkenstein\k\$\fileb
10,964	B	04/01/2008 12:37:07	DEFAULT	A \\barkenstein\k\$\x

#### Estadísticas de resumen

Total arch.	Total dir.	Prom. tam. arch.	Total datos	Est. memoria
25	16	11,41 KB	285,37 KB	10,58 KB

Número estimado de volúmenes: 2

## Quiet

La opción quiet limita el número de mensajes que se muestran en la pantalla durante un proceso.

Por ejemplo, cuando ejecuta los mandatos incremental, selective o archive, es posible que aparezca información sobre cada uno de los archivos de los que se realiza una copia de seguridad. Utilice la opción quiet si no desea visualizar esta información.

Si utiliza la opción quiet, aparece información de error y de proceso en la pantalla, mientras que los mensajes se graban en los archivos de anotaciones. Si no especifica quiet, se utiliza la opción predeterminada, verbose.





## Cientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir la opción quiet y hacer que prevalezca sobre el valor del cliente. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Línea de mandatos, en el recuadro de selección No mostrar información de proceso en pantalla del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Línea de mandatos, en el recuadro de selección No mostrar información de proceso en pantalla del Editor de preferencias.

## Sintaxis

---

```
>>-QUIET-----<<
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Archivo de opciones:

```
quiet
```

Línea de mandatos:

```
-quiet
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Quotesareliteral

---

La opción quotesareliteral especifica si las comillas simples (') o las comillas dobles (") se interpretan literalmente cuando se incluyen en la especificación de una lista de archivos en una opción filelist.

Normalmente, el cliente requiere que se utilicen comillas simples o dobles para delimitar especificaciones de archivos que contienen caracteres de espacios. Algunos sistemas de archivos permiten el uso de comillas simples y dobles en los nombres de archivos y directorios.

Para impedir errores que de lo contrario se podrían producir, cuando se incluyen especificaciones de archivos en una opción filelist y contienen comillas simples (') o comillas dobles ("), establezca quotesareliteral yes. Cuando quotesareliteral se establece en yes, las comillas que se incluyen en una especificación de lista de archivos en una opción filelist se interpretan literalmente, como comillas, y no como delimitadores.

Esta opción se aplica a cualquier mandato que acepta una opción filelist como un parámetro de mandato.

## Cientes soportados

---

Esta opción es válida para todas las plataformas soportadas. La opción se aplica a cualquier mandato que toma una especificación de lista de archivos como parámetro.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones de usuario del cliente (dsm.opt).

## Sintaxis

---

```
.-no-----.  
>>-QUOTEareliteral--+-+-----+-----<<  
                  '-yes-'
```

## Parámetros

no

Especifica que las comillas simples (') y dobles (") se interpretan como delimitadores para las especificaciones de la lista de archivos incluidas en una opción filelist. No es el valor predeterminado.


yes


Especifica que las comillas simples (') y dobles (") se interpretan literalmente, y no como delimitadores, para especificaciones de la lista de archivos que se incluyen en una opción filelist. Especifique este valor si está realizando la copia de seguridad de archivos desde un sistema de archivos que permite las comillas en nombres de archivo o de directorio.


## Ejemplos

Archivo de opciones:


```
QUOTESARELITERAL YES
```

 Sistemas operativos Windows Línea de mandatos:





 Sistemas operativos Windows Suponiendo que el sistema de archivos permita comillas en las vías de acceso, los siguientes son ejemplos de archivos de una especificación de lista de archivos que se pueden procesar correctamente si QUOTESARELITERAL se establece en YES.





 Sistemas operativos Windows Supongamos que el mandato que se emite es `dsmc sel -`





`filelist=c:\important_files.txt`, donde `important_files.txt` contiene la lista de archivos que deben procesarse.

 Sistemas operativos Windows `important_files.txt` contiene la siguiente lista de archivos:

```
c:\home\myfiles\"file"1000
c:\home\myfiles\'file'
c:\home\myfiles\file'ABC
c:\home\myfiles\ABC"file"
```


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Suponiendo que el sistema de archivos permita comillas en las vías de acceso, lo siguiente son ejemplos de archivos en una especificación de lista de archivos que se pueden procesar correctamente si QUOTESARELITERAL se establece en YES

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Supongamos que el mandato que se emite es `dsmc sel -filelist=/home/user1/important_files`, donde `important_files.txt` contiene la lista de archivos a procesar.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
/home/user1/myfiles/"file"1000
/home/user1/myfiles/'file'
/home/user1/myfiles/file'ABC
/home/user1/myfiles/ABC"file"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Removeoperandlimit

La opción `removeoperandlimit` especifica que el cliente elimina el límite de 20 operandos.

Si especifica la opción `removeoperandlimit` con los mandatos `incremental`, `selective` o `archive`, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

La opción `removeoperandlimit` puede ser útil si genera scripts que puedan invocar el cliente de línea de mandatos con un gran número de operandos. Por ejemplo, puede examinar previamente un árbol de directorios para buscar los archivos de los que debe realizarse una copia de seguridad. A medida que se descubre cada uno de los archivos *eligibles*, el archivo se agrega a la lista de operandos de un mandato `selective`. Posteriormente, este mandato `selective` se envía mediante un script de control. En este caso, al especificar la opción `removeoperandlimit` se elimina el límite de 20 operandos.

Nota:

1. La opción `removeoperandlimit` *debe* especificarse inmediatamente después del mandato `incremental`, `selective` o `archive` antes de cualquier especificación de archivo.
2. Esta opción no acepta ningún valor. Si se especifica esta opción en un mandato, se elimina el límite de 20 operandos.
3. Dado que ello afecta negativamente al rendimiento para permitir que el shell expanda caracteres comodín, es aconsejable utilizar la opción `removeoperandlimit` en las operaciones de copia de seguridad o archivado en las que no se utilizan caracteres comodín.
4. La opción `removeoperandlimit` sólo es válida en los mandatos `incremental`, `selective` o `archive` en modalidad por lotes. No es válida en el archivo de opciones de cliente (`dsm.opt`) o en el archivo `dsm.sys`.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux.

## Sintaxis

---

```
>>-REMOVEOPerandlimit-----<<
```

## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---

Línea de mandatos:  
-removeoperandlimit

## Replace

---






La opción replace especifica si ha de grabarse encima de los archivos existentes en la estación de trabajo o si ha de solicitarse al usuario que realice la selección deseada al restaurar o recuperar archivos.

Importante: La opción replace no afecta a la recuperación de los objetos de directorios. Los objetos de directorios siempre se recuperan, aunque se haya especificado replace=no. Para impedir que sobrescriban los directorios existentes, utilice la opción filesonly.

Puede utilizar esta opción con los mandatos siguientes:

- restore
- restore backupset
- restore group
- retrieve

Nota: la solicitud de sustitución no se produce durante una operación planificada. Si establece la opción replace para prompt, el cliente de copia de seguridad y archivado pasará por alto los archivos sin realizar ninguna solicitud durante una operación planificada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Restaurar, en la sección Acción para archivos ya existentes del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Restaurar, en la sección Acción para archivos ya existentes del Editor de preferencias.

## Sintaxis

---









```
>>-REPlace-.-Prompt-.-----<<
+-All-----+
+-Yes-----+
'-No-----'
```


## Parámetros


---

Prompt

Para las operaciones no planificadas, especifica si ha de grabarse encima de los archivos existentes. Para operaciones planificadas, los archivos existentes no se sobrescriben y no se muestran solicitudes. Éste es el valor predeterminado.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XAll  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XSe graba sobre todos los archivos existentes, incluidos los archivos de sólo lectura. Si se deniega el acceso a un archivo, se le solicitará si desea pasarlo por alto o grabar encima. No se emprende ninguna acción sobre el archivo hasta que haya una respuesta a la solicitud.


 Sistemas operativos WindowsAll


 Sistemas operativos WindowsSe graba sobre todos los archivos existentes, incluidos los archivos de sólo lectura. Cuando vuelva a iniciarse el sistema, se sustituirán todos los archivos bloqueados. Si se deniega el acceso a un archivo, se le solicitará si desea pasarlo por alto o grabar encima. No se emprende ninguna acción sobre el archivo hasta que haya una respuesta a la solicitud.









Yes


Se graba sobre todos los archivos existentes, *excepto* los archivos de sólo lectura. Para las operaciones no planificadas, especifica si ha de grabarse encima de los archivos de sólo lectura existentes. Para operaciones planificadas, los archivos existentes de sólo lectura no se sobrescriben y no se muestran solicitudes. Si se deniega el acceso a un archivo, se pasará por alto.

 Sistemas operativos WindowsNo

 Sistemas operativos WindowsNo se graba encima de ningún archivo ya existente. No aparece ninguna solicitud.

 sistemas operativos Mac OS X**Nota:** cuando restaure o recupere archivos con la opción `replace` establecida en no, no se grabará encima de los archivos existentes, pero sí se grabará encima de los directorios existentes. Para dejar intactos los directorios existentes durante una operación de restauración o recuperación, seleccione Opciones > Todos los archivos y directorios seleccionados > Solo archivos en la GUI del cliente de copia de seguridad y archivado.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XNo  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XNo se graba encima de ningún archivo ya existente. No aparece ninguna solicitud.

 Sistemas operativos Windows**Nota:** al reiniciar el sistema, puede optar por sustituir los archivos bloqueados. El cliente no puede realizar una restauración en el sitio de los archivos activos. Sin embargo, presentará versiones restauradas de archivos activos para que sean sustituidos cuando vuelva a arrancar la máquina, salvo los archivos que contengan corrientes especificadas, archivos esparcidos y directorios. Sólo puede restaurar estos archivos si están desbloqueados.

## Ejemplos

---

Archivo de opciones:

```
replace all
```

Línea de mandatos:

```
-replace=no
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo `dsm.opt`, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

## Replserverguid

---

La opción `replserverguid` especifica el GUID (Globally Unique Identifier) que se utiliza cuando el cliente se conecta al servidor secundario durante la migración tras error. El GUID se utiliza para validar el servidor secundario para asegurarse de que es el servidor esperado.

El GUID de réplica es distinto del GUID de máquina del servidor. Se genera una vez para un servidor que está realizando la réplica y no cambia nunca.

Esta opción se debe especificar dentro de una stanza `replservername` en el archivo de opciones del cliente. La stanza `replservername` contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.





- La información del servidor secundario está caducada o es incorrecta.


Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

## Clientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción se coloca en el archivo `dsm.sys` dentro de la stanza `replservername`.

 Sistemas operativos Windows Esta opción se coloca en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

```
>>-replserverguid----serverguid-----<<
```

## Parámetros

`serverguid`

Especifica el GUID del servidor secundario que se utiliza durante una migración tras error.





## Ejemplos





Archivo de opciones:

```
REPLSERVERGUID 91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.02
```

Línea de mandatos:

No se aplica.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción `replservername` y el nombre del servidor secundario. La stanza `servername` debe contener la opción `myreplicationserver`, que apunta al servidor secundario que se especifica mediante la stanza `replservername`. Sólo se puede especificar un servidor secundario por stanza `servername`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SERvername          server_a
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDACCESS      prompt
MYREPLICATIONSERVER TargetReplicationServer1
```

```
SERvername          server_b
COMMethod           TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname2.example.com
PASSWORDACCESS      generate
INCLExcl            /adm/tsm/archive.excl
MYREPLICATIONSERVER TargetReplicationServer2
```


```
SERvername          server_c
COMMethod           TCPip
```

```

TCPport                1500
TCPserveraddress       server_hostname3.example.com
PASSWORDaccess         generate
MYREPLICATIONserver    TargetReplicationServer1

```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo dsm.opt, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza REPLSERVERNAME. La opción MYREPLICATIONServer apunta al nombre de servidor secundario especificado por la stanza REPLSERVERName.

```

REPLSERVERNAME        TargetReplicationServer1
REPLTCPSEVERADDRESS   TargetReplicationServer1
REPLTCPPOINT          1505
REPLSSLPPOINT         1506
REPLSERVERGUID        91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00

COMMethod             TCPip
TCPport               1500
TCPserveraddress      server_hostname1.example.com
PASSWORDaccess        prompt
MYREPLICATIONServer   TargetReplicationServer1
MYPRIMARYSERVER       Server1

```

#### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

#### Tareas relacionadas:

Configuración del cliente de migración automática tras error

## Replservername

---

La opción replservername especifica el nombre del servidor secundario al que se conecta el cliente durante una migración tras error.

La opción replservername empieza una stanza en el archivo de opciones del cliente que contiene información de conexiones sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.





## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción se coloca en las opciones del sistema cliente dsm.sys.

 Sistemas operativos Windows Esta opción se coloca en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-replservername----repl_servername-----<<
```

## Parámetros

---

repl\_servername



Especifica el nombre del servidor secundario que se utilizará durante una migración tras error. Este valor es normalmente el nombre del servidor secundario, no el nombre de host del servidor.

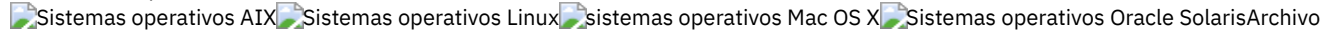
## Ejemplos

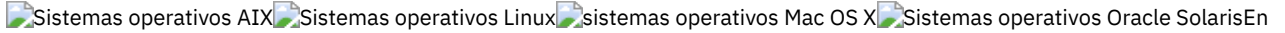
Archivo de opciones:

```
REPLSERVERName TargetReplicationServer1
```

Línea de mandatos:

No se aplica.

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo dsm.sys, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción replservername y el nombre del servidor secundario. La stanza servername debe contener la opción myreplicationserver, que apunta al servidor secundario que se especifica mediante la stanza replservername. Sólo se puede especificar un servidor secundario por stanza servername.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00


REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

SErvername          server_a
COMMMethod          TCPip
TCPPort             1500
TCPSErveraddress    server_hostname1.example.com
PASSWORDAccess     prompt
MYREPLICATIONServer TargetReplicationServer1

SErvername          server_b
COMMMethod          TCPip
TCPPort             1500
TCPSErveraddress    server_hostname2.example.com
PASSWORDAccess     generate
INCLExcl            /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2

SErvername          server_c
COMMMethod          TCPip
TCPPort             1500
TCPSErveraddress    server_hostname3.example.com
PASSWORDAccess     generate
MYREPLICATIONServer TargetReplicationServer1
```

Archivo de opciones:

En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo dsm.opt, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza REPLSERVERName. La opción MYREPLICATIONServer apunta al nombre de servidor secundario especificado por la stanza REPLSERVERName.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00

COMMMethod          TCPip
TCPPort             1500
TCPSErveraddress    server_hostname1.example.com
PASSWORDAccess     prompt
MYREPLICATIONServer TargetReplicationServer1
MYPRIMARYSERVER     Server1
```

### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

### Tareas relacionadas:

Configuración del cliente de migración automática tras error

## Replsslport

---

La opción replsslport especifica el puerto TCP/IP en el servidor secundario que está habilitado para SSL. La opción replsslport se utiliza cuando el cliente se conecta al servidor secundario durante una migración tras error. Esta opción está en desuso si se conecta a un servidor IBM Spectrum Protect V8.1.2 o posterior.

La opción replsslport se envía al cliente mediante el servidor primario sólo si el servidor secundario está configurado para SSL.

Esta opción sólo es aplicable cuando el cliente está configurado para utilizar SSL para proteger las comunicaciones entre el servidor y el cliente de IBM Spectrum Protect. Si el cliente no está configurado para utilizar SSL, se utilizará el puerto especificado por la opción repltcpport. Puede determinar si el cliente utiliza SSL verificando la opción de cliente SSL.

Esta opción se debe especificar dentro de una stanza replservername en el archivo de opciones del cliente. La stanza replservername contiene información de conexión sobre el servidor secundario.

Durante el proceso de inicio de sesión normal (no migración tras error), esta opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción se coloca en el archivo dsm.sys dentro de la stanza replservername.

 Sistemas operativos Windows Esta opción se coloca en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-replsslport----port_address-----<<
```

## Parámetros

---

port\_address

Especifica la dirección del puerto TCP/IP que está habilitada para SSL y que se utiliza para comunicarse con el servidor secundario.

## Ejemplos





---





Archivo de opciones:

```
REPLSSLPORT 1506
```

Línea de mandatos:

No se aplica.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo dsm.sys, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción replservername y el nombre del servidor secundario. La stanza servername debe

contener la opción `myreplicationserver`, que apunta al servidor secundario que se especifica mediante la stanza `replservername`. Sólo se puede especificar un servidor secundario por stanza `servername`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00


REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02

Sservername         server_a
COMMMethod          TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDACCESS     prompt
MYREPLICATIONSERVER TargetReplicationServer1

Sservername         server_b
COMMMethod          TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname2.example.com
PASSWORDACCESS     generate
INCLEXCL            /adm/tsm/archive.excl
MYREPLICATIONSERVER TargetReplicationServer2

Sservername         server_c
COMMMethod          TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname3.example.com
PASSWORDACCESS     generate
MYREPLICATIONSERVER TargetReplicationServer1
```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo `dsm.opt`, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza `REPLSERVERNAME`. La opción `MYREPLICATIONSERVER` apunta al nombre de servidor secundario especificado por la stanza `REPLSERVERNAME`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPPOINT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00

COMMMethod          TCPip
TCPPOINT            1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDACCESS     prompt
MYREPLICATIONSERVER TargetReplicationServer1
MYPRIMARYSERVER     Server1
```

#### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

#### Tareas relacionadas:

Configuración del cliente de migración automática tras error

## Repltcpport

La opción `repltcpport` especifica el puerto TCP/IP en el servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.

Esta opción se debe especificar dentro de una stanza `replservername` en el archivo de opciones del cliente. La stanza `replservername` contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:

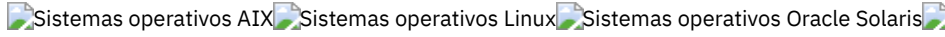
- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.


Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

## Clientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Esta opción se coloca en el archivo dsm.sys dentro de la stanza replservername.

 Esta opción se coloca en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

```
>>-repltcpport----port_address-----<<
```

## Parámetros

port\_address

Especifica la dirección del puerto TCP/IP que se utiliza para comunicarse con el servidor secundario.

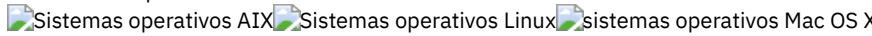
## Ejemplos

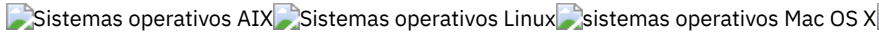
Archivo de opciones:

```
REPLTCPport 1500
```

Línea de mandatos:

No se aplica.

 Archivo de opciones:

 En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo dsm.sys, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción replservername y el nombre del servidor secundario. La stanza servername debe contener la opción myreplicationserver, que apunta al servidor secundario que se especifica mediante la stanza replservername. Sólo se puede especificar un servidor secundario por stanza servername.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPport         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```

```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPport         1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
Sservername      server_a
COMMethod        TCPip
TCPport          1500
TCPserveraddress server_hostname1.example.com
PASSWORDAccess   prompt
MYREPLICATIONServer TargetReplicationServer1
```


```
Sservername      server_b
COMMethod        TCPip
TCPport          1500
TCPserveraddress server_hostname2.example.com
PASSWORDAccess   generate
INCLExcl         /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```

Sservername      server_c
COMMethod        TCPip
TCPport          1500
TCPserveraddress server_hostname3.example.com
PASSWORDaccess   generate
MYREPLICATIONServer TargetReplicationServer1

```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo dsm.opt, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza REPLSERVERName. La opción MYREPLICATIONServer apunta al nombre de servidor secundario especificado por la stanza REPLSERVERName.

```

REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPport         1505
REPLSSLport         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00

COMMethod           TCPip
TCPport             1500
TCPserveraddress    server_hostname1.example.com
PASSWORDaccess      prompt
MYREPLICATIONServer TargetReplicationServer1
MYPRIMARYSERVER     Server1

```

#### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

#### Tareas relacionadas:

Configuración del cliente de migración automática tras error

## Repltcpserveraddress

La opción repltcpserveraddress especifica la dirección TCP/IP del servidor secundario que se utilizará cuando el cliente se conecta al servidor secundario durante una migración tras error.

Esta opción se debe especificar dentro de una stanza replservername en el archivo de opciones del cliente. La stanza replservername contiene información de conexión sobre el servidor secundario.

Esta opción se establece mediante el administrador del servidor de IBM Spectrum Protect para el nodo cliente. Durante el proceso de inicio de sesión normal (no migración tras error), la opción se envía al cliente y se guarda en el archivo de opciones del cliente.

No edite esta opción durante las operaciones normales.

Edite esta opción sólo durante situaciones como las siguientes:





- El servidor primario está fuera de línea y la información para el servidor secundario no se encuentra en el archivo de opciones.
- La información del servidor secundario está caducada o es incorrecta.

Todos los valores que edite se eliminarán o se actualizarán la próxima vez que inicie sesión en el servidor primario.

## Clientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Esta opción se coloca en el archivo dsm.sys dentro de la stanza replservername.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

```
>>-REPLTCPSEVERADDRESS----server_address-----<<
```

## Parámetros

### server\_address

Especifica una dirección TCP/IP para un servidor que tiene entre 1 y 64 caracteres de longitud. Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción `commmethod V6TcPip`.

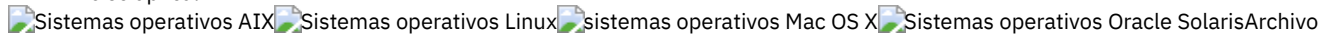
## Ejemplos

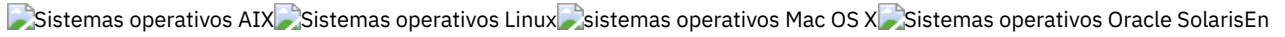
### Archivo de opciones:

```
REPLTCPSEVERADDRESS dsmchost.example.com
```

### Línea de mandatos:

No se aplica.

 Sistemas operativos AIX, Sistemas operativos Linux, sistemas operativos Mac OS X, Sistemas operativos Oracle Solaris Archivo de opciones:

 Sistemas operativos AIX, Sistemas operativos Linux, sistemas operativos Mac OS X, Sistemas operativos Oracle Solaris En el ejemplo siguiente se muestra cómo especificar opciones para tres servidores distintos en el archivo `dsm.sys`, y cómo hacer referencia al servidor secundario. La información de conexión para varios servidor secundario se presenta en stanzas. Cada stanza se identifica mediante la opción `replservername` y el nombre del servidor secundario. La stanza `servername` debe contener la opción `myreplicationserver`, que apunta al servidor secundario que se especifica mediante la stanza `replservername`. Sólo se puede especificar un servidor secundario por stanza `servername`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00
```


```
REPLSERVERNAME      TargetReplicationServer2
REPLTCPSEVERADDRESS TargetReplicationServer2
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.02
```

```
SERvername          server_a
COMMMethod           TCPip
TCPSPort             1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDAccess      prompt
MYREPLICATIONServer TargetReplicationServer1
```

```
SERvername          server_b
COMMMethod           TCPip
TCPSPort             1500
TCPSEVERADDRESS     server_hostname2.example.com
PASSWORDAccess      generate
INCLExcl            /adm/tsm/archive.excl
MYREPLICATIONServer TargetReplicationServer2
```

```
SERvername          server_c
COMMMethod           TCPip
TCPSPort             1500
TCPSEVERADDRESS     server_hostname3.example.com
PASSWORDAccess      generate
MYREPLICATIONServer TargetReplicationServer1
```

 Sistemas operativos Windows Archivo de opciones:

 Sistemas operativos Windows En el ejemplo siguiente se muestra cómo especificar opciones para el servidor secundario en el archivo `dsm.opt`, y cómo hacer referencia al servidor secundario. La información de conexión para el servidor secundario se ubica en la stanza `REPLSERVERName`. La opción `MYREPLICATIONServer` apunta al nombre de servidor secundario especificado por la stanza `REPLSERVERName`.

```
REPLSERVERNAME      TargetReplicationServer1
REPLTCPSEVERADDRESS TargetReplicationServer1
REPLTCPSPORT        1505
REPLSSLPORT         1506
REPLSERVERGUID      91.0f.ef.90.5c.cc.11.e1.ae.34.08.00.00.00.00.00
```

```
COMMMethod           TCPip
TCPSPort             1500
TCPSEVERADDRESS     server_hostname1.example.com
PASSWORDAccess      prompt
```

**Conceptos relacionados:**

Configuración y uso de la migración tras error automática del cliente

**Tareas relacionadas:**

Configuración del cliente de migración automática tras error

 Sistemas operativos Windows

## Resetarchiveattribute

---

Utilice la opción `resetarchiveattribute` para especificar si el cliente de copia de seguridad y archivado restablecerá el atributo de archivado de Windows en los archivos de los que se realiza correctamente una copia de seguridad en el servidor de IBM Spectrum Protect.

El cliente también restablecerá el atributo de archivado durante las copias de seguridad incrementales si se determina que ya existe un objeto activo en el servidor. La opción `resetarchiveattribute` resulta útil en combinación con aplicaciones como IBM Spectrum Control, pues ofrece una forma sencilla de informar acerca del estado de la copia de seguridad de los archivos.

El atributo de archivado de Windows se utiliza para indicar que un archivo ha cambiado desde la última copia de seguridad. Después de que el cliente ha restablecido el atributo de archivado, el sistema operativo Windows volverá a establecer el atributo en ON para activarlo después de que se haya modificado el archivo. El cliente no utiliza el atributo de archivado de Windows para determinar si un archivo es candidato para la copia de seguridad incremental, sino que sólo manipula este atributo para llevar a cabo la generación de informes. El cliente utiliza un método mucho más sofisticado para determinar si es elegible para la copia de seguridad incremental.

Existen varias aplicaciones que manipulan o examinan el atributo de archivado de Windows. Tenga en cuenta todas las implicaciones relacionadas con la utilización de la opción `resetarchiveattribute` junto con estos productos.

Si establece la opción `resetarchiveattribute` en yes, después de que se haya realizado la copia de seguridad de un archivo correctamente en el servidor de IBM Spectrum Protect, el cliente restablecerá el atributo de archivado de Windows en el sistema de archivos local:

- El atributo de archivado de Windows se restablecerá durante las copias de seguridad incrementales y selectivas después de que el archivo se haya validado correctamente en el servidor de base de datos de IBM Spectrum Protect. Este atributo no se restablece para las operaciones de archivado o de imagen.
- El atributo de archivado de Windows no se restablece cuando se procesan objetos del sistema u objetos de estado del sistema.
- El atributo de archivado de Windows no se restablece para las entradas de directorio.

Además, para que el sistema de archivos local refleje el inventario actual de objetos activos en el servidor de IBM Spectrum Protect, la opción `resetarchiveattribute` indicará al cliente que restablezca el atributo de archivado de Windows en el sistema de archivos local si durante la copia de seguridad incremental se determina que ya existe una copia de seguridad válida y activa del archivo en el servidor. Este comportamiento no se dará en los casos siguientes:

- Las operaciones de copia de seguridad incremental que no examinan los atributos de cliente almacenados en el servidor, como la copia de seguridad basada en el registro por diario o el proceso incremental por fecha.
- Los archivos que no se examinan durante una operación de copia de seguridad incremental, porque se excluyen del proceso de copia de seguridad.

El cliente no garantiza la exactitud del valor actual del atributo de archivado de Windows. Por ejemplo, si la opción `resetarchiveattribute` se establece en yes y un archivo que ha examinado el producto de generación de informes indica que el atributo de archivado de Windows está desactivado (OFF) para un archivo en particular, esto no significará necesariamente que existe una copia de seguridad activa válida del archivo en el servidor de IBM Spectrum Protect. Los factores que pueden contribuir a este tipo de situaciones incluyen los siguientes:

- Un producto de proveedor de software independiente manipula el atributo de archivado de Windows.
- Se ha suprimido un espacio de archivos del servidor.
- Se ha perdido o destruido una cinta de copia de seguridad.

No debería producirse una reducción significativa del rendimiento al utilizar la opción `resetarchiveattribute`. La opción `resetarchiveattribute` no afecta al proceso de restauración.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción.

## Archivo de opciones

---

Esta opción es válida en el archivo de opciones del cliente (dsm.opt) o en el conjunto de opciones del servidor. Puede establecer esta opción en la ficha Copia de seguridad del editor de preferencias.

## Sintaxis

---

```
>>-RESETARCHIVEATTRIBUTE = .-No--.-----<<
                          '-Yes-'
```

## Parámetros

---

Yes

Especifica que desea restablecer el atributo de archivado de Windows para archivos durante una operación de copia de seguridad.

No

Especifica que no desea restablecer el atributo de archivado de Windows para los archivos durante una operación de copia de seguridad. Éste es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
resetarchiveattribute yes
```

## Resourceutilization

---

Utilice la opción resourceutilization con el archivo de opciones para regular el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso.





## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo dsm.sys dentro de una stanza de servidor. Puede establecer esta opción en el separador General, en el campo Uso de recursos del editor de preferencias.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador General, en el campo Uso de recursos del editor de preferencias.

## Sintaxis

---

```
>>-RESOURceutilization-- --number-------<<
```

## Parámetros

---

number

Especifica el nivel de recursos que el servidor y el cliente de IBM Spectrum Protect pueden utilizar durante el proceso. El rango de valores que puede especificar es 1 - 100. El valor predeterminado es 2.

## Ejemplos

---

Archivo de opciones:

```
resourceutilization 7
```

Línea de mandatos:

```
-resourceutilization=7
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.



- Regulación de las sesiones de copia de seguridad/archivado  
Si solicita una operación de copia de seguridad o archivado, el cliente puede utilizar más de una sesión del servidor.
- Regulación de las sesiones de restauración  
Si solicita una restauración, el valor predeterminado consiste en utilizar un máximo de una sesión.
- Consideraciones relacionadas con la utilización de varias sesiones de cliente  
En este tema se indican diversos aspectos que deben tenerse en cuenta al trabajar con varias sesiones de cliente.

## Regulación de las sesiones de copia de seguridad/archivado

---

Si solicita una operación de copia de seguridad o archivado, el cliente puede utilizar más de una sesión del servidor.

El valor predeterminado es utilizar dos sesiones como máximo; una para consultar al servidor y la otra para enviar datos de archivo. El cliente sólo puede utilizar una sesión de servidor si establece la opción `resourceutilization` en 1.

Un cliente puede utilizar más del número predeterminado de sesiones cuando se conecta al servidor de IBM Spectrum Protect. Por ejemplo, `resourceutilization 10` permite hasta ocho sesiones con el servidor. Pueden utilizarse varias sesiones para consultar al servidor y enviar datos de archivo.

Se utilizan varias sesiones de consulta cuando se utilizan distintas especificaciones de archivo en un mandato de copia de seguridad o de archivado. Por ejemplo, si especifica los siguientes mandatos y especifica `resourceutilization 5`, puede que el cliente inicie una segunda sesión para consultar los archivos en el espacio de archivos B.

```
inc /Volumes/filespaceA /Volumes/filespaceB
```

Si se inicia la segunda sesión depende del tiempo que se tarda en consultar al servidor sobre los archivos de los que se realiza copia de seguridad en el espacio de archivos A. Puede que el cliente también intente leer datos del sistema de archivos y enviarlos al servidor en varias sesiones.

Nota: Durante una operación de copia de seguridad, si especifica varias especificaciones de archivo, el resultado podría ser que archivos de una especificación de archivo se almacenen en varias cintas y que se entremezclen con archivos de distintas especificaciones de archivo. Esto puede afectar negativamente al rendimiento de la restauración. El establecimiento de la opción `collocatebyfilespec` en `yes` eliminará la entremezcla de archivos de distintas especificaciones de archivo, limitando al cliente a una única sesión de servidor por especificación de archivo. Por consiguiente, si almacena los datos en una cinta, los archivos para cada especificación de archivo se almacenan conjuntamente en una cinta (a menos que se necesite otra para mayor capacidad).

## Regulación de las sesiones de restauración

---

Si solicita una restauración, el valor predeterminado consiste en utilizar un máximo de una sesión.

Las sesiones de restauración adicionales se basan en:

- el valor `resourceutilization`
- cuántas cintas en las que están almacenados los datos solicitados
- cuántas unidades de disco están disponibles
- el número máximo de puntos de montaje permitidos para el nodo

Nota:

1. Si todos los archivos están en el disco, sólo se utiliza una sesión. No se pueden utilizar varias sesiones para una restauración de agrupación de almacenamiento en disco. Sin embargo, si está realizando una restauración en la que los archivos estén en 4 cintas y otros estén en disco, puede utilizar hasta 5 sesiones durante la restauración.
2. El servidor de IBM Spectrum Protect puede establecer el número máximo de puntos de montaje que un nodo puede utilizar en el servidor con el parámetro `MAXNUMMP`. Si el valor de la opción `resourceutilization` excede el valor de `MAXNUMMP` del servidor para un nodo, la copia de seguridad podría fallar y se generaría un mensaje `Error del sistema desconocido`.
3. Puede conseguir una restauración multisesión desde un único mandato `restore`, y desde un único volumen en el servidor, si ese volumen es una clase de dispositivo `FILE`.

Por ejemplo, si los datos que desea restaurar se encuentran en 5 volúmenes de cintas diferentes, el número máximo de puntos de montaje será 5 para el nodo, y si `resourceutilization` se establece en 3, se utilizarán 3 sesiones para la restauración. Si aumenta el valor de `resourceutilization` a 5, se utilizarán 5 sesiones para la restauración. Existe una relación unívoca entre el número de sesiones de restauración que están permitidas y el valor `resourceutilization`. Sólo se permiten varias sesiones de restauración para operaciones de restauración sin consulta.

# Consideraciones relacionadas con la utilización de varias sesiones de cliente

---

En este tema se indican diversos aspectos que deben tenerse en cuenta al trabajar con varias sesiones de cliente.

Los factores siguientes pueden afectar al rendimiento de varias sesiones:

- La capacidad del servidor de gestionar varias sesiones de cliente. ¿Existe suficiente memoria, varios volúmenes de almacenamiento y potencia de procesador para aumentar el rendimiento de la copia de seguridad?
- La capacidad del cliente para dirigir varias sesiones (suficiente procesador, memoria, etc.).
- La configuración del subsistema de almacenamiento del cliente. Los sistemas de archivos que ocupan varios discos, ya sea mediante la subdivisión en bandas por software o mediante RAID-5, pueden gestionar mejor un aumento en las solicitudes de lectura aleatorias que un sistema de archivos que se encuentra en una única unidad. Además, es posible que el rendimiento no mejore en un sistema de archivos de unidad única si intenta gestionar varias solicitudes de lectura aleatorias concurrentes.
- Suficiente ancho de banda en la red para dar soporte a un aumento de tráfico.

Entre los aspectos negativos que pueden darse al ejecutar varias sesiones destacan los siguientes:

- El cliente puede generar varios registros de contabilidad.
- El servidor puede no iniciar suficientes sesiones simultáneas. Para evitarlo, el parámetro *maxsessions* del servidor debe revisarse y posiblemente modificarse.
- Un mandato de consulta de nodo puede no resumir la actividad del cliente.
- Es posible que se restauren archivos en lugar de enlaces fijos.

La restauración de archivos en lugar de enlaces puede producirse cuando los siguientes criterios son verdaderos:


- Restaura todo un sistema de archivos
- Durante la operación de restauración, el valor de la opción *resourceutilization* es mayor que 1.
- El sistema de archivos contenía enlaces fijos cuando se realizaba la copia de seguridad del sistema de archivos.





La probabilidad de restaurar archivos enlazados en lugar de enlaces fijos aumentará cuanto mayor sea el número de sesiones. Al restaurar un sistema de archivos que contenía enlaces fijos cuando se realizaba la copia de seguridad del sistema de archivos, establezca *resourceutilization=1* para garantizar que se restauren los enlaces fijos.

## Retryperiod

---

La opción *retryperiod* especifica el número de minutos que debe esperar el planificador cliente entre intentos de procesar un mandato planificado que da error, o entre intentos infructuosos de informar al servidor de los resultados. Utilice esta opción sólo si el planificador se encuentra en ejecución.

 Sistemas operativos Windows El administrador también puede definir esta opción. Si el administrador especifica un valor para esta opción, ese valor modificará temporalmente el valor del archivo de opciones del cliente después de que el nodo cliente haya establecido contacto correctamente con el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X El administrador también puede definir esta opción. Si el administrador especifica un valor para esta opción, ese valor modificará temporalmente el valor del archivo de opciones del cliente opciones del sistema cliente después de que el nodo cliente haya establecido contacto correctamente con el servidor.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (*dsm.sys*) en una stanza de servidor. Puede establecer esta opción en el separador Planificador, en el campo Período entre reintentos del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (*dsm.opt*). Puede establecer esta opción en el separador Planificador, en el campo Período entre reintentos del editor de preferencias.

## Sintaxis

---

```
>>-RETRYPeriod-- --minutos-----<<
```



La opción runasservice obliga a que siga el proceso de mandatos del cliente, aunque la cuenta que inició el cliente se desconecte.

Utilice esta opción con el mandato AT y el mandato dsmc sched cuando planifique trabajos de proceso por lotes de mandatos de cliente. La opción runasservice *no* es válida en ningún archivo de opciones (dsm.opt o tsmasr.opt).

Importante: Utilice el servidor del planificador cuando ejecute los servicios de IBM Spectrum Protect en modalidad desatendida. Establezca runasservice=yes solo para planificar los mandatos del cliente mediante el mandato Windows AT. El establecimiento de runasservice=yes podría interferir con otros usos interactivos del cliente de copia de seguridad y archivado.

## Cientes soportados

---

Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
                .-No-- .  
>>-RUNASSERvice--+-----+-----><  
                '-Yes-'
```

## Parámetros

---

No

No obliga a que siga el proceso de mandatos del cliente, aunque la cuenta que inició el cliente se desconecte. Éste es el valor predeterminado.

Yes

Fuerza que el proceso de mandatos del cliente continúe ejecutándose, aunque la cuenta que ha iniciado el cliente cierre la sesión.

### Restricciones:

1. Cuando runasservice=yes, el ajuste para REPLACE siempre sustituye al comportamiento de replace=no.
2. La opción de runasservice=yes no se puede utilizar con passwordaccess=prompt.
3. Las operaciones de copia de seguridad, archivado, restauración y recuperación realizadas con runasservice=yes que encuentran solicitudes siempre fallan. Para evitar este problema, guarde la contraseña de cifrado con encryptkey=save, o desactive la opción runasservice.

## Ejemplos

---

Línea de mandatos:  
-runasservice=yes

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Schedcmddisabled

---

La opción schedcmddisabled especifica si ha de desactivarse la planificación de los mandatos mediante la opción action=command del servidor en el mandato de servidor define schedule.

Esta opción no desactiva los mandatos preschedulecmd y postschedulecmd. No obstante, puede especificar preschedulecmd o postschedulecmd con un espacio en blanco o una serie nula para desactivar la planificación de estos mandatos.

Puede desactivar la planificación de los mandatos que ha definido el administrador de IBM Spectrum Protect estableciendo la opción schedcmddisabled en yes.

Utilice el mandato query schedule para consultar las planificaciones definidas por el administrador.

## Cientes soportados





---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo dsm.sys en una stanza de servidor.

## Sintaxis

---

```
>>-SCHEDCMDDisabled--+-No-- .  
                        +-----+-----><  
                        '-Yes-'
```

## Parámetros

---

Yes

Especifica que el servidor inhabilita la planificación de los mandatos mediante la utilización de la opción `action=command` en el mandato de servidor `DEFINE SCHEDULE`.

No

Especifica que el servidor no inhabilita la planificación de los mandatos mediante la utilización de la opción `action=command` en el mandato de servidor `DEFINE SCHEDULE`. Éste es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
    schedcmddisabled no
```

Línea de mandatos:

No se aplica.

## Schedcmexception

---

La opción `schedcmexception` se utiliza conjuntamente con la opción `schedcmddisabled` para desactivar la planificación de mandatos mediante la opción `action=command` del servidor en el mandato del servidor `DEFINE SCHEDULE`, excepto para series de mandatos específicas.

Debe especificar la serie exacta que coincide con la definición de "objects" en la planificación para que el mandato del servidor planificado se acepte. Si la serie no coincide exactamente (por ejemplo, contiene un espacio adicional o el uso de las mayúsculas es diferente), la acción del mandato planificado se bloqueará.

Puede proporcionar varias opciones `schedcmexception` en el archivo de opciones. Esta opción no se cumple si `schedcmddisabled` no está habilitado. El establecimiento de esta opción en el archivo de opciones es independiente del establecimiento de la opción `schedcmddisabled`.

## Clientes soportados





---

Esta opción es válida para todos los clientes. Esta opción no es válida en el conjunto de opciones del cliente del servidor de IBM Spectrum Protect.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor.

## Sintaxis

---

```
>>-SCHEDCMDEXception--serie-----><
```

## Parámetros

---

serie

Para mandatos planificados por la opción `action=command` en el mandato de servidor `DEFINE SCHEDULE`, este parámetro indica que se active el patrón de objetos si se especifica la opción `schedcmddisabled=yes`. Este parámetro es sensible a mayúsculas y minúsculas y debe coincidir con la serie del mandato en la definición de planificación del servidor de IBM Spectrum Protect.

## Ejemplo

---

Archivo de opciones:

```
schedcmddisabled yes
Sistemas operativos Windows schedcmdexception "start dir c: /s"
schedcmdexception "start echo hello, world!"
```

## Schedgroup

---

La opción schedgroup asigna una planificación a un grupo.

Un ejemplo de la utilización de esta opción es agrupar varias planificaciones de copia de seguridad local diaria con una única planificación de copia de seguridad de servidor.

## Clientes soportados

---

Esta opción es válida para todos los clientes como opción de línea de mandatos para el mandato DEFINE SCHEDULE del servidor. Esta opción no se puede añadir a un conjunto de opciones de cliente que se encuentre en el servidor de IBM Spectrum Protect.

## Sintaxis

---

```
>>-SCHEDGROUP-- --nombre_grupo_planificación-----><
```

## Parámetros

---

nombre\_grupo\_planificación

Especifica el nombre del grupo de planificación. Puede especificar hasta 30 caracteres para el nombre.

Para obtener una lista de los caracteres válidos que puede utilizar en el nombre del grupo de planificación, consulte Denominación de objetos de IBM Spectrum Protect

## Ejemplos

---

Los siguientes mandatos de ejemplo agrupan las planificaciones SCHED\_A\_1, SCHED\_A\_2, SCHED\_A\_3, y SCHED\_A\_4 en el grupo de planificación GROUP\_A.

Línea de mandatos:

Este ejemplo muestra una copia de seguridad local a las 6 AM:

```
define schedule standard SCHED_A_1 Type=Client ACTION=Backup SUBACTION=VM OPTIONS='-
vmfulltype=vstor -vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -
asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=06:00:00
SCHEDStyle=Enhanced DAYofweek=ANY
```

Este ejemplo muestra una copia de seguridad local a las 12 PM:

```
define schedule standard SCHED_A_2 Type=Client ACTION=Backup SUBACTION=VM OPTIONS='-
vmfulltype=vstor -vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -
asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=12:00:00
SCHEDStyle=Enhanced DAYofweek=ANY
```

Este ejemplo muestra una copia de seguridad local a las 6 PM:

```
define schedule standard SCHED_A_3 Type=Client ACTION=Backup SUBACTION=VM OPTIONS='-
vmfulltype=vstor -vmbackuptype=fullvm -vmbackuplocation=local -domain.vmfull="SCHEDULE-TAG" -
asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=18:00:00
SCHEDStyle=Enhanced DAYofweek=ANY
```

Este ejemplo muestra una copia de seguridad de servidor y local a medianoche:

```
define schedule standard SCHED_A_4 Type=Client ACTION=Backup SUBACTION=VM OPTIONS='-
vmfulltype=vstor -vmbackuptype=fullvm -vmbackuplocation=both -domain.vmfull="SCHEDULE-TAG" -
asnodename=DC_SARTRE_WB -SCHEDGROUP=GROUP_A' STARTDate=02/06/2017 STARTTime=00:00:00
SCHEDStyle=Enhanced DAYofweek=ANY
```

Consejo: Asegúrese de que cada planificación del grupo pueda completarse antes de establecer el inicio de la siguiente planificación.

Esta opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Schedlogmax

---

La opción schedlogmax especifica el tamaño máximo del registro de planificación (dsmsched.log) y de registro del cliente web (dsmwebcl.log), en megabytes.

Esta opción hace que los archivos de registro creados para sucesos del planificador (dsmsched.log) y los sucesos de cliente web (dsmwebcl.log) se ajusten cuando alcanzan su tamaño máximo. A medida que se registran los sucesos del cliente del planificador y el cliente web, los registros se añaden al final de los archivos de registro hasta que se alcanza el tamaño máximo especificado. Cuando se alcanza el tamaño máximo especificado, se coloca como último registro del archivo un registro de anotaciones que indica `Continued at beginning of file`. Las anotaciones subsiguientes se reanudan al comienzo del archivo. El final de las anotaciones acomodadas se indica mediante un registro que indica `END OF DATA`.

Al establecer la opción schedlogmax, los mensajes de registro del planificador y del cliente web no se guardan en ningún archivo de eliminación. Si desea borrar registros y guardar las entradas de registro eliminadas en otro archivo, consulte la opción schedlogretention.

Si cambia de ajuste de registro (opción schedlogmax) a eliminación de registro (opción schedlogretention), se guardan todas las entradas de registro existentes y el registro se depura mediante el nuevo criterio schedlogretention.

Si cambia de eliminación de registro (opción schedlogretention) a ajuste de registro (opción schedlogmax), todos los registros existentes se copian a un archivo que contiene las entradas eliminadas. Por ejemplo, los registros eliminados del archivo dsmsched.log se copian en dsmsched.pru. Los registros eliminados de dsmwebcl.log se copian a dsmweblog.pru. Los registros (dsmsched.log y dsmwebcl.log) existentes se vacían, y el registro comienza utilizando el nuevo criterio de ajuste.






Si simplemente cambia el valor de la opción schedlogmax, las anotaciones existentes se amplían o reducen para ajustarse al nuevo tamaño. Si el valor se reduce, las entradas más antiguas se suprimen para reducir el tamaño del nuevo archivo.

Si no se especifica schedlogmax ni schedlogretention, la anotación de registro cronológico de errores puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción schedlogretention, se elimina el registro mediante el valor de retención especificado. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción schedlogmax, el registro existente se trata como si fuera un registro eliminado. Es decir, el contenido del archivo dsmsched.log se copia en un archivo llamado dsmsched.pru, el contenido de dsmwebcl.log se copia en dsmwebcl.pru, y las entradas de registro nuevas se crean en dsmsched.log y en dsmwebcl.log y ambos archivos se ajustan cuando alcanzan su tamaño máximo.

Nota: Si especifica un valor distinto de cero para schedlogmax (que permite la acomodación de anotaciones), no puede utilizar la opción schedlogretention para crear registros eliminados. Los registros pueden ser eliminados o ajustados, pero no las dos cosas. Los registros creados con la opción schedlogmax contienen un registro de cabecera de registro que contiene información similar a este registro de ejemplo:

```
LOGHEADERREC 661 104857600 IBM Spectrum Protect 8.1.0.0 Fri Dec 9 06:46:53 2014
```

Tenga en cuenta que las fechas y las indicaciones de la hora del texto LOGHEADERREC no se convierten o formatean utilizando los valores especificados en las opciones dateformat o timeformat.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows





## Clientes soportados

---






Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows También puede establecer esta opción en la ficha Preferencias de cliente > Planificador en la GUI, seleccionando Habilitar ajuste de archivo registro de planificador y especificando un valor distinto de cero para el tamaño máximo para el archivo de anotaciones cronológicas. Para impedir el ajuste del archivo de anotaciones, establezca el valor de tamaño máximo a cero.

Cuando el ajuste máximo se establece en cero, borrar o establecer la opción Habilitar ajuste de archivo de registro de planificador no tiene ningún efecto; el ajuste de anotaciones no se produce si el tamaño máximo se establece en cero.

## Sintaxis

---

```
>>-SCHEDLOGMAX-- --size-----<<
```

## Parámetros

---

size

Especifica el tamaño máximo, en megabytes, del archivo de anotaciones. El rango de valores es de 0 a 2047; el valor predeterminado es 0, que desactiva la acomodación del archivo de anotaciones y deja que el archivo crezca indefinidamente.

## Ejemplos

---

Archivo de opciones:  
    schedlogmax 100  
Línea de mandatos:  
    -schedlogmax=100

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Schedlogname

---

La opción schedlogname especifica la vía de acceso y el nombre del archivo donde desea que se almacene la información de las anotaciones de planificación.

Utilice esta opción sólo cuando desee almacenar información de las anotaciones de planificación. Esta opción sólo se aplica cuando se ejecuta el planificador.

Si no se utiliza esta opción, el archivo `dsmsched.log` se crea en el mismo directorio que el archivo `dsmerror.log`.

Si ejecuta el mandato `schedule`, la salida de los mandatos planificados aparecerá en la pantalla. También se envía la información de salida al archivo especificado con esta opción. Si no existe ninguna parte de la vía de acceso que especifica, el cliente intenta crearla.





## Clientes soportados


---





Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.


## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador Planificador, en el recuadro de texto Anotaciones de planificación del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Planificador, en el recuadro de texto Anotaciones de planificación del Editor de preferencias.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Nota: Establezca la variable de entorno `DSM_LOG` en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente. El directorio raíz no es un valor válido para `DSM_LOG`.

 Sistemas operativos Windows

Nota: Establezca la variable de entorno `DSM_LOG` en el nombre de un directorio en el que se deben colocar las anotaciones. El directorio especificado debe tener permisos que permitan el acceso de grabación desde la cuenta en la que se está ejecutando el cliente.

## Sintaxis

---

```
>>-SCHEDLOGName-- --filespec-----<<
```


## Parámetros





---




## filespec

Especifica la vía de acceso y el nombre de archivo en el que desea restaurar la información de anotaciones de planificación cuando se procesa el trabajo planificado. Si no existe ninguna parte de la vía de acceso que especifica, el cliente intenta crearla.

 Sistemas operativos Windows Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio actual. El valor predeterminado es el directorio de trabajo actual que tiene el nombre de archivo `dsmsched.log`.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si se especifica únicamente un nombre de archivo, el archivo se almacena en el directorio actual. El valor predeterminado es el directorio de trabajo actual que tiene el nombre de archivo `dsmsched.log`. El archivo `dsmsched.log` *no puede* ser un vínculo simbólico.

 sistemas operativos Mac OS X En Mac OS X, si sólo especifica un nombre de archivo, el archivo se almacenará en la carpeta predeterminada. Los directorios predeterminados son:





```
~/Library/Logs/tivoli/tsm  
/Library/Logs/tivoli/tsm
```

## Ejemplos

Archivo de opciones:

 sistemas operativos Mac OS X


```
SCHEDLOGN /Users/user1/Library/Logs/schedlog.jan
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X





```
schedlogname /home/mydir/schedlog.jan
```





 Sistemas operativos Windows

```
schedlogname c:\mydir\schedlog.jan
```


 sistemas operativos Mac OS X Línea de mandatos:

 sistemas operativos Mac OS X `-schedlogname=/Users/user1/Library/Logs/schedlog.jan`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `-schedlogname=/home/mydir/schedlog.jan`

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `-schedlogn=c:\mydir\schedlog.jan`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Schedlogretention

La opción `schedlogretention` especifica el número de días que se mantienen las entradas en el registro de planificación (`dsmsched.log`) y el registro del cliente web (`dsmwebcl.log`), y si deben guardarse las entradas eliminadas en otro archivo.

El registro de planificación (`dsmsched.log`) se elimina cuando se inicia el planificador y después de que finalice un suceso planificado. Las entradas eliminadas se graban en un archivo llamado `dsmsched.pru`.

El registro de cliente web (`dsmwebcl.log`) se elimina durante el primer inicio de `acceptor daemon` de cliente. Las entradas eliminadas se graban en un archivo llamado `dsmwebcl.pru`.






Si cambia de eliminación (opción `schedlogretention`) por el ajuste de registro (opción `schedlogmax`), todos los registros del registro existente se copian en el registro eliminado (`dsmsched.pru` and `dsmwebcl.pru`), y los registros existentes (`dsmsched.log` y `dsmwebcl.log`) se vacían, y el registro comienza utilizando el nuevo criterio de ajuste.

Si cambia de ajuste de registro (opción `schedlogmax`) a eliminación de registro (opción `schedlogretention`), se guardan todas las entradas de registro existentes y el registro se depura mediante el nuevo criterio `schedlogretention`. Las entradas eliminadas se guardan en sus archivos `*.pru` correspondientes.

Si no se especifica `schedlogmax` ni `schedlogretention`, los registros puede crecer sin límite de tamaño. Debe gestionar el contenido de los registros manualmente para evitar que el registro agote los recursos del disco. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogretention`, se elimina el registro mediante el valor de retención especificado. Cuando se ha creado el registro sin ninguna opción especificada, si posteriormente emite un mandato y especifica la opción `schedlogmax`, el registro existente se trata como si fuera un registro eliminado. Es decir, el contenido del archivo

dsm Sched.log se copia en un archivo llamado dsm Sched.pru, el contenido de dsm webcl.log se copia en dsm webcl.pru, y las entradas de registro nuevas se crean en dsm Sched.log y en dsm webcl.log, y ambos archivos se ajustan cuando alcanzan su tamaño máximo.

Nota: Si especifica la opción schedlogretention para crear registros eliminados, no podrá especificar la opción schedlogmax. Los registros pueden ser eliminados o ajustados, pero no las dos cosas.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows





## Cientes soportados

---






Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows También puede establecer esta opción en la ficha Preferencias de cliente > Planificador en la GUI seleccionando Eliminar entradas antiguas y especificando un valor para Eliminar entradas más antiguas que. Al seleccionar la opción Guardar entradas eliminadas se guardan las entradas de registro de planificador eliminadas en el archivo de registro dsm Sched.pru. Al seleccionar Guardar entradas eliminadas también se guardan las entradas de cliente web en el archivo de registro dsm webcl.pru.

## Sintaxis

---

```
>>-SCHEDLOGRetention--+-N----.  .-D-.  
                        '-días-'  '-S-'
```

## Parámetros

---

N o days

Especifica cuánto tiempo se debe esperar antes de eliminar las anotaciones.

N

No se eliminarán las anotaciones. Esto hace que las anotaciones crezcan indefinidamente. Éste es el valor predeterminado.

days

Especifica el número de días que se conservarán las entradas del archivo de anotaciones antes de eliminarlas. El rango de valores oscila entre 0 y 9999.

D o S

Especifica si se deben guardar las entradas eliminadas. Utilice un espacio o una coma para separar este parámetro del anterior.

D

Elimina las entradas de las anotaciones al eliminarlas. Éste es el valor predeterminado.

S

Guarda las entradas de anotaciones al eliminarlas.

Las entradas eliminadas se copian en el archivo de las entradas eliminadas (dsm Sched.pru o dsm Sched.pru), que se encuentra almacenado en el mismo directorio que las anotaciones.

## Ejemplos

---

Archivo de opciones:

```
schedlogretention 30 S
```

Línea de mandatos:

```
-schedlogretention=30,S
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.


## Schedmode





---


La opción `schedmode` especifica si se desea utilizar la modalidad de sondeo de cliente (el nodo cliente periódicamente consulta al servidor sobre los trabajos planificados), o bien la modalidad de solicitud de servidor (el servidor contacta con el nodo cliente en el momento de iniciar una operación planificada).





Todos los métodos de comunicación pueden utilizar la modalidad de sondeo de cliente, pero sólo TCP/IP puede utilizar la modalidad de solicitud de servidor.

Esta opción sólo se aplica si utiliza el método de comunicación TCP/IP y se ejecuta el mandato `schedule`.






 **Sistemas operativos Windows** El administrador puede especificar que el servidor dé soporte a ambas modalidades o sólo a una de ellas. Si el administrador especifica que se dé soporte a ambas modalidades, podrá seleccionar la que desee. Si el administrador sólo ha especificado una única modalidad, deberá especificar esa modalidad en el archivo `dsm.opt`, o el trabajo planificado no se procesará.






 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** El administrador puede especificar que el servidor dé soporte a ambas modalidades o sólo a una de ellas. Si el administrador especifica que se dé soporte a ambas modalidades, podrá seleccionar la que desee. Si el administrador sólo ha especificado una única modalidad, deberá especificar esa modalidad en el archivo `dsm.sys`, o el trabajo planificado no se procesará.

 **Sistemas operativos Windows** Si especifica la modalidad `prompted`, debe considerar la posibilidad de proporcionar valores para las opciones `tcpclientaddress` y `tcpclientport` en el archivo `dsm.opt` o en el mandato de planificación; a continuación, podrá establecerse contacto con el cliente en la dirección o en el puerto deseados (esto es útil para los sistemas cliente que tienen varias tarjetas de interfaz de red).

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Si especifica la modalidad `prompted`, debe considerar la posibilidad de proporcionar valores para las opciones `tcpclientaddress` y `tcpclientport` en el archivo `dsm.sys` o en el mandato de planificación; a continuación, podrá establecerse contacto con el cliente en la dirección o en el puerto deseados (esto es útil para los sistemas cliente que tienen varias tarjetas de interfaz de red).

Nota:

-  **Sistemas operativos Windows** Cuando cambie el valor de esta opción en el archivo de opciones del cliente (`dsm.opt`), deberá detener y reiniciar el servicio de planificador para que el valor entre en vigor.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Cuando cambie el valor de esta opción en el archivo `dsm.sys`, deberá detener y reiniciar el servicio de planificador para que el valor entre en vigor.
- El servidor también puede definir esta opción.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X**  
 **Sistemas operativos Windows**





## Cientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X** Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador Planificador, en la sección Modalidad de planificación del Editor de preferencias.

 **Sistemas operativos Windows** Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Planificador, en la sección Modalidad de planificación del Editor de preferencias.

## Sintaxis

---





```
>>>-SCHEDMODE-+-POLling-+-----+-----<<<
                  '-PRompted-'
```



## Parámetros





---


### POLLing

El planificador cliente consulta al servidor sobre el trabajo planificado en intervalos de tiempo determinados. Éste es el valor predeterminado. Puede establecer los intervalos de tiempo utilizando la opción `queryschedperiod`.


 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X

 Sistemas operativos Windows
  Prompted

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X

 Sistemas operativos Windows
 El planificador cliente espera que el servidor establezca contacto con el nodo cliente cuando se tenga que realizar el trabajo planificado.

Nota:

1.  Sistemas operativos Windows
 Utilice `schedmode prompted` en conjunto con la opción `autodeploy` para permitir que el planificador procese la planificación de despliegue de cliente de inmediato.
2. Si utiliza el mandato `dsmc schedule` y se han especificado las opciones `schedmode prompted` y `commethod V6Tcpi`, el cliente y el servidor de IBM Spectrum Protect deberán configurarse para IPv6. Asimismo, el nombre de host del cliente deberá configurarse para la dirección IPv6.

## Ejemplos

Archivo de opciones:


```
schedmode prompted
```

Línea de mandatos:

```
-schedmod=po
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

**Referencia relacionada:**

 Sistemas operativos Windows
 `Autodeploy`

`Cadlistenonport`

`Tcpclientaddress`

`Tcpclientport`





## Schedrestretrdisabled

La opción `schedrestretrdisabled` especifica si se debe inhabilitar la ejecución de las operaciones de restauración o recuperación planificadas.


## Clientes soportados

Esta opción es válida para todos los clientes. El servidor no puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X

Especifique esta opción en el archivo `dsm.sys` dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador Planificador en la sección de Mandato de planificación del Editor de preferencias.

 Sistemas operativos Windows
 Especifique esta opción en el archivo de opciones del cliente (`dsm.opt`) para el planificador. Puede establecer esta opción en el separador Planificador en la sección de Mandato de planificación del Editor de preferencias.

## Sintaxis

```

>>>-SCHEDRESTRETRDisabled-+-----+-----<<<
                          .-No-- .
                          '-Yes-'
  
```

## Parámetros

No

Especifica que el cliente no inhabilita la ejecución de las operaciones de planificación de restauración ni de recuperación. Este parámetro es el predeterminado.

Yes

Especifica que el cliente inhabilita la ejecución de las operaciones de planificación de restauración ni de recuperación.

## Ejemplos

Archivo de opciones:  
schedrestretrdisabled yes  
Línea de mandatos:  
No se aplica.















## Scrolllines

---

La opción scrolllines especifica el número de líneas de información que deben aparecer en pantalla a la vez.

Utilice esta opción cuando establezca la opción scrollprompt en Yes.

La opción scrolllines sólo puede utilizarse con los mandatos siguientes:

- delete filepace
- query archive
- query backup
- query backupset
- query filepace
- query group
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
query image
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windowsquery nas
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windowsquery node
- query options

## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en Línea de mandatos > Número de líneas que mostrar en el Editor de preferencias.

 Sistemas operativos WindowsEstablezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en Línea de mandatos > Número de líneas que mostrar en el Editor de preferencias.

## Sintaxis

---

```
>>-SCROLLLines-- --number-----<<
```

## Parámetros

---

number  
Especifica el número de líneas de información que deben aparecer en pantalla a la vez. El rango de valores es de 1 a 80, siendo 20 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
scrolllines 25  
Línea de mandatos:  
-scrollll=25

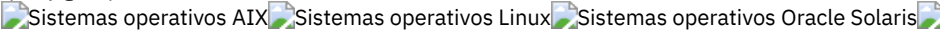
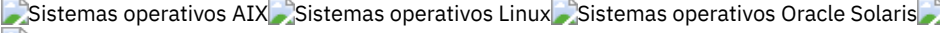
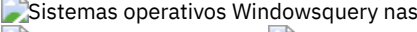
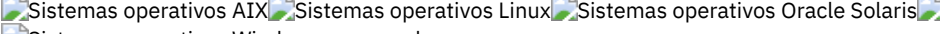
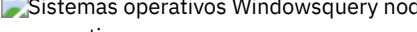
Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

## Scrollprompt

---

La opción scrollprompt especifica si desea que el cliente de copia de seguridad y archivado se detenga y espere después de visualizar el número de líneas de información especificado en la opción scrolllines, o desea que se desplace hasta el final de la lista de información.

La opción scrollprompt sólo puede utilizarse con los mandatos siguientes:

- delete filespace
- query archive
- query backup
- query backupset
- query filespace
- query group
-  Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Sistemas operativos Windows
- query image
-  Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X
-  Sistemas operativos Windowsquery nas
-  Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X
-  Sistemas operativos Windowsquery node
- query options

## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Línea de mandatos, en el campo Detenerse tras mostrar el número de líneas siguiente del Editor de preferencias.

## Sintaxis

```
>>-SCROLLPrompt--+-No--.  
                  |-----|  
                  '-Yes-'
```

## Parámetros

No

Se desplaza hasta el final de la lista y se detiene. Éste es el valor predeterminado.

Yes

Se detiene y espera después de mostrar el número de líneas indicado en la opción scrolllines. Se mostrará la siguiente solicitud en la pantalla:

```
Pulse 'Q' para salir, 'C' para desplazamiento continuo o  
'Intro' para  
continuar.
```

## Ejemplos


Archivo de opciones:

```
scrollprompt yes
```

Línea de mandatos:

```
-scrollp=yes
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X

## Servername

En el archivo `dsm.sys`, la opción `servername` especifica el nombre que desea utilizar para identificar un servidor y para iniciar una sección que contenga opciones para ese servidor. Puede identificar y especificar opciones para varios servidores.

En el ejemplo siguiente se muestra cómo especificar opciones para dos servidores diferentes:

En el archivo de opciones del usuario cliente (`dsm.opt`), la opción `servername` especifica con qué servidor, de los que se especifican en el archivo `dsm.sys`, debe establecerse contacto para obtener los servicios de copia de seguridad/archivado. Cuando se especifica en un archivo de opciones del usuario cliente (`dsm.opt`) o en la línea de mandatos, la opción `servername` modifica temporalmente el servidor predeterminado que se ha especificado en el archivo de opciones del sistema cliente.

Nota:

1. No se puede utilizar la opción `servername` para modificar temporalmente el servidor de migración especificado en el archivo de opciones del sistema cliente.
2. si el nombre de servidor de IBM Spectrum Protect cambia o si los clientes de copia de seguridad y archivado se dirigen a un servidor de IBM Spectrum Protect diferente, deberá inicializarse una nueva contraseña para todos los clientes para el nuevo nombre de servidor.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (`dsm.opt`) y en el archivo de opciones de sistema de cliente (`dsm.sys`). En el archivo `dsm.sys`, la opción `servername` es el comienzo de una stanza de servidor.

No modifique esta opción en `dsm.opt` cuando ejecute el cliente de archivado y copia de seguridad en una sesión de línea de mandatos o cuando ejecute la interfaz gráfica de usuario del cliente de archivado y copia de seguridad.

## Sintaxis

---

```
>>>-SErvername-- --servername----->>>
```

## Parámetros

---

`servername`

En el archivo `dsm.sys`, especifique el nombre que desea asignar a un servidor en particular. En el archivo de opciones del usuario cliente (`dsm.opt`) o en la línea de mandatos, especifique el nombre del servidor con el que desea establecer contacto para los servicios de copia de seguridad/archivado. El valor de `servername` en `dsm.opt` debe coincidir con un valor de `servername` en `dsm.sys`, o el cliente no podrá ponerse en contacto con el servidor.

Un nombre de servidor no es sensible a mayúsculas y minúsculas y puede tener hasta 64 caracteres.

## Ejemplos

---

Archivo de opciones:

```
servername server_a
```

Línea de mandatos:





```
-se=server_b
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.


## Sessioninitiation

---





Utilice la opción `sessioninitiation` para controlar si el servidor o el cliente ha de iniciar las sesiones a través de un cortafuegos. El valor predeterminado especifica que el cliente ha de iniciar las sesiones. Puede utilizar esta opción con el mandato `schedule`.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Para el planificador del cliente, no es necesario abrir ningún puerto en el cortafuegos. Si establece la opción `sessioninitiation` en `serveronly`, el cliente no intentará establecer contacto con el servidor. La planificación por solicitud de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. La opción `sessioninitiation` sólo afecta al comportamiento del planificador cliente que se ejecuta en modalidad por solicitud. Si establece la opción `sessioninitiation` en `serveronly`, a excepción de los

planificadores gestionados por daemon del aceptador de cliente, el cliente de la línea de mandatos, la GUI del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar sesiones.

 Sistemas operativos Windows Para el planificador del cliente, no es necesario abrir ningún puerto en el cortafuegos. Si establece la opción `sessioninitiation` en `serveronly`, el cliente no intentará establecer contacto con el servidor. La planificación por solicitud de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. La opción `sessioninitiation` sólo afecta al comportamiento del planificador cliente que se ejecuta en modalidad por solicitud. Si establece la opción `sessioninitiation` en `serveronly`, a excepción de los planificadores gestionados por daemon del aceptador de cliente, el cliente de la línea de mandatos, la GUI del cliente de archivado y copia de seguridad y la GUI del cliente web seguirán intentando iniciar sesiones.

Atención: No puede utilizar `dsmcad` para la planificación cuando establece la opción `sessioninitiation` en `serveronly`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota: Si establece la opción `sessioninitiation` en `serveronly`, el asistente para la configuración del cliente y el servicio del planificador no podrán autenticarse para el servidor de IBM Spectrum Protect. En este caso, puede ejecutar el planificador desde la línea de mandatos (`dsmc schedule`) y especificar la contraseña del nodo cuando se le solicite.

 Sistemas operativos Windows Nota: Si establece la opción `sessioninitiation` en `serveronly`, el asistente para la configuración del cliente y el servicio del planificador no podrán autenticarse para el servidor de IBM Spectrum Protect. En este caso, puede ejecutar el planificador desde la línea de mandatos (`dsmc schedule`) y especificar la contraseña del nodo cuando se le solicite, o bien utilizar el siguiente mandato `dsmcutil` para actualizar la contraseña:

```
dsmcutil updatepw /node:nnn /commServer:server1.example.com /password:ppp /validate:no
```

Se puede producir un problema similar si se necesita una clave de cifrado para las operaciones de copia de seguridad. En este caso, puede ejecutar el planificador desde la línea de mandatos (`dsmc schedule`) y entrar la clave de cifrado cuando se le solicite. Después de actualizar la contraseña y la clave de cifrado, debe reiniciar el planificador.

Si establece la opción `sessioninitiation` en `client`, el cliente inicia sesiones con el servidor comunicándose en el puerto TCP/IP definido con la opción de servidor `tcpport`. Éste es el valor predeterminado. La planificación por solicitud de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.

Nota:

1. El servidor de IBM Spectrum Protect puede especificar `SESSIONINITiation=clientorserver` o `SESSIONINITiation=serveronly` en los mandatos `register node` y `update node`. Si el servidor especifica `SESSIONINITiation=clientorserver`, el cliente puede decidir qué método utilizar. Si el servidor especifica `SESSIONINITiation=serveronly`, el servidor iniciará todas las sesiones.
2. Si `sessioninitiation` se establece en `serveronly`, el valor de la opción de cliente `tcpclientaddress` debe ser igual al valor de la opción `HLAddress` del mandato de servidor `update node` o `register node`. El valor de la opción de cliente `tcpclientport` debe ser igual al valor de la opción `LLAddress` del mandato de servidor `update node` o `register node`.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en la ficha Planificador, en el campo Iniciación de sesión del Editor de preferencias.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Planificador, en el campo Iniciación de sesión del Editor de preferencias.

## Sintaxis

---

```
.-Client-----
>>-SESSIONINITiation-----+-----<<
'-SERVEROnly-'
```

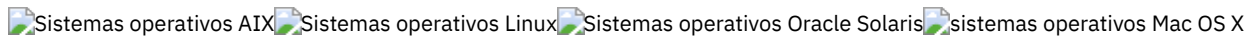
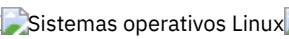
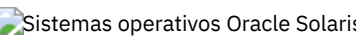
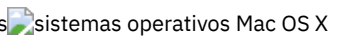
## Parámetros

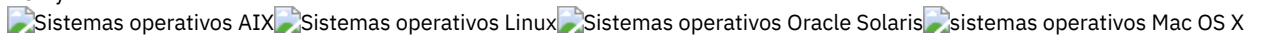
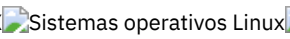
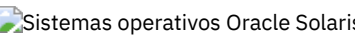
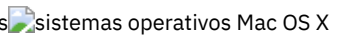
---

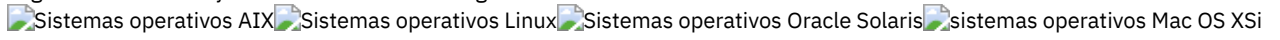
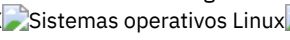
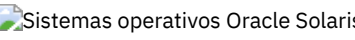
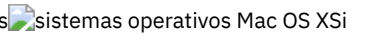
Client

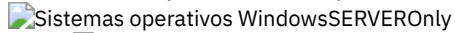
Especifica que el cliente iniciará sesiones con el servidor comunicándose en el puerto TCP/IP definido con la opción de servidor `TCPPORT`. Éste es el valor predeterminado. La planificación por solicitud de servidor puede utilizarse para solicitar al cliente que se conecte con el servidor.

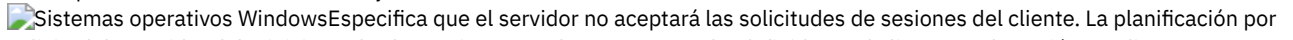


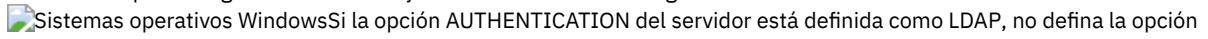
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
SERVEROnly

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica que el servidor no aceptará las solicitudes de sesiones del cliente. La planificación por solicitud de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. A excepción de los planificadores que el daemon de aceptación de clientes gestiona, el cliente de línea de mandatos, la GUI del cliente de copia de seguridad-archivado y la GUI del cliente web seguirán intentando el inicio de las sesiones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Si la opción `AUTHENTICATION` del servidor está definida como LDAP, no defina la opción `sessioninitiation` del cliente como `serveronly`; de hacerlo, las planificaciones no se podrán ejecutar.

 Sistemas operativos WindowsSERVEROnly

 Sistemas operativos WindowsEspecifica que el servidor no aceptará las solicitudes de sesiones del cliente. La planificación por solicitud de servidor debe iniciar todas las sesiones en el puerto que se ha definido en el cliente con la opción `tcpclientport`. A excepción de los planificadores que el daemon de aceptación de clientes gestiona, el cliente de línea de mandatos, la GUI del cliente de copia de seguridad-archivado y la GUI del cliente web seguirán intentando el inicio de las sesiones.

 Sistemas operativos WindowsSi la opción `AUTHENTICATION` del servidor está definida como LDAP, no defina la opción `sessioninitiation` del cliente como `serveronly`; de hacerlo, las planificaciones no se podrán ejecutar.

## Ejemplos

---

Archivo de opciones:

```
sessioninitiation serveronly
```

Línea de mandatos:

```
schedule -sessioninitiation=serveronly
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Setwindowtitle

---

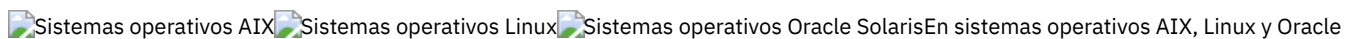

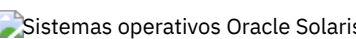
Utilice la opción `setwindowtitle` para modificar el título de la ventana de mandatos de cliente administrativo durante el proceso.

Por ejemplo, cuando se ejecuta el mandato de cliente administrativo (`dsmadm`) en el nodo de cliente y el cliente administrativo se conecta con el servidor de IBM Spectrum Protect, se visualiza el texto siguiente en el título de la ventana de mandatos:

```
CONECTADO A SERVIDOR: nombre servidor(nombre host servidor)
```

donde *nombre servidor* es el nombre del servidor de IBM Spectrum Protect y *nombre host servidor* es el nombre de host de IBM Spectrum Protect.

Cuando utiliza la opción `setwindowtitle`, se sobrescribe cualquier título definido por el usuario de la ventana de mandatos. Después de desconectar el cliente administrativo del servidor de IBM Spectrum Protect, el título de la ventana se restablece en el título de ventana definido por el usuario.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
En sistemas operativos AIX, Linux y Oracle Solaris, el título de ventana de terminal se restablece en el título "Terminal" después de desconectarse del servidor.

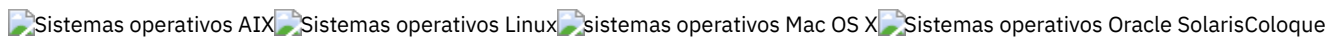
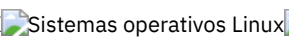
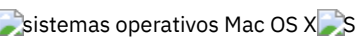
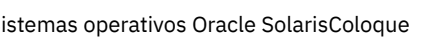
## Clientes soportados

---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`) o el archivo de opciones de sistema del cliente (`dsm.sys`).

 Sistemas operativos WindowsColoque esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-SETWINDOWTITLE--+-No--.  
' -Yes-'
```

## Parámetros

---

No

El título de la ventana de mandatos de cliente administrativo no cambia durante el proceso. Este parámetro es el predeterminado.

Yes (Sí)

El nombre de servidor de IBM Spectrum Protect y el nombre de servidor de host se visualizan en el título de la ventana de mandatos de cliente administrativo.

## Ejemplos

---





Archivo de opciones:

```
SETWINDOWTITLE YES
```

Línea de mandatos:

```
-setwindowtitle=yes
```




Esta opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Shmport

---




La opción shmport especifica la dirección del puerto TCP/IP de un servidor al utilizar la memoria compartida. Todas las comunicaciones de memoria compartida comienzan con una conexión TCP/IP.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Nota: El valor que se especifica en la opción shmport en el archivo dsm.sys debe coincidir con el valor que se ha especificado para shmport en el archivo de opciones de servidor.

 Sistemas operativos Windows Nota: El valor que se especifica en la opción shmport en el archivo de opciones del cliente (dsm.opt) debe coincidir con el valor que se ha especificado para shmport en el archivo de opciones de servidor.

## Clientes soportados




---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis




---


```
>>-SHMPort-- --número_puerto-----><
```

## Parámetros

---

port\_number

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Especifica el número de puerto. Puede especificar un valor de 1000 a 32767. El valor predeterminado es 1510.

 Sistemas operativos Windows Especifica el número de puerto. Puede especificar un valor entre 1 y 32767. El valor predeterminado es 1510.

## Ejemplos





---

Archivo de opciones:

```
shmport 1580
```

Línea de mandatos:




No se aplica.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Showmembers

---

Utilice la opción showmembers para visualizar todos los miembros de un grupo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Puede utilizar la opción showmembers con los mandatos query group y restore group.




 Sistemas operativos Windows Puede utilizar la opción showmembers con los mandatos query group, query systemstate y restore group.

La opción showmembers no es válida con la opción inactive. Si desea visualizar los miembros de un grupo que actualmente no están activos, utilice las opciones pitdate y pittime.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

## Sintaxis

---

```
>>-SHOWMembers-----><
```

## Parámetros

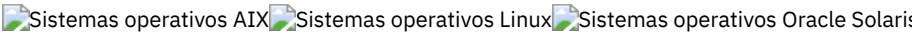


---

No hay parámetros para esta opción.


## Ejemplos

---

Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
restore group /virtfs/* -pick -showmembers
```

 Sistemas operativos Windows

```
restore group {virtfs}\* -pick -showmembers
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Skipacl

---

La opción skipacl permite incluir o excluir datos de la lista de control de acceso (ACL) durante una operación de copia de seguridad o archivado; se incluyen los datos de ACL de forma predeterminada.

Cuando esta opción está establecida en yes, el cliente de copia de seguridad y archivado no incluye los datos de ACL cuando realiza una copia de seguridad o archiva archivos y directorios. El valor predeterminado es no, que permite que los datos de ACL sean incluidos cuando los objetos se copian en el servidor. Sólo debe establecer skipacl en yes cuando las ACL no están definidas en el sistema de archivos, o cuando está seguro de que no necesita los datos de ACL cuando se recuperan o restauran los archivos.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux. En sistemas Linux y AIX, establecer skipacl en yes también omite los atributos ampliados.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (dsm.opt).

## Sintaxis

---

```
.-No--.  
>>-SKIPACL-----><  
'-Yes-'
```

## Parámetros

---

No

Si especifica No, se realizará copia de seguridad de los datos de ACL. Éste es el valor predeterminado.

Yes





Si especifica Yes, no se realiza copia de seguridad de los datos de ACL, y por lo tanto no pueden restaurarse. skipacl=yes modifica los valores de skipaclupdatecheck.

## Ejemplos

---

Archivo de opciones:

```
skipacl yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Skipaclupdatecheck

---

La opción skipaclupdatecheck desactiva la suma de comprobación y las comparaciones de tamaño de los datos de ACL.

Cuando se establece en yes (el valor predeterminado es no), el cliente de copia de seguridad y archivado no realizará la comparación de sumas de comprobación ni de tamaños antes o después de la copia de seguridad y durante el proceso incremental (suma de comprobación de ACL de copia de seguridad anterior y ACL actual) para detectar actualizaciones de ACL. Sin embargo, se hará copia de seguridad de los datos de ACL actuales si el archivo se selecciona para la copia de seguridad por otras razones. Si en un archivo sólo se actualizan las ACL, la copia de seguridad incremental siguiente no reconocerá esta actualización de ACL y no se realizará la copia de seguridad del archivo.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX y Linux.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del usuario cliente (dsm.opt).

## Sintaxis

---

```
.-No--.  
>>-SKIPACLUPdatecheck-----><  
'-Yes-'
```

## Parámetros

---

No

Si especifica No, el cliente lleva a cabo la comparación de sumas de comprobación y tamaños de los datos de ACL, antes y después de la copia de seguridad y durante el proceso incremental. Éste es el valor predeterminado.

Yes

Si especifica Yes, el cliente no realizará la suma de comprobación y las comparaciones de tamaño de los datos de ACL.

## Ejemplos

---

Archivo de opciones:

```
skipaclup yes
```

 Sistemas operativos Windows

## Skipmissingsyswfiles

---

Utilice la opción `Skipmissingsyswfiles` para especificar si el cliente de archivado y copia de seguridad omite determinados archivos de VSS Writer que faltan y continúa la copia de seguridad del estado del sistema.

Si la opción `skipmissingsyswfile` se establece en `Yes`, se omiten los archivos de VSS Writer que no se encuentran durante una copia de seguridad de estado del sistema. Esta opción sólo resulta eficaz para los archivos que faltan en los siguientes VSS Writers:

- System Writer
- Windows Deployment Service Writer
- Event Log Writer

Tenga en cuenta los siguientes puntos antes de utilizar la opción `skipmissingsyswfile`:

- Si establece la opción `skipmissingsyswfile` en `yes`, se habilitan las copias de seguridad que puedan no haber terminado correctamente con versiones anteriores del cliente de copia de seguridad y archivado.
- Existe un pequeño riesgo de que la copia de seguridad sea incoherente si se salta un archivo.
- El riesgo se minimiza por estos factores:
  - La copia de seguridad solo se puede realizar cuando el sistema está en ejecución.
  - Los archivos de sistema críticos están protegidos frente a eliminación por Microsoft Windows.

## Cientes soportados

---

Esta opción es válida para los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
.-Yes-.  
>>-SKIPMISSingsyswfiles-----<<  
'-No--'
```

## Parámetros

---

Yes

Especifica que desea que el cliente de copia de seguridad y archivado omita determinados archivos que no se encuentran durante la copia de seguridad de estado del sistema. Los archivos que no se encuentran se incluirán en el registro de errores y en el registro de actividades del servidor. El código de retorno final se define en 8. Éste es el valor predeterminado.

No

Especifica que desea que el cliente de copia de seguridad y archivado detenga la copia de seguridad cuando no se encuentran determinados archivos durante la copia de seguridad de estado del sistema. Los archivos que no se encuentran se registran en el registro cronológico de errores y en el registro de actividad del servidor. El código de retorno final es 12.

## Ejemplos

---

Archivo de opciones:


```
SKIPMISSingsyswfiles yes
```

Línea de mandatos:

```
-SKIPMISSingsyswfiles=yes
```

### Referencia relacionada:

Backup Systemstate

 Sistemas operativos Windows

## Skipntpermissions

---

La opción `skipntpermissions` pasa por alto el proceso de la información de seguridad del sistema de archivos de Windows.

Puede utilizar esta opción para las copias de seguridad incrementales, las copias de seguridad selectivas, las operaciones de restauración y las operaciones de archivado y recuperación.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Se aplica a los mandatos incremental, selective, restore, archive y retrieve. También puede establecer esta opción en el separador General del editor de preferencias.

## Sintaxis

---

```
                .-No--.  
>>-SKIPNTPermissions--+-+-----+-----><  
                '-Yes-'
```

## Parámetros

---

No

Si especifica No, se realiza una copia de seguridad de la información de seguridad del sistema de archivos de Windows, se restaura, se archiva o se recupera. Este es el valor predeterminado.

Yes

Si especifica Yes, no se realiza una copia de seguridad de la información de seguridad del sistema de archivos de Windows, no se restaura, no se archiva ni se recupera.

## Ejemplos


---

Archivo de opciones:

```
skipntp yes
```

Línea de mandatos:

```
-skipntp=yes
```

 Sistemas operativos Windows

## Skipntsecuritycrc

---

La opción skipntsecuritycrc controla el cálculo de la comprobación de redundancia cíclica (CRC) de seguridad para obtener una comparación de la información de seguridad de NTFS o ReFS durante la realización de una operación de copia de seguridad incremental o de copia de seguridad selectiva, una operación de archivado, de restauración o de recuperación.

Si establece la opción skipntsecuritycrc en no (el valor predeterminado), puede que el rendimiento sea más lento porque el programa debe recuperar todos los descriptores de seguridad.

Esta opción puede utilizarse con los siguientes mandatos:

- archive
- incremental
- restore
- retrieve
- selective

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
                .-No--.  
>>-SKIPNTSecuritycrc--+-+-----+-----><
```

' -Yes- '

## Parámetros

---

No

Si especifica No, la CRC de seguridad se genera durante una copia de seguridad. Este es el valor predeterminado.

Yes

Si especifica Yes, la CRC de seguridad no se genera durante una copia de seguridad. Se realizará copia de seguridad de todos los permisos, pero el programa no podrá determinar si los permisos han cambiado en la siguiente copia de seguridad incremental. Cuando la opción skipntpermissions se establece en yes, la opción skipntsecuritycrc no tiene aplicación.

## Ejemplos

---

Archivo de opciones:

```
skipnts no
```

Línea de mandatos:

```
-skipnts=no
```

 Sistemas operativos Windows

## Skipsystemexclude

---

Utilice la opción skipsystemexclude para especificar cómo procesar sentencias de exclusión para determinados archivos del sistema operativo que el cliente de IBM Spectrum Protect for Virtual Environments omite de forma predeterminada.

De forma predeterminada, los clientes de IBM Spectrum Protect for Virtual Environments omiten determinados archivos del sistema operativo Windows que normalmente no se requieren para la recuperación del sistema para las operaciones de copia de seguridad de máquina virtual (VM). Estos archivos pueden incluir archivos del sistema Windows, archivos temporales de Internet y archivos de la Papelera de reciclaje.

Puede utilizar esta opción para omitir el proceso de sentencias de exclusión para estos archivos del sistema operativo. Si no se procesan estas sentencias de exclusión, es posible que se reduzca el tiempo necesario para realizar la copia de seguridad de las máquinas virtuales.

## Clientes de soporte

---

Esta opción sólo es válida para clientes de IBM Spectrum Protect for Virtual Environments en los sistemas operativos Windows.

## Archivo de opciones

---

Esta opción es válida en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos. La opción se puede establecer en el conjunto de opciones de cliente del servidor de IBM Spectrum Protect. La opción se ignora para todos los demás clientes.

## Sintaxis

---

```
>>-SKIPSYSTEMexclude--+-+-----+-----><
                        .-Yes-.
                        '-No--'
```

## Parámetros

---

Yes

Especifique este parámetro para omitir el proceso de las sentencias de exclusión para determinados archivos del sistema operativo Windows durante las operaciones de copia de seguridad de máquina virtual. Este parámetro es el predeterminado.

No

Especifique este parámetro para procesar sentencias de exclusión de archivos del sistema operativo Windows. Cuando selecciona este parámetro y ejecuta una copia de seguridad de archivos del host Hyper-V, los archivos del sistema operativo se excluyen.

## Ejemplos

---

Archivo de opciones

```
SKIPSYSTEMexclude yes
```

#### Línea de mandatos


```
dsmc backup vm -SKIPSYST=yes  
dsmc incr -skipsyst=no
```


 Sistemas operativos Linux  Sistemas operativos Windows

## Snapdiff

---


Si se utiliza la opción `snapdiff` con el mandato incremental el proceso de copia de seguridad a incrementos se realiza de forma transparente. El mandato ejecuta una copia de seguridad a incrementos de los archivos modificados, según los informes de NetApp, en lugar de explorar todo el volumen en busca de archivos modificados.

 Sistemas operativos Windows La opción `snapdiff` (diferencia de instantánea) se utiliza para realizar copias de seguridad de volúmenes de servidor de archivos NAS/N-Series con conexión NFS o CIFS.

 Sistemas operativos Windows Restricción: Ninguno de las unidades compartidas NetApp predefinidas, incluyendo `C$`, funciona con la opción de diferencia de instantánea de IBM Spectrum Protect porque el cliente de copia de seguridad y archivado no puede determinar los puntos de montaje de forma programada.

Debe configurar un ID de usuario y una contraseña en el cliente de copia de seguridad y archivado para habilitar el proceso de diferencia de instantánea.


Utilice esta opción con una copia de seguridad incremental de un volumen de archivador NAS, en lugar de una copia incremental simple o incremental con la opción `snapshotroot`, siempre que el servidor de archivos NAS se ejecute en ONTAP 7.3.0, o posterior. No utilice al mismo tiempo las opciones `snapdiff` y `snapshotroot`.

 Sistemas operativos Linux Restricción: Las copias de seguridad incrementales con procesamiento de diferencia de instantáneas solo están disponibles con el cliente de archivado y copia de seguridad de Linux x86\_64.

La primera vez que realice una copia de seguridad incremental con la opción de diferencia de instantáneas, se crea una instantánea (la instantánea base) y se ejecuta una copia de seguridad incremental tradicional utilizando esta instantánea como origen. El nombre de la instantánea creada se registra en la base de datos del servidor de IBM Spectrum Protect. La copia de seguridad incremental inicial debe finalizar sin errores para que la siguiente operación de copia de seguridad utilice el proceso de diferencia de instantáneas.

La segunda vez que se ejecuta una copia de seguridad incremental con esta opción, se crea una instantánea más nueva o se utiliza una instantánea existente (en función del valor establecido para la opción `diffsnapshot`) a fin de encontrar las diferencias entre estas dos instantáneas. Esta segunda instantánea se denomina *diffsnapshot*, o instantánea de diferencia. A continuación, el cliente realiza una copia de seguridad incremental de los archivos que se han notificado como cambiados por NetApp en el servidor de IBM Spectrum Protect. El sistema de archivos seleccionado para el proceso de diferencias de instantánea debe estar montado en la raíz del volumen. No puede utilizar la opción `snapdiff` para ningún sistema de archivos que no esté montado en la raíz del volumen. Una vez que haya realizado la copia de seguridad de los datos con la opción `snapdiff`, la instantánea que se ha utilizado como la instantánea base se suprime del directorio de instantánea.

 Sistemas operativos Windows En sistemas Windows, el directorio de instantáneas está en `~snapshot`.

 Sistemas operativos Linux En sistemas Linux, el directorio de instantáneas está en `.snapshot`.

El cliente no suprime ninguna instantánea que no ha creado.

Cuando se completa una operación de copia de seguridad incremental diferencial de instantánea, el cliente asegura que sólo persista la instantánea base registrada más recientemente en el volumen de gestor de archivos. Todas las instantáneas creadas por una copia de seguridad incremental diferencial de instantáneas en el cliente de archivado y copia de seguridad empiezan con los caracteres "TSM\_". Si utiliza una herramienta de instantánea distinta del cliente de copia de seguridad y archivado para producir instantáneas, asegúrese de no utilizar la serie "TSM\_" al principio del nombre de instantánea. Si los nombres de la instantánea empiezan por "TSM\_", los archivos se suprimen cuando el cliente inicia la siguiente operación de copia de seguridad incremental diferencial de instantáneas.

Para ejecutar una copia de seguridad de diferencial de instantánea de volúmenes de archivador de NetApp de sólo lectura, se debe especificar la opción `useexistingbase` para impedir un intento de crear una instantánea en el volumen de sólo lectura. Además, especifique el nombre de la instantánea base a utilizar (la opción `basesnapshotname`) y el nombre de la instantánea diferencial a utilizar (la opción `diffsnapshotname`).

Para los servidores de archivos NAS y N-Series que ejecutan ONTAP 7.3.0, o posterior, puede utilizar la opción `creatnewbase` para realizar una copia de seguridad de los archivos que se han omitido debido a los siguientes motivos:

- Se excluye un archivo porque el archivo de inclusión-exclusión tiene una regla de exclusión en vigor. Se excluye un archivo cuando no ha modificado el archivo de inclusión/exclusión, pero ha eliminado la regla que ha excluido el archivo. La API de NetApp detecta los cambios de archivos sólo entre dos instantáneas, no cambios en el archivo de inclusión/exclusión.



- Si ha añadido una sentencia de inclusión en el archivo de opciones, dicha opción de inclusión no entra en vigor a menos que NetApp detecte que se han producido cambios en el archivo. El cliente no inspecciona cada uno de los archivos del volumen durante la copia de seguridad.
- Ha utilizado el mandato `dsmc delete backup` para suprimir explícitamente un archivo del inventario del servidor de IBM Spectrum Protect. NetApp no detecta que un archivo se ha suprimido manualmente del servidor. Por consiguiente, el archivo sigue sin protección en el almacenamiento de IBM Spectrum Protect hasta que se cambia en el volumen y NetApp detecta el cambio, lo que indica al cliente que vuelva a hacer una copia de seguridad del mismo.
- Los cambios de políticas como, por ejemplo, de `mode=modified` a `mode=absolute` no se detectan.
- El espacio de archivo entero se suprime del inventario IBM Spectrum Protect. Esta acción hace que la opción de diferencia de instantáneas cree una instantánea para que se utilice como origen, y ejecuta una copia de seguridad incremental completa.
- Se excluye un archivo de la instantánea debido a que el nombre de archivo contiene un carácter que no está incluido en el juego de caracteres ASCII de 7 bits. La opción `createnewbase` crea una instantánea base y la utiliza como fuente para ejecutar una copia de seguridad incremental completa. NetApp controla qué es lo que constituye un objeto modificado.

Consejo: Puede utilizar la opción `snapdiffhttps` para ejecutar copias de seguridad incrementales diferenciales de instantánea de los gestores de archivos NetApp con una conexión HTTPS segura. Para ejecutar correctamente las copias de seguridad incrementales diferenciales de instantáneas, los releases anteriores del cliente de archivado de la copia de seguridad requerían acceso administrativo de HTTP para habilitarse en el archivador de NetApp. Con la opción `snapdiffhttps`, puede establecer una sesión de administración segura con el archivador NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador. En la lista de opciones que utiliza el mandato incremental tradicional, la última columna muestra la interacción de cada opción con la opción `snapdiff`. En la información siguiente se describen las definiciones de *válido*, *no válido* y *sin efecto*:

**Válido**

El proceso se ejecuta normalmente cuando se utiliza la opción.


































**No válido**

Si la opción se utiliza con `snapdiff`, se genera un mensaje de error.























































**Sin efecto**

La opción se puede utilizar, pero no se tiene en cuenta.

Tabla 1. Mandato Incremental: opciones relacionadas

Opción	Donde se especifica	Con <code>snapdiff</code>
 Sistemas operativos AIX  Sistemas operativos Linux asnodename	 Sistemas operativos AIX  Sistemas operativos Linux En el archivo de opciones del sistema cliente ( <code>dsm.sys</code> ) o en la línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windows asnodename	 Sistemas operativos Windows Archivo de opciones del cliente ( <code>dsm.opt</code> ) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux automount	 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones del cliente ( <code>dsm.opt</code> ).	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
 Sistemas operativos Windows autofsrename	 Sistemas operativos Windows Sólo archivo de opciones del cliente ( <code>dsm.opt</code> ).	 Sistemas operativos Windows Sin efecto
 Sistemas operativos AIX  Sistemas operativos Linux basesnapshotname	 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones del cliente ( <code>dsm.opt</code> ) o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windows basesnapshotname	 Sistemas operativos Windows Archivo de opciones del cliente ( <code>dsm.opt</code> ) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux changingretries	 Sistemas operativos AIX  Sistemas operativos Linux En el archivo de opciones del sistema cliente ( <code>dsm.sys</code> ) o en la línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto

Opción	Donde se especifica	Con snapdiff
 Sistemas operativos Windowschangingretries	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Sin efecto
 Sistemas operativos Windowscompressalways	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux compressalways	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowscompression	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux compression	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys) dentro de una stanza de servidor o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windowscreatenevbase	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos WindowsSólo línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Válido
diffsnapshot	Sólo línea de mandatos.	Válido
 Sistemas operativos AIX  Sistemas operativos Linux diffsnapshotname	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowsdiffsnapshotname	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
dirsonly	Sólo línea de mandatos.	Válido
 Sistemas operativos Windowsdomain	 Sistemas operativos WindowsSólo archivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linuxdomain	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys), archivo de opciones del usuario cliente (dsm.opt), o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos AIX  Sistemas operativos Linux efsdecrypt	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys), archivo de opciones del usuario cliente (dsm.opt), o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
 Sistemas operativos AIX  Sistemas operativos Linux enablelanfree	 Sistemas operativos AIX  Sistemas operativos LinuxEn el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido

Opción	Donde se especifica	Con snapdiff
 Sistemas operativos Windowsenablelanfree	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux encryptiontype	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowsencryptiontype	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos Windows Válido
 Sistemas operativos Windowsencryptkey	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux encryptkey	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos AIX  Sistemas operativos Linux exclude.fs.nas	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys).	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
 Sistemas operativos Windowsexclude.fs.nas	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos Windows Sin efecto
filelist	Sólo línea de mandatos.	No válido
filesonly	Sólo línea de mandatos.	Válido
 Sistemas operativos AIX  Sistemas operativos Linux followsymboliclink	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
 Sistemas operativos AIX  Sistemas operativos Linux include.fs.nas	 Sistemas operativos AIX  Sistemas operativos LinuxEn el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
 Sistemas operativos Windowsinclude.fs.nas	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Sin efecto
 Sistemas operativos AIX  Sistemas operativos Linuxinlexcl	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys).	 Sistemas operativos AIX  Sistemas operativos Linux Válida, pero solo cuando NetApp detecta un cambio de archivo.
 Sistemas operativos Windowsinlexcl	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos Windows Válida, pero solo cuando NetApp detecta un cambio de archivo.

Opción	Donde se especifica	Con snapdiff
incrbydate	Sólo línea de mandatos.	No válido
 Sistemas operativos Windowsmemoryefficientbackup	 Sistemas operativos WindowsEn el archivo de opciones del cliente (dsm.opt), en el servidor o en la línea de mandatos.	 Sistemas operativos Windows Sin efecto
 Sistemas operativos AIX  Sistemas operativos Linux memoryefficientbackup	 Sistemas operativos AIX  Sistemas operativos LinuxEsta opción se admite en dsm.sys y dsm.opt, pero el valor de dsm.opt se pasa por alto si también se encuentra en dsm.sys. También puede incluir esta opción en una stanza del servidor o en la línea de mandatos inicial.	 Sistemas operativos AIX  Sistemas operativos Linux Sin efecto
monitor	Sólo línea de mandatos.	No válido
 Sistemas operativos AIX  Sistemas operativos Linuxnojournal	 Sistemas operativos AIX  Sistemas operativos LinuxSólo línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux No válido
 Sistemas operativos Windowsnojournal	 Sistemas operativos WindowsSólo línea de mandatos.	 Sistemas operativos Windows No válido
 Sistemas operativos AIX  Sistemas operativos Linux postsnapshotcmd	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowspostsnapshotcmd	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o con la opción include.fs.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux preservelastaccessdate	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowspreservelastaccessdate	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux presnapshotcmd	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowspresnapshotcmd	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o con la opción include.fs.	 Sistemas operativos Windows Válido
 Sistemas operativos AIX  Sistemas operativos Linux removeoperandlimit	 Sistemas operativos AIX  Sistemas operativos LinuxSólo línea de mandatos.	 Sistemas operativos AIX  Sistemas operativos Linux Válido
 Sistemas operativos Windowsresetarchiveattribute	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).	 Sistemas operativos Windows Válido

Opción	Donde se especifica	Con snapdiff
Sistemas operativos AIX  Sistemas operativos Linux skipaclupdatecheck	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del cliente (dsm.opt).	Sistemas operativos AIX Sistemas operativos Linux Válido
Sistemas operativos Windows skipntpermissions	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	Sistemas operativos Windows Válido
Sistemas operativos Windows skipntsecuritycrc	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	Sistemas operativos Windows Válido
Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Windows snapdiffhttps	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Sólo línea de mandatos.	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Windows Válido
Sistemas operativos AIX  Sistemas operativos Linux snapshotcachesize	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.fs.	Sistemas operativos AIX Sistemas operativos Linux Sin efecto
Sistemas operativos AIX  Sistemas operativos Linux snapshotproviderfs	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.	Sistemas operativos AIX Sistemas operativos Linux No válido
Sistemas operativos Windows snapshotproviderfs	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.	Sistemas operativos Windows No válido
Sistemas operativos AIX  Sistemas operativos Linux snapshotproviderimage	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del sistema cliente (dsm.sys) o con la opción include.image.	Sistemas operativos AIX Sistemas operativos Linux No válido
Sistemas operativos Windows snapshotproviderimage	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.image.	Sistemas operativos Windows No válido
snapshotroot	Sólo línea de mandatos.	No válido
subdir	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	No válido
Sistemas operativos AIX  Sistemas operativos Linux tapeprompt	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	Sistemas operativos AIX Sistemas operativos Linux Válido
Sistemas operativos Windows tapeprompt	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.	Sistemas operativos Windows Válido
Sistemas operativos AIX  Sistemas operativos Linux toc	Sistemas operativos AIX Sistemas operativos Linux Sólo línea de mandatos.	Sistemas operativos AIX Sistemas operativos Linux No válido

Opción	Donde se especifica	Con snapdiff
Sistemas operativos Windows	Sistemas operativos Windows Sólo línea de mandatos.	Sistemas operativos Windows No válido
Sistemas operativos AIX  Sistemas operativos Linux useexistingbase	Sistemas operativos AIX Sistemas operativos Linux Sólo línea de mandatos.	Sistemas operativos AIX Sistemas operativos Linux Válido
Sistemas operativos Windows useexistingbase	Sistemas operativos Windows Sólo línea de mandatos.	Sistemas operativos Windows Válido
virtualfsname	Sólo línea de mandatos.	No válido
Sistemas operativos AIX  Sistemas operativos Linux virtualmountpoint	Sistemas operativos AIX Sistemas operativos Linux Archivo de opciones del sistema cliente (dsm.sys).	Sistemas operativos AIX Sistemas operativos Linux No válido

## Clientes soportados

Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

## Sintaxis

```
>>-SNAPDiff-----<<
```

## Parámetros

No hay parámetros para esta opción.

## Ejemplos

Sistemas operativos Linux Línea de mandatos:

Sistemas operativos Linux Realice una copia de seguridad incremental diferencial de instantánea de un sistema de archivos montado en NFS /vol/vol1 que reside en el servidor de archivos homestore.example.com, donde /net/home1 es el punto de montaje de /vol/vol1.

```
incremental -snapdiff -diffsnapshot=latest /net/home1
```

Sistemas operativos Windows Línea de mandatos:

Sistemas operativos Windows Realice una copia de seguridad incremental diferencial de instantánea a partir de una instantánea que se toma de una unidad compartida de red //homestore.example.com/vol/vol1 montada en la unidad H:, donde homestore.example.com es un servidor de archivos.

```
incremental -snapdiff H:
```

Sistemas operativos Windows Realice una copia de seguridad incremental diferencial de instantánea a partir de una instantánea que se toma de una unidad compartida de red //homestore.example.com/vol/vol1 montada en la unidad H:, donde homestore.example.com es un servidor de archivos. El valor de opción de -diffsnapshot de LATEST significa que la operación se producirá utilizando la instantánea más reciente (la instantánea activa) para el volumen H:.

```
incremental -snapdiff H: -diffsnapshot=latest
```

Línea de mandatos:

Ejecute una copia de seguridad incremental completa única tras detectar que el servidor de NetApp ha migrado a un servidor de archivos habilitado para Unicode de un servidor que no soportaba nombres de archivos Unicode. Sistemas operativos AIX

Sistemas operativos Linux

```
dsmc incremental -snapdiff -createnewbase=migrate /net/home1
```

Sistemas operativos Windows

```
dsmc incremental -snapdiff -createnewbase=migrate h:
```

Ejecute una copia de seguridad incremental diferencial de instantáneas tras detectar que el servidor de NetApp ha migrado a un servidor de archivos habilitado por Unicode de un servidor que no soportaba los nombres de archivos Unicode. Este mandato suprime el mensaje de aviso.

```
dsmc incremental -snapdiff -createnewbase=ign /net/home1
```

Sistemas operativos Windows

```
dsmc incremental -snapdiff -createnewbase=ign h:
```

Realice una copia de seguridad incremental completa debido a que ha realizado algunos cambios de inclusión o exclusión:

Sistemas operativos AIX Sistemas operativos Linux

```
dsmc incremental -snapdiff -createnewbase=yes /net/home1
```

Sistemas operativos Windows

```
dsmc incremental -snapdiff -createnewbase=yes h:
```

#### Conceptos relacionados:

Sistemas operativos Linux Copia de seguridad diferencial de la instantánea con una conexión HTTPS

Soporte de SnapMirror para la copia de seguridad a incrementos progresivos asistida por instantáneas NetApp (snapdiff)

#### Tareas relacionadas:

Configuración de NetApp y IBM Spectrum Protect para copias de seguridad incrementales de diferencia de instantánea

#### Referencia relacionada:

Snapdiffhttps

Basesnapshotname

Diffsnapshotname

Useexistingbase

Diffsnapshot

Establecer contraseña

Sistemas operativos Linux Sistemas operativos Windows

## Snapdiffchangelogdir

La opción `snapdiffchangelogdir` define la ubicación donde el cliente almacena los registros de cambios utilizados para operaciones de copia de seguridad diferencial de instantánea.

Importante: si anteriormente ha utilizado copias de seguridad diferenciales de instantánea con un cliente de archivado y copia de seguridad anterior a la Versión 8.1.2, la primera copia de seguridad diferencial de instantánea que ejecute con el cliente V8.1.2 o posterior será una copia de seguridad incremental progresiva completa. Para evitar esta copia de seguridad incremental progresiva, mueva los archivos de registro de cambios existentes de la ubicación antigua especificada por la opción `stagingdirectory` a la nueva ubicación especificada por la opción `snapdiffchangelogdir` antes de ejecutar la primera copia de seguridad diferencial de instantánea. Por ejemplo, ejecute el mandato siguiente:

```
cp -R /tmp/TSM/TsmSnapDiff /opt/tivoli/tsm/client/ba/TsmSnapDiff
```

Sistemas operativos Windows

```
xcopy C:\Users\Bob\AppData\Local\Temp\TSM\TsmSnapDiff  
"C:\Program Files\Tivoli\TSM\baclient\TsmSnapDiff" /s /y
```

Los archivos de registro de cambios tienen las siguientes pautas de nomenclatura:

```
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetAppFiler/  
SnapdiffChangeLog__NombreVolumen__.tsmDB  
.../TSM/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetAppFiler/  
SnapdiffChangeLog__NombreVolumen__.tsmDB.Lock
```

Sistemas operativos Windows


```
... \TSM\TsmSnapDiff\ .TsmSnapdiffChangeLogs\NetAppFiler\  
SnapdiffChangeLog__NombreVolumen__.tsmDB  
... \TSM\TsmSnapDiff\ .TsmSnapdiffChangeLogs\NetAppFiler\  
SnapdiffChangeLog__NombreVolumen__.tsmDB.Lock
```


donde:

- *NetAppFiler* es el nombre de host o la dirección IP de la máquina virtual de almacenamiento (SVM) del servidor de gestión de clústeres o el servidor de archivos 7-mode.
- *NombreVolumen* es el volumen que desea proteger.

## Cientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64. Esta opción también puede definirse en el servidor.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. Esta opción también puede definirse en el servidor.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Cuando snapdiffchangelogdir se especifica en la línea de mandatos, modifica los valores especificados en el archivo de opciones. Puede establecer esta opción en la ficha General del editor de preferencias.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Cuando snapdiffchangelogdir se especifica en la línea de mandatos, modifica los valores especificados en el archivo de opciones. Puede establecer esta opción en la ficha General del editor de preferencias.

## Sintaxis

---


```
>>-SNAPDIFFCHANGELOGDir--vía_acceso-----<<
```

## Parámetros

---

### vía\_acceso

Especifica el directorio donde el cliente almacena los registros de cambios persistentes para operaciones de copia de seguridad diferencial de instantánea. Si no especifica la opción snapdiffchangelogdir, el cliente utiliza el directorio donde está instalado el cliente. El directorio de instalación predeterminado es:


 Sistemas operativos Linux

```
/opt/tivoli/tsm/client/ba
```


 Sistemas operativos Windows

```
C:\Archivos de programa\Tivoli\TSM\baclient
```

El nombre exacto del archivo de registro de cambios está en el formato siguiente:

 Sistemas operativos Linux

```
snapdiff_change_log_dir/TsmSnapDiff/.TsmSnapdiffChangeLogs/NetAppFiler/  
SnapdiffChangeLog__NombreVolumen__.tsmDB
```


 Sistemas operativos Windows

```
snapdiff_change_log_dir\TsmSnapDiff\TsmSnapdiffChangeLogs\NetAppFiler\  
SnapdiffChangeLog__NombreVolumen__.tsmDB
```

donde:

- *snapdiff\_change\_log\_dir* es el nombre del directorio para almacenar los registros de cambios diferenciales de instantánea, según lo especificado por la opción snapdiffchangelogdir.
- *NetAppFiler* es el nombre de host o la dirección IP de la máquina virtual de almacenamiento (SVM) del servidor de gestión de clústeres o el servidor de archivos 7-mode.
- *NombreVolumen* es el volumen que desea proteger.

También se crea un archivo de bloqueo para evitar que copias de seguridad diferenciales de instantánea diferentes ejecutados al mismo tiempo actualicen el archivo de registro de cambios.


 Sistemas operativos Windows En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de unidad:


```
\\computer7\C$\tsmdata
```

## Ejemplos

---


Archivo de opciones:

 Sistemas operativos Linux snapdiffchangelogdir /tmp/tsmdata

 Sistemas operativos Windows snapdiffchangelogdir c:\tsmdata

Línea de mandatos:

 Sistemas operativos Linux -snapdiffchangelogd=/tmp/tsmdata

 Sistemas operativos Windows -snapdiffchangelogd="c:\tsmdata"



## Referencia relacionada:

Diffsnapshot

Snapdiff

 Sistemas operativos Linux  Sistemas operativos Windows

## Snapdiffhttps

---

Especifique la opción `snapdiffhttps` para utilizar una conexión HTTPS segura para comunicarse con un archivador NetApp durante una copia de seguridad diferencial de instantáneas.

Al especificar esta opción, el cliente de archivado de copia de seguridad puede establecer una sesión de administración segura con el archivador de NetApp independientemente de si está habilitado o no el acceso de administración de HTTP en el archivador NetApp.

Importante: El protocolo de comunicación predeterminado que utiliza el cliente de archivado de copia de seguridad para establecer la sesión de administración con el archivador NetApp es HTTP. Para utilizar una conexión HTTPS segura, debe especificar la opción `snapdiffhttps` siempre que se ejecuta una copia de seguridad diferencial de instantáneas.


Restricciones:


Las siguientes restricciones se aplican a copias de seguridad diferencias instantáneas con HTTPS:

- La conexión HTTPS sólo se utiliza para transmitir datos de forma segura a través de la sesión de administración entre el cliente de archivado de copia de seguridad y el archivador de NetApp. Los datos de la sesión de administración incluyen información como credenciales del archivador, información de instantánea y los nombres de archivo y los atributos que se generan mediante el proceso de diferenciación de instantáneas. La conexión HTTPS no se utiliza para transmitir datos de archivos normales a los que se accede en el archivador mediante el cliente a través de la compartición de archivos. La conexión HTTPS tampoco se aplica a los datos de archivos normales transmitidos mediante el cliente al servidor de IBM Spectrum Protect a través del protocolo cliente/servidor de IBM Spectrum Protect normal.
- La opción `snapdiffhttps` no se aplica a vFilers porque el protocolo HTTPS no está admitido en NetApp vFiler.
- La opción `snapdiffhttps` sólo está disponible utilizando la interfaz de línea de mandatos. No está disponible para su utilización con la GUI del cliente de archivado de copia de seguridad.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows.

 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

## Archivo de opciones

---

Esta opción sólo es válida en la interfaz de línea de mandatos. No puede especificarla en un archivo de opciones del cliente.

## Sintaxis

---

```
>>-SNAPDIFFHTTPS-----<<
```


## Parámetros


---

No hay parámetros para esta opción.

## Ejemplos


---

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux Emita el mandato siguiente en un sistema Linux, con un sistema de archivos montado en NFS `/vol/vol1` alojado en el servidor de archivos `homestore.example.com`, donde `/net/home1` es el punto de montaje de `/vol/vol1`.


```
dsmc incr /net/home1 -snapdiff -snapdiffhttps
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Emita el siguiente mandato en un sistema Windows con un recurso de red compartido `\\netapp1\vol1`, donde `netapp1` es un archivador.

```
dsmc incr \\netapp1\vol1 -snapdiff -snapdiffhttps
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Emita el siguiente mandato en un sistema Windows con un recurso compartido de red \\netappl.example.com\petevol montado en la unidad v:, donde netappl.example.com es un archivador.


```
dsmc incr v: -snapdiff -snapdiffhttps
```


```
IBM Spectrum Protect
Interfaz de línea de mandatos del cliente de copia de
seguridad/archivado
  Versión de cliente 8, release 1, nivel 0.0
  Fecha/hora del cliente: 12/09/2016 15:36:53
(c) Copyright by IBM Corporation y otros 1990, 2016. Reservados todos los derechos.
```

```
Nombre de nodo: THINKCENTRE
Sesión establecida con el servidor
BARKENSTEIN_SERVER1: Windows
  Versión de servidor 8, release 1, nivel 0.0
  Fecha/hora de servidor: 12/09/2016 15:36:53  Último acceso: 12/09/2016 11:21:14
```

```
Incremental por diferencia de instantáneas del volumen 'v:'
Conectado al archivador de NetApp netappl.example.com
como usuario pete a través de HTTPS
NetApp Release 8.1.1RC1 7-Mode: Jue 31 may 21:30:59 PDT 2012
Realización de una copia de seguridad diferencial de
instantánea de volumen
'\netappl.example.com\petevol'
Se está creando la instantánea de diferencia.
Utilizando la instantánea base 'TSM_THIN5086B9441A1F8_PETEVOL' con la indicación de fecha y hora
12/09/2016
15:36:53
Utilizando la instantánea diferencial 'TSM_THIN5086B9772AF8_PETEVOL' con la indicación de fecha y
hora 12/09/2016
15:37:44
La copia de seguridad incremental de
'\netappl.example.com\petevol' se ha realizado correctamente
```

#### Conceptos relacionados:

 Sistemas operativos Linux Copia de seguridad diferencial de la instantánea con una conexión HTTPS

 Sistemas operativos Windows Copia de seguridad diferencial de la instantánea con una conexión HTTPS



#### Referencia relacionada:



Snapdiff



## Snapshotcachesize

---

Utilice la opción snapshotcachesize para especificar un tamaño adecuado para crear una instantánea.



 Sistemas operativos AIX  Sistemas operativos Linux Se necesita una estimación de tamaño adecuada para almacenar los bloques de datos originales de los datos modificados y eliminados del instante específico en que se tomó la instantánea.

 Sistemas operativos AIX  Sistemas operativos Linux Para archivado o copia de seguridad de archivos basados en instantánea, utilice la opción snapshotcachesize con la opción include.fs, o bien en la sección del servidor en el archivo dsm.sys.

 Sistemas operativos AIX  Sistemas operativos Linux Para realizar copias de seguridad de imagen basada en instantánea, utilice la opción snapshotcachesize con el mandato backup image, la opción include.image o bien en el archivo dsm.sys.



## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Linux Esta opción *sólo* es válida para los clientes AIX y Linux. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux Especifique esta opción en la stanza de servidor, en el archivo dsm.sys. Puede establecer esta opción en la ficha Imagen-Instantánea del editor de preferencias.

## Sintaxis

---

```
>>-SNAPSHOTCACHESize-- --size-----<<
```

## Parámetros

---

 Sistemas operativos AIX  Sistemas operativos Linux

size




Especifica un tamaño adecuado para crear la instantánea con el fin de almacenar los bloques de datos originales de los datos modificados y eliminados del instante específico en que se tomó la instantánea. El valor es el porcentaje del tamaño del sistema de archivos que se cambia debido a la actividad del sistema de archivos. El rango de valores oscila entre 1 y 100 por cien. Para AIX JFS2 y Linux el valor predeterminado es el 100 por cien del tamaño del sistema de archivos. Si no se dispone de una cantidad suficiente de espacio libre para crear la instantánea, el mandato fallará y mostrará un mensaje de error. A continuación, podrá incrementar el tamaño del grupo de volúmenes o bien volver a intentar la operación. Si la práctica le ha demostrado que para la actividad del sistema de archivos JFS2 de AIX no necesitará un tamaño de instantánea del 100 por cien, puede ajustar el valor con más precisión.

 Sistemas operativos AIX  Sistemas operativos Linux

## Ejemplos

---

Archivo de opciones:

```
snapshotcachesize 95
 Sistemas operativos AIX AIX only: include.fs /kalafs1
snapshotproviderfs=JFS2 snapshotcachesize=95
 Sistemas operativos AIX AIX only: include.image /kalafs2
snapshotcachesize=95
 Sistemas operativos Linux Linux only: include.image /linuxfs1
snapshotcachesize=100
```

Línea de mandatos:


```
-snapshotcachesize=95
```

 Sistemas operativos AIX  Sistemas operativos Windows

## Snapshotproviderfs

---


Utilice la opción `snapshotproviderfs` para habilitar las operaciones de archivado y copia de seguridad de archivo basadas en instantáneas, y para especificar un proveedor de instantáneas.


 Sistemas operativos AIX Debe ser un usuario root para poder realizar una operación de archivado o de copia de seguridad de archivos basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.

 Sistemas operativos AIX  Sistemas operativos Windows

## Clientes soportados


---


 Sistemas operativos AIX Esta opción es válida solo para los clientes AIX. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX Especifique esta opción en la stanza del servidor del archivo de opciones del sistema, `dsm.sys`, con el fin de habilitar instantáneas para todos los sistemas de archivos JFS2 del cliente. Puede alterar temporalmente la opción para todos los clientes de una operación específica si indica esta opción en la línea de mandatos de archivado y copia de seguridad. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia `include.fs` en el archivo `dsm.sys`. También puede establecer esta opción mediante el editor de preferencias.

 Sistemas operativos Windows Especifique esta opción en el archivo de opciones del cliente, `dsm.opt`, para habilitar las instantáneas. Puede alterar temporalmente la opción para todos los clientes de una operación específica si indica esta opción en la línea de mandatos de archivado y copia de seguridad. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia `include.fs` en el archivo `dsm.opt`. También puede establecer esta opción mediante el editor de preferencias.

## Sintaxis

---


```
>>-SNAPSHOTPROVIDERfs-- --value-----><
```


## Parámetros


---


value

Especifique uno de los valores siguientes:


 Sistemas operativos AIXJFS2

 Sistemas operativos AIXEspecifica que desea realizar una operación de archivado o copia de seguridad de archivos basada en instantáneas mientras el sistema de archivos está disponible para otras aplicaciones del sistema. *Sólo* es válido para los sistemas de archivos JFS2 en clientes AIX.


 Sistemas operativos WindowsVSS

 Sistemas operativos WindowsIndica que VSS se debe usar para ofrecer compatibilidad con OFS.

 Sistemas operativos AIXNONE

 Sistemas operativos AIXEspecifica que no se deben utilizar instantáneas. De este modo se realizará una operación de archivado o copia de seguridad de archivos mediante el sistema de archivos especificado. Éste es el valor predeterminado.


 Sistemas operativos WindowsNONE

 Sistemas operativos WindowsEspecifica que no se debe usar un proveedor de instantáneas, ya que así se desactivaría la compatibilidad con OFS. Éste es el valor predeterminado.

## Ejemplos


---

 Sistemas operativos AIXArchivo de opciones:

 Sistemas operativos AIX


```
snapshotproviderfs JFS2
include.fs /kalafsl snapshotproviderfs=JFS
```


 Sistemas operativos WindowsArchivo de opciones:


 Sistemas operativos Windows




```
snapshotproviderfs VSS
include.fs d: snapshotproviderfs=vss
```

 Sistemas operativos AIXLínea de mandatos:

 Sistemas operativos AIX-SNAPSHOTPROVIDERfs=JFS2

 Sistemas operativos WindowsLínea de mandatos:



 Sistemas operativos Windows-SNAPSHOTPROVIDERfs=VSS




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Snapshotproviderimage

---



Utilice la opción `snapshotproviderimage` para activar la copia de seguridad de imágenes basada en instantánea y para especificar un proveedor de instantáneas.


 Sistemas operativos AIX  Sistemas operativos LinuxDebe ser usuario root para realizar una operación de copia de seguridad de imagen basada en instantáneas. Si no es usuario root, la operación fallará y mostrará un mensaje de error.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Clientes soportados



---

 Sistemas operativos AIX  Sistemas operativos LinuxEsta opción es válida solo para los clientes AIX y Linux. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.


 Sistemas operativos WindowsEsta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos LinuxEspecifique esta opción en la stanza del servidor del archivo de opciones del sistema, `dsm.sys`, con el fin de habilitar instantáneas para todos los sistemas de archivos del cliente. Puede alterar temporalmente la

opción para todos los clientes de una operación específica si indica esta opción para el mandato backup image en la línea de mandatos. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia include.image en el archivo dsm.sys. También puede establecer esta opción mediante el editor de preferencias.

 Sistemas operativos WindowsEspecifique esta opción en el archivo de opciones del cliente, dsm.opt, con el fin de habilitar instantáneas para todos los sistemas de archivos del cliente. Puede alterar temporalmente la opción para todos los clientes de una operación específica si indica esta opción para el mandato backup image en la línea de mandatos. También puede alterar temporalmente la opción para todos los clientes de un sistema de archivos específico mediante la sentencia include.image en el archivo dsm.opt. También puede establecer esta opción mediante el editor de preferencias.

## Sintaxis

---


```
>>-SNAPSHOTPROVIDERImage-- --value-----><
```


## Parámetros


---


value


Especifique uno de los valores siguientes:


 Sistemas operativos AIXJFS2

 Sistemas operativos AIXEspecifica que desea realizar una copia de seguridad de imágenes basada en instantánea mientras el sistema de archivos está disponible para otras aplicaciones del sistema. Éste es el valor predeterminado para los sistemas de archivos JFS2. *Sólo* es válido para los clientes AIX.



 Sistemas operativos LinuxLINUX\_LVM


 Sistemas operativos LinuxEspecifica que desea realizar una copia de seguridad de imágenes basada en instantánea mientras el sistema de archivos está disponible para otras aplicaciones del sistema. Es el valor predeterminado para los sistemas de archivos que residen en los volúmenes lógicos que ha creado el Gestor de volúmenes lógicos de Linux. *Sólo* es válido para los clientes Linux.


 Sistemas operativos WindowsVSS

 Sistemas operativos WindowsIndica que el VSS se debe usar para ofrecer compatibilidad con la imagen en línea.

 Sistemas operativos AIX  Sistemas operativos LinuxNONE



 Sistemas operativos AIX  Sistemas operativos LinuxEspecifica que no desea realizar una operación de copia de seguridad de imágenes basada en instantánea. De este modo se realizará una operación de copia de seguridad de imágenes estática mediante el sistema de archivos especificado. Es el valor predeterminado para los sistemas de archivos distintos de JFS2 de AIX y LVM de Linux.

 Sistemas operativos WindowsNONE

 Sistemas operativos WindowsEspecifica que no se debe utilizar un proveedor de instantáneas. De este modo se desactiva la compatibilidad de imagen en línea. Éste es el valor predeterminado.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux

```
snapshotprovideri JFS2
include.image /kalafs1 snapshotprovideri=JFS2
```



 Sistemas operativos WindowsArchivo de opciones:

 Sistemas operativos Windows

```
snapshotprovideri VSS
include.image d: snapshotprovideri=vss
```

Línea de mandatos:


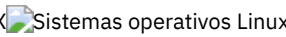

```
-SNAPSHOTPROVIDERImage=NONE
```

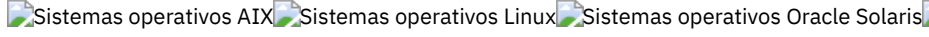
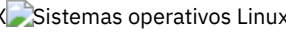


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows


## Snapshotroot


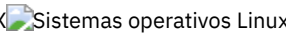

---


Utilice la opción snapshotroot con los mandatos incremental, selective o archive con una aplicación de un proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local a los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris La opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de los sistemas de archivos montados NFS. Tanto la especificación de copia de seguridad (origen) como el valor `snapshotroot` pueden ser una especificación de archivo montado en NFS. Por ejemplo, la opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de un sistema de archivos NFS alojado en un almacenamiento conectado a red (NAS) que dé soporte a las instantáneas.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Esta opción debe utilizarse con una copia de seguridad incremental del volumen de archivador NAS en lugar de una copia incremental simple o incremental con `snapshotroot` siempre que el archivador NAS esté ejecutando ONTAP V7.3 por motivos de rendimiento. Las opciones `snapdiff` y `snapshotroot` no deben utilizarse conjuntamente.

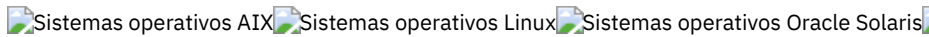
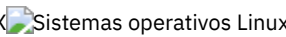


 Sistemas operativos Windows La opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de los sistemas de archivos montados en recursos de red compartidos. Tanto la especificación de copia de seguridad (origen) como el valor `snapshotroot` pueden ser una especificación de archivo montado en recursos de red compartidos. Por ejemplo, la opción `snapshotroot` puede utilizarse para realizar la copia de seguridad de un sistema de archivos de recursos de red compartido alojado en un almacenamiento conectado a red (NAS) que dé soporte a las instantáneas.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris En el siguiente ejemplo, `filesystem test495` se ha montado en NFS desde un archivador NAS `philo` y `/philo/test945/.snapshot/backupsnap` representa la instantánea que se ha creado en el archivador NAS.


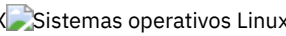

 Sistemas operativos Windows En el siguiente ejemplo, `c:\snapshots\snapshot.0` se ha montado en los recursos de red compartidos desde un archivador NAS y `\\florance\c$` representa la instantánea que se ha creado en el archivador NAS.

 Sistemas operativos Windows


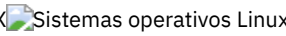

```
dsmc incr \\florance\C$ -snapshotroot=c:\shapshots
\snapshot.0
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows También puede especificar un directorio con la opción `snapshotroot` al realizar la copia de seguridad de cada juego de archivos como un espacio de archivos individual.


La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, solo para gestionar los datos que ha creado una instantánea de volumen.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Por ejemplo, imaginemos que una aplicación toma una instantánea del sistema de archivos `/usr` y que la monta como `/snapshot/day1`. Si realiza la copia de seguridad de estos datos mediante la utilización del siguiente mandato, en el servidor se creará un espacio de archivos exclusivo denominado `/snapshot/day1`.


```
dsmc incremental /snapshot/day1
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Sin embargo, puede que desee asociar los datos de la instantánea a los datos que ya se han procesado para el sistema de archivos `/usr`. Mediante la utilización de la opción `snapshotroot`, puede asociar los datos al espacio de archivos que corresponde al sistema de archivos `/usr` en el servidor de IBM Spectrum Protect:


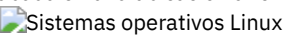

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
```

 Sistemas operativos Windows Por ejemplo, imaginemos que una aplicación que toma una instantánea de la unidad `c:` y la monta como el punto de unión NTFS `\\florence\c$\snapshots\snapshot.0`. Si realiza la copia de seguridad de estos datos mediante la utilización del siguiente mandato, en el servidor se creará un espacio de archivos exclusivo denominado `\\florence\c$\snapshots\snapshot.0`.

```
dsmc incremental \\florence\c$\snapshots\snapshot.0
```

 Sistemas operativos Windows Sin embargo, puede que desee asociar los datos de la instantánea a los datos que ya se han procesado para la unidad `c:` (`\\florence\c$`). Mediante la utilización de la opción `snapshotroot`, puede asociar los datos al espacio de archivos que corresponde a la unidad `c:` (`\\florence\c$`) en el servidor de IBM Spectrum Protect :



```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
-o-
dsmc incr \\florence\c$ -snapshotroot=\\florence\c$\snapshots\
snapshot.0
```

Con posterioridad, otro día, puede realizar la copia de seguridad de una instantánea grabada en una ubicación alternativa, pero gestionada en el mismo espacio de archivos en el servidor:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
dsmc incremental /usr -snapshotroot=/snapshot/day2
```

## Sistemas operativos Windows

```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.1
```




Puede realizar copias de seguridad incrementales, copias de seguridad selectivas u operaciones de archivado de un único directorio, de una estructura de directorios o de un único archivo utilizando la opción `snapshotroot`. En todos los casos, la opción `snapshotroot` debe identificar la raíz del volumen lógico que la instantánea ha creado. Por ejemplo:  Sistemas operativos AIX  Sistemas operativos Linux

## Sistemas operativos Oracle Solaris


```
dsmc incremental /usr/dir1/* -subdir=yes
  -snapshotroot=/snapshot/day1
dsmc selective /usr/dir1/sub1/file.txt
  -snapshotroot=/snapshot/day1
dsmc archive /usr/dir1/sub1/*.txt
  -snapshotroot=/snapshot/day1
```

## Sistemas operativos Windows

```
dsmc incr c:\dir1\* -subdir=yes -snapshotroot=\\florence\c$\
 snapshots\snapshot.1
dsmc sel c:\dir1\sub1\file.txt -snapshotroot=\\florence\c$\
 snapshots\snapshot.1
dsmc archive c:\mydocs\*.doc -snapshotroot=\\florence\c$\
 snapshots\snapshot.1
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si desea incluir o excluir especificaciones de archivo concretas, las sentencias de inclusión y exclusión deben contener el nombre del sistema de archivos que era el origen de la instantánea (el sistema de archivos `/usr`) y no el nombre del destino de la instantánea (`/snapshot/day1`). Esto le permite conservar un conjunto de sentencias de inclusión y exclusión en el que no se considera el nombre del volumen lógico en el que se graba la instantánea. A continuación, se muestran ejemplos de sentencias de inclusión y exclusión.

```
include /usr/dir1/*.txt lyrmgmtclass
exclude /usr/mydocs/*.txt
```

 Sistemas operativos Windows Si desea incluir o excluir especificaciones de archivo concretas, las sentencias de inclusión y exclusión deben contener el nombre del sistema de archivos que era el origen de la instantánea (la unidad `c:`) y no el nombre del destino de la instantánea (`\\florence\c$\snapshots\snapshot.1`). Esto le permite conservar un conjunto de sentencias de inclusión y exclusión en el que no se considera el nombre del volumen lógico en el que se graba la instantánea. A continuación, se muestran ejemplos de sentencias de inclusión y exclusión.

```
include c:\dir1\..\*.txt lyrmgmtclass
exclude \\florence\c$\mydocs\*.doc
```




Las sentencias de inclusión/exclusión siguientes no son válidas, pues contienen el nombre de la instantánea:

## Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris

```
include /snapshot/day1/dir1/*.txt lyrmgmtclass
exclude /snapshot/day1/mydocs/*.txt
```

## Sistemas operativos Windows


```
include \\florence\c$\snapshots\snapshot.1\dir1\...\
 *.txt lyrmgmtclass
exclude \\florence\c$\mydocs\*.doc
```

Para una copia de seguridad incremental o selectiva, o para una operación de archivado, debe utilizar la opción `snapshotroot` con una única especificación de archivo. No puede especificar varias especificaciones de archivo o ninguna especificación de archivo. Por ejemplo, estos mandatos son válidos:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
dsmc incremental /usr -snapshotroot=/snapshot/day1
dsmc incremental /usr/dir1/* -snapshotroot=/snapshot/day1
```

## Sistemas operativos Windows

```
dsmc incr c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
dsmc incr c:\dir1\* -snapshotroot=\\florence\c$\snapshots\
 snapshot.0
```


El mandato siguiente no es válido porque contiene dos especificaciones de archivo:  Sistemas operativos AIX

## Sistemas operativos Linux Sistemas operativos Oracle Solaris

```
dsmc incremental /usr/dir1/* /home/dir2/*
  -snapshotroot=/snapshot/day1
```

## Sistemas operativos Windows

```
dsmc incr c:\dir1\* e:\dir1\* -snapshotroot=\\florence\c$\snapshots\snapshot.0
```

El mandato siguiente no es válido porque no contiene ninguna especificación de archivo:  Sistemas operativos AIX





## Sistemas operativos Linux Sistemas operativos Oracle Solaris

```
dsmc incremental -snapshotroot=/snapshot/day1
```

## Sistemas operativos Windows

```
dsmc incr -snapshotroot=\\florence\c$\snapshots\snapshot.0
```





### Notas:

1. Asegúrese de que la opción snapshotroot haga referencia a una instantánea del volumen correcto. Asegúrese de que la ubicación snapshotroot haga referencia a la raíz de la instantánea. Si no se siguen estas reglas, es posible que se produzcan resultados imprevisibles, como la caducidad incorrecta de los archivos.
2. Si especifica la opción filelist y la opción snapshotroot, se asumirá que todos los archivos especificados en la opción filelist están en el mismo sistema de archivos. Si hay entradas en filelist en un sistema de archivos diferente, serán ignoradas y se registrará un error. Si filelist contiene archivos creados en el sistema de archivos después de tomar la instantánea, se ignorarán dichas entradas y se registrará el error.
3.  Sistemas operativos Windows No puede utilizar la opción snapshotroot con ningún mandato de copia de seguridad, como backup image o backup systemstate, etc.
4.  Sistemas operativos Linux  Sistemas operativos Windows No puede utilizar la opción snapshotroot con la opción snapdiff.
5.  Sistemas operativos Windows Utilice la opción snapshotroot con precaución si está utilizando la función de copia de seguridad con diario de IBM Spectrum Protect. Como no existe coordinación entre el diario de IBM Spectrum Protect y el proveedor de instantáneas de otros fabricantes (VSS), puede producirse un comportamiento no deseado con las notificaciones por diario recibidos después de que se produzca la instantánea. Por ejemplo, no es posible realizar una copia de seguridad de los archivos, o se puede realizar una copia de seguridad redundante en el servidor de IBM Spectrum Protect.
6. Puede utilizar la opción snapshotroot con las opciones preschedulecmd y postschedulecmd o en un script automatizado que se ejecute con el planificador de cliente.

## Clientes soportados

---

Esta opción es válida para los clientes siguientes:

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Clientes UNIX y Linux excepto Mac OS X.
-  Sistemas operativos Windows Todos los clientes Windows.

## Sintaxis

---

```
>>-SNAPSHOTRoot = - --snapshot_volume_name-----<<
```

## Parámetros

---




snapshot\_volume\_name


Especifica la raíz del volumen lógico que ha creado la aplicación de instantáneas de otro proveedor.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Línea de mandatos:

```
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris dsmc incremental /usr -  
SNAPSHOTRoot=/snapshot/day1
```

 Sistemas operativos Windows Línea de mandatos:

```
 Sistemas operativos Windows dsmc incr c: -SNAPSHOTRoot=\\florence\c$\snapshots\snapshot.0
```

## Srvoptsetencryptiondisabled

---

La opción srvoptsetencryptiondisabled permite que el cliente ignore las opciones de cifrado en el conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect.



Si la opción está establecida en yes en el archivo de opciones del cliente, el cliente ignorará las siguientes opciones en un conjunto de opciones del cliente desde el servidor:

- encryptkey generate
- exclude.encrypt
- include.encrypt

## Clientes soportados





---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones del cliente (dsm.sys) de una stanza de servidor.

## Sintaxis

---

```
>>-SRVOPTSETENCrptiondisabled--+-no--.  
                                     |-----|  
                                     '-yes-'<
```

## Parámetros

---

yes

El cliente de copia de seguridad y archivado pasa por alto los valores de las opciones de cifrado listadas en un conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect.

no

El cliente de copia de seguridad y archivado procesa los valores de las opciones de cifrado listadas en un conjunto de opciones del cliente desde el servidor de IBM Spectrum Protect. Éste es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
srvoptsetencryptiondisabled no
```

Línea de mandatos:

No se aplica.

## Srvprepostscheddisabled

---

La opción `srvprepostscheddisabled` especifica si ha de impedirse que los mandatos de preplanificación y de postplanificación que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas.

La opción `srvprepostscheddisabled` puede utilizarse con las opciones `schedcmddisabled` y `srvprepostscheddisabled` para desactivar la posibilidad de que el administrador de IBM Spectrum Protect ejecute mandatos del sistema operativo no deseados en un nodo cliente.





## Clientes soportados


---

Esta opción es válida para todos los clientes de copia de seguridad y archivado que utilizan el planificador cliente de IBM Spectrum Protect. El servidor no puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Especifique esta opción en el archivo `dsm.sys` dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador Planificador del editor de preferencias, en la sección de Mandato de planificación.

 Sistemas operativos Windows Especifique esta opción en el archivo de opciones del cliente (dsm.opt) para el planificador. Puede establecer esta opción en el separador Planificador del editor de preferencias, en la sección de Mandato de planificación.

## Sintaxis

---

```
                .-No--.
>>-SRVPREPOSTSCHeddisabled-----<<
                '-Yes-'
```

## Parámetros

---

### No

Especifica que el cliente ha de permitir que los mandatos de preplanificación y de postplanificación que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato de preplanificación o de postplanificación, el mandato que ha definido el administrador modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Éste es el valor predeterminado.

### Yes

Especifica que el cliente ha de impedir que los mandatos de preplanificación y de postplanificación que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato de preplanificación o de postplanificación, el mandato que ha definido el administrador *no* modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Esta opción se puede utilizar conjuntamente con las opciones `schedcmddisabled` y `srvprepostscheddisabled`.

## Ejemplos

---

Archivo de opciones:

```
srvprepostscheddisabled yes
```

Línea de mandatos:

No se aplica.

 Sistemas operativos Linux  Sistemas operativos Windows

## Srvprepostsnapdisabled


---


La opción `srvprepostsnapdisabled` especifica si ha de impedirse que los mandatos de previos y posteriores a la instantánea que ha especificado el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea.

La opción `srvprepostsnapdisabled` puede utilizarse con las opciones `schedcmddisabled` y `srvprepostsnapdisabled` para desactivar la posibilidad de que el administrador de IBM Spectrum Protect ejecute mandatos del sistema operativo no deseados en un nodo cliente.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para los clientes Linux que admiten el mandato de copia de seguridad de instantánea. El servidor no puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para los clientes Windows que admiten el mandato de copia de seguridad de instantánea. El servidor no puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos Linux Especifique esta opción en el archivo `dsm.sys` dentro de una stanza de servidor para el planificador. Puede establecer esta opción en el separador Instantánea del editor de preferencias, en la sección Opciones de instantáneas.

 Sistemas operativos Windows Especifique esta opción en el archivo de opciones del cliente (`dsm.opt`) para el planificador. Puede establecer esta opción en el separador Instantánea del editor de preferencias, en la sección Opciones de instantáneas.

## Sintaxis

---

```
                .-No--.
>>-SRVPREPOSTSNAPdisabled-----<<
                '-Yes-'
```

## Parámetros

---

No

Especifica que el cliente ha de permitir que los mandatos previos y posteriores a la instantánea que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato previo o posterior a la instantánea, el mandato que ha definido el administrador modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Éste es el valor predeterminado.

Yes

Especifica que el cliente ha de impedir que los mandatos previos y posteriores a la instantánea que ha definido el administrador de IBM Spectrum Protect se ejecuten en el sistema cliente al realizar operaciones planificadas de copia de seguridad de instantánea. Si el cliente y el administrador de IBM Spectrum Protect, ambos, han definido un mandato previo o posterior a la instantánea, el mandato que ha definido el administrador *no* modificará temporalmente el mandato correspondiente que se ha definido en el archivo de opciones del cliente. Esta opción puede utilizarse junto con las opciones `schedcmddisabled` y `srvprepostsnapdisabled`.

## Ejemplos

---

Archivo de opciones:

```
srvprepostsnapdisabled yes
```

Línea de mandatos:

No se aplica.

## Ssl

---

Utilice la opción `ssl` para habilitar Secure Sockets Layer (SSL) para proporcionar comunicaciones de servidor y de cliente seguro. Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.1 o V8 anterior, o V7.1.7 o anterior, el cliente determina si SSL está habilitado. Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.2 o posterior, siempre se utiliza SSL y esta opción controla si se cifran o no los datos de objeto. Por motivos de rendimiento, puede ser aconsejable no cifrar los datos de objeto.





## Clientes soportados


---

Esta opción es válida para todos los clientes soportados.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. También puede establecer esta opción en el separador Comunicación del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). También puede establecer esta opción en el separador Comunicación del editor de preferencias.

## Sintaxis

---

```
. -No- .  
>>-SSL-+-+----->>  
' -Yes- '
```

## Parámetros para comunicarse con un servidor IBM Spectrum Protect V8.1.1 o V8 anterior, y V7.1.7 o anterior.

---

No

Especifica que el cliente de copia de seguridad y archivado no utiliza SSL para cifrar la información. No es el valor predeterminado.

Yes

Especifica que el cliente de copia de seguridad y archivado utiliza SSL para cifrar la información.

Para habilitar SSL, especifique `SSL Yes` y cambie el valor de la opción `TCPSPORT`. Cambiar el valor de la opción `TCPSPORT` es normalmente necesario porque el servidor de IBM Spectrum Protect normalmente está configurado para escuchar conexiones SSL en un puerto distinto.

## Parámetros para comunicarse con un servidor IBM Spectrum Protect V8.1.2 y posterior.

---

No

Especifica que el cliente de archivado y copia de seguridad no utiliza SSL para cifrar datos de objeto cuando se comunica con el servidor. Toda la información restante se cifra. No es el valor predeterminado.

Yes

Especifica que el cliente de archivado y copia de seguridad utiliza SSL para cifrar toda la información, incluidos los datos de objeto, cuando se comunica con el servidor.

Para utilizar SSL para todos los datos, especifique SSL Sí.

## Ejemplos

---

Archivo de opciones:

```
ssl yes
```

Línea de mandatos:

No se aplica.

## Sslacceptcertfromserv

---

Utilice la opción `sslacceptcertfromserv` para controlar si el cliente de archivado y copia de seguridad o la aplicación de API aceptan y confían en el certificado público de SSL (Capa de sockets seguros) del servidor de IBM Spectrum Protect la primera vez que se conectan. Esta opción sólo se aplica la primera vez que el cliente de archivado y copia de seguridad o la aplicación de API se conectan al servidor de IBM Spectrum Protect. Una vez que el certificado público SSL se ha aceptado, los cambios futuros en el certificado no se aceptarán automáticamente y deben importarse manualmente al cliente de archivado y copia de seguridad. Puede utilizar esta opción solo para conectarse a un servidor IBM Spectrum Protect V8.1.2 y posterior.





## Clientes soportados

---

Esta opción es válida para todos los clientes soportados.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-SSLACCEPTCERTFROMSERV--+-Yes-+-----><
                              '-No--'
```

## Parámetros

---

Yes

Especifica que el cliente de archivado y copia de seguridad no acepta automáticamente el certificado público del servidor de IBM Spectrum Protect. Yes es el valor predeterminado.

No

Especifica que el cliente de archivado y copia de seguridad no acepta automáticamente el certificado público del servidor IBM Spectrum Protect.

Para inhabilitar `SSLACCEPTCERTFROMSERV`, especifique `sslacceptcertfromserv no`.

## Ejemplos

---

Archivo de opciones:

```
sslacceptcertfromserv no
```

Línea de mandatos:

No se aplica.

## Ssldisablelegacytls

---

Utilice la opción `ssldisablelegacytls` para no permitir el uso de protocolos SSL que son inferiores a TLS 1.2.





## Cientes soportados


---

Esta opción es válida para todos los clientes soportados.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Establezca esta opción en el archivo `dsm.sys`. También puede establecer esta opción en la GUI seleccionando el recuadro de selección Requerir TLS 1.2 o superior en el separador Comunicación del editor Preferencias. No puede establecer esta opción en la línea de mandatos.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`). También puede establecer esta opción en la GUI seleccionando el recuadro de selección Requerir TLS 1.2 o superior en el separador Comunicación del editor Preferencias. No puede establecer esta opción en la línea de mandatos.

## Sintaxis

---

```
>>>-SSLDISABLELEGACYtls-+-----+-----<<<
                          .-No--.
                          '-Yes-'
```

## Parámetros

---

No

Especifica que el cliente de copia de seguridad y archivado no necesita TLS 1.2 para sesiones de SSL. Permite la conexión en TLS 1.1 y protocolos SSL inferiores. Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.1 o V8 anterior, o V7.1.7 o anterior, No es el valor predeterminado.

Yes

Especifica que el cliente de copia de seguridad y archivado requiere que todas las sesiones de SSL utilicen el protocolo de TLS 1.2 (o superior). Cuando el cliente de archivado y copia de seguridad se comunica con un servidor IBM Spectrum Protect V8.1.2 o posterior, Sí es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:  
`ssldisablelegacytls yes`  
Línea de mandatos:  
No se aplica.

## Sslfipsmode

---

La opción `sslfipsmode` especifica si el cliente utiliza la modalidad de SSL Federal Information Processing Standards (FIPS) para comunicaciones de capa segura de sockets (SSL) con el servidor. El valor predeterminado es no.

## Cientes soportados

---

Esta opción se soporta en todos los clientes.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente. No se puede especificar como un parámetro de línea de mandatos y no se puede establecer esta opción en un conjunto de opciones de cliente.

## Sintaxis

---

```
>>>-SSLFIPSMODE = +-----+-----<<<
                  .-No--.
                  '-Yes-'
```

## Parámetros

---

No

Especifica que el cliente no utiliza la modalidad SSL FIPS para comunicaciones seguras con el cliente. La modalidad SSL FIPS solo se admite en la versión 6.3 y en versiones posteriores del servidor. Establezca esta opción de cliente en no si el cliente utiliza SSL para conectarse a un servidor que no sea V6.3 o posterior.

Yes

Especifica que el cliente utiliza la modalidad SSL FIPS para comunicaciones seguras con el cliente. Establecer esta opción en yes restringe la negociación de la sesión SSL para que utilice sólo suites de cifrado aprobadas por FIPS. La modalidad SSL FIPS solo se admite en el servidor V6.3 (o posterior).

## Ejemplo

---

Para habilitar la modalidad SSL FIPS en el cliente:

```
SSLFIPSMODE yes
```

## Sslrequired

---

La opción `sslrequired` especifica las condiciones en que SSL es o no necesario cuando el cliente inicia la sesión en el servidor o en los agentes de almacenamiento de IBM Spectrum Protect. Para habilitar realmente SSL para que las comunicaciones de cliente a servidor y de cliente a almacenamiento sean seguras, debe configurar la opción de cliente `ssl` en `yes`. Cuando se comunica con un servidor IBM Spectrum Protect V8.1.2 y posterior, esta opción ya no se aplica ya que se utiliza SSL.

## Clientes soportados

---

Esta opción está soportada para todos los clientes.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente o en la GUI, en la ficha Comunicaciones. No puede establecer esta opción en la línea de mandatos.

## Sintaxis

---

```
.-Default----.  
>>-SSLREquired+-----+-----><  
+-Yes-----+  
+-No-----+  
'-SERVERonly-'
```

## Parámetros

---

Default

Este valor indica que el SSL es necesario para proteger las comunicaciones entre el cliente y el servidor, y el cliente y los agentes de almacenamiento, si `AUTHENTICATION=LDAP` se configura en el servidor. Para proteger las comunicaciones utilizando SSL, también debe establecer `ssl=yes` en el cliente.

Si `AUTHENTICATION=LOCAL` se configura en el servidor, este valor indica que el SSL no es necesario. Aunque el SSL no es obligatorio cuando `AUTHENTICATION=LOCAL` y `sslrequired=default`, puede utilizar SSL estableciendo la opción de cliente `ssl` en `yes`.

Yes

Indica que siempre se necesita SSL para proteger las comunicaciones entre el cliente y el servidor, y entre el cliente y el almacenamiento de agentes. `sslrequired=yes` no tiene ninguna dependencia en la opción del servidor `AUTHENTICATION`. Si configura `sslrequired=yes` en el cliente, debe configurar también `ssl=yes` en el cliente.

No

Indica que no necesita utilizar SSL para proteger las comunicaciones entre el cliente y el servidor o entre el cliente y el almacenamiento de agentes. Elija esta opción solo si utiliza una red privada virtual u otro método para proteger las comunicaciones de la sesión. Todavía puede habilitar SSL configurando `ssl=yes` en el cliente; pero `sslrequired=no` especifica que SSL no es un requisito previo.

SERVERonly

Indica que se necesita SSL para comunicaciones de cliente a servidor y no para comunicaciones de servidor a almacenamiento de agentes. Para utilizar SSL para la comunicación de cliente a servidor, configure `sslrequired=serveronly` y `ssl=yes`. El valor del servidor para la opción `AUTHENTICATION` puede ser `LOCAL` o `LDAP`.

Para las comunicaciones de cliente a almacenamiento de agentes, utilice la opción de cliente `lanfreessl` para habilitar SSL.

En la tabla siguiente se describen las situaciones en las que la autenticación se realiza satisfactoriamente o presenta anomalías dependiendo de los valores de la opción `SSLREQUIRED` en el servidor, y el cliente, y el valor de la opción `ssl` en el cliente. Los resultados de la tabla presuponen que se proporcionan credenciales válidas.

Tabla 1. Efectos de los valores SSL de servidor y cliente en el éxito o el fracaso de los intentos de inicio de sesión

opción <code>SSLREQUIRED</code> (valor de servidor)	opción <code>sslrequired</code> (valor de cliente)	opción <code>ssl</code> (valor de cliente)	Éxito o anomalía de autenticación
Yes	Yes	Yes	Autenticación satisfactoria
Yes	Yes	No	Autenticación anómala; el cliente rechaza la sesión
Yes	No	Yes	Autenticación satisfactoria
Yes	No	No	Autenticación anómala; el servidor rechaza la sesión
No	Yes	Yes	Autenticación satisfactoria
No	Yes	No	Autenticación anómala; el cliente rechaza la sesión
No	No	Yes	Autenticación satisfactoria
No	No	No	Autenticación satisfactoria

En el texto siguiente se describe cómo la configuración de `SSLREQUIRED=DEFAULT` y `SSLREQUIRED=SERVERONLY` en el servidor afecta a la opción `ssl` en el cliente.

Si el servidor se configura con `SSLREQUIRED=DEFAULT` y `AUTHENTICATION=LDAP`, el cliente debe configurarse como `ssl=yes`, si no, la autenticación falla.

Si el servidor se configura con `SSLREQUIRED=DEFAULT` y `AUTHENTICATION=LOCAL`, el cliente debe configurarse como `ssl=yes` o `ssl=no`.

Si el servidor se configura con `SSLREQUIRED=SERVERONLY`, debe configurarse `ssl=yes` en el cliente. La opción de cliente `lanfreessl` se puede establecer en `yes`, para proteger la comunicación con un almacenamiento de agentes, o en `no` si las comunicaciones seguras con los almacenamientos de agentes no son necesarias.

## Ejemplos

Archivo de opciones:

```
sslrequired yes
sslrequired no
sslrequired default
sslrequired serveronly
```


Línea de mandatos:

No aplicable; no se puede establecer esta opción en la línea de mandatos.

 Sistemas operativos Linux  Sistemas operativos Windows

## Stagingdirectory


La opción `stagingdirectory` define la ubicación donde el cliente almacena los datos que genera a fin de realizar sus operaciones. Una vez finalizado el proceso se suprimen los datos.

 Sistemas operativos Windows El cliente utiliza la ubicación `stagingdirectory` para las operaciones de consulta y restauración de Active Directory. El cliente también utiliza la ubicación `stagingdirectory` para los archivos temporales cuando procesa los archivos de cliente que se han migrado con IBM Spectrum Protect HSM for Windows.

Importante: A partir de la versión 8.1.2, la opción `snappdiffchangelogdir` se utiliza para especificar la ubicación donde almacenar los registros de cambios para las operaciones de copia de seguridad diferencial de instantánea. La opción `stagingdirectory` ya no se utiliza para este propósito. Para obtener más información, consulte `Snappdiffchangelogdir`.


## Clientes soportados


 Sistemas operativos Linux Esta opción es válida para los clientes de Linux. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Cuando stagingdirectory se especifica en la línea de mandatos, modifica los valores especificados en el archivo de opciones.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Cuando stagingdirectory se especifica en la línea de mandatos, modifica los valores especificados en el archivo de opciones.

## Sintaxis


---


```
>>-STAGINGDIRectory--path-----<<
```

## Parámetros


---

vía de acceso

 Sistemas operativos Linux Especifica la vía de acceso del directorio donde el cliente graba los datos de transición. Si no se especifica ningún directorio intermedio, el cliente almacena datos temporales en el sistema de archivos temporales (normalmente /tmp).

 Sistemas operativos Windows Especifica la vía de acceso del directorio donde el cliente graba los datos de transición. Si no se especifica ningún directorio de transición, el cliente comprueba la existencia de las variables de entorno USER en el orden siguiente y utiliza la primera vía de acceso que encuentra:

1. La vía de acceso especificada por la variable de usuario TMP.
2. La vía de acceso especificada por la variable de sistema TMP.
3. La vía de acceso especificada por la variable de usuario TEMP.
4. La vía de acceso especificada por la variable de sistema TEMP.
5. El directorio del sistema Windows.




 Sistemas operativos Windows En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de unidad D\$:

```
\\computer7\D$\temp\tsmstaging
```



## Ejemplos

---



Archivo de opciones:

 Sistemas operativos Linux `stagingdirectory /usr/tsmdata`  
 Sistemas operativos Linux `stagingdirectory /private/tmp`  
 Sistemas operativos Windows `stagingdirectory c:\tsmdata`

Línea de mandatos:

 Sistemas operativos Linux `-stagingdir="/tmp/tsmtempdata"`  
 Sistemas operativos Windows `-stagingdir="e:\tsmdata"`

### Referencia relacionada:

 Sistemas operativos Windows [Query Abjects](#)  
 Sistemas operativos Windows [Restore Abjects](#)  
[Diffsnapshot](#)  
[Snapdiff](#)

### Información relacionada:

 <http://www.ibm.com/support/knowledgecenter/SSERBH>

## Subdir

---

La opción subdir especifica si desea incluir subdirectorios de los directorios especificados para el proceso.

Puede utilizar la opción subdir con los mandatos siguientes:

- archive
- delete archive
- delete backup



- Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Sistemas operativos Windows incremental
- query archive
- query backup
- restore
- restore backupset
- restore group
- retrieve
- selective

Si establece la opción `subdir` en `yes` al realizar la copia de seguridad de una vía de acceso y un archivo específicos, el cliente de copia de seguridad y archivado busca de forma recursiva en todos los subdirectorios de esa vía de acceso las instancias del archivo especificado que existan en los subdirectorios. Por ejemplo, supongamos que existe un archivo denominado `myfile.txt` en un cliente en los siguientes directorios:

```
//myfile.txt
/dir1/myfile.txt
/dir1/dir_a/myfile.txt
/dir1/dir_b/myfile.txt
```

Si se realiza una copia de seguridad selectiva del archivo, como se muestra a continuación, se realiza una copia de seguridad de todas las instancias de `myfile.txt`:

```
dsmc sel /myfile.txt -subdir=yes
```

De forma parecida, el siguiente mandato muestra todas las instancias de `myfile.txt` si especifica `subdir=yes` en el archivo de opciones de cliente o en un conjunto de opciones de cliente.

```
dsmc restore /myfile.txt -pick
```

## Clientes soportados

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

## Sintaxis

```
.-No--
>>-SUbdir--+-+-----+----->>
          '-Yes-'
```

## Parámetros

No

Los subdirectorios no se procesan. Éste es el valor predeterminado.

Yes

Los subdirectorios se procesan. Debido a que el programa de cliente busca en todos los subdirectorios de un directorio que se está procesando, el proceso puede tardar más tiempo en completarse. Especifique `yes` sólo cuando sea necesario.

Si utiliza la opción `preservepath` además de `subdir=yes`, ello puede afectar a qué subdirectorios han de procesarse.

Si un subdirectorio es un sistema de archivos montado, éste no se procesará, aunque haya especificado `subdir=yes`.

Nota:

1. Cuando ejecuta el cliente en modalidad interactiva, si utiliza la opción `-subdir=yes`, el valor persiste para todos los mandatos especificados en modalidad interactiva hasta que finalice la modalidad interactiva especificando `Quit`.
2. Si `subdir=yes` se aplica cuando restaura varios archivos, coloque un carácter delimitador de directorios al final de la especificación del archivo de destino. Si se omite el delimitador, el cliente muestra un mensaje indicando que la especificación

del archivo de destino no es válida.

3. Se recomienda incluir sólo el valor predeterminado de subdir (No) en un archivo de opciones de cliente o un conjunto de opciones de cliente.


## Ejemplos

---

Archivo de opciones:

```
subdir no
```





Línea de mandatos:

 sistemas operativos Mac OS X Para restaurar la estructura:

```
/Users/mike/dir1  
/Users/mike/dir1/file1  
/Users/mike/dir1/dir2  
/Users/mike/dir1/dir2/file1
```

especifique alguno de los mandatos siguientes:


```
dsmc rest "/Users/van/dir1/*" /Users/mike/ -su=yes  
dsmc rest "/Users/van/dir1/file*" /Users/mike/ -su=yes  
dsmc rest "/Users/van/dir1/file1*" /Users/mike/ -su=yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Para restaurar la estructura:

```
/via2/dir1  
/via2/dir1/arch1  
/via2/dir1/dir2  
/via2/dir1/dir2/arch1
```

especifique alguno de los mandatos siguientes:

```
dsmc rest "/via/dir1/*" /via2/ -su=yes  
dsmc rest "/via/dir1/arch*" /via2/ -su=yes  
dsmc rest "/via/dir1/arch1*" /via2/ -su=yes
```

 Sistemas operativos Windows Para restaurar la estructura:

```
\via2\dir1  
\via2\dir1\arch1  
\via2\dir1\dir2  
\via2\dir1\dir2\arch1
```

especifique alguno de los mandatos siguientes:

```
rest \via\dir1\* \via2\ -su=yes  
rest \via\dir1\arch* \via2\ -su=yes  
rest \via\dir1\arch1* \via2\ -su=yes
```

Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo dsm.opt, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

 Sistemas operativos Windows

## Systemstatebackupmethod

---

Utilice la opción systemstatebackupmethod para especificar qué método de copia de seguridad utilizar para realizar una copia de seguridad de la parte del grabador del sistema de los datos de estado del sistema. El método seleccionado se utiliza cuando se hace una copia de seguridad de los datos de estado del sistema.

### Clientes soportados

---

Esta opción es válida para los clientes Windows.

### Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt). Cuando se especifica en el archivo dsm.opt, esta opción afecta a las copias de seguridad de estado del sistema creadas por el mandato BACKUP SYSTEMSTATE y a los datos de estado del sistema a los

que realiza la copia de seguridad el mandato INCREMENTAL. Sin embargo, el único mandato en el que puede especificar esta opción en el mandato BACKUP SYSTEMSTATE.

## Definiciones de planificación

---

También puede especificar esta opción en el parámetro opciones de una definición de planificación en planificaciones que tienen `action=backup` y `subaction=systemstate` establecido. Definir una planificación poco frecuente con esta opción establecida en FULL asegura que se pueda realizar periódicamente una copia de seguridad completa de los datos de estado del sistema de Windows.

## Sintaxis

---

```
          .-PROGressive---.  
>>-SYSTEMSTATEBACKUPMethod--+-+-----+-----><  
          +-OPPportunistic-+  
          '-FULL-----'
```

## Parámetros

---

### PROGressive

Con el método PROGressive, la porción del grabador de sistema de los datos de estado del sistema se realiza utilizando el método de copia de seguridad incremental progresiva. Es decir, si los archivos del grabador del sistema no han cambiado desde la última copia de seguridad de estado del sistema, no se incluyen en esta copia de seguridad. Sólo se realiza copia de seguridad de los archivos de grabador de sistema que hayan cambiado. Este es el método predeterminado de realizar copias de seguridad de estado de sistema.

Este tipo de copia de seguridad del estado del sistema utiliza el menor ancho de banda de red y almacenamiento de servidor de IBM Spectrum Protect, pero aumenta la cantidad de proceso de base de datos del servidor necesario para realizar un seguimiento de los cambios.

### OPPportunistic

Con el método OPPportunistic, si alguno de los archivos del grabador del sistema han cambiado desde la última copia de seguridad de estado del sistema, se realiza copia de seguridad de todos los archivos del grabador del sistema.

Este método, al igual que el método PROGressive, también utiliza el menor ancho de banda de red y almacenamiento de servidor de IBM Spectrum Protect si los archivos del grabador del sistema no se han modificado desde la última copia de seguridad de estado del sistema. Si alguno de los archivos del grabador del sistema han cambiado desde la última copia de seguridad de estado del sistema, se realiza la copia de seguridad del grabador del sistema en su totalidad, lo cual utiliza más ancho de banda de red y almacenamiento de servidor. Con el método OPPportunistic, la cantidad de proceso de base de datos del servidor que se produce es menor que la causada por el método PROGressive.

### FULL

Cuando se especifica FULL, se realiza copia de seguridad de todos los archivos del grabador, incluso aunque no hayan cambiado desde la última copia de seguridad de estado de sistema realizada.

Este tipo de copia de seguridad de estado del sistema utiliza el mayor ancho de banda de red y almacenamiento de servidor de IBM Spectrum Protect porque se realiza copia de seguridad de todos los archivos del grabador del sistema durante cada operación de copia de seguridad de estado del sistema. Sin embargo, este método de copia de seguridad de estado de sistema provoca poco proceso de base de datos del servidor.

## Ejemplos

---

### Archivo de opciones:

```
SYSTEMSTATEBACKUPMETHOD FULL  
SYSTEMSTATEBACKUPMETHOD OPPORTUNISTIC
```

### Línea de mandatos:

```
backup systemstate -SYSTEMSTATEBACKUPMETHOD=FULL
```

## Tapeprompt

---

La opción `tapeprompt` especifica si el cliente de copia de seguridad y archivado debe esperar el montaje de la cinta cuando éste sea necesario en un proceso de copia de seguridad, archivado, restauración o recuperación, o si se debe preguntar al usuario.

En la GUI del cliente de copia de seguridad y archivado, el cuadro de diálogo Montaje de medio puede visualizar el valor `Información no disponible` en los campos Dispositivo y Etiqueta de volumen si se realiza una operación de restauración o recuperación estándar (también conocida como clásica). Este valor significa que la información sólo está disponible para operaciones de restauración o recuperación sin consulta; no en caso de una operación de restauración o recuperación estándar. El campo Dispositivo muestra el nombre del dispositivo en el que debe montarse el medio para procesar un objeto. El campo Etiqueta de volumen muestra el nombre del volumen necesario para procesar un objeto.

No se producirá ninguna solicitud de cinta durante una operación planificada, independientemente del valor especificado en la opción `tapeprompt`.

La opción `tapeprompt` puede utilizarse con los mandatos siguientes:

- `archive`
- `delete archive`
- `delete backup`
- `incremental`
- `restore`
- `retrieve`
- `selective`

Nota: El servidor también puede definir esta opción.





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en el separador General, en la casilla de verificación Preguntar antes de montar cintas del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador General, en la casilla de verificación Preguntar antes de montar cintas del Editor de preferencias.

## Sintaxis

---

```
. -No-- .  
>>-TAPEPrompt--+-----+----->>  
'-Yes-'
```

## Parámetros

---

No

No se preguntará al usuario. El servidor espera a que la cinta apropiada esté montada. Éste es el valor predeterminado. Nota: En el caso de las aplicaciones API, permite realizar copias de seguridad directamente en cinta.

Yes

Se solicita al usuario el montaje de la cinta cuando éste es necesario en una operación de copia de seguridad, archivado, restauración o recuperación. Al recibir el mensaje de solicitud, el usuario tiene la opción de esperar a que la cinta apropiada se monte, esperar siempre a que se monte una cinta, omitir un objeto determinado, omitir todos los objetos de una sola cinta, omitir todos los objetos de todas las cintas o cancelar toda la operación.

## Ejemplos

---

Archivo de opciones:  
`tapeprompt yes`  
Línea de mandatos:  
`-tape=yes`

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Tcpadminport

---

Utilice la opción `tcpadminport` para especificar un número de puerto TCP/IP por separado en el que el servidor está a la espera de las solicitudes de sesiones de cliente de administración, lo que permite establecer sesiones de administración seguras dentro de una red privada.

El valor `tcpadminport` del cliente depende de cómo se hayan configurado las opciones `tcpadminport` y `adminonclientport` del servidor de IBM Spectrum Protect. El servidor tiene un valor `tcpadminport` que indica en qué puerto debe estar el servidor a la escucha de las sesiones de administración, y el valor `adminonclientport`, que puede ser `yes` o `no`.

Si no se establece `tcpadminport` en el servidor entonces las sesiones administrativas estarán permitidas en el mismo puerto que las sesiones cliente.

Si `tcpadminport` se establece en el servidor, se permitirán las sesiones administrativas en el puerto que especifique ese valor. En este caso, si `adminonclientport yes` está en vigor, las sesiones administrativas se pueden conectar en el puerto de cliente normal o el puerto especificado por `tcpadminport`. Si `adminonclientport no` está en vigor, las sesiones de administración sólo pueden conectarse en el puerto que especifica `tcpadminport`.





## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en el separador Comunicación, en el campo Puerto de administración del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Comunicación, en el campo Puerto de administración del editor de preferencias.

## Sintaxis

---

```
>>-TCPADMINPort--+-+-----+-----<<  
                '-admin_port_address-'
```

## Parámetros

---

`admin_port_address`

Especifica el número de puerto del servidor. El valor predeterminado es el valor de la opción `tcpport`.

## Ejemplos






---

Archivo de opciones:  
`tcpadminport 1502`

## Tcpbuffsize

---

La opción `tcpbuffsize` especifica el tamaño del almacenamiento intermedio de comunicaciones TCP/IP interno utilizado para transferir datos entre el nodo cliente y el servidor. Aunque utilice más memoria, un almacenamiento intermedio de mayor tamaño puede mejorar el rendimiento en las comunicaciones.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador Comunicación, en el campo Tamaño de almacenamiento intermedio del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador Comunicación, en el campo Tamaño de almacenamiento intermedio del editor de preferencias.

## Sintaxis

---

```
>>-TCPBuffsize-- --size-----<
```

## Parámetros

---

size

Especifica el tamaño en kilobytes que se desea utilizar para la memoria intermedia de comunicaciones TCP/IP interno. El rango de valores válidos comprende los valores 1 a 512; el valor predeterminado es 32.

Según los valores de comunicación del sistema operativo, es posible que el sistema no acepte todos los valores comprendidos entre 1 y 512.

## Ejemplos

---

Archivo de opciones:

```
tcpb 32
```

Línea de mandatos:

```
-tcpbuffsize=32
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Tcpcadaddress

---

La opción `tcpcadaddress` especifica una dirección TCP/IP para `dsmcad`. Esta opción no suele ser necesaria. Utilice esta opción sólo si el nodo cliente tiene más de una dirección TCP/IP o bien si TCP/IP no es el método de comunicación predeterminado.

## Clientes soportados





---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor.





## Sintaxis


---





```
>>-TCPCADAddress-- --cad_address-----<
```


## Parámetros

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows `cad_address`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows Especifica un nombre de dominio TCP/IP de Internet o una dirección IP numérica. Si especifica una dirección IPv6, debe especificarse la opción `commmethod V6Tcpi`.

## Ejemplos

---

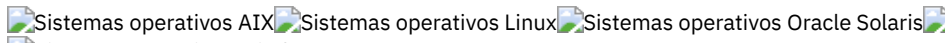




Archivo de opciones:

```
tcpcada dsmclnt.example.com
```

Línea de mandatos:

```
-tcpcadaddress=192.0.2.0
```

```
-tcpcadaddress=mycompany.example.com
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

```
-tcpcadaddress=2001:0DB8:0:0:0:0:0:0
```

Esta opción sólo es válida en la línea de mandatos inicial del programa dsmcad. No es válida con otros módulos dsm.

## Tcpclientaddress

---

La opción tcpclientaddress especifica una dirección TCP/IP si el nodo cliente tiene más de una dirección y quiere que el servidor contacte con una dirección distinta de la utilizada para realizar el primer contacto del servidor.

El servidor utilizará esta dirección cuando comience la operación planificada por solicitud de servidor.

Utilice esta opción sólo si especifica el parámetro prompted con la opción schedmode.

Si sessioninitiation se ha establecido en serveronly, el valor de la opción de cliente tcpclientaddress debe ser igual que el valor del servidor HLAddress.

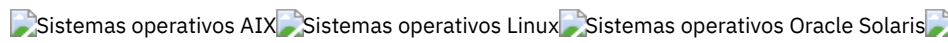



## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Incluya esta opción en el archivo dsm.sys dentro de una stanza de servidor. Puede establecer esta opción en la ficha Planificador, en el campo Su dirección TCP/IP del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Planificador, en el campo Su dirección TCP/IP del Editor de preferencias.

## Sintaxis

---

```
>>-TCPCLIENTAddress-- --client_address-----><
```

## Parámetros

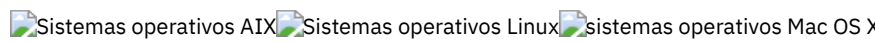



---





client\_address

Especifica la dirección TCP/IP que se desea que utilice el servidor para establecer contacto con el nodo cliente. Especifique un nombre de dominio Internet TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IPv4 o TCP/IPv6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción commmethod V6Tcpiip.

## Ejemplos


---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Archivo de opciones:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
tcpclienta dsmclnt.example.com  
o bien  
tcpclienta 192.0.2.21
```

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows

```
-tcpclientaddress=192.0.2.0  
-tcpclientaddress=ejemplo.miempresa.midominio.com  
-tcpclientaddress=2001:0DB8:0:0:0:0:0:0
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Tcpclientport

---

La opción `tcpclientport` especifica un número de puerto TCP/IP para que el servidor contacte con el cliente cuando el servidor comience la operación planificada por solicitud de servidor.

Utilice esta opción sólo si especifica el parámetro `prompted` con la opción `schedmode`.

Si `sessioninitiation` se ha establecido en `serveronly`, el valor de la opción de cliente `tcpclientport` debe ser igual al valor de la opción de servidor `LLAddress`.

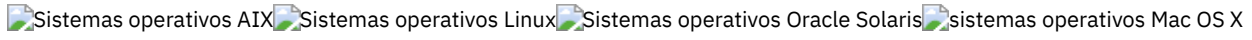
## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Establezca esta opción en el archivo `dsm.sys` dentro de una stanza de servidor. Puede establecer esta opción en el separador Planificador, en el campo Su puerto TCP/IP del editor de preferencias.

 Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Planificador, en el campo Su puerto TCP/IP del editor de preferencias.

## Sintaxis

---

```
>>-TCPCLIENTPort-- --client_port_address-----><
```

## Parámetros

---

`dirección_puerto_cliente`

Especifica la dirección de puerto TCP/IP que se desea que utilice el servidor para establecer contacto con el nodo cliente. El rango de valores es de 1 a 32767; siendo 1501 el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
tcpclientp 1502
```

Línea de mandatos:

```
-tcpclientport=1492
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

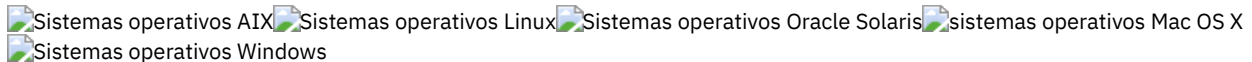
## Tcpnodelay

---

La opción `tcpnodelay` especifica si el cliente desactiva la demora de enviar paquetes pequeños consecutivos en la red, por transacción.

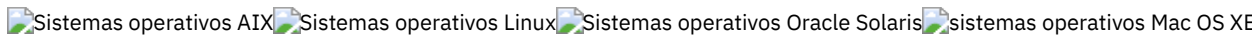
Sólo deberá cambiar el valor predeterminado `yes` cuando se den las condiciones siguientes:

- El soporte técnico de IBM® le ha indicado que debe cambiar la opción.
- Comprende bien los efectos del algoritmo TCP Nagle en las transmisiones en la red. Si se establece la opción en el valor `no` se activará el algoritmo Nagle, que retrasa el envío de paquetes consecutivos pequeños.



## Clientes soportados

---

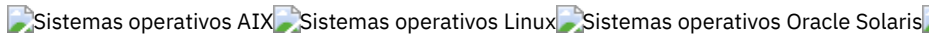

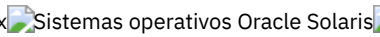

 Esta opción es válida para todos los clientes UNIX y Linux.


 Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---



 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador Communication del editor de preferencias. Seleccione Enviar transacción al servidor inmediatamente.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador Communication del editor de preferencias. Seleccione Enviar transacción al servidor inmediatamente.

## Sintaxis

---

```
>>-TCPNodelay-+-Yes-  
'-----'-----<<  
'-No--'
```

## Parámetros

---

No

Especifica que el servidor no permite enviar paquetes pequeños consecutivos de forma inmediata por la red. Si establece esta opción en no, el rendimiento puede verse afectado negativamente.

Yes

Especifica que el servidor o el cliente permiten enviar paquetes pequeños consecutivos de forma inmediata por la red. El valor predeterminado es yes.

## Ejemplos

---

Archivo de opciones:  
tcpnodelay yes  
Línea de mandatos:  
No se aplica.

## Tcpport

---

La opción tcpport especifica una dirección de puerto TCP/IP para el servidor de IBM Spectrum Protect. Puede obtenerse esta dirección del administrador.

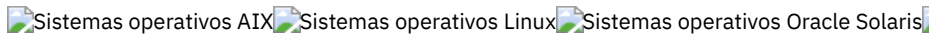

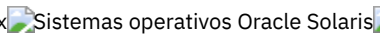

## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador Comunicación, en el campo Puerto de servidor del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador Comunicación, en el campo Puerto de servidor del editor de preferencias.

## Sintaxis

---

```
>>-TCPPort-- --port_address-----<<
```

## Parámetros

---

port\_address

Especifica la dirección de puerto TCP/IP que se utiliza para la comunicación con un servidor. El rango de valores es de 1 a 32767, siendo 1500 el valor predeterminado.





## Ejemplos





---


Archivo de opciones:  
tcp 1501

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `-tcpport=1501`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X No se aplica.

 Sistemas operativos Windows Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Tcpserveraddress

---

La opción `tcpserveraddress` especifica la dirección TCP/IP del servidor de IBM Spectrum Protect. Puede obtener esta dirección de servidor solicitándosela al administrador.





### Clientes soportados


---

Esta opción es válida para todos los clientes.

### Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor. Puede establecer esta opción en el separador Comunicación, en el campo Dirección de servidor del editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en el separador Comunicación, en el campo Dirección de servidor del editor de preferencias.

Si no se especifica esta opción, el cliente intentará establecer contacto con un servidor que se ejecute en el mismo sistema que el cliente de copia de seguridad y archivado.

### Sintaxis

---

```
>>-TCPserveraddress-- --server_address-----<<
```

### Parámetros

---

`server_address`





Especifica una dirección TCP/IP de 1 a 64 caracteres para un servidor. Especifique un nombre de dominio TCP/IP o una dirección IP numérica. La dirección IP numérica puede ser una dirección TCP/IP v4 o TCP/IP v6. Sólo puede utilizar direcciones IPv6 si ha especificado la opción `commmethod V6Tcpi`.





### Ejemplos

---

Archivo de opciones:

```
tcps dsmchost.example.com
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X No se aplica.

 Sistemas operativos Windows Línea de mandatos:

```
 Sistemas operativos Windows -tcpserveraddress=129.33.24.99
```

```
-tcpserveraddress=2002:92b:111:221:128:33:10:249
```

 Sistemas operativos Windows Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Tcpwindowsize

---

Utilice la opción `tcpwindowsize` para especificar el tamaño en kilobytes que desea que tenga la ventana deslizante de TCP/IP para el nodo cliente.

El host que envía los datos no puede enviar más datos hasta que recibe un acuse de recibo y una actualización de la ventana de recepción de TCP. Cada paquete TCP contiene la ventana de recepción de TCP indicada en la conexión. Una ventana más grande

permite al remitente continuar enviando datos y puede mejorar el rendimiento de las comunicaciones.





## Cientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en la ficha Comunicación, en el campo Tamaño de ventana del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Comunicación, en el campo Tamaño de ventana del Editor de preferencias.





## Sintaxis





---





```
>>-TCPWindowsize-- --window_size-----><
```





## Parámetros





---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
window\_size


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica el tamaño en kilobytes que se desea utilizar para la ventana deslizante de TCP/IP del nodo cliente. El rango de valores comprende los valores 0 a 2048. El valor 0 permite que el cliente utilice el tamaño de ventana de TCP predeterminado del sistema operativo. Los valores del 1 al 2048 indican que el tamaño de ventana oscila entre 1 KB y 2 MB. Si especifica un valor menor que 1, el tamaño de la ventana de TCP utilizará el valor predeterminado 1. Si especifica un valor mayor que 2048, el tamaño de la ventana de TCP utilizará el valor predeterminado 2048.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Para los clientes de copia de seguridad- archivado, el valor predeterminado para este parámetro es 63 KB.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, el valor predeterminado para este parámetro es 512 KB.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Notas:


- La ventana de TCP actúa como un almacenamiento intermedio en la red. No está relacionada con la opción tcpbuffsize ni con los almacenamientos intermedios de envío y recepción asignados en la memoria del cliente o del servidor.
- Un tamaño de ventana mayor que el espacio de almacenamiento intermedio en el adaptador de red podría reducir el rendimiento debido al reenvío de paquetes que se perdieron en el adaptador.
- Según los valores de comunicación del sistema operativo, es posible que el sistema no acepte todos los valores del rango.
- La opción tcpwindowsize altera temporalmente los tamaños de ventana de envío y recepción de sesión TCP/IP predeterminados del sistema operativo.

 Sistemas operativos Windows window\_size

 Sistemas operativos Windows Especifica el tamaño en kilobytes que se desea utilizar para la ventana deslizante de TCP/IP del nodo cliente. El rango de valores comprende los valores 0 a 2048. El valor 0 permite que el cliente utilice el tamaño de ventana de TCP predeterminado del sistema operativo. Los valores del 1 al 2048 indican que el tamaño de ventana oscila entre 1 KB y 2 MB. Si especifica un valor menor que 1, el tamaño de la ventana de TCP utilizará el valor predeterminado 1. Si especifica un valor mayor que 2048, el tamaño de la ventana de TCP utilizará el valor predeterminado 2048.

 Sistemas operativos Windows Para los clientes de copia de seguridad- archivado, el valor predeterminado para este parámetro es 63 KB.

 Sistemas operativos Windows Para IBM Spectrum Protect for Virtual Environments: Data Protection for VMware, el valor predeterminado para este parámetro es 512 KB.

 Sistemas operativos Windows

Notas:

- La ventana de TCP actúa como un almacenamiento intermedio en la red. No está relacionada con la opción tcpbuffsize ni con los almacenamientos intermedios de envío y recepción asignados en la memoria del cliente o del servidor.
- Un tamaño de ventana mayor que el espacio de almacenamiento intermedio en el adaptador de red podría reducir el rendimiento debido al reenvío de paquetes que se perdieron en el adaptador.
- Según los valores de comunicación del sistema operativo, es posible que el sistema no acepte todos los valores del rango.

- La opción `tcpwindowsize` altera temporalmente los tamaños de ventana de envío y recepción de sesión TCP/IP predeterminados del sistema operativo.
- Windows proporciona un tamaño de ventana de recepción de TCP mayor cuando se establecen comunicaciones con hosts que también proporcionan este soporte, conocido como RFC1323. En estos entornos, puede ser útil utilizar un valor mayor que 63.

## Ejemplos

```


Archivo de opciones:
    tcpwindowsize 63
Línea de mandatos:
    -tcpw=63

```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Timeformat















La opción `timeformat` especifica el formato en el que desea ver y especificar la hora del sistema.

 Sistemas operativos Windows Utilice esta opción si desea cambiar el formato de hora predeterminado y establecerlo en el idioma del repositorio de mensajes que utiliza.

De manera predeterminada, los clientes de copia de seguridad/archivado y de administración obtienen la información de formato de la definición del entorno regional que esté en funcionamiento en el momento en que se llama al cliente. Consulte la documentación del sistema local para obtener más detalles sobre la configuración del entorno regional.

Nota: La opción `timeformat` no afecta al cliente web. El cliente web utiliza el formato de hora para el entorno regional en el que se está ejecutando el navegador. Si un navegador no se está ejecutando en un entorno regional que admite el cliente, el cliente web utiliza el formato de hora de inglés de Estados Unidos.

Puede utilizar la opción `timeformat` con los mandatos siguientes:





- `delete archive`
- `delete backup`
- `expire`
- `query archive`
-  Sistemas operativos Windows `query asr`
- `query backup`
- `query filespace`
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `query image`
- `query nas`
-  Sistemas operativos Windows `query systemstate`
- `restore`
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `restore image`
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `restore nas`
-  Sistemas operativos Windows `restore registry`
- `retrieve`
- `set event`


Si incluye la opción `timeformat` con un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

## Clientes soportados

Esta opción es válida para todos los clientes.

## Archivo de opciones

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Establezca esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Configuración regional, en el campo Formato de hora del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`). Puede establecer esta opción en la ficha Configuración regional, en el campo Formato de hora del Editor de preferencias.

## Sintaxis

---




```
>>-TIMEformat-- --número_formato-----><
```

## Parámetros

---




### número\_formato

Visualiza la hora en uno de los formatos listados aquí. Seleccione el número que se corresponda con el formato que desee utilizar. Si incluye la opción `timeformat` en un mandato, ésta deberá preceder a las opciones `fromtime`, `pittime` y `totime`.

   Utilice el formato de hora definido para el entorno regional (no se aplica a Mac OS X). Este es el valor predeterminado si el formato que especifica el entorno regional consta de dígitos, caracteres de separación y, si se aplica, la serie AM o PM.

1

23:00:00

   Este es el valor predeterminado si el formato que especifica el entorno regional no consta de dígitos, de caracteres de separación ni, si se aplica, de la serie AM o PM.

2

23,00,00

3

23.00.00

4

12:00:00A/P

5

A/P 12:00:00

## Ejemplos

---

Archivo de opciones:  
`timeformat 4`

Línea de mandatos:  
`-time=3`





Esta opción es válida en la línea de mandatos inicial y en modalidad interactiva. Si utiliza esta opción en modalidad interactiva, sólo afectará al mandato con el que se especifica. Cuando se complete la ejecución de ese mandato, el valor se revierte al comienzo de la sesión interactiva. Será el valor del archivo `dsm.opt`, a menos que se haya modificado mediante la línea de mandatos inicial o mediante una opción que el servidor ha forzado.

## Consideraciones adicionales para especificar los formatos de fecha y hora

---

El formato de fecha y hora que especifique con esta opción debe utilizarse en las opciones que acepten una entrada de fecha y hora. Por ejemplo: `totime`, `fromtime`, `today`, `fromdate` y `pittime`.

Por ejemplo, si especifica la opción `timeformat` como `TIMEFORMAT 4`, el valor que proporciona en la opción `fromtime` o `totime` debe especificarse como una hora, por ejemplo, `12:24:00pm`. Si especifica `13:24:00`, no será válido porque `TIMEFORMAT 4` necesita un entero de hora menor o igual a 12. Si desea especificar valores de hasta 24 horas en una opción y utilizar comas como separadores, debe especificar `TIMEFORMAT 2`.

## Configuración de los formatos de fecha y hora en el archivo de configuración del entorno regional del sistema

---

Puede especificar formatos de fecha y hora configurándolos en el archivo de entorno regional del sistema. Si especifica formatos de fecha y hora en el archivo del entorno regional, deben definirse utilizando un subconjunto de especificadores de formato de producción de números soportados por la función `strftime()` del lenguaje C. Puede utilizar los siguientes especificadores para establecer los formatos de fecha y hora en los valores de configuración del entorno regional.

Especificadores de fecha

- %Y - el año, en cuatro dígitos. Por ejemplo, 2011.
- %y - el año, solo con los dos últimos dígitos. Por ejemplo, 11; no 2011.
- %m - el mes, como un número decimal (1-12).
- %d - el día del mes (1-31).

En los especificadores de fecha, sólo puede especificar un especificador de año. No especifique %Y ni %y. El modificador E (un E en mayúsculas) puede preceder los especificadores de fecha para crear la forma alternativa del entorno local para el año, mes o día. Si no existe ningún formato alternativo, el modificador E se ignora. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,), los puntos (.), (.), guiones (-) o barras diagonales (/). No utilice caracteres de varios bytes como separadores.

#### Especificadores de hora

- %H - la hora, en formato de 24 horas (00-23).
- %I - la hora, en formato de 12 horas (00-12).
- %M - minutos después de la hora (00-59).
- %S - segundos después del minuto (00-59)
- %p - añade el indicador AM (antes de mediodía) o PM (después de mediodía).

En los especificadores de hora, sólo puede especificar un especificador de hora. No especifique %I y %H a la vez.

El modificador O (una O mayúscula) puede ir antes que los especificadores de hora para producir el formato alternativo del entorno regional para la hora, los minutos o los segundos. El modificador O no puede ir antes que el especificador %p. Separe los especificadores con un carácter ASCII de 7 bits. Los separadores más utilizados son los dos puntos (:), las comas (,) o los puntos (.). No utilice caracteres de varios bytes como separadores. No especifique un separador entre el especificador %p y el separador que le precede o le sigue.

#### Ejemplos de formato de hora, configurados en los valores de entorno regional

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris  
Para establecer un formato de hora en particular, edite el archivo de configuración del entorno regional que utiliza y modifique la línea `t_fmt` en función de sus necesidades. Sea cual sea el formato de hora seleccionado, se aplica tanto a la salida como a la entrada. Una vez editado el archivo de configuración del entorno regional, debe ejecutarse el mandato `localedef` para crear el archivo del entorno regional final.

Tabla 1. Valores del formato de hora de ejemplo en la configuración del entorno regional (línea `t_fmt`)

Ejemplo	Resultado
"%H:%M:%S"	Muestra la hora en el formato <code>hh:mm:ss</code> , siendo valores válidos para <code>hh</code> el rango de 0 a 23.
"%H,%M,%S"	Muestra la hora en el formato <code>hh,mm,ss</code> , siendo valores válidos para <code>hh</code> el rango de 0 a 23.
"%I,%M,13p"	Muestra la hora en el formato <code>hh,mm,ssA/P</code> , donde <code>hh</code> puede estar entre 1 y 12, y donde <code>A/P</code> es la abreviatura local de antemeridiano (AM en inglés) o postmeridiano (PM en inglés).

#### Ejemplos de formato de fecha, configurados en los valores de entorno regional

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris  
Para establecer un formato de fecha en particular, edite el archivo de configuración y modifique la línea `d_fmt` en función de sus necesidades. Sea cual sea el formato de fecha seleccionado, se aplica tanto a la salida como a la entrada.

Tabla 2. Valores del formato de fecha de ejemplo en la configuración del entorno regional (línea `d_fmt`)

Ejemplo	Resultado
"%m/%d/%y"	Visualiza la fecha con el formato MM/DD/AA.
"%d.%m.%Y"	Visualiza la fecha con el formato DD.MM.AAAA.

Sistemas operativos AIX Sistemas operativos Oracle Solaris Sistemas operativos Windows



Utilice la opción toc con el mandato backup nas o la opción include.fs.nas para especificar si el cliente de copia de seguridad y archivado ha de guardar la información de la tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos.


Tenga en cuenta las consideraciones siguientes cuando decida si desea guardar la información de TOC:

- Si guarda la información de la TOC, podrá utilizar el mandato de servidor QUERY TOC para determinar el contenido de la copia de seguridad de un sistema de archivos junto con el mandato de servidor RESTORE NODE para restaurar archivos individuales o árboles de directorios.
- También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse.
- Para crear una tabla de contenido, debe definir el atributo TOCDESTINATION en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. Tenga en cuenta que, para crear una tabla de contenido, se necesitan un proceso adicional, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad.
- Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios utilizando el mandato de servidor RESTORE NODE, siempre que conozca el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

## Clientes soportados



---


 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción solo es válida para los clientes AIX y Solaris. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Especifique la sentencia include.fs.nas que contiene el valor toc en el archivo dsm.sys dentro de una stanza de servidor.

 Sistemas operativos Windows Especifique la sentencia include.fs.nas que contiene el valor toc en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
      .-Preferred-.
>>-TOC-+-----+-----><
      +-Yes-----+
      '-No-----'
```

## Parámetros

---

Yes

Especifica que el cliente ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS. Sin embargo, la copia de seguridad no se realizará correctamente si se produce un error durante la creación de la TOC.

No

Especifica que el cliente no ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS.

Preferred

Especifica que el cliente ha de guardar la información de las TOC durante la realización de una copia de seguridad de imagen del sistema de archivos NAS. La copia de seguridad no falla si se produce un error durante la creación de la TOC. Éste es el valor predeterminado.



Nota: Si la opción mode se ha establecido en differential y establece la opción toc en preferred o yes, pero la última imagen completa no dispone de una tabla de contenido, el cliente realizará una copia de seguridad de imágenes completa y creará una tabla de contenido.





## Ejemplos

---

Archivo de opciones:

```
include.fs.nas netappsj/vol/vol0 homemgmtclass toc=yes
```

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris backup nas -nasnodename=netappsj /vol/vol0 -toc=yes  
 Sistemas operativos Windows Línea de mandatos:  
 Sistemas operativos Windows backup nas -nasnodename=netappsj {/vol/vol0} -toc=yes

## Todate

---

Utilice la opción `todate` con la opción `totime` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta.

Utilice las opciones `todate` y `totime` con las opciones `fromtime` y `fromdate` para solicitar una lista de copias de seguridad o archivadas realizadas durante un período de tiempo determinado. Por ejemplo, puede solicitarse una lista de archivos cuya copia de seguridad se realizó entre las 6:00 del 1 de julio de 2002 y las 23:59 del 30 de julio de 2002.

La opción `todate` puede utilizarse con los mandatos siguientes:

- `delete backup`
- `query archive`
- `query backup`
- `restore`
- `restore group`
- `retrieve`

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-TODate = - --date-----<<
```

## Parámetros

---


`date`


Especifica una fecha final. Escriba la fecha en el formato seleccionado con la opción `dateformat`.





Si se incluye la opción `dateformat` con un mandato, ésta debe anteponerse a las opciones `fromdate`, `pitdate` y `todate`.





## Ejemplos


---

 sistemas operativos Mac OS X Línea de mandatos:

 sistemas operativos Mac OS X `dsmc restore "/Users/agordon/Documents/*" -todate=12/11/2003`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X `dsmc restore "/home/user1/*" -todate=12/11/2003`

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `dsmc restore -todate=12/11/2003 c:\myfiles\`

## Totime

---

Utilice la opción `totime` con la opción `todate` para especificar una fecha y una hora finales hasta las que desea buscar copias de seguridad o copias archivadas durante una operación de restauración, recuperación o consulta. El cliente de copia de seguridad y archivado pasa por alto esta opción si no especifica la opción `todate`.

Utilice las opciones `totime` y `todate` con las opciones `fromtime` y `fromdate` para solicitar una lista de archivos cuyas copias de seguridad se realizaron durante un período de tiempo determinado. Por ejemplo, puede solicitarse una lista de archivos cuya copia de seguridad se realizó entre las 6:00 del 1 de julio de 2003 y las 23:59 del 30 de julio de 2003.

La opción `totime` puede utilizarse con los mandatos siguientes:

- `delete backup`
- `query archive`



- query backup
- restore
- restore group
- retrieve

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-TOTime = - --hora-----><
```

## Parámetros

---

hora

Especifica una hora final. Si no se especifica una hora, se toma el valor predeterminado 23:59:59. Especifique la hora en el formato seleccionado con la opción timeformat.





Si incluye la opción timeformat en un mandato, ésta deberá preceder a las opciones fromtime, pittime y totime.

## Ejemplos


---

 sistemas operativos Mac OS XLínea de mandatos:

```
dsmc restore "/Users/van/Documents/myfiles/*" -todate=09/17/2003 -totime=23:00:00
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XLínea de mandatos:

```
dsmc restore "/home/user1/*" -todate=09/17/2003 -totime=23:00:00
```

 Sistemas operativos WindowsLínea de mandatos:

```
dsmc query backup -totime=23:59:00 -todate=06/30/2003 c:\mybackups\
```

## Txnbytelimit






---

La opción txnbytelimit especifica el número de kilobytes que el programa de cliente guarda en el almacenamiento intermedio antes de enviar una transacción al servidor.

Una *transacción* es la unidad de trabajo que se ha intercambiado entre el cliente y el servidor. Una transacción puede contener más de un archivo o directorio, llamado *grupo de transacción*.

Puede controlar la cantidad de datos enviados entre el cliente y el servidor antes de que el servidor valide los datos y cambios en la base de datos del servidor, utilizando la opción txnbytelimit. Controlando la cantidad de datos enviados, cambia la velocidad del cliente para realizar las transacciones. La cantidad de datos enviados se utiliza cuando los archivos se procesan por lotes durante una copia de seguridad o cuando se reciben archivos del servidor durante un procedimiento de restauración.

Una vez que txngroupmax ha alcanzado este número, el cliente envía los archivos al servidor, aunque el límite de bytes de transacción no se ha alcanzado.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Especifique esta opción en el archivo de opciones de sistema de cliente (dsm.sys) en una stanza de servidor. Puede establecer esta opción en el separador General, en el campo Tamaño de almacenamiento intermedio de transacción en el editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en el separador General, en el campo Tamaño de almacenamiento intermedio de transacción en el editor de preferencias.

## Sintaxis

---

```
>>-TXNBytelimit-- --number-----<<
```

## Parámetros

---

number

Especifica el número de kilobytes que el programa cliente envía al servidor antes de enviar una transacción. El rango de valores va de 300 a 34359738368 (32 GB). El valor predeterminado es 25600 KB. Se puede especificar el número como número entero o como número entero con uno de los siguientes cualificadores de unidad:

- K o k (kilobytes)
- M o m (megabytes)
- G o g (gigabytes)

Si no se especifica la unidad del cualificador, el número entero está en kilobytes.

Restricción: La opción txnbytelimit no admite números decimales, y sólo se permiten letras de una unidad. Por ejemplo: K, M o G.

## Ejemplos

---


Archivo de opciones:

```
txnb 25600
txnb 2097152
txnb 2097152k
txnb 2048m
txnb 2g
txnb 32G
```

Línea de mandatos:

```
-txnb=25600
-txnb=16G
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows


## Type

---



Utilice la opción type con el mandato query node para especificar el tipo de nodo que ha de consultarse. Utilice esta opción con el mandato set event para activar, retener o liberar.


## Clientes soportados

---

 Sistemas operativos AIX Esta opción también es válida para el mandato set password con el tipo TSM en clientes AIX.

 Sistemas operativos Windows Esta opción también es válida para el mandato set password con el tipo TSM o FILER.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Esta opción solo es válida para los clientes AIX y Solaris. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos Windows Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Sintaxis

---

```
>>-TYpe = .-any----.
          +-----+
          +-nas----+
          +-server-+
```

'-client-'

## Parámetros






---

- nas  
Especifica todos los nodos NAS inscritos en el servidor.
- servidor  
Especifica nodos cliente que se encuentran en otros servidores de IBM Spectrum Protect.
- client  
Especifica nodos cliente que son clientes de copia de seguridad/archivado.

## Ejemplos

---

Línea de mandatos:

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows `query node -type=nas`  
 Sistemas operativos AIX  Sistemas operativos Linux

## Updatectime

---

Utilice la opción `updatectime` para comprobar el atributo de cambio de hora (`ctime`) durante una operación de copia de seguridad incremental.

## Clientes soportados

---

Esta opción es válida para clientes de AIX y Linux sólo en sistemas de archivos GPFS. El servidor también puede definir esta opción.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-UPDATECTime--+-no-- .  
+-----+  
'-yes-'
```

## Parámetros

---

- no  
El cliente de archivado y copia de seguridad no comprueba el cambio de hora (atributo `ctime`) durante una operación de copia de seguridad. Este es el valor predeterminado.
- yes  
El cliente de archivado y copia de seguridad comprueba el cambio de hora (atributo `ctime`) durante una operación de copia de seguridad. Si el atributo `ctime` ha cambiado desde la última operación de copia de seguridad, el atributo `ctime` se actualizará en el servidor de IBM Spectrum Protect. No se hace copia de seguridad del objeto, a menos que tenga ACLs o atributos ampliados. El cliente comprueba los archivos y directorios.

## Ejemplos

---

Archivo de opciones:

```
updatect yes
```

Línea de mandatos:

```
dsmc incr /proj/gpfs/test/ -updatectime=yes
```

 Sistemas operativos Windows

## Usedirectory

---

La opción `usedirectory` consulta a Active Directory con qué método de comunicación y a qué servidor debe conectarse.

Esta opción modifica los parámetros commmethod que se han especificado en el archivo de opciones del cliente (dsm.opt). Lo óptimo es que el administrador active un solo servidor y un protocolo de comunicaciones específico para un determinado nodo cliente. La especificación de esta información en Active Directory se realiza mediante el servidor de IBM Spectrum Protect en Windows, que cuenta con un asistente que le ayudará a realizar esta configuración. Si un nodo está inscrito en más de un servidor publicado en Active Directory, se utilizará el primer servidor devuelto en la consulta de Active Directory. Si el cliente no puede ponerse en contacto con el servidor, la sesión del cliente fallará.

## Cientes soportados

---

Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Comunicación del editor de preferencias.

## Sintaxis

---

```
.-No--  
>>-USEDIRECTORY-----+-----+-----><  
'-Yes-'
```

## Parámetros

---

### Yes

Especifica que el cliente hará caso omiso de los parámetros de commmethod establecidos en el archivo de opciones del cliente y consultará Active Directory para saber qué método de comunicación debe utilizarse y a qué servidor debe conectarse.

### No


Especifica que el cliente utilizará el método de comunicación especificado en el archivo de opciones. Si no se ha especificado ningún método de comunicación en el archivo de opciones, se utilizará el método de comunicación y el servidor predeterminados.

## Ejemplos

---

Archivo de opciones:  
usedirectory no  
Línea de mandatos:  
-usedir=yes

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows

## Useexistingbase

---


La opción useexistingbase se utiliza cuando se hacen copias de seguridad de instantáneas que se encuentran en volúmenes de archivador NetApp. La opción useexistingbase indica que la instantánea más reciente que existe en el volumen del que se está realizando una copia de seguridad, debe utilizarse como la instantánea base durante una operación de copia de seguridad diferencial de instantáneas.


Si no se especifica esta opción, se crea una nueva instantánea en el volumen del que se está realizando una copia de seguridad. Debido a que los volúmenes de archivador de destino son de sólo lectura, debe especificarse useexistingbase cuando se realizan copias de seguridad diferenciales de instantáneas de volúmenes de archivador de destino. Si no se especifica useexistingbase, las copias de seguridad diferenciales de instantáneas de un volumen de archivador de destino muestran una anomalía porque la instantánea nueva no puede crearse en el volumen de sólo lectura.

Cuando realice una copia de seguridad de volúmenes de archivador de destino, utilice las opciones useexistingbase y diffsnapshot=latest para asegurarse de utilizar la base más reciente y las instantáneas de diferencial más recientes durante la copia de seguridad de volumen.

## Cientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Esta opción sólo es válida en la línea de mandatos.

## Sintaxis

---

```
>>-USEEXISTINGBase-----<<
```

## Parámetros

---

Esta opción no tiene parámetros

## Ejemplos

---

Archivo de opciones:

No se aplica.

Línea de mandatos:

```
dsmc incr \\DRFiler\UserDataVol_Mirror_Share -snapdiff
-useexistingbase -basenameshotname="nightly.?"
```

**Referencia relacionada:**

Basesnapshotname

## Usereplicationfailover

---

La opción usereplicationfailover especifica si se produce la migración tras error automatizada del cliente de un nodo cliente.

Utilice esta opción para permitir que un nodo cliente para migración tras error o para impedir que migre tras error en el servidor secundario. Esta opción altera temporalmente la configuración que se proporciona mediante los valores del administrador del servidor de IBM Spectrum Protect en el servidor primario.





## Clientes soportados


---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Coloque esta opción dentro de una stanza del servidor en el archivo dsm.sys.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-USEREPLICATIONFailover--+-Yes-
'-No--'-----<<
```

## Parámetros

---

Yes

Especifica que desea que el cliente migre tras error automáticamente al servidor secundario si el servidor primario no está disponible. El cliente utiliza la configuración proporcionada por el servidor primario para conectarse al servidor secundario. Este es el valor predeterminado.

No

Especifica que el cliente no migra tras error automáticamente al servidor secundario.

## Ejemplos

---

Archivo de opciones:  
USEREPLICATIONFailover no





Línea de mandatos:  
No se aplica.

**Conceptos relacionados:**

Configuración y uso de la migración tras error automática del cliente

**Tareas relacionadas:**

Configuración del cliente de migración automática tras error

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

## Usuarios (obsoleto)

---

Esta opción está obsoleta.

## V2archive

---

Utilice la opción v2archive con el mandato archive para realizar el archivado sólo de los archivos en el servidor.

El cliente de copia de seguridad y archivado no procesará los directorios que existen en la vía de acceso de la especificación de archivo de origen.

Esta opción difiere de la opción filesonly en que la opción filesonly archiva los directorios existentes en la vía de acceso de la especificación de archivos origen.

Las opciones v2archive y dirsonly se excluyen mutuamente, y se visualizará un mensaje de error si utiliza ambas opciones en el mismo mandato archive.

Si utiliza esta opción también debe tener en cuenta las consideraciones siguientes:

- Puede experimentar problemas de rendimiento al recuperar grandes cantidades de datos archivados con esta opción.
- Plantéese utilizar esta opción únicamente si le preocupa el rendimiento de la función de caducidad en un servidor que ya contenga cantidades ingentes de datos archivados.
- Si hay varios archivos con el mismo nombre para la opción v2archive, los archivos se archivan varias veces, con su estructura de directorios. La opción v2archive sólo archiva los archivos.

## Clientes soportados

---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-V2archive-----<<
```


## Parámetros

---

No hay parámetros para esta opción.

## Ejemplos

---





 sistemas operativos Mac OS X Este mandato:

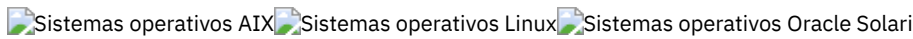

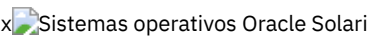
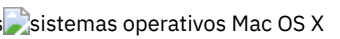
 sistemas operativos Mac OS X `dsmsc archive "/Users/user2/Documents/*" -v2archive -su=y.`

**Realiza el archivado de los archivos siguientes:**

```
/Users/user2/Documents/file1  
/Users/user2/Documents/file2  
/Users/user2/Documents/file3  
/Users/user2/Documents/dir2/file4  
/Users/user2/Documents/dir2/file5
```

Nota: El cliente no archiva `/Users/user2/Documents` ni `/Users/user2/Documents/dir2`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Este mandato:


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
dsmc archive "/home/relx/dir1/\*" -v2archive -su=y.

**Realiza el archivado de los archivos siguientes:**

```
/home/relx/dir1/archivo1  
/home/relx/dir1/archivo2  
/home/relx/dir1/archivo3  
/home/relx/dir1/dir2/archivo4  
/home/relx/dir1/dir2/archivo5
```

Nota: El cliente no archiva /home/relx/dir1 ni /home/relx/dir1/dir2.

 Sistemas operativos Windows Este mandato:

 Sistemas operativos Windows dsmc archive c:\relx\dir1\ -v2archive -su=y

**Realiza el archivado de los archivos siguientes:**

```
c:\relx\dir1\archivo1  
c:\relx\dir1\archivo2  
c:\relx\dir1\archivo3  
c:\relx\dir1\dir2\archivo4  
c:\relx\dir1\dir2\archivo5
```

Nota: El cliente no archiva c:\relx\dir1 ni c:\relx\dir1\dir2.

## Verbose


---

La opción verbose especifica que se desea visualizar información detallada de proceso en la pantalla. Éste es el valor predeterminado.

Cuando se ejecutan los mandatos incremental, selective o archive, se visualiza información acerca de cada archivo del que se hace copia de seguridad. Utilice la opción quiet si no desea visualizar esta información.

El siguiente comportamiento se aplica cuando se utilizan las opciones verbose y quiet.

- Si el servidor especifica la opción quiet o la opción verbose en el conjunto de opciones del cliente del servidor, los valores del servidor modificarán temporalmente los valores del cliente, aunque force se haya establecido en no en el servidor.
- Si especifica quiet en el archivo dsm.opt y especifica -verbose en la línea de mandatos, prevalecerá -verbose.
- Si especifica tanto -quiet como -verbose en el mismo mandato, prevalecerá la última opción detectada durante el proceso de las opciones. Si especifica -quiet -verbose, prevalecerá -verbose. Si especifica -verbose -quiet, prevalecerá -quiet.

 sistemas operativos Mac OS X La información aparece en la pantalla en la ventana de estado del planificador. Esta opción sólo se aplica si se está ejecutando el planificador y el cliente está llevando a cabo un trabajo planificado.

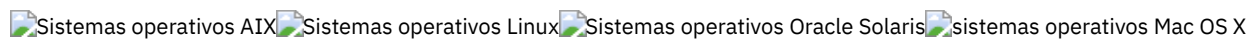

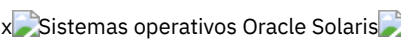
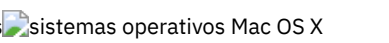
## Clientes soportados


---

Esta opción es válida para todos los clientes. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt). Puede establecer esta opción en la ficha Línea de mandatos, en el recuadro de selección No mostrar información de proceso en pantalla del Editor de preferencias.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt). Puede establecer esta opción en la ficha Línea de mandatos, en el recuadro de selección No mostrar información de proceso en pantalla del Editor de preferencias.

## Sintaxis

---

```
>>>-VErbose----->>
```

## Parámetros

---

No hay parámetros para esta opción.





## Ejemplos

---

Archivo de opciones:

verbose  
Línea de mandatos:  
-verbose

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

## Verifyimage




---


Utilice la opción `verifyimage` con el mandato `restore image` para especificar que desea activar la detección de los sectores defectuosos en el volumen de destino.

Si se detectan sectores defectuosos en el volumen de destino, el cliente de copia de seguridad y archivado emite un mensaje de aviso en la consola y en el registro de errores.

## Clientes soportados

---

   Esta opción solo es válida para clientes de AIX, Oracle Solaris y todos los de Linux. La API de IBM Spectrum Protect no admite esta opción.

 Esta opción es válida para todos los clientes Windows. La API de IBM Spectrum Protect no admite esta opción.

## Sintaxis

---

```
>>-VERIFYImage-----<<
```







## Parámetros



---

No hay parámetros para esta opción.

## Ejemplos

---





   Línea de mandatos:  
   `dsmc restore image /usr -verifyimage`

 Línea de mandatos:  
 `dsmc restore image d: -verifyimage`

## Virtualfsname




---


Utilice la opción `virtualfsname` con el mandato `backup group` para especificar el nombre del espacio de archivos virtual para el grupo en el que desea realizar la operación. El valor de la opción `virtualfsname` no puede ser igual a un nombre de espacio de archivos existente.

## Clientes soportados

---

   Esta opción es válida para todos los clientes UNIX y Linux, a excepción de Mac OS X.

 Esta opción es válida para todos los clientes Windows.

## Sintaxis

---

```
>>-VIRTUALFsname = - --fsname-----<<
```

## Parámetros

---

nombre\_espacio\_archivos




Especifica el nombre del contenedor del grupo en el que desea realizar la operación.




## Ejemplos

---


Línea de mandatos:

 sistemas operativos Mac OS X




```
backup group -filelist=/Users/van/Documents/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

 Sistemas operativos Windows

```
backup group -filelist=c:\dir1\filelist1 -groupname=group1  
-virtualfsname=\virtfs -mode=full
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

## Virtualmountpoint

---

La opción `virtualmountpoint` define un punto de montaje virtual para un sistema de archivos, si desea que se realice una copia de seguridad de los archivos que empiezan en un directorio determinado de dicho sistema de archivos.

La utilización de la opción `virtualmountpoint` para identificar un directorio dentro de un sistema de archivos proporciona una vía de acceso directa a los archivos de los que se quiere efectuar copia de seguridad, ahorrando tiempo de proceso. Es más eficaz definir un punto de montaje virtual en un sistema de archivos que definir dicho sistema de archivos utilizando la opción `domain` y después utilizar la opción `exclude` de la lista de opciones de inclusión/exclusión para excluir los archivos de los que no desea realizar una copia de seguridad.

Utilice la opción `virtualmountpoint` para definir puntos de montaje virtuales en varios sistemas de archivos, para sistemas de archivos locales y remotos y para definir varios puntos de montaje virtuales en el mismo espacio de archivos. Los puntos de montaje virtual no pueden utilizarse en un sistema de archivos gestionado por el montador automático.

Puede utilizar la opción `virtualmountpoint` para hacer copias de seguridad de los sistemas de archivos no soportados, con ciertas limitaciones. Para obtener información sobre cómo utilizar `virtualmountpoint` con sistemas de archivos no soportados, consulte Soporte para sistemas de archivos y ACL.

Nota: si el directorio que desea especificar como punto de montaje virtual es un vínculo simbólico, establezca la opción `followsymbolic` en Yes. Si esta opción se establece en no (valor predeterminado), no se le permitirá utilizar un vínculo simbólico como punto de montaje virtual. Asimismo, si hace una copia de seguridad del sistema de archivos, agrega un punto de montaje virtual, y después efectúa otra copia de seguridad incremental en el sistema de archivos, los archivos y directorios del directorio del punto de montaje virtual caducarán, porque se incluyen de forma lógica en el directorio del punto de montaje virtual y no en el sistema de archivos.

Después de definir un punto de montaje virtual, podrá definir la vía de acceso y nombre de directorio con la opción `domain` en el archivo de opciones del cliente predeterminado o en el mandato incremental para incluirlo en los servicios de copia de seguridad incremental. Cuando realice una operación de copia de seguridad o archivado con la opción `virtualmountpoint`, el mandato `query filespace` mostrará el punto de montaje virtual en su respuesta junto con otros sistemas de archivos. Generalmente, los directorios que se definen como puntos de montaje virtuales se tratan como sistemas de archivos reales y requieren que se especifique la opción `virtualmountpoint` en el archivo `dsm.sys` para restaurar o recuperar los datos.

Nota: cuando se especifica una opción `virtualmountpoint`, la vía de acceso que se especifica se agrega al dominio de copia de seguridad predeterminado (`domain all-local`). La vía de acceso `virtualmountpoint` siempre se considera un "punto de montaje" local independientemente del tipo de sistema de archivos real al que haga referencia.

## Clientes soportados

---

Esta opción es válida para todos los clientes UNIX, a excepción de Mac OS X. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Especifique esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) en una stanza de servidor.

## Sintaxis

---

```
-----  
v |  
>>---VIRTUALMountpoint-- --directorio+-----<<
```

## Parámetros

---

### directorio

Especifica la vía de acceso y el nombre del directorio que desea utilizar como punto de montaje virtual para un sistema de archivos. No puede utilizar caracteres comodín en la vía de acceso ni en el nombre de directorio.

Defina solo un punto de montaje virtual con cada opción virtualmountpoint que incluya en el archivo de opciones del sistema cliente. Utilice la opción virtualmountpoint tantas veces como sea necesario para definir todos los puntos de montaje virtuales que desee utilizar.

## Ejemplos

---

Archivo de opciones:

```
virtualmountpoint /afs/xyzcorp.com/home/ellen  
virtualmountpoint /afs/xyzcorp.com/home/ellen/test/data
```

Línea de mandatos:






No se aplica.

## Virtualnodename

---


La opción virtualnodename especifica el nombre de nodo de la estación de trabajo cuando desea restaurar o recuperar archivos en una estación de trabajo diferente.






Cuando utilice la opción virtualnodename en el archivo de opciones del cliente o con un mandato:

-  Sistemas operativos Windows Debe especificar el nombre que ha especificado con la opción nodename en el archivo de opciones del cliente (dsm.opt). Este nombre debe ser distinto del nombre que devuelve el mandato hostname en la estación de trabajo.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Debe especificar el nombre que ha especificado con la opción nodename en el archivo de opciones del sistema cliente (dsm.sys). Este nombre debe ser distinto del nombre que devuelve el mandato hostname en la estación de trabajo.
- El cliente solicita la contraseña asignada al nodo que se especifique, en caso de que se requiera una contraseña (incluso cuando la opción passwordaccess se ha establecido en generate). Si se escribe la contraseña correcta, se tendrá acceso a todas las copias de seguridad y copias archivadas que se originaron en el nodo especificado.

Al conectarse a un servidor, el cliente debe identificarse ante el servidor. Esta identificación de conexión se determina de los modos siguientes:

- Si no se especifican las opciones nodename y virtualnodename o si no se especifica un nombre de nodo virtual en la línea de mandatos, el identificador de conexión predeterminado será el nombre que devolverá el mandato hostname.
- Si se especifica la opción nodename, el nombre que se especifique con la opción nodename modificará temporalmente el nombre que devuelve el mandato hostname.
- Si se especifica la opción virtualnodename o se especifica un nombre de nodo virtual en la línea de mandatos, este nombre no podrá ser igual al nombre que devuelve el mandato hostname.

 Sistemas operativos Windows Nota: El cliente puede utilizar la información de espacio de archivos al restaurar archivos. La información de espacio de archivos puede contener el nombre del sistema desde el que se ha realizado la copia de seguridad de los archivos. Si realiza la restauración desde otro nodo cliente y no especifica un destino para los archivos restaurados, el cliente utilizará la información de espacio de archivos para restaurar los archivos. En este caso, el cliente intentará restaurar los archivos en el sistema de archivos del sistema original. Si el sistema de la restauración dispone de acceso al sistema de archivos del sistema original, puede restaurar archivos en el sistema de archivos original. Si el sistema de archivos de la restauración no dispone de acceso a la unidad del sistema original, el cliente puede devolver un mensaje de error de red. Si desea restaurar la estructura de directorios original pero en un sistema distinto, especifique sólo el sistema de archivos de destino cuando realice la restauración. Ello tiene aplicación cuando se restauran archivos de otro nodo y cuando se recuperan archivos de otro nodo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows


## Clientes soportados





---

Esta opción es válida para todos los clientes.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Establezca esta opción en el archivo de opciones de usuario del cliente (dsm.opt).

## Sintaxis

---

```
>>-VIRTUALNodename-- --nodename-----<<
```

## Parámetros

---

nodename

Especifica un nombre de 1 a 64 caracteres que identifica el nodo para el que se desea solicitar servicios de IBM Spectrum Protect. No hay valor predeterminado.

## Ejemplos

---


Archivo de opciones:

```
virtualnodename pilar
```

Línea de mandatos:

```
-virtualn=marisa
```

Esta opción solo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos Windows

## Vmautostartvm


---

Utilice la opción vmautostartvm con el mandato restore VM vmrestoretype=instantaccess para especificar si la máquina virtual creada durante el proceso de acceso instantáneo se ha encendido automáticamente.

Esta opción sólo es válida para máquinas virtuales de VMware. Las máquinas virtuales deben estar alojadas en servidores VMware ESXi 5.1 o versiones posteriores. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos. Esta opción sólo es válida cuando se utiliza para una operación donde vmrestoretype=instantaccess.

## Sintaxis

---

```
>>-VMAUTOSTARTvm--+-NO-- .  
                    +-----+  
                    '-YES-'
```

## Parámetros

---

NO

La máquina virtual creada para el acceso instantáneo no se inicia automáticamente. La máquina virtual debe iniciarse manualmente. Este es el valor predeterminado. El valor predeterminado proporciona una oportunidad de volver a configurar la máquina virtual antes de encenderla, para evitar conflictos potenciales con máquinas virtuales existentes.

YES

La máquina virtual creada para el acceso instantáneo se inicia automáticamente.

## Ejemplos

---

Archivo de opciones:

```
VMAUTOSTARTvm NO
```

Línea de mandatos:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess -vmname=Oslo_verify  
-VMAUTOSTARTvm=YES
```

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmbackdir

---

La opción `vmbackdir` especifica la ubicación del disco temporal en el que el cliente guarda los archivos de control que se han creado durante las operaciones de copia de seguridad y restauración de VM completa de máquinas virtuales .

## Transportadores de datos soportados



---

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

Cuando un cliente en un nodo transportador de datos inicia una copia de seguridad de máquina virtual completa, el cliente crea los metadatos en los archivos asociados con la copia de seguridad de máquina virtual y sus datos. Los archivos que contienen los metadatos se conocen como *archivos de control*.

Durante las operaciones de copia de seguridad de VM completas, los metadatos se guardan en un disco en el nodo transportador de datos hasta que la copia de seguridad termina y tanto los datos de la máquina virtual como los archivos de control se guardan en el almacenamiento del servidor. Durante una operación de restauración de máquina virtual completa, los archivos de control se copian desde el servidor y se guardan temporalmente en el disco del transportador de datos, donde se utilizan para restaurar la máquina virtual y sus datos. Cuando termina una copia de seguridad o una operación de restauración, los archivos de control ya no son necesarios y el cliente los suprime desde la ubicación de disco temporal.

El directorio especificado por esta opción debe encontrarse en una unidad con suficiente espacio libre para contener la información de control de una copia de seguridad de máquina virtual completa.

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para transportadores de datos de Linux y Windows instalados en un servidor de copia de seguridad vStorage.

 Sistemas operativos Windows Esta opción es válida para transportadores de datos de Windows instalados en un servidor Hyper-V.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente, en la línea de mandatos como una opción para los mandatos `backup vm` o `restore vm`.

## Sintaxis

---


```
>>-VMBACKDir--directorio-----<<
```


## Parámetros

---

directorio

Especifica la vía de acceso en la que se guardan los archivos de control en el servidor de copia de seguridad.


 Sistemas operativos Windows El valor predeterminado es `c:\mnt\tsmvmbackup\fullvm\`


 Sistemas operativos Linux El valor predeterminado es `/tmp/tsmvmbackup/fullvm/`

## Ejemplos

---





Archivo de opciones:

 Sistemas operativos Windows `VMBACKD c:\mnt\tsmvmbackup\`

 Sistemas operativos Linux `VMBACKD /tmp/tsmvmbackup/`

Línea de mandatos:

```

 Sistemas operativos Windows dsmc backup vm -VMBACKUPT=fullvm -
VMBACKD=G:\virtual_machine\control_files\
 Sistemas operativos Windows dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=G:\san_temp\
 Sistemas operativos Linux dsmc backup vm -VMBACKUPT=fullvm -VMBACKD=/home/vmware/control_files
 Sistemas operativos Linux dsmc restore vm -VMBACKUPT=fullvm -VMBACKD=/home/mine/bkup_ctrl

```

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmbackuplocation


Utilice la opción `vmbackuplocation` con los mandatos `backup vm` o `restore vm` para especificar la ubicación de copia de seguridad para las operaciones de copia de seguridad y restauración de máquinas virtuales.

Esta opción sólo es válida para máquinas virtuales de VMware. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Para las operaciones de restauración, esta opción se ignora si la opción `vmrestoretype` está establecida en `mountcleanup` o `mountcleanupall`.

## Clientes soportados

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux X86\_64.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

Esta opción se debe especificar en la línea de mandatos de un mandato `backup vm` o `restore vm`. No puede establecer esta opción en el archivo de opciones del cliente.

## Sintaxis

```

>>- -VMBACKUPLoCation-- .-SERVER-.
                        ---+LOCAL---+-----><
                        '-BOTH---'

```

## Parámetros

### SERVER

Para las operaciones de copia de seguridad, especifica que se hace copia de seguridad de las máquinas virtuales en el servidor de IBM Spectrum Protect.

Para las operaciones de restauración, especifica que las máquinas virtuales se restauran desde el servidor de IBM Spectrum Protect.

Este es el valor predeterminado.

### LOCAL

Para las operaciones de copia de seguridad, especifica que se hace copia de seguridad de las máquinas virtuales en el almacenamiento de hardware. La copia de seguridad es una instantánea de imagen de máquina virtual completa, incluso si se especifica una copia de seguridad incremental.

Para crear una copia de seguridad local, la máquina virtual debe almacenarse en un almacén de datos de volumen virtual VMware (VVOL). Si algún disco virtual de la máquina virtual no está en un almacén de VVOL, no se permite la copia de seguridad local.

Para las operaciones de restauración, especifica que las máquinas virtuales se restauran de las instantáneas persistentes que están en el almacenamiento de hardware.

Mediante la restauración desde una instantánea local, sólo puede revertir una máquina virtual existente. No puede restaurar una máquina virtual suprimida ni restaurar una máquina virtual a una ubicación o nombre distinto.

La restauración local no es válida si se utilizan los parámetros siguientes para el mandato `restore vm`:

- VMNAME
- DATACENTER
- HOST
- DATASTORE
- :vmdk

Este valor tampoco es válido si la opción `vmrestoretype` está establecida en uno de los valores siguientes. Si se establecen estos valores, se muestra un mensaje de error.

- `instantaccess`
- `instantrestore`
- `mount`

Debido a que no se requiere ningún movimiento de datos de red para las instantáneas locales, las operaciones de copia de seguridad y restauración pueden ser más rápidas que las operaciones de copia de seguridad y restauración del servidor.

BOTH

Para las operaciones de copia de seguridad, especifica que se hace copia de seguridad de las máquinas virtuales en el servidor de IBM Spectrum Protect y que también se hace copia de seguridad localmente. La copia de seguridad local es siempre una instantánea de imagen completa de las máquinas virtuales, incluso si hay copias de seguridad incrementales configuradas para el servidor.

Para las operaciones de restauración, especifica que las máquinas virtuales se restauran desde la última versión activa independientemente de si es una copia de seguridad local o de servidor. Si ambas copias de seguridad activas tienen la misma indicación de fecha y hora, se utiliza la copia de seguridad local para la restauración.

Este valor no es válido con los parámetros y valores de la opción `vmrestoretype` indicados anteriormente para el valor `LOCAL`.

## Ejemplos

---

Línea de mandatos:

Realizar una copia de seguridad local y de servidor completa para la máquina virtual `vm1`:

```
dsmc backup vm vm1 -vmbackuplocation=BOTH -vmbackuptype=Fullvm
```

Realizar una restauración local para la máquina virtual `vm1`:

```
dsmc restore vm vm1 -vmbackuplocation=LOCAL
```



## Vmbackupmailboxhistory


---

La opción `vmbackupmailboxhistory` especifica si el historial del buzón se carga automáticamente con la copia de seguridad de la máquina virtual (VM) cuando se detecta IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en una máquina virtual.

## Clientes soportados

---

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los clientes que actúan como nodos de movimiento de datos para copias de seguridad de huésped VMware.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Archivo de opciones

---

 Sistemas operativos Linux Especifique esta opción en el archivo de opciones del cliente (`dsm.sys`) de una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

## Sintaxis

---

```
>>-VMBACKUPMAILBoxhistory--+-Yes-+-----><
                              '-No--'
```

## Parámetros

---

Yes

El historial del buzón se carga automáticamente con la copia de seguridad de la VM si se detecta IBM Spectrum Protect for Mail: Data Protection for Microsoft Exchange Server en una VM.

No

El historial del buzón no se carga automáticamente con la copia de seguridad de la VM.

## Ejemplos

---


Archivo de opciones:  
vmbakupmailboxhistory yes


 Sistemas operativos Linux  Sistemas operativos Windows

## Vmbakuptype


---

Utilice la opción vmbakuptype con el mandato backup VM o restore VM para especificar el tipo de copia de seguridad de máquina virtual para completar. También puede utilizar esta opción en mandatos query VM para filtrar los resultados de la consulta e incluir solo máquinas virtuales cuya copia de seguridad haya sido realizada por un tipo de copia de seguridad específico. Para obtener ejemplos, consulte la descripción del mandato query VM.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

 Sistemas operativos Linux


Puede especificar una copia de seguridad completa de la máquina virtual VMware.


 Sistemas operativos Windows


Puede especificar una copia de seguridad de máquina virtual de VMware completa o una copia de seguridad de máquina virtual Hyper-V completa.

## Clientes soportados

---


 Sistemas operativos Linux Esta opción es válida en transportadores de datos Linux instalados en un servidor de copia de seguridad vStorage. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida en transportadores de datos Windows instalados en un servidor de copia de seguridad vStorage. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida en transportadores de datos Windows instalados en un sistema Microsoft Hyper-V. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Linux Especifique esta opción en el archivo de opciones del cliente (dsm.sys) de una stanza de servidor.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

 Sistemas operativos Linux

## Sintaxis

---

```
.- Fullvm- .  
>>-VMBACKUPTYPE-- +-----+----->>
```

 Sistemas operativos Linux

## Parámetros

---

Fullvm

Especifique este valor para ejecutar una copia de seguridad de la máquina virtual completa tradicional de una máquina virtual VMware. Este es el tipo de copia de seguridad predeterminada para clientes Linux.


 Sistemas operativos Windows

## Sintaxis

---

```
.- Fullvm----- .
```

```
>>-VMBACKUPTYPE--+-HYPERVFULL+-----><
```

 Sistemas operativos Windows

## Parámetros

---

### Fullvm

Especifique este valor para ejecutar una copia de seguridad de la máquina virtual completa tradicional de una máquina virtual VMware. Este es el tipo de copia de seguridad predeterminado para clientes Windows que se ejecutan en sistemas de servidor Windows, donde el rol de servidor de Hyper-V no está habilitado. Compárese con `vmbackuptype=hypervfull`.

### HYPERVFULL

Especifica que está realizando la copia de seguridad de una o varias máquinas virtuales Hyper-V. Si habilita el rol de servidor de Hyper-V, este valor es el tipo de copia de seguridad predeterminado. Si especifica `vmbackuptype=hypervfull`, se ignoran todas las opciones que están asociadas con la copia de seguridad de archivos VMware de un servidor de copia de seguridad vStorage (por ejemplo: VMCHOST, VMCUSER, VMCPW, VMFULLNODELETE).



## Ejemplos

---


### Archivo de opciones:

```
VMBACKUPT full
```

### Línea de mandatos:

  `dsmsmc backup vm vm1 -VMBACKUPT=full -vmchost=virtctr -vmcuser=virtctr_admin -vmcpw=xxxxx`

Realiza una copia de seguridad de máquina virtual completa de `vm1.example.com` con la máquina VMware VirtualCenter, `virtctr.example.com`, en el servidor de IBM Spectrum Protect, utilizando el nombre de máquina `vm1`.

 `dsmsmc backup vm -VMBACKUPT=hypervfull -vmlist="VM 1,VM 2"`

Realiza una copia de seguridad de máquina virtual completa de las máquinas virtuales Hyper-V denominadas "VM 1" y "VM 2", en el servidor de IBM Spectrum Protect.


  Sistemas operativos Linux/Sistemas operativos Windows

## Vmchost

---

Utilice la opción `vmchost` con los mandatos `backup VM`, `restore VM` o `query VM` para especificar el nombre de host de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.


Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados

---


Este mandato es válido para los clientes que están configurados para realizar una copia de seguridad consolidada de una máquina virtual VMware. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción no es válida para copias de seguridad de Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), en el archivo de opciones del sistema del cliente (`dsm.sys`) o en la línea de mandatos.

## Sintaxis

---

```
>>-VMCHost-- --hostname-----><
```



## Parámetros

---

nombre\_host

Especifica el nombre de host de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

## Ejemplos

---

Archivo de opciones:

```
VMCH vcenter.storage.usca.example.com
```

Línea de mandatos:

```
-VMCH=esx1.storage.usca.example.com
```


 Sistemas operativos Linux  Sistemas operativos Windows

## Vmcpw

---


Utilice la opción `vmcpw` con los mandatos `backup VM`, `restore VM` o `query VM` para especificar la contraseña del ID de usuario de VMware VirtualCenter o de ESX que se ha especificado con la opción `vmcuser`.


Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción sólo es válida en clientes Linux soportados que estén instalados en un servidor de copia de seguridad vStorage utilizado para realizar copias de seguridad de una máquina virtual de VMware.

 Sistemas operativos Windows Esta opción sólo es válida en clientes Windows soportados que estén instalados en un servidor de copia de seguridad vStorage utilizado para realizar copias de seguridad de una máquina virtual de VMware. Esta opción no es válida para copias de seguridad de Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de sistema de cliente (`dsm.sys`) o en la línea de mandatos.

1. Pulse Editar > Preferencias del cliente > Copia de seguridad de máquina virtual. En el campo Contraseña, escriba la contraseña que desea guardar.
2. Pulse en Aceptar.

Como alternativa al editor de preferencias, puede almacenar la contraseña localmente usando el mandato `set password`. Por ejemplo:

```
dsmc SET PASSWORD -type=vm
vcenter.us.ibm.com Administrator secret
```

## Sintaxis

---

```
>>-VMCPw-- --pwname-----<<
```

## Parámetros

---

nombre\_contraseña

Especifica la contraseña de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

## Ejemplos

---

Archivo de opciones:  
VMCPw SECRET  
Línea de mandatos:  
-VMCPw=SECRET

**Referencia relacionada:**


Establecer contraseña

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmctlmc

---

Esta opción especifica la clase de gestión que utilizar al hacer copias de seguridad archivos de control de máquina virtual.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

De forma predeterminada, los archivos de control de máquina virtual están vinculados a la clase de gestión predeterminada. La opción vmmc se puede usar para especificar una clase de gestión diferente a la que estén vinculados los datos de virtual y los datos de control de máquina virtual. La opción vmctlmc altera temporalmente la clase de gestión predeterminada y la opción vmmc para los archivos de control de máquina virtual.



En determinadas condiciones, es posible que sea deseable o necesario vincular los archivos de control a una clase de gestión diferente a los archivos de datos.


La opción vmctlmc es necesaria si se realiza una copia de seguridad de los archivos de datos de máquina virtual en cinta. Debe realizarse una copia de seguridad de los archivos de control de máquina virtual en una agrupación de almacenamiento basada en disco que no migre a una cinta. La agrupación de almacenamiento puede estar compuesta de volúmenes de acceso aleatorios y volúmenes de archivos secuenciales; también puede ser una agrupación desduplicada. Utilice la opción vmctlmc para especificar una clase de gestión que almacene datos en dicha agrupación de almacenamiento.

Restricción: La clase de gestión que especifica la opción vmctlmc sólo determina la agrupación de almacenamiento de destino para los archivos de control de máquina virtual. La retención de los archivos de control viene determinada por la opción vmmc, si está especificada, o por la clase de gestión predeterminada. La retención de los archivos de control de máquina virtual siempre coincide con la retención de los archivos de datos de máquina virtual.

## Clientes soportados

---

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los clientes que son nodos de movimiento de datos que protegen las máquinas virtuales de VMware.


 Sistemas operativos Windows Esta opción es válida para los clientes que actúan como nodos de transportador de datos que protegen máquinas virtuales Microsoft Hyper-V.


La opción sólo se puede utilizar para copias de seguridad de máquina virtual que utilizan una modalidad de copia de seguridad incremental, constante.

Esta opción solo está disponible si tiene licencia para utilizar IBM Spectrum Protect para entornos virtuales: Protección de datos para o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del sistema dsm.sys.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente dsm.opt.

## Sintaxis

---

```
>>-VMCTLmc--class_name-----<<
```

## Parámetros

---

nombre\_clase

Especifica una clase de gestión que se aplica para realizar copia de seguridad de los archivos de control de máquina virtual. Si no establece esta opción, se utiliza la clase de gestión que se especifica en la opción vmmc. Si no establece esta opción y no está

establecida la opción vmc, se utilizará la clase de gestión predeterminada del nodo.

## Ejemplos

---

Archivo de opciones:  
vmctlmc diskonlymc  
Línea de mandatos:  
No se aplica.


 Sistemas operativos Linux  Sistemas operativos Windows

## Vmcuser

---

Utilice la opción vmcuser con los mandatos backup VM, restore VM o query VM para especificar el nombre de usuario de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.


Utilice VirtualCenter si está disponible. Si no puede utilizar un servidor de VirtualCenter y necesita realizar copias de seguridad de varios sistemas de archivos en varios servidores de ESX, no especifique esta opción; en lugar de ello, especifique la opción con el mandato para que pueda cambiarse en función de cada servidor de ESX.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados

---


Esta opción es válida para los clientes que están configurados para realizar una copia de seguridad consolidada de máquinas virtuales VMware. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción no es válida para copias de seguridad de Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del cliente (dsm.opt), en el archivo de opciones del sistema del cliente (dsm.sys) o en la línea de mandatos.

## Sintaxis

---

```
>>-VMCuser-- --username-----><
```

## Parámetros

---

nombre\_usuario

Especifica el nombre de usuario de VMware VirtualCenter o del servidor ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad.

Cuando se trabaja con un centro virtual, es necesario un ID de usuario con acceso al sistema Windows que aloja el centro virtual. Este ID de usuario debe tener privilegios de administrador o los privilegios mínimos que se identifican en la nota técnica 1659544.

## Ejemplos

---

Archivo de opciones:  
VMCuser administrator

Línea de mandatos:

```
backup vm -VMCuser=nombredominio\administrador
```

Línea de mandatos:

Ejemplo de conexión a un servidor de ESX:

```
backup vm -VMCuser=root
```


 Sistemas operativos Linux  Sistemas operativos Windows

## Vmdatastorethreshold

---


Utilice la opción `vmdatastorethreshold` para establecer el porcentaje de umbral de uso de espacio de cada almacén de datos de VMware de una máquina virtual.


Cuando especifica esta opción, el uso de espacio se comprueba antes de que se cree una instantánea de máquina virtual. Si se excede el umbral, no se hace una copia de seguridad de la máquina virtual. Si establece esta opción, puede evitar errores de falta de espacio cuando realice copias de seguridad de máquinas virtuales.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados


---


 Sistemas operativos Linux Puede utilizar esta opción con clientes x86\_64 Linux admitidos.

 Sistemas operativos Windows Puede utilizar esta opción con clientes Windows de 64 bits admitidos.

## Archivo de opciones

---

 Sistemas operativos Linux Puede especificar esta opción en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos mediante el mandato `backup vm`. También puede incluir esta opción en el servidor de IBM Spectrum Protect Versión 7.1.5 o posterior en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

 Sistemas operativos Windows Puede especificar esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos mediante el mandato `backup vm`. También puede incluir esta opción en el servidor de IBM Spectrum Protect Versión 7.1.5 o posterior en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

## Sintaxis

---

```
>>-VMDATASTOREThreshold---porcentaje-----><
```

## Parámetros

---

### *porcentaje*

Especifica el porcentaje de umbral de cada almacén de datos de VMware de la máquina virtual de la que se va a realizar una copia de seguridad. Puede especificar un entero comprendido entre 0 y 100. El valor predeterminado es 100. Si no establece esta opción, el cliente inicia la copia de seguridad de máquina virtual sin verificar primero el uso de espacio existente.

Requisitos:

- Asegúrese de que el umbral sea lo suficientemente bajo para que la instantánea no utilice todo el espacio disponible en los almacenes de datos de VMware. De lo contrario, se quedará sin espacio en los almacenes de datos de VMware y la instantánea no se creará.
- Si utiliza varios clientes que actúan como nodos de transportador de datos, debe añadir esta opción al archivo de opciones para cada transportador de datos.
- El cliente comprueba el uso de datos del almacén de datos de VMware que contiene las instantáneas de disco de máquina virtual. De forma predeterminada, las instantáneas se crean en el mismo directorio que el del archivo de disco virtual (`.vmdk`).

Si cambia la ubicación de la instantánea a un directorio nuevo en el mismo almacén de datos o a otro almacén de datos con la opción `workingDir` en el archivo de configuración de la máquina virtual, asegúrese de que la vía de acceso del directorio de trabajo sea correcta. Si la vía de acceso es incorrecta, el cliente podría validar el uso de datos del almacén de datos erróneo.

Si utiliza la opción `EXCLUDE.VMDISK` para excluir uno o varios discos de una copia de seguridad, la comprobación de umbral continúa ejecutándose en esos discos. Aunque no se realice la copia de seguridad de esos discos, VMware continúa realizando una instantánea de ellos.

Los discos independientes no se comprueban durante la verificación de espacio porque una instantánea de estos discos no utiliza espacio de ningún almacén de datos de VMware.

## Ejemplo 1

---

La máquina virtual `vm1` abarca `datastore1` y `datastore2`. Establezca la opción `vmdatastorethreshold` en 90 para asegurarse de que ambos almacenes de datos de VMware estén al 90% de su capacidad antes de que se realice la copia de seguridad de la máquina virtual.

Archivo de opciones:

```
vmdatastorethreshold 90
```

Línea de mandatos:

```
dsmc backup vm vm1 -vmdatastorethreshold=90
```

## Ejemplo 2

---

El umbral del almacén de datos de `datastore2` está establecido en 85. El umbral del almacén de datos se ha superado durante la copia de seguridad de la máquina virtual `vm5`. Se visualiza el siguiente mensaje de error:

```
ANS14200E No se ha podido realizar una copia de seguridad de la máquina virtual
'vm5' porque el
uso de datos del almacén de datos 'datastore2' ha excedido el
umbral de almacén de datos
del 85%.
```

Aumente el valor de la opción `vmdatastorethreshold` a 95 y reinicie la copia de seguridad.

Archivo de opciones:

```
vmdatastorethreshold 95
```

Línea de mandatos:

```
dsmc backup vm vm5 -vmdatastorethreshold=95
```

**Referencia relacionada:**


Backup VM

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmdefaultdvportgroup

---

Utilice esta opción para especificar el grupo de puertos que utilizarán las NIC durante las operaciones `restore vm` para una máquina virtual que estaba conectada a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no contiene un grupo de puerto virtual distribuido similar.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción no se aplica a operaciones de copia de seguridad o restauración para máquinas virtuales Microsoft Hyper-V.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

 Sistemas operativos Windows Esta opción es válida para clientes Windows instalados en un servidor de copia de seguridad vStorage.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (`dsm.opt`), en el archivo de opciones del sistema cliente (`dsm.sys`), o bien especifíquela como parámetro de línea de mandatos en el mandato `restore vm`.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), o especifíquela como un parámetro de línea de mandatos en el mandato `restore vm`.

## Sintaxis

---

```
>>-VMDEFAULTDVPORTGROUP--portgroup_name-----<<
```

## Parámetros

---

*portgroup name*

Especifica el nombre del grupo de puertos que se utilizará. El nombre de grupo de puertos distingue entre mayúsculas y minúsculas.

## Ejemplos

---

Archivo de opciones:

```
VMDEFAULTDVPORTRGROUP dvPortGroup
```

Línea de mandatos:

```
dsmc restore vm vm123 -VMDEFAULTDVPORTRGROUP=dvPortGroup
```

### Referencia relacionada:

Vmdefaultnetwork


Vmdefaultdvswitch

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmdefaultdvswitch

---

Utilice esta opción para especificar el conmutador virtual distribuido (dvSwitch) que contiene el grupo de puertos que establezca en la opción vmdefaultdvportgroup. La opción no tiene efecto a menos que también especifique la opción vmdefaultdvportgroup.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción no se aplica a operaciones de copia de seguridad o restauración para máquinas virtuales Microsoft Hyper-V.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

 Sistemas operativos Windows Esta opción es válida para clientes Windows instalados en un servidor de copia de seguridad vStorage.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato restore vm.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt), o especifíquela como un parámetro de línea de mandatos en el mandato restore vm.

## Sintaxis

---

```
>>-VMDEFAULTDVSWITCH--dvSwitch-----<<
```

## Parámetros

---

*dvSwitch*

Especifica el nombre del conmutador virtual que se utilizará. El nombre de conmutador virtual distingue entre mayúsculas y minúsculas.

## Ejemplos

---

Archivo de opciones:

```
VMDEFAULTDVSWITCH dvSwitch
```

Línea de mandatos:

```
dsmc restore vm vm123 -VMDEFAULTDVSWITCH=dvSwitch -VMDEFAULTDVPORTRGROUP=dvPortGroup
```

### Referencia relacionada:


Vmdefaultdvportgroup

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmdefaultnetwork

---


Utilice esta opción para especificar la red para que utilizarán las NIC durante una operación restore vm, para una máquina virtual que se había conectado a un grupo de puertos virtuales distribuidos cuando se realizó la copia de seguridad, pero el host de destino para la operación de restauración no tiene ningún grupo de puerto conmutador distribuido configurado.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción no se aplica a operaciones de restauración para máquinas virtuales Microsoft Hyper-V.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes Linux instalados en un servidor de copia de seguridad vStorage.

 Sistemas operativos Windows Esta opción es válida para clientes Windows instalados en un servidor de copia de seguridad vStorage.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato restore vm.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt), o especifíquela como un parámetro de línea de mandatos en el mandato restore vm.

## Sintaxis

---

```
>>-VMDEFAULTNETWORK--vm_network_name-----<<
```

## Parámetros

---

*vm\_network\_name*

Especifica el nombre de la red de máquina virtual que se utilizará. El nombre de red distingue entre mayúsculas y minúsculas. Si el nombre contiene caracteres de espacio, ciérrelo entre comillas.

## Ejemplos

---

Archivo de opciones:

```
VMDEFAULTNETWORK "VM Network"
```


Línea de mandatos:

```
dsmc restore vm vm123 -VMDEFAULTNETWORK="VM Network"
```

### Referencia relacionada:

Vmdefaultdvportgroup

Vmdefaultdvswitch

 Sistemas operativos Windows

## Vmdiskprovision


---

Utilice la opción vmdiskprovision para especificar una política de suministro para el archivo de disco virtual que se utiliza para restaurar los datos de la máquina virtual VMware. Esta opción es válida sólo para las operaciones restore vm donde se especifique `vmrestoretype=instantrestore`.

Esta opción sólo es válida para máquinas virtuales de VMware. Las máquinas virtuales deben estar alojadas en servidores VMware ESXi 5.1 o versiones posteriores. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

## Sintaxis

---

```
. -THICK- .  
>>-VMDISKPROvision-----<<  
'-THIN--'
```

## Parámetros

---

### THICK

Crea un disco virtual en el formato thick predeterminado; donde el espacio necesario para el disco virtual se asigna cuando se crea el disco virtual. Éste es el valor predeterminado.

### THIN

Crea un disco virtual en un formato thin.

Nota: Si va a restaurar una máquina virtual y especifica el suministro ligero, el almacén de datos en el que restaura la máquina virtual debe tener suficiente espacio libre para acomodar la capacidad total del disco de VM y no solo la cantidad de disco que se utiliza. Por ejemplo, una máquina virtual de aprovisionamiento fino tiene 300 GB de capacidad total para el disco, no puede restaurar esa máquina virtual a un almacén de datos que tenga menos de 300 GB disponibles, incluso si solo se utiliza una porción de la capacidad total.

## Ejemplos

---

Archivo de opciones:

```
VMDISKPROvision THIN
```

Línea de mandatos:

```
dsmc restore vm Mainz -VMRESToretype=INSTANTRestore  
-VMTEMPDatastore=Temporary_Datastore -VMDISKPROvision=THIN
```


 Sistemas operativos Linux  Sistemas operativos Windows

## Vmenabletemplatebackups

---

La opción `vmenabletemplatebackups` especifica si el cliente realiza una copia de seguridad de máquinas virtuales de plantillas de VMware cuando protege máquinas virtuales en un servidor vCenter. No se puede realizar la copia de seguridad de las máquinas virtuales de plantillas de VMware cuando éstas están en un host ESXi porque ESXi no soporta plantillas.

Cuando esta opción está habilitada, puede incluir máquinas plantilla de VMware en las operaciones de copia de seguridad de máquina virtual completa. Puede utilizar el mandato Backup VM existente y la opción `DOMAIN.VMFULL` para especificar las máquinas virtuales que se incluirán en la operación de copia de seguridad.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


No se admiten las copias de seguridad incrementales y no se toman instantáneas, por lo que debe utilizar `MODE=IFFULL`. Utilice `MODE=IFFULL` para forzar una copia de seguridad nueva de las máquinas virtuales de plantilla de VMware, incluso si no se han modificado desde la última copia de seguridad.

Si se habilita la opción `vmenabletemplatebackups`, cualquier proceso de copia de seguridad iniciado utilizando `MODE=IFINCREMENTAL` se procesa mediante `MODE=IFFULL`. Las máquinas virtuales de plantilla de VMware se incluyen en una copia de seguridad sólo si se han modificado desde que se produjo la última copia de seguridad.

Con esta opción habilitada, asegúrese de que las opciones de `vmvstortransport` incluyen `NBDSSL` o `NBD`. Si sólo se utilizan las modalidades de transporte `SAN` o `HOTADD` con esta opción habilitada, las copias de seguridad de las máquinas de plantilla fallarán.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.



 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.



## Archivo de opciones

 Sistemas operativos Linux Puede definir esta opción en la línea de mandatos, el archivo de opciones de sistema de cliente (dsm.sys), el archivo de opciones de cliente (dsm.opt) o en un conjunto de opciones de cliente del servidor.

 Sistemas operativos Windows Puede establecer esta opción en la línea de mandatos, en el archivo de opciones de cliente (dsm.opt), o en un conjunto de opciones de cliente del servidor.

 Sistemas operativos Linux  Sistemas operativos Windows También puede establecerla en el editor de preferencias en la ficha Copia de seguridad de la máquina virtual (seleccione la opción Plantillas de máquina virtual para copia de seguridad).

## Sintaxis

```
          .-No-----.  
>>-VMENABLETEMPlebackups---+---+-----+---+-----<<  
          '-Yes-'
```

## Parámetros

No

Especifica que las máquinas virtuales de plantilla no se incluyen en las operaciones de copia de seguridad de máquina virtual completa; este es el valor predeterminado.

Yes

Especifica que las máquinas virtuales de plantilla se incluyen en las operaciones de copia de seguridad de máquina virtual completa.

## Ejemplos

Archivo de opciones

```
vmenabletemplatebackups yes
```

Línea de mandatos

Realizar una copia de seguridad de una máquina virtual de plantilla de VMware

```
dsmc backup vm vmname -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla.

Línea de mandatos

Restaurar una máquina virtual de plantilla de VMware en la misma ubicación y con el mismo nombre

```
dsmc restore vm vmname -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla.

Línea de mandatos

Restaurar una máquina virtual de plantilla en una ubicación nueva

```
dsmc restore vm nombre_máquina_virtual -vmname=win7x64  
-datastore=datastore22 -host=supersht.labx.com  
-datacenter="Lab Center" -VMENABLETEMPLATEBACKUPS=YES
```

donde *vmname* es el nombre de la máquina de plantilla. "win7x64" es el nuevo nombre de máquina virtual de plantilla. También se incluirán el centro de datos, el host y el almacén de datos nuevos.

### Referencia relacionada:

Backup VM

Restore VM

Domain.vmfull

 Sistemas operativos Windows


## Vmexpireprotect


Utilice esta opción para proteger instantáneas de máquina virtual, de forma que no puedan caducar mientras está en curso una operación de restauración instantánea o acceso instantáneo de máquinas virtuales VMware o una restauración de nivel de archivo de una máquina virtual VMware. Utilice esta opción para proteger instantáneas de máquina virtual, de forma que no puedan caducar mientras está en curso una operación de restauración instantánea o acceso instantáneo de máquinas virtuales Hyper-V o una restauración de nivel de archivo de una máquina virtual Hyper-V.

Durante una operación de montaje o restauración, la instantánea en el servidor de IBM Spectrum Protect se bloquea para impedir que caduque durante la operación. En cambio, se puede producir el vencimiento si otra instantánea se añade a la secuencia de instantáneas. Esta opción especifica si impedir o permitir la caducidad de instantáneas durante una operación de restauración o montaje.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción se puede utilizar con clientes Windows soportados que están configurados para restaurar máquinas virtuales.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

## Archivo de opciones

---

Para restaurar máquinas virtuales VMware, establezca esta opción en el archivo de opciones del cliente (dsm.opt) o en un mandato restore vm donde la opción vmrestoretype se define en instantaccess o instantrestore.

Para restaurar copias de seguridad a nivel de archivo de las máquinas virtuales, especifique esta opción en el archivo de opciones del cliente o en el mandato restore vm.

Nota: Las copias de seguridad de nivel de archivo se han creado con clientes de copia de seguridad y archivado de la versión 7.1 o anteriores.

## Sintaxis

---

```
.-No--.  
>>-VMEXPIREPROTECT---+-Yes-+-----<<
```

## Parámetros

---

Yes

Especifique Sí para evitar que la instantánea caduque. La instantánea en el servidor de IBM Spectrum Protect se bloquea y se protege que la instantánea caduque durante una operación de restauración o montaje.

No

Especifique No para inhabilitar la protección de caducidad. Este es el valor predeterminado. La instantánea en el servidor de IBM Spectrum Protect no se bloquea y la instantánea no está protegida frente a la caducidad. Si la instantánea que se está montando o restaurando caduca, el resultado de dicha operación será imprevisible. Por ejemplo, el punto de montaje puede quedar inutilizable o contener errores. Sin embargo, la caducidad no afecta la copia activa actual de las máquinas virtuales. La copia activa no puede vencer durante una operación.

Cuando la instantánea se encuentra en un servidor de réplica de destino, no se puede bloquear porque se encuentra en modalidad de sólo lectura. Un intento de bloqueo por parte del servidor puede provocar que la operación de montaje o restauración falle.

Para evitar el intento de bloqueo e impedir que se produzca este error, inhabilite la protección de caducidad especificando No, o estableciendo esta opción a predeterminada.

## Ejemplos

---

Archivo de opciones del cliente:

```
VMEXPIREPROTECT YES
```

Línea de mandatos:

Ejecute una operación de acceso instantáneo para una máquina virtual VMware:

```
dsmc restore vm vml -vmname=new_vml -vmrestoretype=instantaccess  
-vmexpireprotect=no
```

Para restaurar archivos de una copia de seguridad de máquina virtual, utilice la GUI de Agente de recuperación de IBM Spectrum Protect.

Para obtener información sobre el Agente de recuperación de IBM Spectrum Protect, consulte la documentación de IBM Spectrum Protect para entornos virtuales.

 Sistemas operativos Windows

## Vmiscsiadapter

---

Esta opción especifica qué adaptador iSCSI, en el host ESX, se debe utilizar para la restauración instantánea y las operaciones de acceso instantáneo de máquinas virtuales VMware.

### Clientes soportados

---

Esta opción es válida para clientes Windows de 64 bits que están configurados como transportadores de datos que realizan copias de seguridad de máquinas virtuales VMware.

### Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt). También puede especificar esta opción como un parámetro de línea de mandato en el mandato `restore vm` que inicia una restauración instantánea o una operación de acceso instantáneo. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

### Sintaxis

---

```
>>-VMISCSIAdapter=--iSCSI_adapter_name-----<<
```

iSCSI\_adapter\_name

Especifica el nombre del adaptador iSCSI que se conectará en el host ESX. Si no especifica esta opción, se utiliza el primer adaptador iSCSI que se encuentra en el host.

### Ejemplos

---

Archivo de opciones:

```
vmiscsiadapter "vmhba36"
```

Línea de mandatos:

```
dsmc restore vm "Haifa" -VMREStoretype=INSTANTAccess -vmname="Haifa_verify" -  
VMISCSIAdapter="vmhba36"
```

 Sistemas operativos Windows

## Vmiscsiserveraddress

---


Utilice la opción `vmiscsiserveraddress` con el mandato `restore VM` para especificar el nombre de host o la dirección IP del servidor iSCSI que proporciona los destinos iSCSI para las operaciones de restauración instantánea y de acceso instantáneo.

La opción `vmiscsiserveraddress` es válida para todas las operaciones instantáneas (`vmrestoretype=instantaccess` y `vmrestoretype=instantrestore`) para las máquinas virtuales de VMware.

Las máquinas virtuales deben estar alojadas en servidores VMware ESXi 5.1 o versiones posteriores. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

### Clientes soportados

---

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

### Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

### Sintaxis

---

```
>>-VMISCSIserveraddress-- --nombre de host de servidor iSCSI o dirección IP-<<
```

### Parámetros

---

nombre de host de servidor iSCSI o dirección IP

Especifique el nombre de host o la dirección IP del servidor iSCSI que suministra los discos de destino de iSCSI. Este servidor iSCSI se debe conectar a la máquina transportadora de datos con todos los hosts de ESX que se utilizan para las operaciones de restauración instantánea. Si no se especifica `vmiscsiserveraddress`, se utilizará el nombre de host o la dirección IP de la máquina transportadora de datos.

Para operaciones de restauración instantáneas, la dirección IP de la tarjeta de red de la máquina del transportador de datos que se utiliza para la transferencia de iSCSI debe ser la misma en la misma subred que el adaptador iSCSI del host ESX.

Para operaciones de montaje de restauración de archivo, los sistemas proxy de montaje de Windows y Linux deben estar en el mismo rango de red.

## Ejemplos

---

Archivo de opciones:

```
VMISCSIServeraddress 192.168.42.50
```

Línea de mandatos:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess -vmname=Oslo_verify  
-VMISCSIServeraddress=odin.oslo.no.xyzco.com
```

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmlimitperdatastore

---

La opción `vmlimitperdatastore` especifica el número de máquinas virtuales (VM) y discos virtuales en un almacén de datos que se pueden procesar durante una operación de copia de seguridad optimizada.


Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.


La opción `vmlimitperdatastore` funciona con las opciones `vmmaxparallel`, `vmmaxbackupsessions` y `vmlimitperhost` para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows compatibles. Esta opción no es válida para copias de seguridad de Data Protection for Microsoft Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Linux Esta opción es válida en el archivo de opciones del sistema del cliente (`dsm.sys`), en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
>>>-VMLIMITPERDatastore-- .-0-----.  
--++-----++-----<<<  
'-entero-'
```

## Parámetros

---

*entero*

Especifica el número máximo en cualquier almacén de datos de máquinas virtuales que se incluyen durante una operación de seguridad optimizada. El máximo que puede especificar es 50 máquinas virtuales. El valor predeterminado es 0 (cero).

Si se especifica 0, se indica que no está preocupado por la cantidad de máquinas virtuales (VM) de las que se pueden hacer copias de seguridad en paralelo desde un almacén de datos. En lugar de ello, quiere limitar el número máximo de máquinas virtuales que incluir en una copia de seguridad utilizando el valor que se especifique en la opción vmmxparallel. La opción vmlimitperdatastore se impone incluso cuando existen datos de máquina virtual en dos o más almacenes de datos.

## Ejemplos




Archivo de opciones  
VMLIMITPERD 5

Línea de mandatos:  
dsmc backup vm -VMLIMITPERD=5

### Referencia relacionada:

Backup VM  
Domain.vmfull  
Vmmxbackupsessions  
Vmmxparallel  
Vmlimitperhost

### Información relacionada:


 Realización de copias de seguridad de varias máquinas virtuales en paralelo  
 Sistemas operativos Linux  Sistemas operativos Windows

## Vmlimitperhost


La opción vmlimitperhost especifica el número de máquinas virtuales (VM) y discos virtuales de un host que se pueden procesar en paralelo durante una operación de seguridad optimizada.


Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.

La opción vmlimitperhost funciona con las opciones vmmxparallel, vmmxbackupsessions y vmlimitperdatastore para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


## Clientes soportados

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows compatibles. Esta opción no es válida para copias de seguridad de Data Protection for Microsoft Hyper-V.

## Archivo de opciones

 Sistemas operativos Linux Esta opción es válida en el archivo de opciones del sistema del cliente (dsm.sys), en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

```
>>-VMLIMITPERHost-- .-0-----  
                    --+-----+-----><  
                    '-entero-'
```

## Parámetros

entero

Especifica el número máximo de máquinas virtuales en cualquier servidor ESX que se pueden incluir en una operación de seguridad optimizada. El máximo que puede especificar es 50 máquinas virtuales. El valor predeterminado es 0 (cero). Si se especifica 0 se indica que no está preocupado por la cantidad de máquinas virtuales (VM) de las que se pueden hacer copias de seguridad en paralelo desde un servidor ESX. En lugar de ello, quiere limitar el número máximo de máquinas virtuales que incluir en una copia de seguridad utilizando el límite especificado en la opción vmmxparallel.

## Ejemplos

---

Archivo de opciones

```
VMLIMITPERH 5
```

Línea de mandatos:

```
dsmc backup vm -VMLIMITPERH=5
```

### Referencia relacionada:


Backup VM


Domain.vmfull

Vmmxparallel

Vmlimitperhost

### Información relacionada:

 Realización de copias de seguridad de varias máquinas virtuales en paralelo

 Sistemas operativos Windows

## Vmlist

---

La opción vmlist está en desuso para operaciones de copia de seguridad de Hyper-V. Para especificar que una o más máquinas virtuales (VM) de Hyper-V se incluyan en operaciones de copia de seguridad de Data Protection for Microsoft Hyper-V, utilice la opción domain.vmfull o especifique las máquinas virtuales cuando ejecute el mandato backup vm.

Si necesita utilizar la opción vmlist, consulte la documentación en los releases anteriores de IBM Spectrum Protect.

### Referencia relacionada:

Domain.vmfull

Backup VM

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmmxbackupsessions

---


La opción vmmxbackupsessions especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que trasladan de la máquina virtual (VM) al servidor datos que se pueden incluir en una operación de seguridad optimizada.


Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.


La opción vmmxbackupsessions funciona con las opciones vmmxparallel, vmlimitperdatastore y vmlimitperhost para optimizar las operaciones de copia de seguridad y ayudar a controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.

## Clientes soportados

---


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows compatibles. Esta opción no es válida para copias de seguridad de Data Protection for Microsoft Hyper-V.

## Archivo de opciones

---

 Sistemas operativos Linux Esta opción es válida en el archivo de opciones del sistema del cliente (dsm.sys), en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
.-vmmaxparallelvalue-.
>>-VMMAXBACKUPSEssions-- --+-----+-----+-----><
                              '-entero-'
```

## Parámetros

---

### entero

Especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que se pueden crear durante la operación de seguridad.

Revise la información siguiente para utilizar la opción vmmaxbackupsessions junto con la opción vmmaxparallel o el parámetro de servidor maxnummp:

### vmmaxparallel

La opción vmmaxparallel especifica el número máximo de máquinas virtuales de las que se puede realizar copia de seguridad en el Servidor de IBM Spectrum Protect en un momento dado. El valor de la opción vmmaxbackupsessions tiene que ser igual o superior al valor de la opción vmmaxparallel.

Si el valor es inferior al valor de la opción vmmaxparallel, se devuelve el siguiente mensaje y el valor cambia al mismo valor que la opción vmmaxparallel:

```
ANS9995W El valor de la opción VMMAXBACKUPSESSIONS es valor_número. Este valor debe ser mayor o igual que el valor de la opción VMMAXPARALLELm, que es valor_número. El valor se establecerá en el valor de la opción VMMAXPARALLEL.
```

### maxnummp

El parámetro de servidor maxnummp especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor cuando el destino de la copia de la agrupación de almacenamiento es FILE o TAPE. El parámetro maxnummp tiene que ser igual o mayor que los valores de opción vmmaxparallel y vmmaxbackupsessions. Cuando varias instancias del cliente están realizando copias de seguridad de archivos o cuando un único cliente realiza copias de seguridad paralelas, pueden ser necesarios más puntos de montaje.

Si los valores de vmmaxparallel o vmmaxbackupsessions superan el valor de maxnummp, se mostrarán los mensajes ANS0266I y otros. Según el mensaje, el cliente reduce el valor de la opción vmmaxparallel para que coincida con el número especificado por el parámetro maxnummp o prohíbe que se abran sesiones adicionales para la máquina virtual especificada. En cualquiera de estas situaciones, la operación de seguridad continúa.

Si se detectan errores ANS0266I adicionales, el cliente reduce el valor vmmaxparallel en 1 e intenta continuar con la copia de seguridad. Si vmmaxparallel se reduce a 1 y el cliente recibe más errores ANS0266I, el cliente finaliza la copia de seguridad y emite el error siguiente:

```
ANS5228E Una operación de copia de seguridad ha fallado porque VMMAXPARALLEL fue reducida a 1 y el cliente todavía no puede obtener un punto de montaje del servidor.
```

Póngase en contacto con el administrador del servidor si quiere que el valor actualmente definido para maxnummp aumente, con el fin de que el nodo pueda dar soporte a sesiones adicionales de copias de seguridad paralelas.

En Windows Server 2012 y 2012 R2, durante las copias de seguridad de máquina virtual Hyper-V, IBM Spectrum Protect crea instantáneas VSS de todos los volúmenes que contienen datos de máquina virtual. Los datos de seguridad se leen desde las instantáneas de VSS y no desde los datos que hay en el sistema de archivos en directo. En muchos casos, cuando IBM Spectrum Protect intenta crear varias instantáneas de forma simultánea, el proveedor de software VSS puede no ser capaz de cumplir una solicitud de instantánea para varias máquinas virtuales. Las anomalías se producen debido a que el proveedor de instantáneas de software VSS no puede gestionar la carga que crean varias copias de seguridad que se intentan en paralelo. Para evitar este problema, use un proveedor de instantáneas de hardware VSS en lugar de un proveedor de software VSS.

El valor máximo que puede especificar es de 100 sesiones. El predeterminado es el valor definido para la opción vmmaxparallel.

## Ejemplos

---


Archivo de opciones  
VMMAXBACKUPS 10

Línea de mandatos:  
dsmc backup vm -VMMAXBACKUPS=10

### Referencia relacionada:

Backup VM  
Domain.vmfull  
Vmmaxparallel  
Vmlimitperdatastore  
Vmlimitperhost

**Información relacionada:**

 Realización de copias de seguridad de varias máquinas virtuales en paralelo

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmmaxparallel

---

La opción `vmmaxparallel` se utiliza para configurar copias de seguridad optimizadas de varias máquinas virtuales utilizando una sola instancia del cliente de archivado y copia de seguridad. Esta opción especifica el número máximo de máquinas virtuales de las que se puede hacer una copia de seguridad en el Servidor de IBM Spectrum Protect en cualquier momento dado.

Una operación de seguridad optimizada es aquella en la que se habilita la funcionalidad de copia de seguridad en paralelo a nivel de máquina virtual, disco virtual o subdisco.


La opción `vmmaxparallel` funciona con las opciones `vmmaxbackupsessions`, `vmlimitperhost` y `vmlimitperdatastore` para optimizar las operaciones de copia de seguridad y controlar la cantidad de recursos que puede crear la copia de seguridad en un host de la infraestructura vSphere. Ajuste los valores de estas opciones para encontrar los valores que proporcionen un rendimiento óptimo para las copias de seguridad del entorno.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

Para Data Protection for Microsoft Hyper-V, esta opción sólo es válida para operaciones de copia de seguridad Hyper-V en los sistemas operativos Windows Server 2012 y 2012 R2.

## Clientes soportados


---


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

 Sistemas operativos Linux Esta opción es válida en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos para el mandato Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos para el mandato Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
..-4-----.  
>>-VMMAXParallel--+-----+-----<<  
                  '-entero-'
```

## Parámetros

---

*entero*

Especifica el número máximo de máquinas virtuales de las que se puede hacer una copia de seguridad en cualquier momento dado durante una operación de copia de seguridad optimizada. El valor predeterminado es 4. El máximo es 50.

Consejo: Cuando utiliza la eliminación de duplicados del lado del cliente, se inicia una sesión de eliminación de duplicados de datos para cada máquina virtual. Esta sesión de eliminación de duplicados de datos no se cuenta como una de las sesiones de `vmmaxparallel`.

Revise la información siguiente para utilizar la opción `vmmaxparallel` junto con la opción `vmmaxbackupsessions` o el parámetro de servidor `maxnummp`:

`vmmaxbackupsessions`



vmmaxbackupsessions especifica el número máximo de sesiones que trasladan datos de la máquina virtual al servidor que se pueden incluir en una operación de seguridad optimizada. El valor de la opción vmmaxbackupsessions tiene que ser igual o superior al valor de la opción vmmaxparallel.

#### maxnummp

El parámetro de servidor maxnummp especifica el número máximo de puntos de montaje que un nodo puede utilizar en el servidor cuando el destino de la copia de la agrupación de almacenamiento es FILE o TAPE. El parámetro maxnummp tiene que ser igual o mayor que los valores de opción vmmaxparallel y vmmaxbackupsessions. Cuando varias instancias del cliente están realizando copias de seguridad de archivos o cuando un único cliente realiza copias de seguridad paralelas, pueden ser necesarios más puntos de montaje.

Si los valores de vmmaxparallel o vmmaxbackupsessions superan el valor de maxnummp, se mostrarán los mensajes ANS0266I y otros. Según el mensaje, el cliente reduce el valor de la opción vmmaxparallel para que coincida con el número especificado por el parámetro maxnummp o prohíbe que se abran sesiones adicionales para la máquina virtual especificada. En cualquiera de estas situaciones, la operación de seguridad continúa.

Si se detectan errores ANS0266I adicionales, el cliente reduce el valor vmmaxparallel en 1 e intenta continuar con la copia de seguridad. Si vmmaxparallel se reduce a 1 y el cliente recibe más errores ANS0266I, el cliente finaliza la copia de seguridad y emite el error siguiente:

ANS5228E Una operación de copia de seguridad ha fallado porque VM\_MAXPARALLEL fue reducida a 1 y el cliente todavía no puede obtener un punto de montaje del servidor.


Póngase en contacto con el administrador del servidor si quiere que el valor actualmente definido para maxnummp aumente, con el fin de que el nodo pueda dar soporte a sesiones adicionales de copias de seguridad paralelas.

En Windows Server 2012 y 2012 R2, durante las copias de seguridad de máquina virtual Hyper-V, IBM Spectrum Protect crea instantáneas VSS de todos los volúmenes que contienen datos de máquina virtual. Los datos de seguridad se leen desde las instantáneas de VSS y no desde los datos que hay en el sistema de archivos en directo. En muchos casos, cuando IBM Spectrum Protect intenta crear varias instantáneas de forma simultánea, el proveedor de software VSS puede no ser capaz de cumplir una solicitud de instantánea para varias máquinas virtuales. Las anomalías se producen debido a que el proveedor de instantáneas de software VSS no puede gestionar la carga que crean varias copias de seguridad que se intentan en paralelo. Para evitar este problema, use un proveedor de instantáneas de hardware VSS en lugar de un proveedor de software VSS.

## Ejemplos

Archivo de opciones

VM\_MAXP 10

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `dsmc backup vm -VM_MAXP=10`

#### Referencia relacionada:


Backup VM


Domain.vmfull

Vmlimitperhost

Vmlimitperdatastore

#### Información relacionada:

 Realización de copias de seguridad de varias máquinas virtuales en paralelo


 Sistemas operativos Windows

## Vmmaxpersnapshot

Utilice la opción vmmaxpersnapshot para especificar el número máximo de máquinas virtuales (VM) que deben incluirse en una instantánea de Hyper-V. La copia de seguridad de las máquinas virtuales de la instantánea se realiza en el servidor de IBM Spectrum Protect.

Aumentando el número de VMs de una instantánea, puede reducir el número de instantáneas que se toman para una operación de copia de seguridad. Esta capacidad reduce la contienda de planificación que puede producirse durante las operaciones de copia de seguridad de clúster de las VM en Volúmenes compartidos en clúster (CSV).

una instantánea con más VMs tarda más tiempo en finalizar y aumenta la carga del sistema. Un número mayor de máquinas virtuales significa que la instantánea persiste más tiempo, lo que puede afectar al rendimiento.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Esta opción sólo es válida para operaciones de copia de seguridad de Hyper-V en sistemas operativos Windows Server 2012 y 2012 R2.

## Clientes soportados

Esta opción es válida para todos los clientes Windows soportados. Esta opción también puede definirse en el servidor.

## Archivo de opciones

---

Esta opción es válida en el archivo de opciones de cliente (dsm.opt) o en la línea de mandatos para el mandato Backup VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
                .-20-----.  
>>-VMMAXPERSnapshot--+-entero+-----><
```

## Parámetros

---

### *entero*

Especifica el número máximo de VM que pueden incluirse en una instantánea de Hyper-V. El valor predeterminado es 20. El número máximo es 100. El mínimo es 1.

Si algunas máquinas virtuales residen en volúmenes locales y algunas máquinas virtuales residen en volúmenes compartidos en clúster (CSV), el número de máquinas virtuales de una instantánea puede ser inferior al valor `vmmaxpersnapshot`. Una instantánea no puede contener una combinación de VMs locales y de volúmenes CSV.

Para evitar crear una instantánea que abarque volúmenes, el número de máquinas virtuales en una instantánea puede ser inferior al número máximo si las máquinas virtuales están en volúmenes diferentes. Por ejemplo, cuatro máquinas virtuales están en el Volumen A y una máquina virtual está en el Volumen B. Se toma una instantánea con sólo cuatro máquinas virtuales (del Volumen A) aunque el valor máximo es cinco. Se toma una segunda instantánea para el Volumen B.

## Ejemplos

---

### Archivo de opciones

```
vmmaxpersnapshot 10
```


### Línea de mandatos

```
dsmc backup vm -vmmaxpers=10
```

### Referencia relacionada:

Vmmxsnapshotretry

### Información relacionada:

 [Ajuste de copias de seguridad de máquina virtual planificadas para clústeres de Windows Server 2012 y 2012 R2](#)

 [Sistemas operativos Linux](#)  [Sistemas operativos Windows](#)

## Vmmaxrestoresessions


---


La opción `vmmaxrestoresessions` especifica el número máximo de sesiones de Servidor de IBM Spectrum Protect que se pueden incluir en una operación de restauración optimizada para una máquina virtual (VM).


Una operación de restauración optimizada es aquella en la que se ha habilitado la prestación de restauración paralela en el nivel de subdisco de un disco virtual.

## Clientes soportados

---


 [Sistemas operativos Linux](#) Esta opción puede utilizarse con clientes Linux x86\_64 soportados.


 [Sistemas operativos Windows](#) Esta opción puede utilizarse con clientes Windows compatibles. Esta opción no es válida para copias de seguridad de Data Protection for Microsoft Hyper-V.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Archivo de opciones

---

 [Sistemas operativos Linux](#) Esta opción es válida en el archivo de opciones del sistema del cliente (dsm.sys), en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Restore VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos para Restore VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
>>-VMMAXRESTORESessions-- .-1-----.  
--++-----++-----><  
'-entero-'
```

## Parámetros

---

*entero*


Especifica el número de sesiones de Servidor de IBM Spectrum Protect que se han creado durante la operación de restauración. El valor predeterminado es 1.


## Ejemplos

---

Archivo de opciones

VMMAXRESTORES 10

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows `dsmc restore vm -VMMAXRESTORES=10`

### Referencia relacionada:

Restore VM

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmmaxrestoreparalleldisks


---


La opción `vmmaxrestoreparalleldisks` permite que un Cliente IBM Spectrum Protect restaure varios discos virtuales al mismo tiempo.


Puede especificar el número de sesiones de disco que se deben abrir, hasta un máximo de 50. El número de sesiones de restauración de disco disponible se especifica mediante la opción `vmmaxrestoresessions`. Las sesiones disponibles se asignan entre en el número de sesiones de disco especificadas por `vmmaxrestoreparalleldisks`, redondeando el número de sesiones por disco al número entero más cercano.

## Clientes soportados

---


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.


 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows compatibles. Esta opción no es válida para copias de seguridad de Data Protection for Microsoft Hyper-V.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Archivo de opciones

---

 Sistemas operativos Linux Esta opción es válida en el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos para Restore VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

 Sistemas operativos Windows Esta opción es válida en el archivo de opciones de cliente (dsm.opt) o en la línea de mandatos para Restore VM. También puede incluirse en el servidor en un conjunto de opciones del cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
>>-VMMAXRESTOREPARALLELDisks-- .-1-----.  
--++-----++-----><  
'-entero-'
```

## Parámetros

---

*entero*

Especifica el número de discos duros virtuales que pueden restaurarse simultáneamente. El valor predeterminado es 1. El máximo es 50.

## Ejemplos

---

Tarea

Establezca un máximo de 10 operaciones de restauración simultáneas para discos virtuales en la máquina virtual vm1:

```
dsmc restore vm vm1 -vmmaxrestoreparalleldisks=10 -vmmaxrestoresessions=20
```

Esto asignará 2 sesiones de restauración simultáneas para el disco virtual.

### Referencia relacionada:

Restore VM

 Sistemas operativos Windows

## Vmmaxsnapshotretry


---

Utilice la opción `vmmaxsnapshotretry` para especificar el número máximo de veces que se debe reintentar una operación de instantánea de una máquina virtual (VM) si la instantánea inicial falla con una condición recuperable.

Durante una copia de seguridad de VM, si falla una instantánea de una máquina virtual debido a una condición temporal, Data Protection for Microsoft Hyper-V reintenta automáticamente la operación de instantánea hasta el número de veces especificado por la opción `vmmaxsnapshotretry`. Si la instantánea sigue fallando después de que se haya alcanzado el número máximo de reintentos, la operación de instantánea para la máquina virtual no se vuelve a intentar y falla el intento de copia de seguridad.

Por ejemplo, una condición recuperable puede deberse a dos solicitudes de copia de seguridad que se han iniciado aproximadamente a la misma hora, haciendo copia de seguridad de máquinas virtuales en el mismo volumen. Una operación de seguridad informa que la instantánea ha fallado porque la copia de seguridad no se puede iniciar mientras se ejecuta otra copia de seguridad para la misma máquina virtual. En este caso, Data Protection for Microsoft Hyper-V volverá a intentar la operación de instantánea después de que se haya completado la primera copia de seguridad de máquina virtual.

Si el error inicial no es recuperable, no se intenta ninguna instantánea. Por ejemplo, si se produce un error con el grabador de Servicios de duplicación de volúmenes (VSS) durante el proceso de instantánea inicial, el proceso de copia de seguridad se detiene y Data Protection for Microsoft Hyper-V no vuelve a intentar la operación de instantánea.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Esta opción sólo es válida para operaciones de copia de seguridad de Hyper-V en sistemas operativos Windows Server 2012 y 2012 R2.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows soportados. Esta opción también puede definirse en el servidor.

## Archivo de opciones

---

Esta opción es válida en el archivo de opciones de cliente (`dsm.opt`) o en la línea de mandatos para el mandato Backup VM. También puede incluirse en el servidor de un conjunto de opciones de cliente. No puede establecerse en el Editor de preferencias.

## Sintaxis

---

```
.-20-----.  
>>-VMMAXSNAPSHOTRETRY--+-entero+-----<<
```

## Parámetros

---

*entero*

Especifica el número máximo de veces para reintentar la operación de instantánea de una máquina virtual si el intento de instantánea inicial falla con una condición recuperable. El valor predeterminado es 20. El valor máximo es 30. El mínimo es 1.

Por ejemplo, si la opción `vmmaxsnapshotretry` se establece en 12, Data Protection for Microsoft Hyper-V reintenta la operación de instantánea hasta 12 veces después de que la instantánea inicial haya fallado durante una operación de copia de seguridad de máquina virtual. Si la instantánea sigue fallando después de 12 intentos, no se vuelven a realizar más intentos y el intento de copia de seguridad falla.

Deben transcurrir al menos 10 minutos antes de que se vuelva a realizar el siguiente intento de instantánea. El tiempo entre intentos será más largo cuando la máquina virtual que ha fallado forma parte de una instantánea con máquinas virtuales de las que actualmente se está realizando una copia de seguridad. Se debe completar la operación de copia de seguridad de las demás máquinas virtuales y la operación de copia de seguridad eliminará la instantánea antes de que se pueda volver a realizar un intento.

## Ejemplos

Archivo de opciones

```
vmmaxsna 12
```


Línea de mandatos

```
dsmc backup vm -vmmaxsna=12
```

**Referencia relacionada:**

Vmmaxpersnapshot


**Información relacionada:**

 Ajuste de copias de seguridad de máquina virtual planificadas para clústeres de Windows Server 2012 y 2012 R2

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmmaxvirtualdisks


La opción `vmmaxvirtualdisks` especifica el tamaño máximo de los discos de máquina virtual VMware (VMDK) para incluir en una operación de copia de seguridad.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Utilice la opción `vmmaxvirtualdisks` con la opción `vmskipmaxvirtualdisks` para especificar cómo el cliente procesa VMDK grandes durante una operación de copia de seguridad.


- Establezca la opción `vmmaxvirtualdisks` para especificar el tamaño máximo de los VMDK a incluir.
- Establezca la opción `vmskipmaxvirtualdisks` para hacer copias de seguridad de los VMDK que no exceden el tamaño máximo (y excluir los VMDK que sí lo exceden) o la operación fallará.


## Clientes soportados

 Sistemas operativos Linux Esta opción es válida para clientes de Linux de 64 bits que se configuran como transportadores de datos que realizan copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción es válida para clientes Windows de 64-bits que se han configurado como transportadores de datos que hacen copias de seguridad de máquinas virtuales VMware.

## Archivo de opciones

 Sistemas operativos Linux Establezca la opción `vmmaxvirtualdisks` en el archivo de opciones de sistema de cliente (`dsm.sys`). También puede especificar esta opción como un parámetro de línea de mandato en el mandato `backup vm`.

 Sistemas operativos Windows Establezca la opción `vmmaxvirtualdisks` en el archivo de opciones de cliente (`dsm.opt`). También puede especificar esta opción como un parámetro de línea de mandato en el mandato `backup vm`.

## Sintaxis

```
.-2-----.  
>>-VMMAXVIRTUALDisks--+-tamaño-----+----->>  
'-2...8, 999-'
```

## Parámetros

tamaño

Especifica el tamaño máximo, en terabytes, de los VMDK a incluir en una operación de copia de seguridad. El rango es un entorno entre 2 y 8; el valor predeterminado es 2. El máximo es 8.

Para asegurarse de que el tamaño de VMware VMDK que está incluido en operaciones de copia de seguridad siempre es el tamaño máximo, especifique 999. Utilice este valor como el método más eficaz para asegurarse de que siempre está establecido el valor máximo. Este valor evita la necesidad de modificar de forma continuada los archivos de opciones.

Cuando también se especifica la opción `vmskipmaxvirtualdisks yes`, se excluyen los VMDKs que tienen el tamaño máximo especificado o menor de los que se han hecho copias de seguridad y los VMDK que superan que el tamaño máximo especificado. Cuando también se especifica la opción `vmskipmaxvirtualdisks no`, las operaciones de copia de seguridad fallan si un VMDK supera el tamaño máximo especificado.

## Ejemplos

---

Archivo de opciones:

```
vmmaxvirtualdisks 3
```

Línea de mandatos:

Haga una copia de seguridad de los VMDK que tienen 5 TB o menos y excluya los VMDK que tienen más de 5 TB:

```
backup vm VM1 -vmmaxvirtualdisks=5 -vmskipmaxvirtualdisks=yes
```

Haga una copia de seguridad de los VMDK que tienen 3 TB o menos y haga fallar la operación de copia de seguridad si un VMDK tiene más de 3 TB:

```
backup vm VM1 -vmmaxvirtualdisks=3 -vmskipmaxvirtualdisks=no
```

Haga una copia de seguridad de los VMDK que tienen 8 TB o menos y excluya los VMDK que tienen más de 8 TB:

```
backup vm VM1 -vmmaxvirtualdisks=8 -vmskipmaxvirtualdisks=yes
```

o bien

```
backup vm VM1 -vmmaxvirtualdisks=999 -vmskipmaxvirtualdisks=yes
```

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmmc



---


Utilice la opción `vmmc` para almacenar las copias de seguridad de máquina virtual con una clase de gestión distinta a la clase de gestión predeterminada. Para copias de seguridad de VM de VMware, la opción `vmmc` sólo es válida si se ha establecido la opción `vmbackuptype=fullvm`.

## Clientes soportados

---


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para clientes que estén configurados para realizar copia de seguridad de las máquinas virtuales VMware. El servidor también puede definir esta opción.

 Sistemas operativos Windows Esta opción es válida para clientes que estén configurados para realizar copia de seguridad de las máquinas virtuales Hyper-V. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente `dsm.opt`, el archivo de opciones de sistema de cliente `dsm.sys` o la línea de mandatos.

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

## Sintaxis

---

```
>>-VMMC--management_class_name-----<<
```

## Parámetros

---

`mgmtclassname`


Especifica una clase de gestión que se aplica a la copia de seguridad de los datos de la máquina virtual. Si no se define esta opción, se utiliza la clase de gestión predeterminada del nodo.

## Ejemplos

---

Tarea:

Ejecute una copia de seguridad de la máquina virtual denominada `myVirtualMachine` y guarde la copia de seguridad de acuerdo con la clase de gestión denominada `myManagementClass`.  
`dsmc backup vm "myVirtualMachine" -vmc=myManagementClass`

 Sistemas operativos Windows


## Vmmountage


---

Utilice la opción `vmmountage` con el mandato `restore VM "*" -vmrestoretype=mountcleanupall` para especificar el número de horas durante las cuales debe estar activo un montaje de restauración de nivel de archivo de MV para borrar.

## Clientes soportados


---

 Sistemas operativos Windows Esta opción solo es válida para los clientes Windows.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Archivo de opciones

---

 Sistemas operativos Windows Ninguna. Esta opción sólo puede especificarse en la línea de mandatos.

## Sintaxis

---

```
>>-VMMOUNTAge = - --horas-----<<
```

## Parámetros

---

horas

Especifica el número de horas que un montaje de restauración a nivel de archivo de máquina virtual debe estar activo para realizar la limpieza. Todas las operaciones de montaje activas que excedan el tiempo especificado se limpiarán. El valor especificado debe ser un número entero entre 0 y 10000. El valor predeterminado es 0.

## Ejemplos

---

Línea de mandatos:

Realice una limpieza de todas las operaciones de montajes que estén activas más de 24 horas:

```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL -VMMOUNTAge=24
```

Limpie todas las operaciones de montaje activas:

```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL -VMMOUNTAge=0
```

o bien


```
dsmc restore vm "*" -VMRESToretype=MOUNTCLEANUPALL
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmnoprmdisks

---

Esta opción permite al cliente restaurar la información de configuración para los volúmenes pRDM que están asociados con una máquina virtual VMware, aunque no se puedan encontrar las LUN que estaban asociadas con los volúmenes. Dado que los volúmenes pRDM no se incluyen en la instantánea de máquina virtual, solo se puede restaurar la información de configuración y no los datos que estaban en los volúmenes.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción no se aplica a copias de seguridad de máquinas virtuales Microsoft Hyper-V.


## Clientes soportados


---

Esta opción es válida para los clientes Windows y Linux que están instalados en un servidor de copia de seguridad de vStorage.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt), o especifíquela como un parámetro de línea de mandatos en el mandato restore vm.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato restore vm.

## Sintaxis

---

```
.-NO--.  
>>-VMNOPRDMdisks--+-+-----+-----<<  
'-YES-'
```

## Parámetros

---

### YES

Especifique este valor si debe restaurar una máquina virtual de la que ha hecho copia de seguridad con `-vmprocesswithprdm=yes` y las LUN originales que se han correlacionado mediante el archivo de correlaciones de dispositivo en bruto no se pueden ubicar. Este valor hace que el cliente omita los intentos de localizar las LUN que faltan utilizadas por los volúmenes pRDM y restaure la información de configuración (etiquetas de disco) que estaba asociada a ellos. Los volúmenes pRDM se restauran como VMDK VMFS con suministro fino. Entonces puede utilizar el cliente vSphere para crear las correlaciones pRDM necesarias.

### NO

El establecimiento de `-vmoprmdisk=no` hace que fallen las operaciones de restauración para máquinas virtuales de las que se ha hecho copia de seguridad con `-processvmwithprdm=yes` si no se pueden ubicar las LUN originales con las que el archivo de correlaciones de dispositivo en bruto las ha correlacionado. Este valor es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
VMNOPRDMDISKS YES
```

Línea de mandatos:


```
dsmc restore vm vm123 -vmoprmdisks=yes
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmnovrdmdisks

---

Esta opción permite al cliente restaurar la información de configuración y los datos para volúmenes de pRDM asociados a una máquina virtual VMware virtual, incluso si no se encuentran los LUN que estaban asociados a los volúmenes.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción no se aplica a copias de seguridad de máquinas virtuales Microsoft Hyper-V.

## Clientes soportados


---


Esta opción es válida para clientes Windows y Linux instalados en un servidor de copia de seguridad vStorage.

## Archivo de opciones

---



 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt), o especifíquela como un parámetro de línea de mandatos en el mandato restore vm.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (dsm.opt), en el archivo de opciones del sistema cliente (dsm.sys), o bien especifíquela como parámetro de línea de mandatos en el mandato restore vm.

## Sintaxis

---

```
>>-VMNOVRDmdisks-.-NO--.-----<<
                    +-----+
                    '-YES-'
```

## Parámetros

---

### YES

Especifique este valor si tiene que restaurar una máquina virtual con copia de seguridad realizada, y no se puedan localizar los LUN originales correlacionados por el archivo Raw Device Mappings. Este valor provoca que el cliente omita intentos de localizar los LUN que faltan utilizados por los volúmenes vRDM, y restaura la información de configuración (etiquetas de disco) y los datos con copia de seguridad. Los volúmenes vRDM se restauran como VMFS VMDKs de aprovisionamiento fino.

### NO

Establecer `-vmnovrdmdisk=no` provoca que las operaciones de restauración para máquinas virtuales que tenían un volumen vRDM fallen si no se pueden localizar los LUN originales correlacionados por el archivo Raw Device Mappings. Este valor es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
VMNOVRDMDISKS YES
```

Línea de mandatos:

```
dsmc restore vm vm123 -vmnovrdmdisks=yes
```

## Vmpreferdagpassive

---



La opción `vmpreferdagpassive` especifica si se debe realizar una copia de seguridad de una copia activa o pasiva de una base de datos que forma parte de un grupo de disponibilidad de base de datos (DAG) de Microsoft Exchange Server.

Esta opción se aplica a cargas de trabajo de Microsoft Exchange Server que se ejecutan dentro de sistemas invitados de máquina virtual de VMware protegidos por IBM Spectrum Protect for Virtual Environments.

Utilice la opción `vmpreferdagpassive` con el mandato `backup vm`.


## Clientes soportados

---

 Sistemas operativos Linux  Sistemas operativos Windows Esta opción es válida para los clientes que actúan como nodos de movimiento de datos para copias de seguridad de huésped VMware.

## Archivo de opciones

---

 Sistemas operativos Linux Especifique esta opción en el archivo de opciones del cliente (dsm.sys) de una stanza de servidor.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-VMPREFERDAGPassive-.-No--.-----<<
                    +-----+
                    '-Yes-'
```

## Parámetros

---

No

Realice una copia de seguridad de la base de datos de Microsoft Exchange Server de un DAG independientemente de si se trata de una copia activa o pasiva. Este es el valor predeterminado.

Yes

Omita la copia de seguridad para una copia de la base de datos activa de un DAG si dispone de una copia pasiva válida en otro servidor. Si no dispone de ninguna copia pasiva válida, se hace una copia de seguridad de la copia de la base de datos activa.

## Ejemplos

---

Archivo de opciones:  
vmpreferdagpassive yes

 Sistemas operativos Linux  Sistemas operativos Windows


## Vmprocessvmwithindependent

---

Utilice esta opción para controlar si las copias de seguridad completas de máquinas virtuales de VMware son procesadas si la máquina se suministra con uno o más volúmenes de discos independientes.

Los volúmenes de discos independientes no dan soporte a instantáneas. Cualquier volumen de disco independiente en una máquina virtual no será procesado como parte de la operación de copia de seguridad. Cuando se restaure la máquina virtual, el cliente de copia de seguridad y archivado recupera la máquina virtual y sólo se restaurarán los volúmenes que han participado en las operaciones de instantáneas. La información de configuración y contenido de los volúmenes de disco independientes no se conserva en la información almacenada en el servidor de IBM Spectrum Protect. Los usuarios deben recrear los volúmenes de disco independientes en la máquina restaurada.

Si la máquina virtual también contiene uno o más volúmenes de correlación de dispositivos RAW (RDM), utilice la opción `vmprocessvmwithprdm` para controlar si el cliente realiza cualquier copia de seguridad en la máquina virtual si hay presente un disco independiente.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción sólo es válida para copias de seguridad de VMware y no para copias de seguridad de Microsoft Hyper-V.

## Clientes soportados


---

Esta opción es válida para clientes Windows y Linux configurados como servidores de copia de seguridad de VMware. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`), en el archivo de opciones del sistema (`dsm.sys`) o en la línea de mandatos.

## Sintaxis

---

```
.-NO-- .  
>>-VMPROCESSVMWITHINDEPENDENT--+-+-----+----->>  
'-YES-'
```

## Parámetros

---

No

La copia de seguridad de a máquina virtual falla si se detecta uno o más volúmenes de discos independientes. No es el valor predeterminado.

Sí

Las máquinas virtuales que contienen uno o más volúmenes de discos independientes se incluyen en la copia de seguridad. Sin embargo, los volúmenes de discos independientes no se procesan como parte de la operación de copia de seguridad de máquinas virtuales.

Si la máquina virtual también contiene uno o más discos RDM (correlación de dispositivos RAW) proporcionados en modalidad de compatibilidad física, deberá especificarse también la opción VMPROCESSVMWITHPRDM.

## Ejemplos

---

Archivo de opciones:

```
VMPROCESSVMWITHINDEPENDENT Yes
```

Línea de mandatos:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm  
-vmprocessvmwithindependent=yes
```

 Sistemas operativos Windows


## Vmprocessvmwithphysdisks

---

Utilice la opción `vmprocessvmwithphysdisks` para controlar si las copias de seguridad de máquina virtual (VM) Hyper-V RCT se procesan si la VM tiene uno o más discos físicos (discos de paso a través) suministrados.

Una VM puede acceder al almacenamiento de un disco físico que está conectado directamente al servidor de Hyper-V. Este disco físico se denomina *disco de paso a través*.

Si establece esta opción en `yes`, los datos de los discos físicos se excluyen de las operaciones de copia de seguridad, pero la información de configuración del disco físico se guarda con la copia de seguridad de la VM. Durante una operación de restauración, puede restaurar la configuración de disco físico estableciendo la opción `vmskipphysdisks no`. Si los discos físicos originales están disponibles, se reconectan a la VM restaurada.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Esta opción sólo es válida para copias de seguridad de Microsoft Hyper-V y no es aplicable a copias de seguridad de VMware.

Esta opción sólo es válida para copias de seguridad con RCT en Windows Server 2016. Esta opción no se aplica a copias de seguridad Hyper-V con VSS en Windows Server 2012 o Windows Server 2012 R2.

## Clientes soportados

---

Esta opción es válida para clientes de sistemas operativos Windows Server 2016 o posteriores.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o especifíquela como un parámetro de línea de mandatos en el mandato `backup vm`.

## Sintaxis

---

```
.-NO--.  
>>-VMPROCESSVMWITHPHYSDISKS--+-----+-----<<  
'-YES-'
```

## Parámetros

---

No

La operación de copia de seguridad de la VM falla si se detecta uno o más discos físicos. Este es el valor predeterminado.

Yes

Se realiza la copia de seguridad de las VM que contienen uno o más discos físicos. Esta opción realiza la copia de seguridad de la configuración de discos físicos sin realizar la copia de seguridad de los datos de los discos físicos.

## Ejemplos

---

Archivo de opciones:

```
VMPROCESSVMWITHPHYSDISKS Yes
```

Línea de mandatos:

```
dsmc backup vm vmlocal -vmprocessvmwithphysd=yes
```

#### Referencia relacionada:

Vmskipphysdisks

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmprocessvmwithprdm


---

Utilice esta opción para controlar si las copias de seguridad de máquina virtual de VMware completa son procesadas si la máquina tiene uno o más volúmenes RDM (dispositivos de correlación RAW) proporcionados en modalidad de compatibilidad física (pRDM).

Los volúmenes pRDM no dan soporte a instantáneas. Cualquier volumen pRDM que se encuentre en una máquina virtual no será procesado como parte de la operación de copia de seguridad. Cuando se restaure la máquina virtual, el cliente de copia de seguridad y archivado recupera la máquina virtual y sólo se restaurarán los volúmenes que han participado en las operaciones de instantáneas. La información de configuración y contenido de los volúmenes pRDM no se conserva en la información almacenada en el servidor de IBM Spectrum Protect. Los usuarios deben recrear los volúmenes pRDM en la máquina restaurada.

Esta opción no se aplica a las máquinas virtuales que tengan uno o más volúmenes RDM proporcionados en modalidad de compatibilidad virtual (vRDM). Puesto que los volúmenes vRDM no dan soporte a operaciones de instantáneas, se incluyen en una copia de seguridad de máquina virtual de VMware completa.

Si la máquina virtual también contiene uno o más discos independientes, utilice la opción `vmprocessvmwithindependent` para controlar si el cliente realiza cualquier copia de seguridad en la máquina virtual si hay presente un disco independiente.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Esta opción sólo es válida para copias de seguridad de VMware y no para copias de seguridad de Microsoft Hyper-V.


## Clientes soportados


---

Esta opción es válida para clientes Windows y Linux configurados como servidores de copia de seguridad de VMware. El servidor también puede definir esta opción.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

 Sistemas operativos Linux Coloque esta opción en el archivo de opciones de cliente (`dsm.opt`), el archivo de opciones de sistema de cliente (`dsm.sys`) o la línea de mandatos.

## Sintaxis

---

```
.-NO--.  
>>-VMPROCESSVMWITHPRDM-+-----+-----<<  
'-YES-'
```

## Parámetros

---

No

La copia de seguridad de a máquina virtual falla si se detecta uno o más volúmenes pRDM. No es el valor predeterminado.

Yes

Las máquinas virtuales que contengan uno o más volúmenes RDM (correlación de dispositivos RAW) proporcionados en modalidad de compatibilidad física (pRDM) serán incluidos en la copia de seguridad. Sin embargo, los volúmenes pRDM no se procesan como parte de la operación de copia de seguridad de máquinas virtuales.

Si la máquina virtual también contiene uno o más discos independientes, deberá también especificarse la opción `vmprocessvmwithindependentdisk`.

## Ejemplos


---

Archivo de opciones:

```
VMPROCESSVMWITHPRDM Yes
```

Línea de mandatos:

```
dsmc backup vm vmlocal -vmbackuptype=fullvm -vmprocessvmwithprdm=yes
```

 Sistemas operativos Windows

## Vmrestoretype


---

Utilice la opción `vmrestoretype` con los mandatos `query VM` o `restore VM` para especificar el tipo de operación de restauración a realizar o consultar.

Esta opción sólo es válida para máquinas virtuales de VMware. Las máquinas virtuales deben estar alojadas en servidores VMware ESXi 5.1 o versiones posteriores. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

## Clientes soportados

---

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Esta opción se debe especificar en la línea de mandatos de un mandato `restore vm` o `query vm`. No puede establecer esta opción en el archivo de opciones del cliente.

## Sintaxis

---

```
.-NONinstant-----.  
>>-VMRESToretype-----><  
+-INSTANTRestore--+  
+-INSTANTAccess---+  
+-VMCleanup-----+  
+-VMFULLCleanup---+  
+-ALLtype-----+  
'-MOUNTCLEANUPAll-'
```

## Parámetros

---

### noninstant

Especifica que se ha realizado la restauración de la máquina virtual completa clásica. Este es el tipo de restauración predeterminado.

### instantrestore

Especifica que se realice una restauración instantánea. Durante una operación de restauración instantánea, la máquina virtual se inicia durante la operación de restauración. Cuando se especifica este tipo de restauración en un mandato `query VM`, el mandato devuelve una lista de máquinas virtuales que ejecutan una operación de restauración instantánea.

Importante: Para las operaciones de restauración instantáneas, asegúrese de que tanto el almacén de datos temporal que especifique con la opción `vmtempdatastore` como el almacén de datos de VMware que especifique mediante la opción `datastore` en el mandato `restore VM` tengan suficiente almacenamiento libre para guardar la máquina virtual que está restaurando, y el archivo de instantáneas que contiene cambios realizados a los datos.

### instantaccess

Especifica que se ha realizado una restauración temporal de la máquina virtual de la que se ha realizado copia de seguridad.

Utilice este tipo de restauración cuando desee restaurar una máquina virtual temporalmente, para probar la integridad de una copia de seguridad, antes de ejecutar una restauración instantánea. Los cambios realizados a la máquina virtual temporal no se guardan.

Cuando se especifica este tipo de restauración en un mandato `query vm`, el mandato devuelve una lista de máquinas virtuales que ejecutan una operación de acceso instantáneo.

### vmcleanup

Especifica que se está realizando una limpieza de la máquina virtual seleccionada y de sus componentes.

Para operaciones de acceso instantáneo, esta opción elimina la máquina virtual temporal y todos sus componentes.

Para operaciones de restauración instantáneas, esta opción elimina sólo los componentes que ya no son necesarios (por ejemplo, los montajes iSCSI). La máquina virtual no se elimina. Las operaciones de limpieza no se permiten cuando la máquina virtual aún se está ejecutando en los discos iSCSI. Para forzar este comportamiento, consulte `vmfullcleanup`.

### vmfullcleanup

La máquina virtual y todos sus componentes se eliminarán sin tener en cuenta el estado actual. No inicie una operación de limpieza completa mientras que `vMotion` sigue migrando una máquina virtual.

alltype

Consulta todos los accesos instantáneos activos y las sesiones de restauración instantáneas.

mountcleanupall

Limpia operaciones de montaje de restauración a nivel de archivo de máquina virtual que son anteriores al periodo específico con la opción vmmountage. Debe especificar restore vm "\*" para utilizar la opción mountcleanupall.

## Ejemplos

---

Línea de mandatos:

Realice un acceso instantáneo de la máquina virtual denominada Oslo. La máquina virtual original todavía existe. Como resultado, se utilizará la opción -vmname para asignar el nuevo nombre Oslo\_verify.

```
dsmc restore vm Oslo -vmrest=instantaccess -vmname=Oslo_verify
```

Realice una restauración instantánea de la máquina virtual denominada Cologne.

```
dsmc restore vm Cologne -vmrest=instantrestore  
-vmtempdatastore=Verify_datastore
```

Realice una restauración normal (máquina virtual completa) de la máquina virtual denominada San\_Jose.

```
dsmc restore vm San_Jose
```

Como alternativa, también puede utilizar el mandato siguiente: `dsmc restore vm San_Jose -vmrest=noni`

Realice una restauración instantánea de la máquina virtual denominada Oslo con la opción -pick para seleccionar una versión de copia de seguridad específica.

```
dsmc restore vm Oslo -vmrest=instantrestore -pick
```

Realice una limpieza de la máquina virtual y de todos sus componentes. Estos componentes incluyen montajes, dispositivos y datos temporales de iSCSI que están asociados con el nombre de la máquina virtual en el host ESX.

```
dsmc restore vm Oslo -VMRESToretype=VMCleanup -vmname=Oslo_Verify
```

Realice una consulta para buscar todas las sesiones de restauración instantáneas activas y mostrar un estado abreviado para cada una.

```
dsmc query vm * -VMRESToretype=INSTANTRestore
```

Realice una consulta para buscar todas las modalidades de restauración instantáneas activas y las máquinas virtuales de la modalidad de acceso instantáneo.

```
dsmc query vm * -VMRESToretype=ALLtype
```

Realice una consulta para buscar todas las máquinas virtuales de la modalidad de restauración instantánea activa, y obtenga el estado detallado para cada máquina virtual.

```
dsmc query vm * -VMRESToretype=INSTANTRestore -Detail
```

Realice una consulta para buscar todas las sesiones de acceso instantáneo activas.

```
dsmc query vm * -VMRESToretype=INSTANTAccess
```

Realice una limpieza de montaje de todas las operaciones de montaje que estén activas más de 24 horas.

```
dsmc restore vm "*" -vmrestoretype=mountcleanupall -vmmountage=24
```

 Sistemas operativos Windows  Sistemas operativos Linux

## Vmskipctlcompression

---

Utilice la opción vmskipctlcompression para copias de seguridad de máquina virtual para especificar si los archivos de control (\*.ctl) se comprimen durante una copia de seguridad de máquina virtual. La opción no afecta a la compresión de los archivos de datos (\*.dat)

Puede comprimir archivos de control de máquina virtual y archivos de datos sólo cuando los archivos se almacenan en una agrupación de almacenamiento habilitada para optimización del cliente. Utilice la siguiente configuración de opciones para comprimir los archivos de datos y no comprimir los archivos de control:


```
compression yes  
vmskipctlcompression yes
```

Debe dirigir los archivos de datos a una agrupación de almacenamiento habilitada para la optimización del cliente. Puede dirigir los archivos de control a una agrupación de almacenamiento que no esté habilitado para la optimización del cliente

Debe tener licencia para utilizar IBM Spectrum Protect for Virtual Environments para utilizar esta opción.

## Cientes soportados

---

 Sistemas operativos Windows Esta opción se puede utilizar con clientes Windows y Linux soportados.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

## Sintaxis

---

```
>>-VMSKIPCTLCOMPRESSION--+-Yes- .-----><
                          |-----|
                          '-No--'
```

## Parámetros

---

Yes

No comprimir archivos de control (\*.ctl) durante una copia de seguridad de máquina virtual. La opción no afecta a la compresión de archivos de datos (\*.dat).

No


Los archivos de control (\*.ctl) se pueden comprimir durante la copia de seguridad de máquina virtual. Si los archivos de control se comprimen depende del valor de la opción compression.

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmskipmaxvirtualdisks

---

La opción vmskipmaxvirtualdisks especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDKs) que exceden el tamaño máximo de disco.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


Utilice la opción vmskipmaxvirtualdisks con la opción vmmaxvirtualdisks para especificar cómo el cliente procesa VMDK grandes durante una operación de copia de seguridad:


- Establezca la opción vmskipmaxvirtualdisks para hacer copias de seguridad de los VMDKs que no exceden el tamaño máximo (y excluir los VMDK que sí lo exceden) o la operación fallará.
- Establezca la opción vmmaxvirtualdisks para especificar el tamaño máximo de los VMDK a incluir.

En V7.1.3 y anterior, la opción vmskipmaxvirtualdisks se llamaba vmskipmaxvmdks. En V7.1.4 y posteriores, vmskipmaxvirtualdisks es el nombre de opción preferido. Sin embargo, el cliente sigue procesando operaciones de copia de seguridad con el nombre vmskipmaxvmdks.

## Cientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes de Linux de 64 bits que se configuran como transportadores de datos que realizan copias de seguridad de máquinas virtuales VMware.

 Sistemas operativos Windows Esta opción es válida para clientes Windows de 64-bits que se han configurado como transportadores de datos que hacen copias de seguridad de máquinas virtuales VMware.

## Archivo de opciones

---

 Sistemas operativos Linux Establezca la opción vmskipmaxvirtualdisks en el archivo de opciones de sistema de cliente (dsm.sys). También puede especificar esta opción como un parámetro de línea de mandato en el mandato backup vm.

 Sistemas operativos Windows Establezca la opción vmskipmaxvirtualdisks en el archivo de opciones de cliente (dsm.opt). También puede especificar esta opción como un parámetro de línea de mandato en el mandato backup vm.

## Sintaxis

---

```
>>-VMSKIPMAXVIRTUALDISKS--+-No-- .  
                                     '-Yes-'
```

## Parámetros

---

### No

Especifica que las operaciones de copia de seguridad fallan si una máquina virtual VMware tiene uno o más VMDK que superan el tamaño máximo. Éste es el valor predeterminado.

### Yes

Especifica que las operaciones de copia de seguridad incluyen VMware VMDK que tienen el tamaño máximo (o menos) y excluyen los VMDK que superan el tamaño máximo.

## Ejemplos

---

Archivo de opciones:

```
vmskipmaxvirtualdisks yes
```

Línea de mandatos:

La operación copia de seguridad falla si un VMDK es mayor de 2 TB:

```
backup vm VM1 -vmskipmaxvirtualdisks=no
```

La operación copia de seguridad falla si un VMDK es mayor de 5 TB:

```
backup vm VM1 -vmskipmaxvirtualdisks=no -vmmaxvirtualdisks=5
```

Haga una copia de seguridad de los VMDK que tienen 8 TB o menos y excluya los VMDK que tienen más de 8 TB:

```
backup vm VM1 -vmskipvirtualdisks=yes -vmmaxvirtualdisks=8
```


 Sistemas operativos Linux  Sistemas operativos Windows


## Vmskipmaxvmdks

---

La opción `vmskipmaxvmdks` especifica cómo la operación de copia de seguridad procesa discos de máquina virtual VMware (VMDK) que exceden el tamaño máximo de disco.

En V7.1.4 y posteriores, `vmskipmaxvmdks` se renombra a `vmskipmaxvirtualdisks`. Aunque `vmskipmaxvirtualdisks` es el nombre preferido, el cliente sigue procesando las operaciones de copia de seguridad con el nombre `vmskipmaxvmdks`.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


 Sistemas operativos Windows

## Vmskipphysdisks

---

Utilice la opción `vmskipphysdisks` para restaurar la información de configuración para los discos físicos (discos de paso a través) que están asociados con una máquina virtual (VM) Hyper-V, si los números de unidad lógica (LUN) que están asociados con los volúmenes en los discos físicos están disponibles.

Dado que los discos físicos no se incluyen en una instantánea de VM, solo se puede restaurar la información de configuración, pero no los datos de los volúmenes.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V.

Esta opción sólo es válida para copias de seguridad de Microsoft Hyper-V y no es aplicable a copias de seguridad de VMware.

Esta opción sólo es válida para restaurar máquinas virtuales Hyper-V en Windows Server 2016. Esta opción no se aplica a hosts Hyper-V en Windows Server 2012 o Windows Server 2012 R2.

## Clientes soportados

---



Esta opción es válida para clientes de sistemas operativos Windows Server 2016 o posteriores.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt), o especifíquela como un parámetro de línea de mandatos en el mandato restore vm.

## Sintaxis

---

```
. -NO-- .  
>>-VMSKIPPHYSDisks--+-+-----+----->>  
'-YES-'
```

## Parámetros

---

### NO

Si los discos físicos originales están disponibles, especifique este valor para restaurar la información de configuración de disco físico de la que se ha realizado copia de seguridad con la opción vmprocessvmwithphysdisks yes. Los discos físicos originales se reconectan a la VM restaurada. Si los discos físicos originales no pueden localizarse, la operación de restauración fallará. Este es el valor predeterminado.

### YES

Especifique este valor si tiene que restaurar una VM cuya copia de seguridad se ha realizado con la opción vmprocessvmwithphysdisks yes, y no pueden localizar los discos físicos originales. Este valor provoca que el cliente omita intentos de localizar los discos físicos y no restaura la información de configuración de discos físicos.

## Ejemplos

---

Archivo de opciones:


```
VMSKIPPHYSDISKS YES
```

Línea de mandatos:

```
dsmc restore vm vm123 -vmskipphysd=yes
```

### Referencia relacionada:

Vmprocessvmwithphysdisks

 Sistemas operativos Windows

## Vmstoragetype

---

Utilice la opción vmstoragetype con el mandato restore VM para especificar el tipo de dispositivo de almacenamiento desde el que se monta la instantánea con Agente de recuperación de IBM Spectrum Protect.

 Sistemas operativos Windows


Puede especificar la opción vmstoragetype con los mandatos restore VM -VMRESToretype=INSTANTRestore o restore VM -VMRESToretype=INSTANTAccess.

Cuando se especifica vmstoragetype, no es necesario establecer la opción de tipo de almacenamiento en la GUI de Agente de recuperación de IBM Spectrum Protect. vmstoragetype sobrescribe el valor de tipo de almacenamiento en la interfaz gráfica de usuario del agente de recuperación.

## Clientes soportados


---

 Sistemas operativos Windows Esta opción solo es válida en Windows.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Archivo de opciones

---

 Sistemas operativos Windows Coloque esta opción en el archivo de opciones del cliente (dsm.opt) en el sistema proxy de montaje de Windows, o en la línea de mandatos.


 Sistemas operativos Windows


## Sintaxis

```
. -DISK- .  
>>-VMSTORAGEType--+VTL--+-----<<  
'-TAPE-'
```


## Parámetros


 Sistemas operativos WindowsDISK

 Sistemas operativos WindowsLas instantáneas que montará el agente de recuperación están en las agrupaciones de almacenamiento Disk o File. Este es el valor predeterminado.

 Sistemas operativos WindowsVTL

Las instantáneas que montará el agente de recuperación están en las agrupaciones de almacenamiento VTL.

 Sistemas operativos WindowsTAPE

 Sistemas operativos WindowsLas instantáneas que montará el agente de recuperación están en las agrupaciones de almacenamiento Tape.

## Ejemplos

Archivo de opciones:

```
VMSTORAGETYPE TAPE
```

Línea de mandatos:

 Sistemas operativos WindowsRestaura una máquina virtual denominada Orion utilizando el siguiente mandato:


```
dsmc restore vm Orion -Host=esxi.example.com -datacenter=mydatacenter  
-VMTEMPDatastore=temp_datastore -VMRESToretype=INSTANTRestore  
-datastore=mydatastore -VMSTORAGETYPE=VTL
```

Este mandato especifica el nombre de la máquina virtual que se va a restaurar, el centro de host y de datos en el que se va a restaurar y el tipo de restauración (-VMRESToretype=INSTANTRestore). La opción -VMSTORAGETYPE=VTL identifica la instantánea (Orion) que montará el agente de recuperación en las agrupaciones de almacenamiento VTL. La opción VMTEMPDatastore es un parámetro obligatorio para las operaciones de restauración instantáneas.

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmtagdatamover

Utilice la opción vmtagdatamover para habilitar el soporte de codificación en el cliente de archivado y copia de seguridad (transportador de datos). Cuando esta opción está habilitada, el cliente gestiona copias de seguridad de máquinas virtuales en objetos de inventario de VMware de acuerdo con los códigos de protección de datos que se han establecido mediante la Plug-in de cliente de IBM Spectrum Protect vSphere del cliente web vSphere, o que se establecen con herramientas como VMware vSphere PowerCLI Versión 5.5 R2 o posterior.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Para obtener más información sobre los códigos de protección de datos, consulte "Visión general de códigos de protección de datos".

El transportador de datos procesa los códigos de protección de datos si la opción vmtagdatamover está establecida en yes. Asegúrese de que se cumplan los siguientes requisitos.

Requisitos:




- Para el transportador de datos:
  - El servidor de VMware vCenter debe tener la Versión 6.0, Actualización 1 o posterior.
  - Se necesitan permisos adicionales para la cuenta que se utiliza para operaciones de copia de seguridad o restauración. Estos nuevos permisos de vCenter se necesitan para realizar las operaciones de codificación y de categoría. Asegúrese de que los siguientes permisos están establecidos en el servidor vCenter raíz:

```
Inventory Service > vSphere Tagging > Assign or Unassign vSphere Tag  
Inventory Service > vSphere Tagging > Create vSphere Tag  
Inventory Service > vSphere Tagging > Create vSphere Tag Category  
Inventory Service > vSphere Tagging > Delete vSphere Tag  
Inventory Service > vSphere Tagging > Delete vSphere Tag Category  
Inventory Service > vSphere Tagging > Modify UsedBy Field For Tag  
Inventory Service > vSphere Tagging > Modify UsedBy Field For Category
```

Para obtener más información sobre la configuración de permisos de vCenter para operaciones de copia de seguridad y restauración, consulte la nota técnica 7047438.


- Para que la GUI de Data Protection for VMware vSphere funcione correctamente con el soporte de códigos, asegúrese de cumplir los requisitos siguientes durante la instalación de la GUI:
  - Deben instalarse al menos un transportador de datos y la GUI de Data Protection for VMware vSphere en el mismo servidor. Este nodo de transportador de datos debe configurarse para que se guarden las credenciales del servidor de vCenter. Puede guardar las credenciales ejecutando el asistente de configuración para guardar la contraseña del nodo de transportador de datos, o bien utilizando el mandato `dsmc set password` en la línea de mandatos del transportador de datos.


Si utiliza otros transportadores de datos, ejecutados en máquinas virtuales o máquinas físicas como transportadores de datos adicionales, puede instalarlos en otros servidores. Para el soporte de códigos, todos estos transportadores de datos también deben configurarse con la opción `vmtagdatamover=yes`. Estos transportadores de datos adicionales no requieren que la GUI de Data Protection for VMware vSphere esté instalada en el mismo servidor para funcionar correctamente como transportadores de datos basados en códigos.

-  Sistemas operativos Linux En el caso de transportadores de datos de Linux, asegúrese de especificar el directorio de instalación del transportador de datos y la biblioteca compartida de Java™ `libjvm.so` en la variable de entorno `LD_LIBRARY_PATH`. La vía de acceso a `libjvm.so` se utiliza para el soporte de codificación cuando se habilita la opción `vmtagdatamover` en el transportador de datos. Para obtener instrucciones, consulte "Configuración de nodos del transportador de datos en un entorno de vSphere".
-  Sistemas operativos Linux En sistemas operativos Linux, la GUI de Data Protection for VMware vSphere se debe instalar utilizando el nombre de usuario predeterminado (`tdpvmware`).
-  Sistemas operativos Linux En los nodos de transportador de datos de Linux, debe utilizar el archivo de contraseña predeterminado (`/etc/adsm/TSM.sth`).

## Clientes soportados


---


 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux `x86_64` soportados.

 Sistemas operativos Windows Esta opción se puede utilizar con los clientes admitidos de Windows de 64 bits.

## Archivo de opciones

---

 Sistemas operativos Linux Puede especificar esta opción en el archivo de opciones del sistema cliente (`dsm.sys`) o en la línea de mandatos mediante el mandato `backup vm`. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

 Sistemas operativos Windows Puede especificar esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos mediante el mandato `backup vm`. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

## Sintaxis

---

```
>>-VMTAGDATamover--+-No-- .
                    +-Yes- '-----><
```

## Parámetros

---

No

El cliente no tiene en cuenta los valores de protección de datos ni los códigos que se atribuyen al activo VMware. Este es el valor predeterminado.

Yes

El cliente gestiona las copias de seguridad basándose en los valores de protección de datos de la Plug-in de cliente de IBM Spectrum Protect vSphere o basándose en los valores de código que se han atribuido al activo de VMware.

Si el soporte a la codificación está habilitado, algunas opciones de cliente podrían verse afectadas por los valores de protección de datos. Para obtener información acerca de las opciones afectadas, consulte "Códigos de protección de datos soportados".

En los ejemplos siguientes se muestra cómo se pueden ver afectadas las opciones de cliente por los códigos de protección de datos:

- Cuando se utilizan los valores o códigos de protección de datos para controlar las máquinas virtuales VMware de las que se realiza una copia de seguridad, los valores de código se pueden solapar con el valor de la opción del cliente `domain.vmfull`. Aunque la opción `domain.vmfull` define las máquinas virtuales que protege el cliente, los códigos `Excluded` e `Included` sustituyen a lo que se ha definido con la opción `domain.vmfull`. Por ejemplo, la siguiente sentencia del archivo de opciones especifica lo que se copia durante operaciones de copia de seguridad completa de la máquina virtual:

```
DOMAIN.VMFULL VMHOSTCLUSTER=cluster01,cluster02;VM=Dept20*
```

Si utiliza valores o códigos de protección de datos para excluir la máquina virtual `Dept204`, no se realizará una copia de seguridad de la máquina virtual `Dept204`.

- El valor de política de retención en la Plug-in de cliente de IBM Spectrum Protect vSphere o el valor de código para la categoría `Clase de gestión (IBM Spectrum Protect)` altera temporalmente las opciones de cliente `include.vm` y `vmmc`, pero no altera temporalmente la opción `vmctlmc`.

Consejo: si desea configurar un transportador de datos como transportador de datos predeterminado, utilice la opción `Vmtagdefaultdatamover`.

## Ejemplos

Archivo de opciones:

```
vmtagdat yes
```

Línea de mandatos:

```
-vmtagdat=yes
```

### Conceptos relacionados:

Visión general de los códigos de protección de datos

### Tareas relacionadas:

 [Habilitación del soporte de codificación](#)

### Referencia relacionada:

Códigos de protección de datos admitidos

[Vmtagdefaultdatamover](#)

[Domain.vmfull](#)

[Include.vm](#)

[Vmmc](#)


[Vmctlmc](#)

[Set Vmtags](#)

 [Sistemas operativos Linux](#)  [Sistemas operativos Windows](#)

## Vmtagdefaultdatamover

Utilice la opción `vmtagdefaultdatamover` para proteger máquinas virtuales definidas en una planificación que no tengan una categoría o código `Transportador de datos` asignada o heredada.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.


Si especifica un nodo de transportador de datos con la opción `vmtagdefaultdatamover` y la opción `vmtagdatamover yes`, el transportador de datos realiza una copia de seguridad de todas las máquinas virtuales nuevas añadidas a cualquier contenedor del centro de datos, si el contenedor ya se encuentra en un conjunto de protección. Un conjunto de protección consta de las máquinas virtuales de un contenedor asignado al código y la categoría `Schedule (IBM Spectrum Protect)`. El transportador de datos predeterminado también realiza copias de seguridad de las máquinas virtuales del conjunto de protección a las que no se ha asignado el código `Data Mover`.


Si hay más de un transportador de datos asociado a una planificación, defina un transportador de datos como el predeterminado con la opción `vmtagdefaultdatamover`. Si solo hay un transportador de datos asociado a una planificación, asígnelo como predeterminado.

Consejo: Para cada planificación, especifique como predeterminado solo un transportador de datos de la lista de transportadores de datos asociados. En caso contrario, se realizará más de una copia de seguridad de las máquinas virtuales nuevas y de aquellas a las que no se les haya asignado el código `Data Mover`.

Se pueden asignar códigos de protección de datos al inventario de vSphere para gestionar la protección de máquinas virtuales. Para obtener la lista de categorías y códigos soportados, consulte "Códigos de protección de datos soportados".


## Clientes soportados


 Sistemas operativos Linux Esta opción se puede utilizar con los transportadores de datos admitidos de Linux x86\_64.

 Sistemas operativos Windows Esta opción se puede utilizar con los transportadores de datos admitidos de Windows de 64 bits.

## Archivo de opciones

---

 Sistemas operativos Linux Puede especificar esta opción en el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos mediante el mandato backup vm. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

 Sistemas operativos Windows Puede especificar esta opción en el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos mediante el mandato backup vm. También puede incluir esta opción en el servidor de IBM Spectrum Protect en un conjunto de opciones de cliente. No puede establecer esta opción en el Editor de preferencias.

## Sintaxis

---

```
>>-VMTAGDEFAULTdatamover--+-No-----+-----><
                               +-Sí-----+
                               '-nombre_td-'
```

## Parámetros

---

No

El transportador de datos local no funciona como un transportador de datos predeterminado. Las máquinas virtuales a las que no se haya asignado el código `Data Mover` no serán protegidas por este transportador de datos. Este es el valor predeterminado.

Sí

Especifica que el transportador de datos local (el transportador de datos donde se especifica esta opción) funciona como transportador de datos predeterminado.

Tiene que habilitar también el transportador de datos para que dé soporte a la codificación especificando la opción `vmtagdatamover yes`.

*nombre\_td*

Nombre del transportador de datos que se quiere utilizar como transportador de datos predeterminado. Esta opción solo es necesaria si quiere definirla en el archivo de opciones para el transportador de datos predeterminado. Esta opción se omite en el caso de cualquier transportador de datos que no sea el transportador de datos predeterminado.

Es posible transmitir esta opción a todos los transportadores de datos del mandato de planificación del servidor o incluirla en todos los archivos de opción del transportador de datos. Solo el transportador de datos predeterminado utiliza esta opción. Por lo tanto, defina solo un transportador de datos.

También tiene que especificar la opción `vmtagdatamover yes` en el archivo de opciones del transportador de datos que quiere designar como transportador de datos predeterminado.

## Ejemplo

---

La configuración de Data Protection for VMware de Windows utiliza dos transportadores de datos, `VC1_DC1_DM1` y `VC1_DC1_DM2`. Para designar el transportador de datos `VC1_DC1_DM1` como transportador de datos predeterminado, complete los pasos siguientes:

1. En el archivo de opciones del transportador de datos `VC1_DC1_DM1` (dsm.VC1\_DC1\_DM1.opt), añada las sentencias siguientes:

```
vmtagdatamover
yes
vmtagdefaultdatamover yes
```

o bien

```
vmtagdatamover
yes
vmtagdefaultdatamover VC1_DC1_DM1
```

2. En el archivo de opciones del transportador de datos `VC1_DC1_DM2` (dsm.VC1\_DC1\_DM2.opt), añada las sentencias siguientes:

```
vmtagdatamover
yes
vmtagdefaultdatamover VC1_DC1_DM1
```

La opción `vmtagdefaultdatamover` también se puede pasar a un mandato o una definición de planificación para asignar el transportador de datos predeterminado. Si el transportador de datos predeterminado está definido en la definición de planificación, todos los transportadores de datos asociados a la planificación podrán identificar el transportador de datos predeterminado del conjunto de protección.

Por ejemplo: `dsmc backup vm -vmtagdefaultdatamover=VC1_DC1_DM1`

**Tareas relacionadas:**

 [Habilitación del soporte de codificación](#)

**Referencia relacionada:**

[Domain.vmfull](#)

[Vmtagdatamover](#)

[Set Vmtags](#)

 [Sistemas operativos Windows](#)

## Vmtempdatastore

---


Utilice la opción `vmtempdatastore` con el mandato `restore VM` para definir un almacén de datos temporal en el host de ESX para una operación de restauración instantánea.

El almacén de datos creados con la opción `vmtempdatastore` se utiliza para almacenar temporalmente la configuración de la máquina virtual creada durante el proceso de restauración. Esta opción es necesaria durante las operaciones de restauración instantáneas (`-vmrestoretype=instantrestore`).

Esta opción sólo es válida para máquinas virtuales de VMware. Las máquinas virtuales deben estar alojadas en servidores VMware ESXi 5.1 o versiones posteriores. Para utilizar esta opción, debe tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

## Clientes soportados

---

 [Sistemas operativos Windows](#) Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (`dsm.opt`) o en la línea de mandatos.

## Sintaxis

---

```
>>-VMTEMPDatastore-- --datastore_name-----><
```

## Parámetros

---

`datastore_name`

Especifique el nombre de un almacén de datos existente en el host de ESX. El almacén de datos temporales debe ser distinto del almacén de datos original, o del almacén de datos especificado por la opción `datastore`. El almacén de datos que especifique debe ser un almacén de datos VMFS.

## Ejemplos

---

Archivo de opciones:

```
VMTEMPDatastore Verify_Datastore
```

Línea de mandatos:

```
dsmc restore vm Oslo -VMRESToretype=INSTANTAccess  
-vmname=Oslo_instant_restored -VMTEMPDatastore=Temporary_Datastore
```

 [Sistemas operativos Linux](#)  [Sistemas operativos Windows](#)

## Vmverifyfaction


---

Utilice esta opción para especificar la acción a realizar si el transportador de datos detecta problemas de integridad con los archivos CTL y bitmap más recientes para una máquina virtual.

Esta opción afecta al proceso de copia de seguridad de un huésped de máquina virtual solo cuando todas las condiciones siguientes son verdaderas:


- La operación de copia de seguridad anterior para el huésped de máquina virtual era una copia de seguridad incremental-constante-incremental (`mode=ifincremental`)
- La operación de copia de seguridad actual para el huésped de máquina virtual es una copia de seguridad incremental-constante-incremental
- El transportador de datos ha detectado un problema de integridad con los datos CTL y bitmap de una operación de copia de seguridad incremental-constante-incremental anterior
- La opción `vmverifyiflatest` está establecida en `yes`


Si todas estas condiciones no son verdaderas para una máquina virtual, la copia de seguridad se produce como habitualmente; la acción especificada por esta opción no se inicia.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Clientes soportados

---


 Sistemas operativos Linux Esta opción es válida para clientes Linux que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

 Sistemas operativos Windows Esta opción es válida para clientes Windows que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (`dsm.opt`).

 Sistemas operativos Linux Establezca esta opción en el archivo de opciones de cliente (`dsm.opt`) o el archivo de opciones del sistema del cliente (`dsm.sys`).

Esta opción también se puede incluir en un conjunto de opciones de cliente, como parámetro en un mandato `backup vm`, o en la definición del parámetro `options`.

## Sintaxis

---

```
.-FAILbackup-.
>>-VMVERIFYIFAction----->>
+-FORCEfull--+
'-PREview----'
```

## Parámetros

---

### FAILbackup

Esta acción falla en la operación de copia de seguridad. Se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (`dsmerror.log`):

```
ANS9921E Disco de máquina virtual, nombre_mv (etiqueta_disco),
ha fallado la comprobación de verificación (xxx/yyy).
```

`xxx/yyy` en el mensaje indican el tamaño de los archivos bitmap (`xxx`) y CTL (`yyy`).

```
ANS9919E No se han podido encontrar los archivos de control esperados
para nombre_mv
```

Realice una copia de seguridad de máquina virtual completa (establezca `-mode=IFFull` para las máquinas virtuales afectadas en el momento que elija. Una alternativa es utilizar `-vmverifyifaction=forcefull` en la siguiente operación de incremental-constante-incremental planificada para forzar una copia de seguridad completa de dichas máquinas virtuales, si determina que la ventana de copia de seguridad planificada puede contener las copias de seguridad de máquina virtual completas para estas máquinas virtuales. Este valor es el valor de acción predeterminado.

### FORCEfull

Esta acción cambia la modalidad de copia de seguridad de `-mode=ifincremental` a `-mode=iffull`; la copia de seguridad actual se convierte en una copia de seguridad de máquina virtual completa. Se inicia la copia de seguridad de máquina virtual completa. Se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (`dsmerror.log`):

```
ANS9921E Disco de máquina virtual, nombre_mv (etiqueta_disco),  
ha fallado la comprobación de verificación (xxx/yyy)
```

xxx/yyy en el mensaje indican el tamaño de los archivos bitmap (xxx) y CTL (yyy).

```
ANS9919E No se han podido encontrar los archivos de control esperados  
para nombre_mv
```

```
ANS9922I VMVERIFYIFlatest está habilitado para nombre_mv (acción: FORCEFULL).
```

```
ANS9920W Forzando una copia de seguridad de máquina virtual completa  
para nombre_mv
```

Utilice esta opción si la ventana de copia de seguridad actual puede contener una copia de seguridad de máquina virtual completa de las máquinas virtuales afectadas.

#### PREview

Esta acción no realiza ninguna copia de seguridad. En cambio, los datos CTL y bitmap para cada huésped de máquina virtual que procesa el mandato backup vm se almacena en una ubicación temporal, donde se comprueba la integridad. Si la comprobación de integridad falla, se escriben los siguientes mensajes en el archivo de registro de errores del transportador de datos (dsmerror.log):

```
ANS9921E Disco de máquina virtual, nombre_mv (etiqueta_disco),  
ha fallado la comprobación de verificación (xxx/yyy)
```

xxx/yyy en el mensaje indican el tamaño de los archivos bitmap (xxx) y CTL (yyy).

```
ANS9919E No se han podido encontrar los archivos de control esperados  
para nombre_mv
```

```
ANS9922I VMVERIFYIFlatest está habilitado para nombre_mv (acción: PREVIEW)
```

Utilice esta opción para validar la integridad de copias de seguridad incrementales-constant-incrementales (-mode=ifincremental) que haya creado previamente para una o más máquinas virtuales.

Si los mensajes indican que ha fallado la comprobación de integridad en algunas máquinas virtuales, inicie una copia de seguridad de máquina virtual completa (-mode=iffull) en el momento que elija. Como alternativa, establezca -vmverifyifaction=forcefull en la siguiente operación incremental-constante-incremental planificada para forzar una copia de seguridad completa de esas máquinas virtuales. La ventana de copia de seguridad debe ser lo bastante grande para acomodar una o más copias de seguridad de máquina virtual completas.

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmverifyiflatest

---

Esta opción solo se aplica a operaciones de copia de seguridad de máquina virtual VMware que utilicen la modalidad de copia de seguridad incremental-constante-incremental (es decir, un mandato a backup vm con -mode=IFIncremental especificado). Si se habilita esta opción vmverifyiflatest, el transportador de datos ejecuta una comprobación de integridad en los archivos CTL y bitmap que se crearon en un servidor durante la última copia de seguridad, si la última copia de seguridad fue una copia de seguridad incremental-constante-incremental.

Si los archivos pasan las pruebas de integridad, la máquina virtual es restaurable. La copia de seguridad actual continúa y añade otra instantánea a la cadena de instantáneas para la máquina virtual.


Si los archivos fallan las pruebas de integridad, la máquina virtual no es restaurable. En este caso, el transportador de datos realiza otra acción, que ha especificado en la opción (vmverifyifaction). Puede establecer vmverifyifaction para crear una copia de seguridad de máquina virtual completa inmediatamente, o puede fallar toda la copia de seguridad y ejecutar una copia de seguridad de máquina virtual completa en otro momento. Se puede establecer un tercer parámetro para verificar los archivos CTL y bitmap para una máquina virtual, sin crear una nueva instantánea de copia de seguridad.

La verificación solo se puede realizar si la operación de copia de seguridad anterior para la verificación utilizó mode=IFIncr, y si la operación de copia de seguridad actual también utiliza mode=IFIncr. Esta opción no tiene efecto en las otras modalidades de copia de seguridad de máquina virtual.

#### Importante:


Si esta opción se establece en no, el proceso de copia de seguridad de máquina virtual continuará sin ninguna prueba de verificación. Los recursos de procesamiento implicados en realizar las comprobaciones de integridad no tienen valor. Para garantizar la integridad continuada de la cadena de copia de seguridad incremental-constante-incremental, establezca o utilice el valor predeterminado (vmverifyiflatest yes). No establezca esta opción en no, a menos que así se lo indique el soporte de IBM®.




 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

## Cientes soportados


---


 Sistemas operativos Linux Esta opción es válida para clientes Linux que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

 Sistemas operativos Windows Esta opción es válida para clientes Windows que son nodos de movimiento de datos para copias de seguridad de huésped VMware.

## Archivo de opciones

---

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

 Sistemas operativos Linux Establezca esta opción en el archivo de opciones de cliente (dsm.opt) o el archivo de opciones del sistema del cliente (dsm.sys).

Esta opción también se puede incluir en un conjunto de opciones de cliente, como parámetro en un mandato backup vm, o en la definición del parámetro options.

## Sintaxis

---

```
    .-YES- .  
>>-VMVERIFYIFlatest-----<<  
    '-NO--'
```

## Parámetros

---

### YES

Este valor especifica que la validación de los datos CTL y bitmap se realiza para cada máquina virtual procesada por la operación actual de copia de seguridad incremental-constante-incremental (mode=IFIncr), si la operación de copia de seguridad anterior para la máquina virtual también era una copia de seguridad incremental-constante-incremental. Este valor es el valor predeterminado.

### NO

Este valor especifica que la validación de datos CTL y bitmap no se produce durante el proceso de copia de seguridad incremental-constante-incremental. No establezca este valor a menos que así se lo indique el soporte de IBM.

## Ejemplos

---

Archivo de opciones:

```
vmverifyiflatest yes
```

Línea de mandatos:

```
dsmc backup vm vml -mode=ifincremental -vmverifyiflatest=yes
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmvstortransport

---

La opción vmvstortransport especifica el orden de transportes preferido (jerarquía) que utilizar cuando se realizan copias de seguridad de o restaurar máquinas virtuales de VMware. Si no incluye un transporte determinado utilizando esta opción, se excluirá el transporte y no se utilizará para transferir los datos.

El orden de transporte que especifique determina cómo accede VMware API for Data Protection (VADP) a los datos en los discos virtuales, pero no afecta a la vía de acceso de datos utilizada entre el cliente de copia de seguridad y archivado y el servidor de IBM Spectrum Protect. Los transportes válidos incluyen cualquier orden o combinación de las opciones siguientes:

### nbd

Transferencia de datos basada en la red. Acceda a los datos del disco virtual utilizando la LAN. Esta vía de transporte suele estar disponible en todas las configuraciones.

### nbdssl

Igual que nbd, pero los datos se cifran antes de enviarlos por la LAN. El cifrado puede reducir el rendimiento.

### san

Transferencia de red de área de almacenamiento: Acceda a los datos del disco virtual utilizando la SAN.


hotadd


Si utiliza un cliente de archivado-copia de seguridad en una máquina virtual, el transporte hotadd permite el transporte de datos de los que se haya realizado una copia de seguridad a almacenamiento añadido dinámicamente.

Separe cada opción de transporte de las demás con dos puntos, por ejemplo, san:nbd:nbdssl:hotadd.

Si no especifica una jerarquía de transporte, el orden de selección de transporte predeterminado es san:hotadd:nbdssl:nbd.


El primer transporte que está disponible se utiliza para transferir los datos. Si impedir el transporte de datos sobre una determinada vía de acceso, no la incluya en la lista de transportes. Por ejemplo, si es importante no interrumpir el tráfico de la LAN, omita los transportes nbd de la jerarquía.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

 Sistemas operativos Linux Establezca esta opción en dsm.sys.

 Sistemas operativos Windows Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Clientes soportados

 Sistemas operativos Windows Esta opción es válida para clientes Windows configurados para realizar copias de seguridad de o restaurar máquinas virtuales utilizando VDAP.

 Sistemas operativos Linux Esta opción es válida para clientes Linux configurados para realizar copias de seguridad de o restaurar máquinas virtuales utilizando VDAP.

## Sintaxis

```

      .- - - - - .
      V           |
>>-VMVSTORTransport-----+-----><
      +-NBD-----+
      +-NBDSSL-+
      +-SAN-----+
      '-HOTADD-'
```

## Ejemplos

Si la SAN está disponible, no transporte copias de seguridad ni restauraciones sobre la LAN

```
VMVSTORTRANSPORT san
```

El cliente de archivado-copia de seguridad se ejecuta en una máquina virtual, pero no utilice el transporte hotadd


```
VMVSTORTRANSPORT nbdssl:nbd
```

Utilice el transporte de LAN, incluso si nbdssl está disponible, para obtener un rendimiento superior

```
VMVSTORTRANSPORT nbd
```

Es preferible utilizar el transporte SAN, pero utilice nbd cuando SAN no esté disponible, y no utilice nbdssl u hotadd

```
VMVSTORTRANSPORT san:nbd
```

 Sistemas operativos Windows

## Vssaltstagingdir

La opción vssaltstagingdir especifica la vía de acceso totalmente calificada que contiene la caché de exclusión del sistema y datos temporales para el funcionamiento de instantáneas de VSS.

El cliente de copia de seguridad y archivado determina la vía de acceso para los archivos de VSS temporales a partir de las siguientes opciones de prioridad:

1. La opción vssaltstagingdir se define en el archivo dsm.opt.
2. El directorio c:\adsm.sys existe y no está vacío.
3. Si vssaltstagingdir no está definido y el directorio c:\adsm.sys no existe, el cliente obtendrá la vía de acceso a partir de la clave de registro. La vía de acceso para archivos de VSS temporales es el valor DefaultVssStagingDir, y se genera desde el valor Path bajo la clave HKLM\SOFTWARE\IBM\ADSM\CurrentVersion\BackupClient. Una vez creado el valor DefaultVssStagingDir, el valor no se modifica si el cliente se reinstala en una nueva ubicación.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-VSSALTSTAGINGDIR--vía_acceso_archivo-----<<
```

## Parámetros

---

vía\_acceso\_archivo

Especifique la vía de acceso totalmente calificada para archivos temporales que estén relacionados con operaciones de instantáneas de VSS. Si alguna parte de la vía de acceso no existe, el cliente de copia de seguridad y archivado intentará crearla. El valor predeterminado es el directorio de instalación del cliente.

En formato Uniform Naming Convention (UNC), la vía de acceso debe contener una letra de unidad. En el siguiente ejemplo de formato UNC, la vía de acceso contiene la letra de la unidad D\$: \\computer7\D\$\temp\snapshot.

## Ejemplos

---

Archivo de opciones:

```
vssaltstagingdir "c:\Users\All Users\Tivoli\adsm.sys"
```

Línea de mandatos:

```
-vssaltstagingdir ="c:\Users\All Users\Tivoli\adsm.sys"
```

La opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.

 Sistemas operativos Windows

## Vssusesystemprovider

---

La opción vssusesystemprovider especifica si se debe utilizar el proveedor de sistemas de Windows, o permitir a Windows decidir qué proveedor es más apropiado utilizar.

Utilice la opción vssusesystemprovider para las operaciones de Microsoft Windows Volume Shadow Copy Service (VSS), como la copia de seguridad del estado del sistema o IBM Spectrum Protect para las copias de seguridad de Copy Services.

## Clientes soportados

---

Esta opción es válida para todos los clientes Windows. El servidor también puede definir esta opción. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

Establezca esta opción en el archivo de opciones del cliente (dsm.opt).

## Sintaxis

---

```
>>-VSSUSESYSTEMProvider--.-No-- .  
+-----+-----<<  
'-Yes-'
```

## Parámetros

---

Yes

Especifica que se está utilizando el proveedor de sistemas de Microsoft Windows VSS.

No

Especifica que se está utilizando el proveedor de sistemas predeterminado. Este proveedor puede o no ser el mismo proveedor de sistemas, dependiendo de qué otros proveedores están instalados en el sistema. Utilice no si desea utilizar el proveedor de sistemas predeterminado y éste no es el proveedor Microsoft Windows VSS. No es el valor predeterminado.

## Ejemplos

---

Archivo de opciones:

```
vssusesystemprovider yes
```

Línea de mandatos:

No se aplica.

 Sistemas operativos Linux  Sistemas operativos Windows

## Vmtimeout


---


VMTIMEOut especifica el tiempo máximo, en segundos, que se debe esperar antes de abandonar una operación backup vm, cuando se utiliza la opción INCLUDE.VMTSMVSS para proporcionar protección de aplicaciones. Para utilizar esta opción, debe haber instalado la licencia de IBM Spectrum Protect para entornos virtuales.

Las operaciones backup vm realizadas en una máquina virtual protegida por una opción INCLUDE.VMTSMVSS están sujetas a un temporizador. El valor del temporizador determina cuántos segundos debe esperar el cliente para pausar la actividad de la aplicación y truncar sus registros para poder realizar la copia de seguridad. El valor de tiempo predeterminado es suficiente para la mayoría de los entornos. Sin embargo, si no se puede realizar copia de seguridad de los datos de la aplicación porque la aplicación necesita tiempo adicional para preparar la instantánea, puede aumentar el valor de tiempo de espera. Este temporizador sólo se aplica a operaciones backup vm cuando se establece la opción INCLUDE.VMTSMVSS para una máquina virtual.

## Clientes soportados

---

 Sistemas operativos Linux Esta opción puede utilizarse con clientes Linux x86\_64 soportados.

 Sistemas operativos Windows Esta opción puede utilizarse con clientes Windows soportados.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones del cliente. No puede establecerse en la línea de mandatos ni el editor de preferencias.

## Sintaxis

---

```
.-180-----.  
>>-VMTIMEout-+-+-----+----->>  
      '-time_out-'
```

## Parámetros

---

*tiempo\_espera*

Especifica el tiempo, en segundos, que hay que dejar para que finalicen las operaciones de copia de seguridad cuando una máquina virtual está protegida por la opción de protección de aplicaciones, INCLUDE.VMTSMVSS. El valor especificado debe ser un número entero entre 180 y 500. El valor predeterminado es de 180 segundos.

## Ejemplos

---

Archivo de opciones

```
VMTIMEout 500
```

Línea de mandatos

No aplicable; esta opción no puede establecerse en la línea de mandatos.

**Referencia relacionada:**





INCLUDE.VMTSMVSS


## Webports





---


La opción webports habilita el uso del cliente web fuera de un cortafuegos.

La opción webports permite utilizar el cliente web fuera de un cortafuegos mediante la especificación del número de puerto TCP/IP que utilizan el servicio de aceptación de clientes de IBM Spectrum Protect y el servicio del agente de cliente web para las comunicaciones con el cliente web.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XEs necesario especificar valores para el aceptador de clientes y para el servicio del agente de cliente web.

 Sistemas operativos WindowsEs necesario especificar valores para el servicio de aceptación de clientes y para el servicio del agente de cliente web.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XSi no especifica esta opción, se utiliza el valor predeterminado, cero (0), en ambos puertos. Esto da lugar a que TCP/IP asigne aleatoriamente un número de puerto libre para el aceptador de clientes y el servicio del agente de cliente web.

 Sistemas operativos WindowsSi no especifica esta opción, se utiliza el valor predeterminado, cero (0), en ambos puertos. Esto da lugar a que TCP/IP asigne aleatoriamente un número de puerto libre para el servicio de aceptación de clientes y el servicio del agente de cliente web.





## Clientes soportados


---

Esta opción es válida para todos los clientes. La API de IBM Spectrum Protect no admite esta opción.

## Archivo de opciones

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XEstablezca esta opción en el archivo dsm.sys dentro de una stanza de servidor. Para establecer esta opción en el editor Preferencias del cliente, pulse Editar > Preferencias del cliente > Cliente web y especifique los puertos en los campos Puerto del agente web y Puerto del aceptador de clientes web.

 Sistemas operativos WindowsEstablezca esta opción en el archivo de opciones del cliente (dsm.opt). Para establecer esta opción en el editor Preferencias del cliente, pulse Editar > Preferencias del cliente > Cliente web y especifique los puertos en los campos Puerto del agente web y Puerto del aceptador de clientes web.









## Sintaxis



---

```
>>-WEBPorts-- --cadport-- --agentport-----><
```

## Parámetros

---

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solariscadport  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle SolarisEspecifica el número de puerto necesario del aceptador de clientes. El rango de valores oscila entre 1000 y 32767. Si no se especifica ningún valor, el valor predeterminado, cero (0), hace que TCP/IP asigne al azar un número de puerto libre.

 Sistemas operativos Windowscadport  Sistemas operativos WindowsEspecifica el número de puerto necesario del servicio de aceptación de clientes. El rango de valores oscila entre 1000 y 32767. Si no se especifica ningún valor, el valor predeterminado, cero (0), hace que TCP/IP asigne al azar un número de puerto libre.

puerto\_agente

Especifica el número de puerto necesario del servicio del agente de cliente web. El rango de valores oscila entre 1000 y 32767. Si no se especifica ningún valor, el valor predeterminado, cero (0), hace que TCP/IP asigne al azar un número de puerto libre.

## Ejemplos

---

Archivo de opciones:

```
webports 2123 2124
```

Línea de mandatos:

 Sistemas operativos Windows

```
webports 2123, 2124
```

## Wildcardsareliteral

---

La opción `wildcardsareliteral` especifica si los signos de interrogación (?) y los asteriscos (\*) se interpretan literalmente, cuando están incluidos en una especificación de una lista de archivos en una opción `filelist`.

Normalmente, el cliente no acepta caracteres comodín (?) y (\*) en una especificación de lista de archivos que se incluye en una opción `filelist`. Algunos sistemas de archivos permiten el uso de comillas simples y dobles en los nombres de archivos y directorios. Para impedir errores que de lo contrario se podrían producir, cuando se incluyen especificaciones de archivos en una opción `filelist` y contienen caracteres comodín, establezca `wildcardsareliteral yes`. Cuando `wildcardsareliteral` tiene el valor `yes`, los signos de interrogación (?) y los asteriscos (\*) que se incluyen en una especificación de lista de archivos en la opción `filelist` se interpretan literalmente, y no como caracteres comodín.

Esta opción se aplica a cualquier mandato que acepta una opción `filelist` como un parámetro de mandato.

## Clientes soportados

---

Esta opción es válida para todas las plataformas soportadas. La opción se aplica a cualquier mandato que toma una especificación de lista de archivos como parámetro.

## Archivo de opciones

---

Coloque esta opción en el archivo de opciones de usuario del cliente (`dsm.opt`).

## Sintaxis

---

```
                .-no-----.  
>>-WILDCARDSareliteral-+++-+-----+-----<<  
                '-yes-'
```

## Parámetros

---

no

Especifica que las interrogaciones y los asteriscos se interpretan como comodines cuando se utilizan en una especificación de lista de archivos que se incluye en una opción `filelist`. No es el valor predeterminado. Si una especificación de lista de archivos en una opción `filelist` incluye una interrogación o un asterisco, se produce un error y no se puede procesar la especificación de archivo.

yes


Especifica que los asteriscos y las interrogaciones en una especificación de lista de archivos que se incluye en una opción `filelist` se interpretan literalmente, y no como caracteres comodín. Especifique este valor si está realizando la copia de seguridad de archivos desde un sistema de archivos que permite los caracteres comodín en nombres de archivo o de directorio.


## Ejemplos


---


Archivo de opciones:

```
WILDCARDSARELITERAL YES
```


 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Suponiendo que el sistema de archivos permita caracteres comodín en las vías de acceso, los siguientes son ejemplos de archivos de una especificación de lista de archivos que se pueden procesar correctamente si `WILDCARDSARELITERAL` se establece en `YES`.

 Sistemas operativos Windows Supongamos que el mandato que se emite es `dsmc sel -filelist=c:\important_files.txt`, donde `important_files.txt` contiene la lista de archivos que deben procesarse.

 Sistemas operativos Windows `important_files.txt` contiene la siguiente lista de archivos:

```
c:\home\myfiles\file?9000  
c:\home\myfiles\?file  
c:\home\myfiles\**README**version2  
c:\home\myfiles\ABC?file*
```

 Sistemas operativos Windows Si `WILDCARDSARELITERAL` y `QUOTESARELITERAL` se establecen en `YES`, las siguientes copias de seguridad se pueden procesar satisfactoriamente:

```

c:\home\myfiles\"file?
c:\home\myfiles\?file'
c:\home\myfiles\**"README Tomorrow"***
c:\home\myfiles\file*

```

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Línea de mandatos:

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Suponiendo que el sistema de archivos permita caracteres comodín en las vías de acceso, los siguientes son ejemplos de archivos de una especificación de lista de archivos que se pueden procesar correctamente si WILDCARDSARELITERAL se establece en YES.

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Supongamos que el mandato emitido es `dsmc sel -filelist=/home/user1/important_files`, donde `important_files.txt` contiene la lista de archivos a procesar.

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris `important_files.txt` contiene la siguiente lista de archivos:

```

/home/user1/myfiles/file?9000
/home/user1/myfiles/?file
/home/user1/myfiles/**README**version2
/home/user1/myfiles/ABC?file*

```

Sistemas operativos AIX Sistemas operativos Linux sistemas operativos Mac OS X Sistemas operativos Oracle Solaris Si WILDCARDSARELITERAL y QUOTESARELITERAL se establecen en YES, las siguientes copias de seguridad se pueden procesar satisfactoriamente:

```

/home/user1/myfiles/"file?
/home/user1/myfiles/?file'
/home/user1/myfiles/**"README Tomorrow"***
/home/user1/myfiles/file*

```

## Utilización de los mandatos

































El cliente de copia de seguridad y archivado proporciona una interfaz de línea de mandatos (CLI) que puede utilizar como alternativa a la interfaz gráfica de usuario (GUI). En este tema se describe cómo iniciar o finalizar una sesión de mandatos de cliente y cómo escribir los mandatos.

- Inicio y finalización de una sesión de mandatos de cliente
- Especificación de los nombres, opciones y parámetros de los mandatos de cliente
- Caracteres comodín

































En la siguiente tabla se muestran una lista alfabética de los mandatos y una breve descripción.















Tabla 1. Mandatos

Mandato	Descripción
archive	Archiva los archivos de una estación de trabajo en el almacenamiento de IBM Spectrum Protect.
Sistemas operativos Windows <code>archive fastback</code>	Sistemas operativos Windows Volúmenes de archivos especificados por las opciones <code>fbpolicyname</code> , <code>fbclientname</code> y <code>fbvolumename</code> para una retención larga.
Sistemas operativos Linux  Sistemas operativos Windows <code>backup fastback</code>	Sistemas operativos Linux  Sistemas operativos Windows Volúmenes de copias de seguridad especificados por las opciones <code>fbpolicyname</code> , <code>fbclientname</code> y <code>fbvolumename</code> para una retención larga.
backup group	Crea y realiza una copia de seguridad de un grupo que contiene una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.
Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows <code>backup image</code>	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Crea una copia de seguridad de imágenes de uno o varios sistemas de archivos o volúmenes lógicos que especifique.
Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows <code>backup nas</code>	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Crea una copia de seguridad de imágenes de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (Almacenamiento conectado en red).

<b>Mandato</b>	<b>Descripción</b>
 Sistemas operativos Windows backup systemstate	 Sistemas operativos Windows Realiza la copia de seguridad de todos los componentes de inicio de servicios del sistema y del estado del sistema como si fueran un solo objeto, para proporcionar una instantánea de instante específico coherente del estado del sistema. Este mandato es válido para los clientes Windows admitidos.
 Sistemas operativos Linux  Sistemas operativos Windows backup vm	 Sistemas operativos Linux  Sistemas operativos Windows Realiza una copia de seguridad de máquinas virtuales especificadas en la opción vmlist.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows cancel process	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Visualiza una lista de los procesos actuales de copia de seguridad de imágenes y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización.
cancel restore	Muestra una lista de sesiones de restauración reiniciables donde puede seleccionar una para cancelarla.
delete access	Suprime reglas de autorización para archivos que se han almacenado en el servidor.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows En los clientes que admiten la copia de seguridad de imágenes, este mandato suprime reglas de autorización para imágenes que se han almacenado en el servidor.
delete archive	Suprime copias archivadas del almacenamiento del servidor de IBM Spectrum Protect.
delete backup	Suprime archivos de copia de seguridad activos e inactivos del almacenamiento del servidor de IBM Spectrum Protect.
delete filespace	Suprime los espacios de archivos del almacenamiento del servidor de IBM Spectrum Protect.
delete group	Suprime una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.
expire	Desactiva los objetos de copia de seguridad indicados en la especificación de archivo o mediante la opción filelist.
help	Muestra una tabla de contenido de los temas de ayuda para el cliente de línea de mandatos.
incremental	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Realiza la copia de seguridad de todos los archivos o directorios nuevos o cambiados del dominio de cliente predeterminado o de los sistemas de archivos, directorios o archivos que ha especificado, a menos que los haya excluido de los servicios de copia de seguridad.
loop	Inicia una sesión interactiva de mandatos.
macro	Ejecuta mandatos dentro del archivo de macro que especifique.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows monitor process	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS desde la que puede seleccionar el proceso que desea cancelar.
preview archive	Simula un mandato de archivado sin enviar datos al servidor.
preview backup	Simula un mandato de copia de seguridad sin enviar datos al servidor.
query access	Visualiza una lista de las reglas actuales de autorización.
 Sistemas operativos Windows query adobjects	 Sistemas operativos Windows Visualiza una lista de las reglas actuales de autorización.
query archive	Visualiza una lista de las copias archivadas.
query backup	Visualiza una lista de las versiones de copia de seguridad.























Mandato	Descripción
query backupset	Consulta un juego de copias de seguridad de un archivo local o del servidor de IBM Spectrum Protect. En los clientes que admiten dispositivos de cinta, este mandato puede consultar un juego de copias de seguridad de un dispositivo de cinta.
query filespace	Visualiza una lista de los espacios de archivos del almacenamiento de IBM Spectrum Protect. También puede especificar un único nombre de espacio de archivos para su consulta.
query group	Visualiza información acerca de las copias de seguridad de grupo y sus miembros.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowsquery image	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos WindowsVisualiza información acerca de las copias de seguridad de imagen.
query inclxcl	Visualiza una lista de sentencias de inclusión/exclusión en el orden en que se procesan durante las operaciones de copia de seguridad/archivado.
query mgmtclass	Muestra información sobre las clases de gestión disponibles.
query node	Muestra todos los nodos en los que un identificador de usuario de administración dispone de autorización para realizar operaciones.
query options	Muestra todas o parte de las opciones y sus valores actuales.
query restore	Visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor.
query schedule	Muestra información sobre los sucesos planificados para el nodo.
query session	Muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.
query systeminfo	Recopila información del sistema de IBM Spectrum Protect y envía esta información a un archivo o la visualiza en la consola.
 Sistemas operativos Windowsquery systemstate	 Sistemas operativos WindowsVisualiza información acerca de la copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect. Este mandato es válido para todos los clientes Windows admitidos.
 Sistemas operativos Windows  Sistemas operativos Linuxquery vm	 Sistemas operativos Windows  Sistemas operativos LinuxVerifica las copias de seguridad correctas de las máquinas virtuales del servidor de copia de seguridad vStorage.
restart restore	Muestra una lista de sesiones de restauración reiniciables donde puede seleccionar una para reiniciarla.
restaurar	Restaura copias de versiones de copias de seguridad de los archivos desde el servidor de IBM Spectrum Protect.
 Sistemas operativos Windowsrestore adobjects	 Sistemas operativos WindowsRestaura objetos individuales de Active Directory del contenedor de objetos suprimidos de Active Directory local.
restore backupset	Restaura un juego de copias de seguridad desde el servidor de IBM Spectrum Protect o un archivo local. En los clientes que admiten dispositivos de cinta, este mandato puede restaurar un conjunto de copias de seguridad de un dispositivo de cinta.
restore group	Restaura miembros específicos o todos los miembros de una copia de seguridad de grupo.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowsrestore image	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos WindowsRestaura un sistema de archivos o una copia de seguridad de imágenes de volumen RAW.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windowsrestore nas	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos WindowsRestaura la imagen de un sistema de archivos que pertenece a un servidor de archivos NAS (Network Attached Storage).












Mandato	Descripción
 Sistemas operativos Windows restore systemstate	 Sistemas operativos Windows Restaura una copia de seguridad del estado del sistema. Este mandato queda en desuso para las operaciones de restauración del sistema en línea. Para obtener más información, consulte el apartado Restore Systemstate.
 Sistemas operativos Linux  Sistemas operativos Windows restore vm	 Sistemas operativos Linux  Sistemas operativos Windows Restaura una copia de seguridad de la máquina virtual completa y devuelve los archivos de copia de seguridad de la máquina virtual completa al directorio vmbackdir del servidor de copia de seguridad vStorage.
retrieve	Recupera copias archivadas del servidor de IBM Spectrum Protect.
schedule	Inicia el planificador cliente de la estación de trabajo.
selective	Realiza copia de seguridad de los archivos seleccionados.
set access	Otorga autorización a otro usuario para que éste pueda acceder a sus versiones de copia de seguridad o a sus copias archivadas.   Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows En los clientes que admiten la copia de seguridad de imágenes, este mandato puede establecer reglas de autorización para imágenes que se han almacenado en el servidor.
set event	Permite especificar las circunstancias que se deben dar cuando se suprimen datos archivados.
 Sistemas operativos Linux  Sistemas operativos Windows set netappsvm	 Sistemas operativos Linux  Sistemas operativos Windows Asocia las credenciales de inicio de sesión para un servidor de gestión de clústeres con una máquina virtual de almacenamiento NetApp y el nombre del SVM de datos (Vserver de datos). Este mandato debe especificarse antes de crear una copia de seguridad incremental por diferencia de instantánea de un volumen de NetApp en clúster.
set password	Cambia la contraseña de IBM Spectrum Protect de la estación de trabajo.

Para que el funcionamiento sea correcto, el nodo was debe restaurarse en la misma ubicación y con el mismo nombre.






Importante: Para evitar problemas, restaure los datos sólo en el nodo de Network Deployment Manager o en el nodo de Application Server.

- Inicio y finalización de una sesión de mandatos de cliente  
Una sesión de mandatos de cliente se puede iniciar o finalizar en modalidad de proceso por lotes o en modalidad interactiva.
- Especificación de los nombres, opciones y parámetros de los mandatos de cliente  
Un mandato de cliente incluye uno o varios de estos componentes: *nombre del mandato*, *opciones* y *parámetros*. Las secciones que aparecen a continuación describen cada uno de estos componentes.
- Caracteres comodín  
Utilice los caracteres comodín cuando quiera especificar varios archivos con nombres similares en *un* mandato. Si no los utiliza, tendrá que repetir el mandato para cada archivo.
- Consulta de mandatos de cliente  
Las secciones que figuran a continuación contienen información detallada sobre cada uno de los mandatos del cliente de copia de seguridad y archivado.
- Archive  
El mandato archive archiva un solo archivo, los archivos seleccionados o todos los archivos de un directorio y sus subdirectorios en un servidor.
-  Sistemas operativos Linux  
 Sistemas operativos Windows  
Archivado de FastBack  
Utilice el mandato archive fastback para archivar volúmenes de Tivoli Storage Manager FastBack especificados por las opciones fbpolycname, fbclientname y fbvolumename para una retención a largo plazo.
-  Sistemas operativos Linux  
 Sistemas operativos Windows  
Copia de seguridad de FastBack  
Utilice el mandato backup fastback para realizar copia de seguridad de los volúmenes de Tivoli Storage Manager FastBack especificados por las opciones fbpolycname, fbclientname y fbvolumename para una retención a largo plazo.
- Backup Group  
Utilice el mandato backup group para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.
-  Sistemas operativos AIX  
 Sistemas operativos Linux  
 Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows  
Backup Image  
El mandato backup image crea una copia de seguridad de imagen de uno o varios volúmenes del sistema.

-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Backup NAS  
 El mandato backup nas crea una copia de seguridad de imagen de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (Network Attached Storage), también conocido como copia de seguridad NDMP. Se le solicitará el ID de administrador de IBM Spectrum Protect.
-  Sistemas operativos Windows Backup Systemstate  
 Utilice el mandato backup systemstate para realizar la copia de seguridad de todos los componentes arrancables de servicios del sistema y de estado del sistema como si fueran un solo objeto, para proporcionar una instantánea de instante específico coherente del estado del sistema.
-  Sistemas operativos Linux  Sistemas operativos Windows Backup VM  
 Utilice el mandato backup vm para iniciar una copia de seguridad completa de una máquina virtual.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Cancel Process  
 El mandato cancel process visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.
- Cancel Restore  
 El mandato cancel restore visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor.
- Delete Access  
 El mandato delete access suprime reglas de autorización para los archivos que están almacenados en el servidor.
- Delete Archive  
 El mandato delete archive suprime las copias archivadas del almacenamiento del servidor de IBM Spectrum Protect. Su administrador debe concederle la autoridad para suprimir los archivos archivados.
- Delete Backup  
 El mandato delete backup suprime archivos, imágenes y máquinas virtuales de las que se ha realizado copia de seguridad en el almacenamiento del servidor de IBM Spectrum Protect. El administrador debe otorgar autorización para suprimir objetos.
- Delete Filespace  
 El mandato delete filespace suprime espacios de archivos del almacenamiento del servidor de IBM Spectrum Protect. Un espacio de archivos es un espacio lógico del servidor que contiene archivos de los que se realizó copia de seguridad o de archivado.
- Delete Group  
 Utilice el mandato delete group para suprimir una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.
- Expire  
 El mandato expire desactiva los objetos de copia de seguridad que especifica en la especificación de archivos o con la opción filelist. Puede especificar un archivo individual para que caduque, o un archivo que contiene una lista de archivos que caducarán. Si `OBJTYPE=VM`, este mandato desactivará la copia de seguridad actual para una máquina virtual.
- Help  
 Utilice el mandato help para visualizar información acerca de mandatos, opciones y mensajes.
- Incremental  
 El mandato incremental realiza la copia de seguridad de todos los datos nuevos o modificados de las ubicaciones que especifique, a menos que los excluya de los servicios de copia de seguridad.
- Loop  
 El mandato loop inicia una sesión de línea de mandatos interactiva que se mantiene hasta que el usuario escribe `quit`.
- Macro  
 El mandato macro ejecuta una serie de mandatos que se especifican en un archivo de macros.
-  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Monitor Process  
 El mandato monitor process visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.
- Preview Archive  
 El mandato preview archive simula un mandato de copia de seguridad sin enviar los datos al servidor.
- Previsualizar copia de seguridad  
 El mandato preview simula un mandato de copia de seguridad sin enviar los datos al servidor.
- Query Access  
 El mandato query access muestra los usuarios a los que ha otorgado acceso a las versiones de copia de seguridad o copias archivadas de archivos específicos.
-  Sistemas operativos Windows Query Adobjects  
 Utilice el mandato query adobjects para mostrar información acerca de los objetos suprimidos ubicados en el dominio local de Active Directory.
- Query Archive  
 El mandato query archive muestra una lista de las copias archivadas y la siguiente información acerca de cada archivo: tamaño de archivo, fecha de archivado, especificación de archivo, fecha de caducidad y descripción de archivado.
- Query Backup  
 El mandato query backup muestra una lista de versiones de copia de seguridad de los archivos almacenadas en el servidor de IBM Spectrum Protect, o del interior de un juego de copias de seguridad del servidor cuando se especifica la opción `backupsetname`.

- **Query Backupset**  
El mandato query backupset consulta un juego de copias de seguridad de un archivo local, de un dispositivo de cinta (si es aplicable) o del servidor de IBM Spectrum Protect.
- **Query Filespace**  
El mandato query filespace muestra una lista de espacios de archivos para un nodo. Los espacios de archivos se almacenan en el servidor de IBM Spectrum Protect o en el interior de un juego de copias de seguridad del servidor cuando se especifica la opción backupsetname. También puede especificar un único nombre de espacio de archivos para su consulta.
- **Query Group**  
Utilice el mandato query group para que se visualice información acerca de una copia de seguridad de grupo y sus miembros.
- **Query Image**  
El mandato query image muestra información sobre las imágenes del sistema de archivos que se almacenan en el servidor de IBM Spectrum Protect, o en el interior de un juego de copias de seguridad del servidor de IBM Spectrum Protect, cuando se especifica la opción backupsetname.
- **Query Inclexcl**  
El mandato query inclexcl visualiza una lista de sentencias de inclusión/exclusión en el orden en que se procesan durante las operaciones de copia de seguridad/archivado. La lista visualiza el tipo de opción, el ámbito de la opción (archive, all, etc.), y el nombre del archivo fuente.
- **Query Mgmtclass**  
El mandato query mgmtclass visualiza la información sobre las clases de gestión disponibles en el conjunto de políticas activo.
- **Query Node**  
El mandato query node muestra todos los nodos en los que un identificador de usuario de administración dispone de autorización para realizar operaciones. Se le solicitará el ID de administrador de IBM Spectrum Protect.
- **Query Options**  
Utilice el mandato query options para que se visualicen todas o parte de las opciones y sus valores actuales relacionados con el cliente de línea de mandatos.
- **Query Restore**  
El mandato query restore visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor. La lista contiene los siguientes campos: owner, replace, subdir, preservepath, source y destination.
- **Query Schedule**  
El mandato query schedule visualiza los sucesos planificados de su nodo. El administrador puede establecer planificaciones para realizar operaciones de copia de seguridad/archivado de forma automática. A fin de planificar el trabajo, utilice este mandato para determinar cuándo van a ocurrir los siguientes sucesos planificados.
- **Query Session**  
El mandato query session muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.
- **Query Systeminfo**  
Utilice el mandato query systeminfo para recopilar información y enviar esta información a un archivo o a la consola.
-  **Sistemas operativos WindowsQuery Systemstate**  
Utilice el mandato query systemstate para visualizar información sobre la copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect, o en el estado del sistema en un conjunto de copias de seguridad de un servidor de IBM Spectrum Protect, cuando se especifica la opción backupsetname.
-  **Sistemas operativos Linux**  **Sistemas operativos WindowsQuery VM**  
Utilice el mandato query VM para listar y verificar las copias de seguridad correctas de las máquinas virtuales (VM).
- **Restart Restore**  
El mandato restart restore visualiza una lista de las sesiones de restauración reiniciables en la base de datos del servidor.
- **Restore**  
El mandato restore obtiene copias de versiones de las copias de seguridad de los archivos del servidor de IBM Spectrum Protect o en el interior de un conjunto de copias de seguridad.
-  **Sistemas operativos WindowsRestore Adobjects**  
Utilice el mandato restore adobjects para restaurar objetos de Active Directory individuales del contenedor de objetos suprimidos local.
- **Restore Backupset**  
El mandato restore backupset restaura un juego de copias de seguridad del servidor de IBM Spectrum Protect, de un archivo local o de un dispositivo de cinta local. Puede restaurar todo el juego de copias de seguridad o, en algunos casos, archivos específicos del juego de copias de seguridad.
- **Restore Group**  
Utilice el mandato restore group para restaurar miembros específicos o todos los miembros de una copia de seguridad de grupo.
-  **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos WindowsRestore Image**  
El mandato restore image restaura un sistema de archivos o una imagen de volumen RAW cuya copia de seguridad se ha realizado con el mandato backup image.
-  **Sistemas operativos AIX**  **Sistemas operativos Oracle Solaris**  **Sistemas operativos WindowsRestore NAS**  
El mandato restore nas restaura la imagen de un sistema de archivos perteneciente a un servidor de archivos NAS

(almacenamiento conectado a red). Cuando se utilice una sesión de línea de mandatos interactiva con un ID que no es un ID de administración, se le solicitará un ID de administrador.

-  Sistemas operativos Windows Restore Systemstate  
El mandato restore systemstate está en desuso para las operaciones de restauración del estado del sistema en línea.
-  Sistemas operativos Linux  Sistemas operativos Windows Restore VM  
Utilice el mandato restore vm para restaurar una máquina virtual de la que se había realizado previamente una copia de seguridad.
- Retrieve  
El mandato retrieve obtiene copias de archivos archivados del servidor de IBM Spectrum Protect. Puede recuperar archivos específicos o directorios completos.
- Schedule  
El mandato schedule inicia el planificador cliente en la estación de trabajo. El planificador cliente debe estar en ejecución para que se pueda iniciar el trabajo planificado.
- Selective  
El mandato selective realiza copias de seguridad de los archivos que especifique. Si estos archivos se dañan o se pierden, podrá sustituirlos por las versiones de copia de seguridad del servidor.
- Set Access  
El mandato set access otorga a usuarios determinados de otros nodos acceso a las versiones de copia de seguridad o copias archivadas.
- Set Event  
Con el mandato set event puede especificar las circunstancias que se deben dar cuando se suprimen datos archivados.
- Establecer Netappsvm  
El mandato set netappsvm asocia las credenciales de inicio de sesión para un servidor de gestión de clústeres, que se especifican en el mandato set password, con una máquina virtual de almacenamiento NetApp y el nombre de máquina virtual de almacenamiento (SVM) de datos (Vserver de datos). Debe especificar este mandato antes de crear una copia de seguridad incremental por diferencia de instantánea de un volumen de NetApp en clúster.
- Establecer contraseña  
El mandato set password cambiará la contraseña de IBM Spectrum Protect para la estación de trabajo o establece las credenciales que se utilizan para acceder a otro servidor.
-  Sistemas operativos Linux  Sistemas operativos Windows Set Vmtags  
El mandato set vmtags crea códigos y categorías de protección de datos que se pueden añadir a objetos de inventario VMware. Puede gestionar copias de seguridad de IBM Spectrum Protect de máquinas virtuales en estos objetos de VMware especificando los códigos con herramientas como, por ejemplo, VMware vSphere PowerCLI versión 5.5 R2 o posterior.

#### Referencia relacionada:

Lectura de diagramas de sintaxis

## Inicio y finalización de una sesión de mandatos de cliente

---

Una sesión de mandatos de cliente se puede iniciar o finalizar en modalidad de proceso por lotes o en modalidad interactiva.

Utilice la modalidad de proceso por lotes si desea entrar un *único* mandato de cliente. El cliente de copia de seguridad y archivado procesa el mandato y vuelve al indicador de mandatos.

Utilice la modalidad interactiva si desea entrar una *serie* de mandatos. Puesto que el cliente establece una sola vez la conexión con el servidor para la modalidad interactiva, el conjunto de mandatos se puede procesar más rápidamente. El cliente procesa los mandatos y vuelve al indicador de `Protect>`.

- Proceso de mandatos en modalidad por lotes  
Algunas opciones *sólo* son válidas en la línea de mandatos inicial pero no en modalidad interactiva. Por lo general, estas opciones afectan al funcionamiento de toda la sesión.
- Proceso de mandatos en modalidad interactiva  
Utilice la modalidad *interactiva* (o la modalidad de *bucle*) para especificar series de mandatos.

## Proceso de mandatos en modalidad por lotes

---

Algunas opciones *sólo* son válidas en la línea de mandatos inicial pero no en modalidad interactiva. Por lo general, estas opciones afectan al funcionamiento de toda la sesión.

Por ejemplo, el mandato **dsmc query session -errorlogname=myerror.log** se acepta y asigna un nombre a la anotación de errores. Sin embargo, se acepta solamente porque aparece en el mandato inicial, aunque la opción no es válida para el mandato de consulta.

También hay algunas opciones que son siempre válidas en la línea de mandatos inicial, así como en mandatos individuales en la modalidad interactiva. Por ello, algunas opciones se aceptan en la línea de mandatos inicial aunque no tienen efecto en el mandato que

se especifica. Por ejemplo, **dsmc query session -subdir=yes** es un mandato válido, pero en este caso la opción *-subdir* no tiene efecto en el mandato que se ha especificado.

Si especifica un *único* mandato en modalidad de proceso por lotes, deberá incluir, delante de éste, el nombre del programa ejecutable, **dsmc**. Por ejemplo, para procesar el mandato incremental en la modalidad por lotes, escribiría:

```
dsmc incremental
```

Cada vez que especifique un mandato, el cliente de copia de seguridad y archivado le preguntará si la opción *passwordaccess* se ha establecido en *prompt* y si la autenticación del servidor se ha establecido en *On*. Escríbala y pulse Intro.

También se puede entrar la contraseña mediante la opción *password* con un mandato, pero la contraseña aparece en la pantalla. Por ejemplo, si la contraseña es **secreto**, se entra:

```
dsmc incremental -password=secreto
```

Si establece la opción *passwordaccess* en *generate* en el archivo *dsm.opt*, no es necesario que especifique la contraseña con el mandato. El cliente solo solicita la contraseña si el usuario está inscribiendo la estación de trabajo en un servidor o si está modificando manualmente la contraseña.

## Proceso de mandatos en modalidad interactiva





---

Utilice la modalidad *interactiva* (o la modalidad de *bucle*) para especificar series de mandatos.

Escriba *dsmc* en la línea de mandatos y pulse Intro. Cuando aparezca el indicador de mandatos *Protect>*, escriba el nombre del mandato y pulse Intro. No preceda cada mandatos con el nombre del programa ejecutable, *dsmc*. Otra alternativa consiste en escribir *dsmc loop* en la línea de mandatos para iniciar una sesión de mandatos de cliente en modalidad interactiva. *Loop* es el mandato predeterminado de *dsmc*.

Si se necesita una contraseña, el cliente de copia de seguridad y archivado la solicita antes de que entre el primer mandato.





 Sistemas operativos Windows Escribala y pulse Intro.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Escriba el identificador de usuario y la contraseña y pulse Intro.

También puede especificar la contraseña mediante la utilización de la opción *password* con el mandato *loop*, pero la contraseña aparecerá en la pantalla. Por ejemplo, si la contraseña es **secreto**, se entra:

```
dsmc loop -password=secreto
```

Para finalizar una sesión interactiva, escriba *quit* en el indicador.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota para los clientes UNIX y Linux:

En la modalidad de bucle, después de una operación de restauración directamente desde cinta, el punto de montaje no se libera por si se realizan solicitudes de restauración adicionales de dicho volumen. Si solicita una operación de copia de seguridad en la misma sesión y dicho punto de montaje es el único que está disponible, la operación de copia de seguridad se interrumpirá con el mensaje siguiente:

```
Esperando a que se monte un medio fuera de línea.
```

En este caso, el punto de montaje no se libera hasta que se cumple una de las condiciones siguientes:

- Se satisface el límite *MOUNTRETENTION* de la clase de dispositivo.
- Se satisface el período de inactividad (*idletimeout*) del cliente.
- La sesión de bucle *dsmc* se cierra una vez que ha finalizado la operación de restauración, lo que permite iniciar otra sesión en modalidad de bucle para realizar la operación de copia de seguridad.

## Especificación de los nombres, opciones y parámetros de los mandatos de cliente

---

Un mandato de cliente incluye uno o varios de estos componentes: *nombre del mandato*, *opciones* y *parámetros*. Las secciones que aparecen a continuación describen cada uno de estos componentes.

- Nombre de mandato

La primera parte de un mandato es el nombre de mandato. El nombre de mandato consiste en una única palabra, como **help** o

**schedule** o una palabra de acción y un objeto para esa acción, tal como **query archive**.

- Opciones  
Cuando escriba opciones con un mandato, anteponga siempre un guión (-) a la opción. No incluya ningún espacio entre el guión y el nombre de la opción.
- Parámetros  
Los mandatos pueden tener parámetros obligatorios, parámetros optativos o pueden no tener parámetros.
- Sintaxis de especificación de archivo  
A continuación se presentan diversas reglas de sintaxis que deberá conocer al especificar parámetros de especificación de archivo, como `filespec`, `sourcefilespec` y `destinationfilespec`.

## Nombre de mandato

---

La primera parte de un mandato es el nombre de mandato. El nombre de mandato consiste en una única palabra, como **help** o **schedule** o una palabra de acción y un objeto para esa acción, tal como **query archive**.

Escriba el nombre completo del mandato o la abreviatura mínima.

Por ejemplo, puede entrar cualquiera de las siguientes versiones del mandato `query schedule`:

```
query schedule
q sc
q sched
query sc
```

## Opciones

---

Cuando escriba opciones con un mandato, anteponga siempre un guión (-) a la opción. No incluya ningún espacio entre el guión y el nombre de la opción.

Pueden entrarse las opciones de los mandatos en cualquier orden, antes o después de la especificación de archivo. Separe las diferentes opciones con un espacio en blanco.

Existen dos grupos de opciones que puede utilizar con los mandatos: opciones del cliente (se establecen en el archivo de opciones) u opciones de mandatos de cliente (se utilizan en la línea de mandatos).

- **Opciones de cliente:** grupo de opciones que se establecen en el archivo de opciones del cliente. Puede modificar temporalmente una opción en el archivo de opciones del cliente cuando especifica la opción con un mandato en la línea de mandatos.
- **Opciones de línea de mandatos:** utilice una opción de mandato de cliente *sólo* cuando especifique la opción con un mandato en la línea de mandatos. No puede establecer estas opciones en un archivo de opciones.
- Opciones en la modalidad interactiva  
En la modalidad interactiva, las opciones que especifique en la línea de mandatos inicial modificarán temporalmente el valor que ha especificado en el archivo de opciones.





## Parámetros

---

Los mandatos pueden tener parámetros obligatorios, parámetros optativos o pueden no tener parámetros.

Los obligatorios proporcionan la información necesaria para realizar una tarea. El que más se utiliza es la especificación de archivo.

Por ejemplo, si desea realizar el archivado de un archivo denominado `budget.fin` desde el directorio `project`, debe especificar lo siguiente:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X






```
dsmc archive /project/budget.fin
```

 Sistemas operativos Windows

```
dsmc archive c:\project\budget.fin
```


Algunos mandatos tienen parámetros optativos. Si no se entra el valor de un parámetro opcional, el cliente de copia de seguridad y archivado utiliza el valor predeterminado. Por ejemplo, el mandato `restore` tiene un parámetro obligatorio, `especificaciónarchivooorigen`, que indica la vía de acceso y el nombre de archivo del almacenamiento que desea restaurar. El parámetro opcional, `destinationfilespec`, especifica la vía de acceso donde desea colocar los archivos restaurados. Si no se especifica una `especificaciónarchivodestino`, el

cliente restaura los archivos en la vía de acceso de origen. Si desea restaurar los archivos en un directorio *distinto*, especifique un valor para especificación de archivo de destino.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 sistemas operativos Mac OS X

Ejemplo: restaurar el archivo `/project/budget.fin` en la nueva vía de acceso `/newproj/newbudg.fin`

```
dsmc restore /project/budget.fin /newproj/
```

 Sistemas operativos Windows

Ejemplo: restaurar el archivo `c:\project\budget.fin` en la nueva vía de acceso `c:\newproj\newbudg.fin`

```
dsmc restore c:\project\budget.fin c:\newproj\newbudg.fin
```





Los parámetros deben entrarse según el orden indicado en el diagrama de sintaxis del mandato.

## Sintaxis de especificación de archivo

A continuación se presentan diversas reglas de sintaxis que deberá conocer al especificar parámetros de especificación de archivo, como `filespec`, `sourcefilespec` y `destinationfilespec`.





A continuación se muestran las reglas de sintaxis:

- No utilice caracteres comodín como parte del nombre de espacio de archivos ni al indicar espacio de archivos de destino. La única excepción a esta regla es el mandato `set access`, donde se permiten caracteres comodín en los dos niveles más inferiores de la especificación de archivo.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

Ejemplo: Permitir el acceso a todos los archivos de todos los directorios dentro y subordinados en el directorio `/home`:

```
set access backup /home/* * *
set access backup /home/*/* * * *
```





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X Con los clientes UNIX, no utilice caracteres comodín para el nombre de la vía de acceso del directorio, por ejemplo:

```
/home/j*asler/file1.c
```

 Sistemas operativos Windows

Ejemplo: Permitir el acceso a todos los archivos de todos los directorios dentro y subordinados al directorio `d:\test`:




```
set access backup d:\test\* * *
set access backup d:\test\*\* * * *
```

- Existe un número máximo de especificaciones de archivo por mandato:
  - Los mandatos `Query` sólo admiten una especificación de archivo.
  - Los mandatos `restore` y `retrieve` pueden aceptar una especificación de archivo de origen y una especificación de archivo de destino.
  -  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Existe un límite de 20 operandos en algunos mandatos. Este límite es para evitar un número excesivo de sesiones causado cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín.

Puede impedir que la expansión del shell supere el límite de 20 operandos especificando entre comillas los caracteres de expansión de la especificación de archivo de origen para los mandatos `restore`.


Nota: El efecto secundario de la utilización de comillas es la generación de una restauración sin consulta.


Puede utilizar la opción `removeoperandlimit` para especificar que el cliente de copia de seguridad y archivado ha de eliminar el límite de 20 operandos. Si especifica la opción `removeoperandlimit` con los mandatos `incremental`, `selective` o `archive`, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.


- La longitud de una especificación de archivo está limitada.
  -  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En AIX, Solaris y Mac: el número máximo de caracteres en un nombre de archivo es 255. La longitud máxima combinada del nombre del archivo y







del nombre de la vía de acceso es de 1024 caracteres. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.


-  Sistemas operativos LinuxEn Linux: la longitud máxima de un nombre de archivo es 255 bytes. La longitud máxima combinada del nombre del archivo y del nombre de la vía de acceso es de 4096 bytes. Esta longitud coincide con el valor PATH\_MAX soportado por el sistema operativo. La representación Unicode de un carácter puede ocupar varios bytes, por lo tanto, el número máximo de caracteres de los que consta un nombre de vía de acceso y de archivo puede variar. La limitación real es el número de bytes de los componentes de vía de acceso y archivo, que podría corresponder a un número de caracteres igual.





 Sistemas operativos LinuxEn Linux: para las operaciones de archivado o recuperación, la longitud máxima que puede especificar para un nombre de vía de acceso y de archivo (combinado) sigue siendo de 1024 bytes.


-  Sistemas operativos WindowsEl número máximo de bytes para el conjunto formado por un nombre de archivo y una vía de acceso de archivo es 6255. Sin embargo, el nombre de archivo propiamente dicho no puede sobrepasar los 255 bytes. Asimismo, los nombres de los directorios (incluido el delimitador de directorio) de una vía de acceso tienen un límite de 255 bytes. La representación Unicode de un carácter puede ocupar varios bytes, de modo que el número máximo de caracteres que un nombre de archivo contiene puede variar.





Cuando se utiliza la función de soporte de archivos abiertos con VSS, el cliente de copia de seguridad y archivado agrega el nombre de volumen de instantánea a la vía de acceso de los objetos que se están procesando. La vía de acceso resultante (nombre de volumen de instantánea más vía de acceso de objeto) debe adherirse a los límites mostrados. El nombre del volumen de instantánea puede tener un máximo de 1024 bytes.

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Cuando especifique sourcefilespec, si el nombre del directorio acaba con /, entonces se presupone /\*.


 Sistemas operativos WindowsCuando especifique sourcefilespec, si el nombre del directorio acaba con \, entonces se presupone \\*.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Cuando se especifica una destinationfilespec, si el nombre finaliza con /, se considera que es un directorio; de otro modo, se considera que es un archivo.






 Sistemas operativos WindowsCuando se especifica una destinationfilespec, si el nombre finaliza con \, se considera que es un directorio; de otro modo, se considera que es un archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
En el ejemplo siguiente se muestran estas dos reglas: Aunque mydir y yourdir son directorios, el mandato no se ejecutará correctamente porque se presupone /\* a continuación de mydir, y se considera que yourdir es un archivo.





```
restore /home/mydir/ /away/yourdir
```


 Sistemas operativos WindowsEn el ejemplo siguiente se muestran estas dos reglas: Aunque mydir y yourdir son directorios, el mandato no se ejecutará correctamente porque se presupone \\* a continuación de mydir, y se considera que yourdir es un archivo.









```
restore c:\home\mydir\ c:\away\yourdir
```

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

Si una especificación de archivo no comienza con un delimitador de directorio, se presupone que la especificación de archivo es un subdirectorio del directorio de trabajo actual. El cliente añade la especificación de archivo al directorio de trabajo para crear la vía de acceso completa.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Por ejemplo, si el directorio de trabajo actual es /home/me y el mandato es `dsmc res "/fs/dir1/*" mydir`, la vía de acceso de restauración completa es la siguiente: /home/me/mydir


 Sistemas operativos WindowsPor ejemplo, si el directorio de trabajo actual es c:\home\me y el mandato es `dsmc res c:\fs\dir1\ mydir`, la vía de acceso de restauración completa es la siguiente: c:\home\me\mydir

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
El único mandato que acepta un nombre de espacio de archivos simple es el mandato incremental. El ejemplo siguiente es válido:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
dsmc i /Users
```

El ejemplo siguiente no es válido, ya que el mandato es el mandato selectivo:

```
dsmc sel /Users
```

-  Sistemas operativos Windows Cuando una especificación de archivo contiene espacios, debe especificarse entre comillas. Por ejemplo:

```
dsmc sel "x:\dir one\file1"
```

Cuando una especificación de archivo finaliza con una barra inclinada invertida y se cierra entre comillas, debe añadirse una barra inclinada invertida (\) adicional al final de la especificación del archivo. Si no se añade una barra inclinada invertida adicional, la especificación de archivo no se procesará correctamente y puede que la operación genere resultados no esperados.

El siguiente ejemplo no es correcto:


```
dsmc sel "x:\dir one\"
```

El siguiente ejemplo es correcto:

```
dsmc sel "x:\dir one\\"
```

A continuación, se muestra un ejemplo de restauración del contenido de un directorio en otro directorio cuando ambos nombres de directorio contienen espacios:

```
dsmc rest "x:\dir one\\" "x:\dir two\\"
```

-  Sistemas operativos Windows El acceso a los volúmenes Dfs de Microsoft se realiza mediante la utilización de nombres UNC estándar. A continuación, se indican ejemplos de sintaxis válida para acceder a volúmenes de DFS de Microsoft:

```

\\Nombre_servidor\Nombre_raíz_Dfs\ vía de acceso
\\Nombre_tolerancia_errores\Nombre_raíz_Dfs\ vía de acceso
    
```

## Caracteres comodín

Utilice los caracteres comodín cuando quiera especificar varios archivos con nombres similares en un mandato. Si no los utiliza, tendrá que repetir el mandato para cada archivo.

En un mandato, los caracteres comodín pueden utilizarse *sólo* en el nombre o la extensión del archivo. No puede utilizarlos para especificar archivos de destino, sistemas de archivos o nombres de servidor. No puede especificar un directorio cuyo nombre contenga un asterisco (\*) o un signo de interrogación (?).

Los caracteres comodín válidos que pueden utilizarse son los siguientes:

\*

Asterisco: representa cero o más caracteres.

?





Interrogante: representa cualquier único carácter que se encuentre en la posición del comodín.

La tabla siguiente muestra ejemplos de cada carácter comodín.

Tabla 1. Caracteres comodín

Patrón	Coincide con	No coincide con
<b>Asterisco (*)</b>		
ab*	ab, abb, abxxx	a, b, aa, bb
ab*rs	abrs, abtrs, abrsrs	ars, aabrs, abrss
ab*ef*rs	abefrs, abefghrs	abefr, abers
abcd.*	abcd.c, abcd.txt	abcd, abcdc, abcdtxt
<b>Signo de interrogación (?)</b>		
ab?	abc	ab, abab, abzzz
ab?rs	abrs	abrs, abllrs
ab?ef?rs	abdefjrs	abefrs, abdefrs, abefjrs
ab??rs	abcdrs, abzrs	abrs, abjrs, abkkrs

Importante: Utilice un asterisco (\*) en lugar de una interrogación (?) como carácter comodín cuando intente buscar la coincidencia de un patrón en una página de códigos de varios bytes con el fin de evitar que se produzcan resultados no esperados.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota: En la modalidad de proceso por lotes, especifique entre comillas los valores que contengan caracteres comodín. De lo contrario, los shells de UNIX expanden los caracteres comodín que no están entrecomillados y es fácil exceder el límite de 20 operandos. Es más eficiente dejar que el cliente procese las especificaciones de archivo comodín porque se necesitan menos interacciones de servidor para completar la tarea. Por ejemplo:

```
dsmc selective "/home/me/*.c"
```

## Consulta de mandatos de cliente

---

Las secciones que figuran a continuación contienen información detallada sobre cada uno de los mandatos del cliente de copia de seguridad y archivado.

La información sobre cada mandato incluye lo siguiente:

- Una descripción del mandato.
- Un diagrama de sintaxis del mandato.
- Descripciones detalladas de los parámetros del mandato. Si el parámetro es una constante (un valor que no cambia), la abreviatura mínima aparece en letras mayúsculas.
- Ejemplos de cómo utilizar el mandato.


## Archive

---

El mandato archive archiva un solo archivo, los archivos seleccionados o todos los archivos de un directorio y sus subdirectorios en un servidor.

Las copias archivadas que desee conservar en su condición actual. Para liberar espacio de almacenamiento de la estación de trabajo, suprima los archivos según los vaya archivando mediante la opción `deletfiles`. Recupere las copias archivadas en la estación de trabajo siempre que las necesite de nuevo.

Utilice la opción `snapshotroot` con el mandato archive junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, solo para gestionar los datos que ha creado una instantánea de volumen.

 Sistemas operativos AIX Sólo AIX: puede activar el archivado de archivos basado en instantáneas mediante la utilización de la opción `snapshotproviderfs=JFS2`.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```

      .----- .
      |         |
      v         |
>>-Archive----- --filespec-----+-----+-----><
                                   '- --options-'
```





## Parámetros

---


### filespec

Especifica la vía de acceso y el nombre del archivo que se desea archivar. Utilice caracteres comodín para incluir un grupo de archivos o todos los archivos de un directorio.





Para incluir varias especificaciones de archivos, separe cada parámetro de `filespec` con un carácter de espacio. Si se incluyen varias especificaciones de archivo, y dos o más de las especificaciones tienen directorios padre comunes, entonces es posible archivar los objetos de directorio comunes más de una vez. Las condiciones bajo las que este comportamiento ocurre son dependientes del tiempo de ejecución, pero el comportamiento por sí mismo no tiene efectos adversos.





 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Por ejemplo, si la especificación de archivo es `/home/amr/ice.doc /home/amr/fire.doc`, entonces se pueden archivar `/home` y





/home/amr dos veces. Los objetos de archivo ice.doc y fire.doc se archivan solo una vez.

 Sistemas operativos Windows Por ejemplo si la especificación de archivo es C:\proposals\drafts\ice.doc C:\proposals\drafts\fire.doc, entonces se puede archivar C:\proposals y C:\proposals\drafts dos veces. Los objetos de archivo ice.doc y fire.doc se archivan solo una vez.


Si desea evitar incluir el directorio padre compartido más de una vez, utilice separar, no superponer mandatos archive para archivar cada especificación de archivo.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Si archiva un sistema de archivos, incluya una barra inclinada final (/home/).

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Existe un límite de 20 operandos. Este límite previene un número excesivo de sesiones cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín. Puede impedir que la expansión del shell supere el límite de 20 operandos colocando entre comillas las especificaciones de archivo que contienen caracteres comodín ("home/docs/\*").

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Puede utilizar la opción removeoperandlimit para especificar que se elimina el límite de 20 operandos. Si especifica la opción removeoperandlimit, el límite de 20 operandos no se aplica y queda restringido únicamente a los recursos disponibles u otros límites del sistema operativo. Por ejemplo, elimine el límite de 20 operandos para archivar 21 especificaciones de archivo:











































```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

 Sistemas operativos Windows Si archiva un sistema de archivos, incluya una barra inclinada final (C:\).

 Sistemas operativos Windows Puede especificar tantas especificaciones de archivo como lo permitan los recursos disponibles u otros límites del sistema operativo.









Puede utilizar la opción filelist, en lugar de las especificaciones de archivo, para identificar qué archivos se han de incluir en esta operación. Sin embargo, estos dos métodos se excluyen mutuamente. No puede incluir parámetros de especificación de archivo y utilizar la opción filelist. Si se especifica la opción filelist, cualquiera de las especificaciones de archivo que se incluyen se ignoran.

Tabla 1. mandato Archive: opciones relacionadas


Opción	Dónde se utiliza
archmc	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X archsymlinkasfile	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 sistemas operativos Mac OS X  Sistemas operativos Windows autofsrename	 sistemas operativos Mac OS X  Sistemas operativos Windows Sólo archivo de opciones del cliente (dsm.opt).
 Sistemas operativos Windows changingretries	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X changingretries	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema cliente o línea de mandatos.
 Sistemas operativos Windows compressalways	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compressalways	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows compression	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compression	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo dsm.sys de una stanza del servidor o línea de mandatos.


Opción	Dónde se utiliza
deletefiles	Sólo línea de mandatos.
description	Sólo línea de mandatos.
dirsonly	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X encryptiontype	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo dsm.sys dentro de una stanza de servidor.
 Sistemas operativos Windows encryptiontype	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt).
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X encryptiontype	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo dsm.sys dentro de una stanza de servidor.
 Sistemas operativos Windows encryptiontype	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt).
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
 Sistemas operativos Windows postsnapshotcmd	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X presavelastaccessdate	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows presavelastaccessdate	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows presnapshotcmd	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X removeoperandlimit	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Sólo línea de mandatos.
 Sistemas operativos Windows skipntpermissions	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows skipntsecuritycrc	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux snapshotcachesize	 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
snapshotroot	Sólo línea de mandatos.
subdir	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
v2archive	Sólo línea de mandatos.

## Ejemplos









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar el archivado de un único archivo denominado `budget` en el directorio `/home/proj1`.

**Mandato:** `archive /home/proj1/budget`


 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Realizar el archivado de un único archivo denominado `budget.jan` en el directorio `c:\plan\proj1`.

**Mandato:** `archive c:\plan\proj1\budget.jan`









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar el archivado de todos los archivos en el directorio `/home/proj1` que tienen la extensión de archivo `.txt`.

**Mandato:** `archive "/home/proj1/*.txt"`


 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Realizar el archivado de todos los archivos en el directorio `c:\plan\proj1` que tienen la extensión de archivo `.txt`.

**Mandato:** `archive c:\plan\proj1\*.txt`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar el archivado de todos los archivos en el árbol de directorios que encabeza el directorio `/home`.


**Mandato:** `archive -subdir=yes "/home/*"`

 Sistemas operativos Windows Tarea









 Sistemas operativos Windows Archivado de todos los archivos en la unidad `c:\`.

**Mandato:** `archive -subdir=yes c:\*.*`

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Realizar el archivado de todos los archivos en el volumen Dfs de Microsoft, `MyDfsVolume`. Debe especificar **subdir=yes** para realizar el archivado de *todos* los archivos en el volumen.

**Mandato:** `archive \\myserver\mydfsroot\mydfsvolume\*.* -subdir=yes`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar el archivado, dándose por supuesto que ha iniciado una instantánea del sistema de archivos `/usr` y que ha montado la instantánea como `/snapshot/day1`, del árbol de directorios `/usr/dir1/sub1` desde la instantánea local y gestionar éste en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos `/usr`.

**Mandato:** `dsmc archive /usr/dir1/sub1/ -subdir=yes -snapshotroot=/snapshot/day1`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Suponiendo que ha iniciado una instantánea de la unidad `C:\` y que ha montado la instantánea como `\\florence\c$\snapshots\snapshot.0`, archive el árbol de directorio `c:\dir1\sub1` de la instantánea local y gestiónelo en el servidor de IBM Spectrum Protect en el nombre de espacio de archivos `C:`.

**Mandato:** `dsmc archive c:\dir1\sub1\* -subdir=yes -snapshotroot=\\florence\c$\snapshots\snapshot.0`


-  Sistemas operativos Windows Soporte de archivos abiertos  
Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).


 Sistemas operativos Linux  Sistemas operativos Windows

## Archivado de FastBack

Utilice el mandato `archive fastback` para archivar volúmenes de Tivoli Storage Manager FastBack especificados por las opciones `fbpolicynname`, `fbclientname` y `fbvolumename` para una retención a largo plazo.

Antes de utilizar este mandato, configure el cliente para realizar copias de seguridad y archivar datos de Tivoli Storage Manager FastBack. Asimismo, antes de emitir este mandato, debe existir al menos una instantánea en el repositorio de FastBack para la política de FastBack que se archiva o de la que se realiza copia de seguridad.


 Sistemas operativos Windows Si una especificación de políticas contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes de Windows, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Windows.


 Sistemas operativos Linux Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.

Puede utilizar las opciones de Tivoli Storage Manager FastBack para archivar las últimas instantáneas de los volúmenes siguientes:

- Todos los clientes y volúmenes asociados a una política específica de FastBack o una lista de políticas de FastBack.
- Todos los volúmenes asociados a un cliente específico de FastBack o una lista de clientes de FastBack para una determinada política de FastBack.
- Un volumen o varios volúmenes específicos asociados a un cliente específico de FastBack para una política de FastBack determinada.

## Clientes soportados

 Sistemas operativos Linux Esta opción es válida para clientes de Linux x86\_64.

 Sistemas operativos Windows Esta opción es válida para todos los clientes de Windows configurados como proxies dedicados de FastBack. Este mandato también es válido para los clientes de Windows instalados en la estación de trabajo del servidor de FastBack o FastBack Disaster Recovery Hub.

## Sintaxis

```

>>--ARCHIVE FASTBack--FBPolicyname-----nombre+----->
                                     .-,----- .
                                     v          |
>>--FBServer-----nombre+----->
                                     |          .-,----- . |
                                     |          v          | |
                                     |'-FBClientname-----nombre+--'|
>+-----+-----+-----+----->
|          .-,----- . |
|          v          | |
|'-FBVolumename-----nombre+--'|
>+-----+-----+-----+----->
|'-FBReposlocation-----nombre-' |'-FBBranch-----nombre-'
>+-----+-----+-----+-----<
|'-ARCHMc-----nombre-'

```

Importante:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Puede especificar hasta 10 valores para FBClientName si solo se ha especificado un PolicyName y no se ha especificado ningún valor para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar siempre la opción FBReposLocation para Linux.


## Parámetros


Tabla 1. mandato Archive Fastback: opciones relacionadas

Opción	Dónde se utiliza
fbpolicyname	Línea de mandatos y planificador.
fbserver	Línea de mandatos y planificador.
fbclientname	Línea de mandatos y planificador.
fbvolumename	Línea de mandatos y planificador.
fbreposlocation	Línea de mandatos y planificador.

Opción	Dónde se utiliza
fbbranch	Línea de mandatos y planificador.
archmc	Línea de mandatos y planificador.

## Ejemplos

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux El cliente de archivado y copia de seguridad está instalado en una máquina de cliente proxy de Linux. Utilice este mandato para archivar todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para policy1 de FastBack:


```
dsmc archive fastback -fbpolicyname=Policy1
-fbserver=myfbserver -fbreposlocation=myfbserver@WORKGROUP
```

El nombre del servidor de FastBack, -myFbDrHub es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio.

El parámetro -fbreposlocation especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se produce un error en el mandato.

En este caso, FBServer debería apuntar al nombre de host abreviado del FastBack DR Hub.

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux El repositorio, rep\_server1, se encuentra en el FastBack DR Hub, myFbDrHub.


```
dsmc archive fastback -fbpolicyname="Policy 1"
-fbserver=myFbDrHub -fbreposlocation=\myFbDrHub\rep_server1
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se produce un error en el mandato.

El nombre de servidor de FastBack, -myFbDrHub, es el nombre de host abreviado del FastBack Disaster Recovery Hub donde se encuentra el repositorio.


En este caso, FBServer debería apuntar al nombre de host abreviado del FastBack DR Hub.

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux Archivar todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:

```
dsmc archive fastback -Fbpolicyname=policy1
-FBServer=basil -ARCHMC="my_tsm_mgmt_class"
-fbreposlocation=basil@WORKGROUP
```

 Sistemas operativos Windows Línea de mandatos:


 Sistemas operativos Windows El cliente de archivado y copia de seguridad está instalado en el servidor de FastBack. Utilice este mandato para archivar todos los volúmenes de FastBack para todos los clientes FastBack de Windows definidos para policy1 de FastBack:

```
dsmc archive fastback -fbpolicyname=Policy1
-fbserver=myfbserver
```

La ubicación del repositorio no es necesaria. Si proporciona la ubicación del repositorio, se ignora.

El nombre de servidor de FastBack, -myfbserver, es el nombre de host abreviado del servidor de FastBack donde se ejecuta el cliente.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad está instalado en el FastBack Disaster Recovery Hub. Utilice este mandato para archivar todos los volúmenes de FastBack de todos los clientes de FastBack que se encuentren en la política denominada Policy 1:


```
dsmc archive fastback -fbpolicyname="Policy 1"
-fbserver=myFbServer -fbbranch=branch1
```

La ubicación del repositorio no es necesaria. Si proporciona la ubicación del repositorio, se ignora.

El parámetro myFbServer especifica el nombre de host abreviado del servidor de FastBack cuya rama FastBack se haya especificado utilizando la opción FBBranch

 Sistemas operativos Windows Línea de mandatos:




 Sistemas operativos Windows El cliente de archivado y copia de seguridad está instalado en una máquina de proxy dedicada con la línea de mandatos administrativa de Tivoli Storage Manager FastBack y el montaje de FastBack. El cliente se está conectando al repositorio de servidor de FastBack. Utilice este mandato para archivar todos los volúmenes de FastBack de todos los clientes de FastBack que se encuentren en la política denominada Policy 1:

```
dsmc archive fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\myFbServer.company.com\REP
```

La ubicación del repositorio es necesaria.

El nombre de host abreviado de la máquina donde está instalado el servidor de FastBack es myFbServer.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows El cliente de archivado y copia de seguridad está instalado en una máquina de proxy dedicada con la línea de mandatos administrativa de Tivoli Storage Manager FastBack y el montaje de FastBack. El cliente se conecta a un repositorio de ramificaciones remotas en el FastBack Disaster Recovery Hub. Utilice este mandato para archivar todos los volúmenes de FastBack de todos los clientes de FastBack que se encuentren en la política denominada Policy 1:


```
dsmc archive fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\myfbdrhub.company.com\REP  
-fbbranch=aFbServerBranch
```

La ubicación del repositorio es necesaria.

El valor de myFbServer especificado con la opción -fbserver es el nombre de host abreviado del servidor de FastBack cuya ramificación de FastBack se especifica utilizando la opción FBBranch.

La opción fbbranch especifica el ID de la ramificación del servidor FastBack en el concentrador de recuperación tras desastre.

 Sistemas operativos Windows Línea de mandatos:

 Sistemas operativos Windows Archivar todos los volúmenes protegidos por la política de FastBack denominada policy1 desde el servidor de FastBack denominado basil, y aplicar la clase de gestión "my\_tsm\_mgmt\_class" a los volúmenes archivados.

```
dsmc archive fastback -Fbpolicyname=policy1  
-FbServer=basil -ARCHMC="my_tsm_mgmt_class"
```

#### Conceptos relacionados:

Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack

#### Tareas relacionadas:

Configuración de clientes de copia de seguridad/archivado


 Sistemas operativos Linux  Sistemas operativos Windows


## Copia de seguridad de FastBack

---

Utilice el mandato backup fastback para realizar copia de seguridad de los volúmenes de Tivoli Storage Manager FastBack especificados por las opciones fbpolicyname, fbclientname y fbvolumename para una retención a largo plazo.

Antes de utilizar este mandato, configure el cliente para realizar copias de seguridad y archivar datos de Tivoli Storage Manager FastBack. Asimismo, antes de emitir este mandato, debe existir al menos una instantánea en el repositorio de Tivoli Storage Manager FastBack para la política de Tivoli Storage Manager FastBack que se archiva o de la que se realiza copia de seguridad.

 Sistemas operativos Windows Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará copia de seguridad o se archivarán los volúmenes de Windows en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Windows.


 Sistemas operativos Linux Si una especificación de política contiene clientes FastBack de Windows y Linux, solo se hará una copia de seguridad de los volúmenes Linux, o bien se archivarán, en el servidor de IBM Spectrum Protect mediante el cliente de copia de seguridad y archivado de Linux.


Las opciones de Tivoli Storage Manager FastBack están soportadas para la copia de seguridad incremental de las últimas instantáneas, dependiendo de la opción especificada:

- Todos los clientes y volúmenes asociados a la política de FastBack o una lista de políticas de FastBack.
- Todos los volúmenes asociados a un cliente específico de FastBack o una lista de clientes de FastBack para una determinada política de FastBack.
- Un volumen o varios volúmenes específicos asociados a un cliente específico de FastBack para una política de FastBack determinada.

## Clientes soportados

---

 Sistemas operativos Linux Este mandato es válido para clientes Linux x86\_64 configurados como proxies dedicados de Tivoli Storage Manager FastBack.

 Sistemas operativos Windows Este mandato es válido para todos los clientes de Windows que estén configurados como proxies dedicados de Tivoli Storage Manager FastBack. Este mandato también es válido para los clientes de Windows instalados en la estación de trabajo del servidor de Tivoli Storage Manager FastBack o Tivoli Storage Manager FastBack Disaster Recovery Hub.

 Sistemas operativos Linux

## Sintaxis

---


```

                                     .-,-----.
                                     v          |
>>-BACKUP FASTBack--FBPolicyname-----nombre+----->
>--FBServer-----nombre+----->
|                                     .-,-----. |
|                                     v          | |
|                                     '-FBClientname-----nombre+--'
>+-----+----->
|                                     .-,-----. |
|                                     v          | |
|                                     '-FBVolumename-----nombre+--'
>--FBReposlocation-----nombre+----->
|                                     '-FBBranch-----nombre-'
>+-----+-----<
|                                     '-BACKMc-----nombre-'

```

### Importante:

1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.
7. Debe especificar la opción FBReposLocation.

 Sistemas operativos Windows

## Sintaxis

---

```

                                     .-,-----.
                                     v          |
>>-BACKUP FASTBack--FBPolicyname-----nombre+----->
>--FBServer-----nombre+----->
|                                     .-,-----. |
|                                     v          | |
|                                     '-FBClientname-----nombre+--'
>+-----+----->
|                                     .-,-----. |
|                                     v          | |
|                                     '-FBVolumename-----nombre+--'
>+-----+-----+----->
|                                     '-FBReposlocation-----nombre-'   '-FBBranch-----nombre-'
>+-----+-----<
|                                     '-BACKMc-----nombre-'

```


### Importante:


1. Como mínimo es necesario siempre un FBpolicyName.
2. Podrá especificar hasta 10 valores para FBPolicyName, si no se ha especificado ningún valor ni para FBClientName ni para FBVolumeName.
3. Si se especifica un valor de FBClientName, debe haber solo un valor para FBPolicyName.
4. Podrá especificar hasta 10 valores para FBClientName si se ha especificado solo un valor para PolicyName y ninguno para FBVolumeName.
5. Cuando se especifica la opción FBVolumeName, se puede tener solo un FBPolicy y un FBClientName especificados.
6. Podrá especificar varios FBVolumeNames si se cumple la condición 5.

Tabla 1. mandato Backup FastBack: opciones relacionadas

Opción	Dónde se utiliza
fbpolicyname	Línea de mandatos y planificador.
fbserver	Línea de mandatos y planificador.
fbclientname	Línea de mandatos y planificador.
fbvolumename	Línea de mandatos y planificador.
fbrepositlocation	Línea de mandatos y planificador.
fbbranch	Línea de mandatos y planificador.
backmc	Línea de mandatos y planificador.

## Ejemplos


 Sistemas operativos Linux Línea de mandatos:


 Sistemas operativos Linux El cliente de archivado y copia de seguridad está instalado en una máquina de cliente proxy de Linux. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de FastBack para todos los clientes FastBack de Linux definidos para policy1 de FastBack:

```
dsmc backup fastback -fbpolicyname=Policy1
-fbserver=myfbserver
-fbrepositlocation=myfbserver@WORKGROUP
```

La ubicación del repositorio es necesaria. Si no proporciona la ubicación del repositorio, se producirá un error en el mandato.

El nombre de servidor de FastBack, -myfbserver, es el nombre de host abreviado del servidor de FastBack donde se encuentra el repositorio.

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux El repositorio, rep\_server1, se encuentra en el FastBack Disaster Recovery Hub, myFbDrHub


```
dsmc backup fastback -fbpolicyname="Policy 1"
-fbserver=myFbDrHub -fbrepositlocation=\myFbDrHub\rep_server1
```

El nombre de servidor de FastBack, -myFbDrHub, es el nombre de host abreviado del servidor de FastBack Disaster Recovery Hub donde se encuentra el repositorio.

La opción -fbrepositlocation especifica la ubicación del repositorio. La ubicación del repositorio es necesaria. Si no se proporciona la ubicación de repositorio, el mandato falla.


La opción FBServer debe señalar al nombre de host abreviado del FastBack DR Hub en este caso.

 Sistemas operativos Linux Línea de mandatos:

 Sistemas operativos Linux Realizar una copia de seguridad de todos los volúmenes protegidos por la política de FastBack denominada policy1 del servidor de FastBack denominado basil:

```
dsmc backup fastback -Fbpolicyname=policy1
-FBServer=basil -BACKMC="my_tsm_mgmt_class"
-fbrepositlocation=basil@WORKGROUP
```

 Sistemas operativos Windows Línea de mandatos:


 Sistemas operativos Windows El cliente de archivado y copia de seguridad está instalado en el servidor de FastBack. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de Tivoli Storage Manager FastBack para todos los clientes FastBack de Windows definidos para policy1 de Tivoli Storage Manager FastBack:

```
dsmc backup fastback -fbpolicyname=Policy1
-fbserver=myfbserver
```

La ubicación del repositorio no es necesaria. Si proporciona la ubicación del repositorio, se ignora.

El nombre de servidor de FastBack, -myfbserver, es el nombre de host abreviado del servidor de FastBack donde se ejecuta el cliente.


 Sistemas operativos WindowsLínea de mandatos:


 Sistemas operativos WindowsEl cliente de archivado y copia de seguridad está instalado en el concentrador de recuperación tras desastre de FastBack. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de FastBack para todos los clientes de FastBack que se encuentran en la política denominada Policy 1:

```
dsmc backup fastback -fbpolicyname="Policy 1"  
-fbserver=myFbServer -fbbranch=branch1
```

La ubicación del repositorio no es necesaria. Si proporciona la ubicación del repositorio, se ignora.

El nombre de servidor de FastBack, myFbServer, es el nombre de host abreviado del servidor de FastBack cuya ramificación de FastBack se especifica mediante la opción FBBranch


 Sistemas operativos WindowsLínea de mandatos:


 Sistemas operativos WindowsEl cliente de archivado y copia de seguridad está instalado en una máquina de proxy dedicada con la línea de mandatos administrativa de FastBack y el montaje de FastBack. El cliente se está conectando al repositorio de servidor de FastBack. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de FastBack para todos los clientes de FastBack que se encuentran en la política denominada Policy 1:

```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\myFbServer.company.com\REP
```

La ubicación del repositorio es necesaria.

El nombre de host abreviado de la máquina donde está instalado el servidor de FastBack es myFbServer.

 Sistemas operativos WindowsLínea de mandatos:

 Sistemas operativos WindowsEl cliente de archivado y copia de seguridad está instalado en una máquina de proxy dedicada con la línea de mandatos administrativa de FastBack y el montaje de FastBack. El cliente se conecta a un repositorio de ramificaciones remotas en el FastBack Disaster Recovery Hub. Utilice este mandato para realizar una copia de seguridad de todos los volúmenes de FastBack para todos los clientes de FastBack que se encuentran en la política denominada Policy 1:


```
dsmc backup fastback -fbpolicyname="Policy 1" -fbserver=myFbServer  
-fbreposlocation=\myfbdrhub.company.com\REP  
-fbbranch=aFbServerBranch
```

La ubicación del repositorio es necesaria.

El valor de myFbServer especificado con la opción -fbserver es el nombre de host abreviado del servidor de FastBack cuya ramificación de FastBack se especifica utilizando la opción FBBranch.

La opción fbbranch especifica el ID de la ramificación del servidor FastBack en el concentrador de recuperación tras desastre.

 Sistemas operativos WindowsLínea de mandatos:

 Sistemas operativos WindowsRealizar una copia de seguridad de todos los volúmenes protegidos por la política FastBack denominada policy1 desde el servidor de FastBack denominado basil, y aplicar la clase de gestión "my\_tsm\_mgmt\_class" a los volúmenes con copia de seguridad:

```
dsmc backup fastback -Fbpolicyname=policy1  
-FBServer=basil -BACKMC="my_tsm_mgmt_class"
```

#### **Conceptos relacionados:**

Configuración del cliente para realizar una copia de seguridad y archivado de los datos de Tivoli Storage Manager FastBack


#### **Tareas relacionadas:**

Configuración de clientes de copia de seguridad/archivado

## Backup Group

---

Utilice el mandato backup group para crear y realizar la copia de seguridad de un grupo que contenga una lista de archivos de uno o más orígenes de espacio de archivos en un espacio de archivos virtual en el servidor de IBM Spectrum Protect.

 Sistemas operativos AIXSólo AIX: puede activar la copia de seguridad de grupo basada en instantáneas mediante la utilización de la opción snapshotproviderfs=JFS2.

Una copia de seguridad de grupo permite crear una copia de seguridad de punto en el tiempo coherente de un grupo de archivos que se gestiona como una entidad lógica individual. Los objetos del grupo están sujetos a las siguientes reglas:

- Operación de volver a vincular con clase de gestión para objetos agrupados:
  - Durante las copias de seguridad completa, todos los objetos de un grupo de copia de seguridad están asignados a la misma clase de gestión.
  - Durante las copias de seguridad diferenciales, si se especifica una nueva la clase de gestión en una sentencia include para un grupo de copia de seguridad existente, el comportamiento será el siguiente:
    - Los objetos nuevos y modificados del grupo de copia de seguridad están vinculados a la nueva clase de gestión.
    - Los objetos de miembro del grupo que no se modifican aparecen como si no se hubiesen vinculado a la nueva clase de gestión. Estos objetos sin modificar no se incluyen en las estadísticas Número total de objetos revinculados que se muestran cuando finaliza el mandato Backup Group.
    - Los objetos que no se han modificado se vuelven a asignar a un backup group creado recientemente y el nuevo backup group se vincula a la nueva clase de gestión. Sin embargo, el nombre de clase de gestión original todavía se muestra para los objetos de grupo que no se han modificado.

Aunque el nombre de la clase de gestión original continúe apareciendo para los objetos sin modificar, están vinculados con la nueva clase de gestión del grupo de copias de seguridad.

- Las sentencias exclude existentes que se aplican a cualquier archivo del grupo se pasan por alto.
- Todos los objetos del grupo se exportan juntos.
- Todos los objetos del grupo caducan al mismo tiempo, tal como se ha especificado en la clase de gestión. Ninguno de los objetos de un grupo caduca hasta que caducan los demás objetos del grupo, incluso cuando caduque otro grupo al que pertenecen.
- Si realiza copias de seguridad de grupo completas o diferenciales en un dispositivo secuencial, durante una restauración, los datos no se encontrarán en más de dos ubicaciones. Para optimizar el tiempo de restauración, realice copias de seguridad completas periódicamente para realizar la copia de seguridad de los datos en una única ubicación en los medios secuenciales.
- Durante una copia de seguridad de grupo completa, todos los datos de la lista de archivos se envían al servidor. Durante una copia de seguridad de grupo diferencial, sólo se envían al servidor los datos que han cambiado desde la última copia de seguridad completa. Los objetos de la lista de archivos que no han cambiado desde las últimas copias de seguridad completas se asignan como miembros de la copia de seguridad de grupo diferencial. Estos datos no vuelven a enviarse al servidor, con lo que se reduce el tiempo de la copia de seguridad.

El mandato backup group necesita las opciones siguientes:

filelist

Especifica una lista de archivos que ha de agregarse a un nuevo grupo.

groupname

Especifica el nombre calificado al completo del grupo que contiene una lista de archivos.

virtualfsname





Especifica el nombre del espacio de archivos virtual del grupo en el que desea realizar la operación. La opción virtualfsname no puede ser igual a un nombre de espacio de archivos existente.

mode

Especifica si desea realizar la copia de seguridad de todos los archivos de la lista de archivos o sólo de los archivos que han cambiado desde la última copia de seguridad completa.




Nota:

1. Si falla alguno de los archivos de la copia de seguridad del grupo, fallará toda la copia de seguridad del grupo.
2. Utilice el mandato query group para consultar los miembros de una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.
3. Utilice el mandato restore group para restaurar miembros específicos o todos los miembros de una copia de seguridad de grupo en el servidor.
4. A menos que esté ejecutando Mac OS X, utilice el mandato delete group para suprimir una copia de seguridad de grupo específica del servidor.
5. Utilice el mandato query filespace para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor.
6. Una copia de seguridad de grupo puede agregarse a un juego de copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

---







 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Este mandato es válido para todos los clientes UNIX y Linux, a excepción de Mac OS X.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.









```
>>-Backup GRoup-- --options-----<<
```

## Parámetros

Tabla 1. Mandato backup group: opciones relacionadas

Opción	Dónde se utiliza
filelist	Sólo línea de mandatos.
groupname	Sólo línea de mandatos.
mode	Sólo línea de mandatos.
 Sistemas operativos AIX snapshotproviderfs	 Sistemas operativos AIX Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.
 Sistemas operativos Windows snapshotproviderfs	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos Windows snapshotproviderimage	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.image.
virtualfsname	Sólo línea de mandatos.


## Ejemplos

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 Realizar una copia de seguridad completa de todos los archivos del archivo /home/dir1/filelist1 en el nombre de espacio de archivos virtual accounting que contiene el archivo /home/group1 de líder de grupo.

**Mandato:**

```
backup group -filelist=/home/dir1/filelist1 -groupname=group1  
-virtualfsname=/virtfs -mode=full
```

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar una copia de seguridad completa de todos los archivos del archivo c:\dir1\filelist1 en el nombre de espacio de archivos virtual \virtfs que contiene el archivo group1 de líder de grupo.

**Mandato:**


```
backup group -filelist=c:\dir1\filelist1 -groupname=group1  
-virtualfsname=\virtfs -mode=full
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Backup Image


El mandato backup image crea una copia de seguridad de imagen de uno o varios volúmenes del sistema.

Puede utilizar el mandato backup image para hacer una copia de seguridad de volúmenes NTFS o ReFS, o bien RAW no formateados. Si un volumen tiene formato NTFS, sólo se realizará copia de seguridad de los bloques que utiliza el sistema de archivos. En volúmenes de ReFS, se realizará copia de seguridad de todos los bloques.

 Sistemas operativos AIX Si establece la opción imagegapsize en 0, se realizará copia de seguridad de todos los bloques, incluidos los bloques que no se utilizan situados al final del volumen.

 Sistemas operativos AIX Si especifica un sistema de archivos JFS2 de AIX para la copia de seguridad de imágenes, solo se realizará la copia de seguridad de los bloques que el sistema de archivos utiliza. Si establece la opción imagegapsize en cero, se realizará copia de seguridad de todos los bloques, incluidos los bloques no situados al final del volumen.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Nota:




-  Sistemas operativos AIX Sólo AIX: de forma predeterminada, la copia de seguridad de imágenes basada en instantáneas está activada para los volúmenes JFS2. Para desactivar las copias de seguridad de imágenes basadas en instantáneas, establezca - snapshotproviderimage=NONE en este mandato.




filespec

Especifica el nombre de uno o varios volúmenes lógicos. Si desea hacer una copia de seguridad de más de un sistema de archivos, separe los nombres con espacios. No utilice caracteres de coincidencia con patrón. Si no especifica un nombre de volumen, se procesarán los volúmenes lógicos que se especifican con la opción domain.image. Si no utiliza la opción domain.image para especificar los sistemas de archivos que se procesarán, aparece un mensaje de error y no se lleva a cabo ninguna copia de seguridad de imágenes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Especifique el espacio de archivos sobre el que se monta el volumen lógico, o el nombre del volumen lógico. Si existe un sistema de archivos configurado en el sistema para un volumen determinado, no puede realizar la copia de seguridad del volumen con el nombre de dispositivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Por ejemplo, si el espacio de archivos /dev/lv01 está montado en el volumen /home, puede emitir backup image /home, pero backup image /dev/lv01 falla con un error:

ANS1063E Se ha especificado una vía de acceso no válida

 Sistemas operativos Oracle Solaris Nota: En sistemas Sun, especifique un nombre de sistema de archivos o un nombre de dispositivos RAW (tipo de dispositivo de bloque).











































 Sistemas operativos Windows La copia de seguridad de imagen sólo se admite en un volumen que tiene asignada una letra de montaje o de unidad a él. No puede realizarse la copia de seguridad de un volumen que no tenga una letra de unidad o un punto de montaje.




Tabla 1. Mandato Backup Image: opciones relacionadas

Opción	Dónde se utiliza
 Sistemas operativos Windows asnodename	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris asnodename	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del sistema del cliente (dsm.sys) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris compressalways	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del sistema del cliente (dsm.sys) o línea de mandatos.
 Sistemas operativos Windows compressalways	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
compression	En el archivo de opciones del cliente o en la línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris dynamicimage	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice esta opción con el mandato backup image o la opción include.image del archivo de opciones.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows imagegapsize	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Utilice esta opción con el mandato backup image, la opción include.image o en el archivo de opciones.
mode	Sólo línea de mandatos.
postsnapshotcmd	Utilice esta opción con el mandato backup image, la opción include.image o en el archivo de opciones.
presnapshotcmd	Utilice esta opción con el mandato backup image, la opción include.image o en el archivo de opciones.
 Sistemas operativos AIX  Sistemas operativos Linux snapshotcachesize	 Sistemas operativos AIX  Sistemas operativos Linux Utilice esta opción con el mandato backup image, la opción include.image o en el archivo de opciones.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows snapshotproviderimage	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Archivo de opciones del cliente o con la opción include.image.





## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Realizar una copia de seguridad del espacio de archivos /home/prueba sobre el que está montado el volumen lógico y realizar una copia de seguridad de imágenes incremental que solamente efectúe una copia de seguridad de los archivos nuevos y de los archivos que se han modificado desde la copia de seguridad de imágenes completa más reciente.


```
dsmc backup image /home/test -mode=incremental
```

 Sistemas operativos Windows

 Sistemas operativos Windows Realizar una copia de seguridad de un volumen que no tiene letra de unidad pero que está montando como punto de montaje.



```
dsmc backup image m:\mnt\myntfs
```

 Sistemas operativos Windows


 Sistemas operativos Windows Realice una copia de seguridad de la unidad h utilizando una copia de seguridad de imágenes incremental. Una copia de seguridad de imagen incremental realiza una copia de seguridad de los archivos nuevos o modificados desde la última copia de seguridad de imagen completa.


```
dsmc backup image h: -mode=incremental
```

 Sistemas operativos AIX  Sistemas operativos Linux




 Sistemas operativos AIX  Sistemas operativos Linux Realizar una copia de seguridad de imagen estática del volumen lógico que se ha montado en el directorio /home.




```
dsmc backup image /home -snapshotproviderimage=none
```

 Sistemas operativos Windows

 Sistemas operativos Windows Realice una copia de seguridad de imagen desactivada de la unidad f.



```
dsmc backup image f: -snapshotproviderimage=none
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Realizar una copia de seguridad de imagen dinámica del volumen lógico que se ha montado en el directorio /home.

**Mandato:** `dsmc backup image /home -dynamicimage=yes`

 Sistemas operativos AIX  Sistemas operativos Linux

 Sistemas operativos AIX  Sistemas operativos Linux Realizar una copia de seguridad de instantánea del directorio /home.


```
 Sistemas operativos AIX AIX client: dsmc backup image /home  
-snapshotproviderimage=JFS2
```




```
 Sistemas operativos Linux Cliente LINUX: dsmc backup image /home  
-snapshotproviderimage=LINUX_LVM
```

 Sistemas operativos Windows

 Sistemas operativos Windows Realice una copia de seguridad de imagen activada de la unidad f.


```
dsmc backup image f: -snapshotproviderimage=VSS
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Realizar la copia de seguridad del volumen lógico RAW /dev/lv01.

```
dsmc backup image /dev/lv01
```

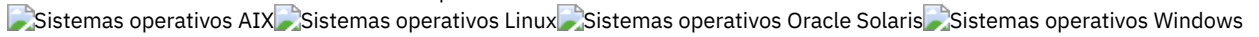



 Sistemas operativos Windows

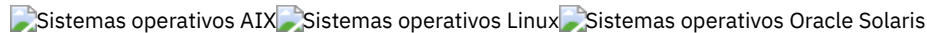


 Sistemas operativos Windows Realice una copia de seguridad de la unidad f, que se correlaciona con un volumen que no se ha formateado con un sistema de archivos.

```
dsmc backup image f:
```

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Copia de seguridad de imagen estática, dinámica y de instantánea  
La copia de seguridad de imagen tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen.
-  Sistemas operativos Windows Copia de seguridad de imagen desactivada y activada  
La copia de seguridad de imagen desactivada tradicional no permite que otras aplicaciones del sistema tengan acceso de

escritura al volumen mientras se realiza la operación.


-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows  
Utilización de la copia de seguridad de imagen para realizar una copia de seguridad incremental del sistema de archivos  
Existen dos métodos de utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos. Estos métodos de copia de seguridad permiten realizar restauraciones a un instante específico de los sistemas de archivos y mejorar el rendimiento de las operaciones de copia de seguridad y restauración.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris


## Copia de seguridad de imagen estática, dinámica y de instantánea


La copia de seguridad de imagen tradicional impide que durante la operación otras aplicaciones del sistema accedan con permiso de escritura al volumen.

Utilice la opción `dynamicimage` para realizar una copia de seguridad del volumen tal cual sin volver a montarlo como de sólo lectura. La copia de seguridad se puede dañar si las aplicaciones escriben datos en el volumen mientras se está realizando la copia de seguridad. En este caso, ejecute `fsck` después de una restauración.

 Sistemas operativos AIX La opción `dynamicimage` no se admite para volúmenes JFS2.

 Sistemas operativos Linux Solo para clientes Linux `x86_64`: de forma predeterminada, el cliente de archivado y copia de seguridad ejecuta una copia de seguridad de imágenes de instantánea de sistemas de archivos que residen en un volumen lógico creado por el Gestor de volúmenes lógicos de Linux, durante la cual el volumen está disponible para otras aplicaciones de sistemas. La copia de seguridad de imagen de instantánea necesita la versión 5.1 de un servidor de IBM Spectrum Protect.

 Sistemas operativos AIX Solo para clientes AIX: de forma predeterminada, el cliente de archivado y copia de seguridad ejecuta una copia de seguridad de imágenes de instantánea de volúmenes JFS2 durante la cual el volumen está disponible para otras aplicaciones del sistema. AIX permite la creación de una instantánea de un volumen JFS2 mientras todavía está en línea. La instantánea se crea dentro del mismo grupo de volúmenes que el volumen de origen. Debe asegurarse de que el grupo de volúmenes proporcione el espacio de disco libre suficiente para crear la instantánea. La instantánea contiene los bloques de datos antiguos y los datos modificados se almacenan en el volumen de origen. Utilice la opción `snapshotcachesize` con el mandato de imagen de copia de seguridad, en el archivo `dsm.sys`, o bien con la opción `include.image` para especificar un tamaño de instantánea adecuado para que todos los bloques de datos antiguos se puedan almacenar mientras se realiza la copia de seguridad de imagen..

 Sistemas operativos Linux El gestor de volúmenes lógicos (LVM) de Linux permite crear una instantánea de un volumen lógico mientras el volumen lógico continúa activado. La instantánea se crea dentro del mismo grupo de volúmenes que el volumen lógico de origen. Debe asegurarse de que el grupo de volúmenes proporcione el espacio de disco libre suficiente para crear la instantánea. La instantánea contiene los bloques de datos antiguos y los datos modificados se almacenan en el volumen lógico de origen. Utilice la opción `snapshotcachesize` con el mandato `backup image`, en el archivo `dsm.sys`, o con la opción `include.image` para especificar un tamaño de instantánea adecuado, de modo que todos los bloques de datos antiguos se puedan guardar mientras se realiza la copia de seguridad de imagen. Un tamaño de instantánea del 100% asegurará que la instantánea sea válida.

 Sistemas operativos Windows

## Copia de seguridad de imagen desactivada y activada

La copia de seguridad de imagen desactivada tradicional no permite que otras aplicaciones del sistema tengan acceso de escritura al volumen mientras se realiza la operación.





Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).

Utilice VSS como el proveedor de instantáneas para el soporte de archivos abiertos.

Las consideraciones siguientes se aplican a las copias de seguridad de imagen activadas o desactivadas.

- Si crea una imagen de la unidad del sistema, no podrá restaurarla en la ubicación original. Para restaurar cualquier imagen es necesario que el cliente tenga un bloqueo exclusivo del volumen en el que se realiza la restauración; por consiguiente, la unidad del sistema no podrá restaurarse debido a que el cliente no puede desbloquear la unidad del sistema. Una copia de seguridad de imagen de la unidad del sistema se puede restaurar en una ubicación alternativa.
- Debido a las diferentes configuraciones de los componentes del sistema, es posible que la imagen del sistema no sea coherente entre los componentes (como, por ejemplo, Active Directory). Algunos de estos componentes se pueden configurar para que utilicen volúmenes diferentes, de modo que unos se instalen en la unidad del sistema y otros en volúmenes que no son del sistema.
- Instale el programa cliente de IBM Spectrum Protect en la unidad del sistema. El cliente no puede restaurar una imagen en el mismo volumen en el que está instalado el programa del cliente.

- La copia de seguridad de imagen solamente se admite en volúmenes que tienen asignado un punto de montaje o una letra de unidad. El cliente no realizará una copia de seguridad de un volumen sin un punto de montaje o una letra de unidad.
- Si se detectan sectores de disco con errores en la unidad de origen durante una copia de seguridad de imagen en la LAN o fuera de la LAN, pueden dañarse los datos. En este caso, los sectores con errores se pasan por alto al enviar los datos de imagen al servidor de IBM Spectrum Protect. Si se detectan sectores de disco anómalos durante la copia de seguridad de imagen, aparecerá un mensaje de aviso una vez finalizada la operación de copia de seguridad de imagen.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Utilización de la copia de seguridad de imagen para realizar una copia de seguridad incremental del sistema de archivos

Existen dos métodos de utilizar las copias de seguridad de imágenes para realizar copias de seguridad incrementales eficaces del sistema de archivos. Estos métodos de copia de seguridad permiten realizar restauraciones a un instante específico de los sistemas de archivos y mejorar el rendimiento de las operaciones de copia de seguridad y restauración.

La copia de seguridad sólo la puede realizar en volúmenes con formato y no en volúmenes lógicos RAW. Puede utilizar la *copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos* o puede utilizar la *copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen* para realizar las copias de seguridad de los volúmenes que tienen sistemas de archivos montados.

A continuación, se muestran varios ejemplos de la utilización de la *copia de seguridad de imágenes con la copia de seguridad incremental del sistema de archivos*.




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris


- Para realizar una copia de seguridad incremental completa del sistema de archivos: `dsmc incremental /myfilesystem`
- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image /myfilesystem`
- Para realizar copias de seguridad incrementales periódicamente: `dsmc incremental /myfilesystem`

 Sistemas operativos Windows

- Para realizar una copia de seguridad incremental completa del sistema de archivos: `dsmc incremental h:`
- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image h:`
- Para realizar copias de seguridad incrementales periódicamente: `dsmc incremental h:`

Deberá seguir los siguientes pasos en el orden que se indica para asegurarse de que el servidor registra las adiciones y las supresiones con precisión.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Utilice este mandato para restaurar el sistema de archivos en el estado que tenía exactamente en la última copia de seguridad incremental: `dsmc restore image /myfilesystem -incremental -deletefiles`.

 Sistemas operativos Windows Utilice este mandato para restaurar el sistema de archivos en el estado que tenía exactamente en la última copia de seguridad incremental: `dsmc restore image h: -incremental -deletefiles`.




Durante la restauración, el cliente realiza lo siguiente:

- Restaura la imagen más reciente en el servidor.
- Suprime todos los archivos restaurados en el paso anterior que están desactivados en el servidor. Éstos son los archivos que existían en el momento de realizar la copia de seguridad de imágenes pero que después se suprimieron y grabaron en una copia de seguridad incremental.
- Restaura los archivos nuevos y modificados a partir de las copias de seguridad incrementales.

Si no realiza los pasos en el orden exacto, pueden suceder dos cosas:

1. Después de haber restaurado la imagen original, se restaurarán individualmente todos los archivos cuya copia de seguridad se ha realizado con el mandato incremental.
2. Si realiza una copia de seguridad de imágenes antes de realizar una copia de seguridad incremental, los archivos suprimidos de la imagen original *no* se suprimirán del sistema de archivos restaurado final.

A continuación, se muestran varios ejemplos de la utilización de la *copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen*.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image /myfilesystem`

- Para realizar una copia de seguridad de imágenes incremental del sistema de archivos: `dsmc backup image /myfilesystem -mode=incremental`

Con ello solamente se envían al servidor los archivos que se han añadido o modificado desde la copia de seguridad de imágenes más reciente.

- Para realizar copias de seguridad de imágenes completas periódicamente: `dsmc backup image /myfilesystem`
- Para restaurar la imagen: `dsmc restore image /misistemaarchivos -incremental`

Durante la restauración, el cliente de copia de seguridad y archivado pasa por alto la opción `deletfiles` cuando se utiliza la técnica de copia de seguridad de imágenes combinada con la copia de seguridad de imágenes incremental. La restauración incluirá los archivos que se suprimieron después de la última copia de seguridad de imágenes completa además de las últimas versiones de los archivos añadidos o modificados después de la copia de seguridad de imágenes más reciente.

#### Sistemas operativos Windows

- Para realizar una copia de seguridad de imágenes del mismo sistema de archivos: `dsmc backup image h:`
- Para realizar una copia de seguridad de imágenes incremental del sistema de archivos: `dsmc backup image h: -mode=incremental`

Con ello solamente se envían al servidor los archivos que se han añadido o modificado desde la copia de seguridad de imágenes más reciente.

- Para realizar copias de seguridad de imágenes completas periódicamente: `dsmc backup image h:`
- Para restaurar la imagen: `dsmc restore image h: -incremental`

Durante la restauración, el cliente de copia de seguridad y archivado pasa por alto la opción `deletfiles` cuando se utiliza la técnica de copia de seguridad de imágenes combinada con la copia de seguridad de imágenes incremental. La restauración incluirá los archivos que se suprimieron después de la última copia de seguridad de imágenes completa además de las últimas versiones de los archivos añadidos o modificados después de la copia de seguridad de imágenes más reciente.

Nota: Deberá realizar copias de seguridad de imágenes completas periódicamente en los casos siguientes. De este modo se reducirá el tiempo necesario para la restauración, ya que se aplican menos cambios de las copias de seguridad incrementales.

- Cuando un sistema de archivos ha cambiado sustancialmente (más del 40%).
- Una vez al mes.
- Según sea adecuado en su entorno.

A continuación, se indican las restricciones que tienen aplicación cuando se utiliza la copia de seguridad de imágenes con la modalidad de copia de seguridad incremental de imagen:

- El sistema de archivos no puede tener copias de seguridad incrementales completas anteriores, generadas mediante el mandato incremental.
- La copia de seguridad de imágenes incremental por fecha no desactiva los archivos en el servidor; por consiguiente, cuando los archivos se restauren no podrá suprimirse ninguno.
- Si se trata de la primera copia de seguridad de imágenes del sistema de archivos, se realiza una copia de seguridad de imágenes completa.
- La utilización de `mode=incremental` sólo realiza la copia de seguridad de los archivos cuya fecha ha cambiado, no de los archivos cuyos permisos han cambiado.
- Si los sistemas de archivos están funcionando completos o casi completos, puede provocarse una condición de falta de espacio durante la restauración.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Backup NAS

El mandato `backup nas` crea una copia de seguridad de imagen de uno o varios sistemas de archivos pertenecientes a un servidor de archivos NAS (Network Attached Storage), también conocido como copia de seguridad NDMP. Se le solicitará el ID de administrador de IBM Spectrum Protect.

El servidor de archivos NAS realiza el proceso de traspaso de datos externos. Se inicia un proceso del servidor para realizar la copia de seguridad.

Utilice la opción `nasnodename` para especificar el nombre de nodo del servidor de archivos NAS. El nombre del nodo NAS identifica el servidor de archivos NAS ante el servidor de IBM Spectrum Protect. El nombre del nodo NAS debe estar inscrito en el servidor. Especifique la opción `nasnodename` en el archivo de opciones del cliente (`dsm.opt`). El valor del archivo de opciones del cliente es el valor predeterminado, pero puede modificarse temporalmente en la línea de mandatos.

Utilice la opción `toc` con el mandato `backup nas` o la opción `include.fs.nas` para especificar si el servidor de IBM Spectrum Protect ha de guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos. Si guarda la información de la TOC, podrá utilizar el mandato de servidor `QUERY TOC` para determinar el contenido de la copia de seguridad de un sistema de archivos con el mandato de servidor `RESTORE NODE` para restaurar archivos individuales o árboles de directorios.

También puede utilizar el cliente web de IBM Spectrum Protect para examinar todo el árbol del sistema de archivos y seleccionar los archivos y los directorios que han de restaurarse. Para crear una tabla de contenido, debe definir el atributo `tocdestination` en el grupo de copias de seguridad para la clase de gestión a la que se vincula esta imagen de copia de seguridad. La creación de TOC necesitan más procesamiento, recursos de red, espacio de agrupación de almacenamiento y, posiblemente, un punto de montaje durante la operación de copia de seguridad. Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios utilizando el mandato de servidor `RESTORE NODE`, siempre que conozca el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

La opción `toc` sólo recibe soporte para las imágenes cuya copia de seguridad ha realizado el cliente y el servidor de la versión 5.2 o posterior.

La especificación de `mode=differential` en el mandato de servidor `BACKUP NODE` o en el mandato `backup nas` donde no exista ninguna imagen completa mostrará que se ha iniciado una copia de seguridad completa. Utilizar el mandato de servidor `QUERY PROCESS` muestra que una copia de seguridad completa está en proceso.


Utilice la opción `mode` para especificar si se realiza una copia de seguridad de imagen NAS diferencial o completa. Una copia de seguridad de imagen completa realiza una copia de seguridad de todo el sistema de archivos. El valor predeterminado es una copia de seguridad de imagen NAS diferencial en los archivos que se han modificado después de la copia de seguridad de imagen completa más reciente. Si no hay una copia de seguridad de imagen completa que pueda seleccionarse, se realiza una copia de seguridad de imagen completa. Si existe una imagen completa, tanto si es restaurable como si está caducada y está siendo mantenida debido a las imágenes diferenciales dependientes, especificar `mode=differential` envía una copia de seguridad de imágenes diferenciales. Si una imagen completa se envía durante una copia de seguridad diferencial, esto queda reflejado como una imagen completa utilizando el mandato de servidor `QUERY NASBACKUP`. El mandato de servidor `QUERY NASBACKUP` también muestra imágenes NAS que son restaurables y se mostrarán imágenes completas o imágenes diferenciales como tipo de objeto.

Utilice la opción `monitor` para especificar si desea supervisar una copia de seguridad de imagen del sistema de archivos NAS y visualizar la información sobre el proceso en la pantalla.



Utilice el mandato `monitor process` para visualizar una lista de todos los procesos para los que un ID de usuario de administración tiene autorización. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la Web.


Utilice el mandato `cancel process` para detener el proceso de copia de seguridad de NAS.

Con independencia de la plataforma del cliente utilizada, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: `/vol/vol0`.

 Sistemas operativos Windows En el sistema de archivos NAS es necesario utilizar llaves {} como delimitadores de los nombres de sistemas de archivos cuando se utiliza la línea de mandatos, por ejemplo: `{/vol/vol0}`.

## Clientes soportados

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Este mandato sólo es válido para los clientes AIX y Solaris.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

```
>>-Backup NAS--+-----+----- --filespec--+----->>
                   |                         |
                   v                         |
'- --options-'
```













## Parámetros

### filespec





Especifica el nombre de uno o varios sistemas de archivos del servidor de archivos NAS. Si no especifica este parámetro, el cliente de copia de seguridad y archivado procesa todos los sistemas de archivos definidos por la opción `domain.nas`.

Si no especifica la opción *especificación* archivo o la opción `domain.nas`, se utilizará el valor predeterminado `all-nas` para `domain.nas` y se realizará la copia de seguridad de todos los sistemas de archivos del servidor de archivos NAS.



Tabla 1. mandato backup NAS: opciones relacionadas

Opción	Dónde se utiliza
mode	Sólo línea de mandatos.
monitor	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris nasnodename	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Archivo de opciones del cliente (dsm.sys) o línea de mandatos.
 Sistemas operativos Windows nasnodename	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris toc	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Línea de mandatos o con la opción include.fs.nas del archivo de opciones del cliente (dsm.sys).
 Sistemas operativos Windows toc	 Sistemas operativos Windows Línea de mandatos o con la opción include.fs.nas del archivo de opciones del cliente (dsm.opt).

## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Tarea  
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.





**Mandato:** backup nas -mode=full -nasnodename=nas1 /vol/vol0 /vol/vol2

 Sistemas operativos Windows  
Tarea  
 Sistemas operativos Windows  
Realizar la copia de seguridad de imágenes NAS de todo el sistema de archivos.



**Mandato:** backup nas -mode=full -nasnodename=nas1 {/vol/vol0} {/vol/vol2}

Tarea  
Realizar la copia de seguridad de imagen NAS de todo el servidor de archivos.

**Mandato:** backup nas -nasnodename=nas1

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Tarea  
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Realizar una copia de seguridad de imágenes NAS de todo el sistema de archivos y guardar información de la tabla de contenido (TOC) para la copia de seguridad del sistema de archivos.

**Mandato:** backup nas -mode=full -nasnodename=netappsj /vol/vol0 -toc=yes

 Sistemas operativos Windows  
Tarea  
 Sistemas operativos Windows  
Realizar una copia de seguridad de imágenes NAS de todo el sistema de archivos y guardar información de la tabla de contenido (TOC) para la copia de seguridad del sistema de archivos.

**Mandato:** backup nas -mode=full -nasnodename=netappsj {/vol/vol0} -toc=yes

 Sistemas operativos Windows

## Backup Systemstate

Utilice el mandato backup systemstate para realizar la copia de seguridad de todos los componentes arrancables de servicios del sistema y de estado del sistema como si fueran un solo objeto, para proporcionar una instantánea de instante específico coherente del estado del sistema.

Los componentes arrancables de estado del sistema pueden incluir lo siguiente:

- Active Directory (sólo controlador de dominio)
- Volumen del sistema (sólo controlador de dominio)
- Base de datos de servidor de certificados
- Base de datos COM+
- Registro de Windows
- Archivos de arranque y del sistema
- Grabador ASR

Los componentes de servicios del sistema pueden incluir lo siguiente:

- Background Intelligent Transfer Service (BITS)
- Anotaciones de sucesos
- Base de datos de RSM (Removable Storage Management)
- Base de datos de clústeres (sólo nodo de clúster)
- Servicio de almacenamiento remoto
- Licencias de Terminal Server
- Windows Management Instrumentation (WMI)
- Base de metadatos IIS (Internet Information Services)
- Base de datos DHCP
- Base de datos Wins

La lista de componentes arrancables de los servicios del sistema y estado del sistema es dinámica y podría cambiar en función del paquete de servicio y de las características del sistema operativo que se hayan instalado. El cliente de copia de seguridad y archivado permite la recuperación dinámica y la copia de seguridad de estos componentes.

El estado del sistema se representa mediante varios grabadores VSS de tipo "estado del sistema arrancable" y "servicio del sistema". De estos, System Writer es la mayor parte del estado del sistema en términos de número de archivos y tamaño de datos. De forma predeterminada, la copia de seguridad de System Writer es incremental. Puede utilizar la opción `systemstatebackupmethod` para realizar copias de seguridad completas de System Writer. Para obtener más información sobre esta opción, consulte `Systemstatebackupmethod`. El cliente siempre realizará la copia de seguridad completa de todas las demás grabadoras.

Este mandato también hace copia de seguridad de datos ASR para los clientes Windows; las arquitecturas de arranque BIOS y UEFI reciben soporte.

Nota:

1. La copia de seguridad del componente de archivos del sistema y de arranque del estado del sistema sólo se realiza si un miembro (archivo) de ese componente ha cambiado desde la última copia de seguridad. Si un miembro ha cambiado, se realiza la copia de seguridad de todo el grupo de archivos que forman parte de ese componente.
2. El cliente de copia de seguridad y archivado Windows no permite la realización de la copia de seguridad de ningún componente individual.
3. De forma predeterminada, las copias de seguridad de estado del sistema están vinculadas a la clase de gestión predeterminada. Para vincularlas a una clase de gestión diferente, utilice la opción `include.systemstate`; especifique `all` como el patrón, y especifique el nombre de la nueva clase de gestión.

Por ejemplo: `include.systemstate ALL BASVT2`.

4. Utilice el mandato `query systemstate` para que se visualice información acerca de una copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect.
5. Ya no puede restaurar el estado del sistema en un sistema que sigue en línea. En lugar de ello, utilice el método de recuperación basado en ASR para restaurar el estado del sistema en modo Windows PE fuera de línea. Para obtener más información, consulte los siguientes artículos de la wiki de IBM Spectrum Protect:
  - Best Practices for Recovering Windows Server 2012 and Windows 8
  - Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

Si intenta restaurar el estado del sistema con el mandato `dsmc restore systemstate`, desde la GUI del cliente de archivado y copia de seguridad, o desde el cliente web, aparecerá el siguiente mensaje:

```
ANS5189E Online SystemState restore has been deprecated. Please use offline
WinPE method for performing system state restore.
```

## Clientes soportados

---

Este mandato es válido para todos los clientes Windows admitidos.

## Sintaxis

---

```
>>>-Backup SYSTEMStAt----->>>
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

## Tarea

Realizar la copia de seguridad del estado del sistema.


**Mandato:** `backup systemstate`

 Sistemas operativos Linux  Sistemas operativos Windows


## Backup VM

---

Utilice el mandato `backup vm` para iniciar una copia de seguridad completa de una máquina virtual.

 Sistemas operativos Windows

El mandato `backup vm` se puede utilizar para hacer copia de seguridad de las máquinas virtuales Microsoft Hyper-V y las máquinas virtuales VMware. La información para cada hipervisor se presenta en su propio encabezado. Si está realizando una copia de seguridad de una máquina virtual que forma parte de un conjunto de Hyper-V, no necesita leer el texto *Copia de seguridad de máquinas virtuales VMware*. Si está realizando una copia de seguridad de una máquina virtual VMware, no necesita leer el texto de *Copia de seguridad de máquinas virtuales Microsoft Hyper-V*.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

 Sistemas operativos Linux  Sistemas operativos Windows

## Realización de copia de seguridad de máquinas virtuales VMware

---

Utilice el mandato `backup vm` para realizar copias de seguridad de máquinas virtuales VMware.

El nodo transportador de datos de IBM Spectrum Protect hace copia de seguridad de una o varias máquinas virtuales. *El nodo transportador de datos* es el nombre que recibe una configuración en la que el cliente de archivado y copia de seguridad se ejecuta en un servidor de copia de seguridad vStorage y está configurado para proteger las máquinas virtuales de un centro virtual o un servidor ESX/ESXi. Debe configurar la máquina virtual VMware antes de utilizar este mandato. Para obtener información sobre cómo configurar la máquina virtual VMware, consulte Preparación del entorno para copias de seguridad paralelas de máquinas virtuales VMware.

Una copia de seguridad de máquina virtual completa almacena una copia de seguridad de la información de configuración e imágenes de disco virtual completas de una máquina virtual. Las copias de seguridad completas de máquinas virtuales permiten una restauración completa de una máquina virtual, pero llevan más tiempo y necesitan más espacio de servidor que una copia de seguridad incremental.

Si establece la opción `vmenabletemplatebackups` en *yes*, una operación `backup vm` incluye las VM de plantilla, pero sólo si el servidor de copia de seguridad vStorage está conectado a un servidor vCenter y no a un host ESX o ESXi.

Si una instantánea falla durante el copia de seguridad, el cliente intenta realizar la copia de seguridad de la máquina virtual VMware una vez más. Para controlar el número de intentos de instantáneas totales, defina la opción `INCLUDE.VMSNAPSHOTATTEMPTS` en el archivo de opciones de cliente.

Los códigos de protección de datos se utilizan para configurar la política de copia de seguridad de las máquinas virtuales en objetos de VMware. Los códigos y las categorías el usuario utiliza uno de los métodos siguientes:

- Habilita el soporte de codificación en el nodo del transportador de datos con la opción `vmtagdatamover` y ejecuta del mandato `backup vm`.
- Utiliza la Plug-in de cliente de IBM Spectrum Protect vSphere para gestionar copias de seguridad de IBM Spectrum Protect.
- Ejecuta el mandato `set vmtags` en cualquier nodo transportador de datos.

Cuando la opción `vmtagdatamover` se establece en *yes*, se realiza una copia de seguridad de todos los códigos que se asignan a una máquina virtual durante las operaciones `backup vm`. Los códigos se restauran cuando se ejecuta el mandato `restore vm`. No se efectúan copias de seguridad de los códigos que se asignan a otros objetos de inventario, por lo que no se pueden restaurar.

Para obtener más información sobre los códigos de protección de datos, consulte el apartado Visión general de los códigos de protección de datos.

Una copia de seguridad de VM completa utiliza el CBT (Changed Block Tracking - Seguimiento de bloques cambiados) de VMware para crear copias de seguridad que reconocen el contenido (sólo de bloque utilizado). El cliente permite el seguimiento de bloques cambiados (CBT) en un servidor ESX o ESXi cuando empieza una copia de seguridad. CBT de VMware necesita un host ESX 4.1 (o posterior), con hardware virtual 7 (o posterior). No puede realizar copias de seguridad de VM incrementales o completas en máquinas virtuales que no soportan CBT.

Cuando CBT está habilitado, realiza el seguimiento de los cambios de disco cuando la pila de almacenamiento de servidor ESX o ESXi procesa las operaciones de E/S en los discos siguientes:



- Un disco virtual almacenado en VMFS; el disco puede ser un disco iSCSI, un disco local o un disco que está en una SAN.
- Un disco virtual almacenado en NFS.
- Una RDM que está en modalidad de compatibilidad virtual.

Cuando la pila de almacenamiento ESX o ESXi no procesa las operaciones de E/S, no se puede utilizar el seguimiento de bloques cambiados para hacer el seguimiento de cambios de disco. Los discos siguientes no pueden utilizar CBT:

- Una RDM que está en modalidad de compatibilidad física.
- Un disco al que se accede directamente desde dentro de una máquina virtual. Por ejemplo, vSphere no puede hacer el seguimiento de los cambios realizados en una LUN iSCSI a la que se accede mediante un iniciador iSCSI en la máquina virtual.

La información completa sobre los requisitos de seguimiento de bloques cambiados se describe en la publicación *VMware Virtual Disk API Programming Guide* en la documentación del producto VMware. En la guía, busque "Low Level Backup Procedures" y lea la sección "Changed Block Tracking on Virtual Disks".

Para servidores VMware que no soporten CBT, se hace una copia de seguridad de las áreas utilizadas y de las no utilizadas del disco y se registra un mensaje informativo en el archivo `dsmerror.log`. Utilice la opción `-preview` en el mandato `backup vm` para ver el estado CBT actual. El estado de CBT tiene tres valores:

#### Desactivado

Indica que el parámetro de configuración de CBT (`ctkEnabled`) no está habilitado en los parámetros de configuración de la máquina virtual. Off es el valor predeterminado.

#### No soportado

Indica que la máquina virtual no da soporte a CBT. No es posible hacer copias de seguridad sólo de bloques cambiados.


#### Activado



Indica que la máquina virtual da soporte a CBT y que CBT está habilitado en los parámetros de configuración de la máquina virtual (`ctkEnabled=true`).

El cliente activa la CBT (se establece `ctkEnable=true`) con cada intento de copia de seguridad. Cuando el cliente activa la CBT, continúa activada, incluso si se suprime la máquina virtual del servidor de IBM Spectrum Protect. Con la CBT habilitada, una vez realizada la primera copia de seguridad de VM completa, sólo se puede hacer una copia de seguridad de o restaurar los bloques cambiados del disco.

Si ya no realiza copias de seguridad de IBM Spectrum Protect de una máquina virtual, puede desactivar la CBT. Para desactivar la CBT, pulse el botón derecho del ratón en la máquina virtual para la que desea desactivar la CBT en el cliente vSphere. Pulse Editar valores > Opciones > General > Parámetros de configuración. A continuación, establezca el parámetro de configuración `ctkEnabled` como `false`.

Consejo: Puede utilizar la opción de compresión con copias de seguridad sólo si la copia de seguridad se guarda en una agrupación de almacenamiento habilitada para la eliminación de duplicados.

 Sistemas operativos Windows Para obtener más información sobre la compresión, consulte Proceso de compresión y cifrado.

 Sistemas operativos Windows  Sistemas operativos Linux Especifique las opciones `-vmbackuptype` y `-mode` para indicar cómo deben realizarse las copias de seguridad. Para copias de seguridad completas, utilice `-vmbackuptype=fullvm` y especifique cualquiera de las siguientes modalidades de opciones:

#### IFFull


Modalidad completa-constante-incremental. En esta modalidad, se realiza una copia de seguridad en el servidor de una instantánea de todos los bloques de utilizados en los discos de una máquina virtual. Tiene que tener licencia de uso de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.


#### IFIncremental

Incremental-constante-incremental. En esta modalidad, se crea una instantánea de los bloques que han cambiado desde la última copia de seguridad. Tiene que tener licencia de uso de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware o IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

Para obtener información sobre la estrategia de copia de seguridad incremental-constante, consulte IBM Spectrum Protect for Virtual Environments, Data Protection for VMware: tipos de copia de seguridad y restauraciones .

## Clientes soportados

 Sistemas operativos Windows Este mandato es válido en clientes Windows soportados instalados en un servidor de copia de seguridad vStorage que protege las máquinas virtuales VMware.

 Sistemas operativos Linux Este mandato sólo es válido en clientes Linux soportados instalados en un servidor de copia de seguridad vStorage que protege las máquinas virtuales VMware.

## Sintaxis

```

      .-.,-----.
      V            |
      .---vmname---+-.
>>-Backup VM-+-----+-----+-----+-----+-----+----->
>+-----+-----+-----+-----+-----+-----+-----+----->
| .-.,-----. |
| V            | |
|'---vmname---:vmdk---etiqueta_disco---+'
>+-----+-----+-----+-----+-----+-----+-----+-----<
|'  -VMBACKUPUPDATEGUID-'  '|-  -PREView--  --options-'

```

## Parámetros

### *nombre\_máquina\_virtual*

Especifique el nombre de las máquinas virtuales de las que quiera realizar copias de seguridad. El nombre es el de visualización de la máquina virtual. Separe los nombres de distintas máquinas virtuales con comas. Si establece la opción `vmenabletemplatebackups` en yes, `vmname` puede especificar el nombre de una máquina virtual de plantilla para realiza una copia de seguridad.

vCenter de VMware permite que dos o más máquinas virtuales tengan el mismo nombre de visualización. No obstante, el cliente de copia de seguridad y archivado requiere que todos los nombres de máquina virtual de una configuración de servidor de vCenter sean exclusivos. Para evitar errores durante el proceso, asegúrese de que todas las máquinas virtuales tienen un nombre de visualización exclusivo.

Se pueden utilizar caracteres comodín en nombres de máquinas virtuales que se especifican como este parámetro. Sin embargo, el proceso de comodines difiere en función de la modalidad de copia de seguridad que se utiliza.

- Para copias de seguridad que utilizan `mode=iffull` o `mode=ifincremental`, se pueden utilizar caracteres comodín para que coincidan con los patrones de nombres de máquina virtual. Por ejemplo:
  - `backup vm VM_TEST*` incluye todas las máquinas virtuales que tienen nombres que empiezan por `VM_TEST`
  - `backup vm VM??` incluye cualquier máquina virtual que tenga un nombre que empiece por las letras "VM", seguido de 2 caracteres

Si no especifica `vmname`, puede identificar la máquina virtual con la opción `domain.vmdisk`.

### `:vmdk=etiqueta_disco`

Esta palabra clave es una extensión de `vmname`. Especifica la etiqueta (nombre) del disco de la máquina virtual que hay que incluir en la operación de copia de seguridad. Puede excluir un disco poniendo el operador de exclusión (-) delante de la palabra clave. Para obtener procedimientos adicionales para incluir o excluir los discos de proceso, consulte `Domain.vmdisk`, `Exclude.vmdisk`, `Include.vmdisk`.

### `-VMBACKUPUPDATEGUID`

Para utilizar esta opción, tiene que tener un acuerdo de licencia para utilizar IBM Spectrum Protect for Virtual Environments: Data Protection for VMware.

Esta opción actualiza el identificador exclusivo global (GUID) para la máquina virtual de la cual realiza la copia de seguridad. Este parámetro está destinado para utilizar sólo en el siguiente caso de ejemplo:

Desea restaurar una máquina virtual de la cual previamente se ha realizado una copia de seguridad, llamada ORION. Pero, antes de concluir y sustituir la copia de ORION que está ejecutándose en su entorno de producción, desea verificar la configuración de la máquina virtual restaurada antes de utilizarla para sustituir la ORION existente.

1. Restaura la máquina virtual ORION y le asigna un nombre nuevo: `dsmc restore vm Orion -vmname=Orion2`
2. Actualiza y verifica la máquina virtual ORION2 y determina que está preparada para sustituir la máquina virtual existente denominada ORION.
3. Apaga y suprime ORION.
4. Renombra ORION2, de modo que ahora se llama ORION.
5. La próxima vez que realice una copia de seguridad de ORION, utilizando una copia de seguridad incremental-constante-completa, o incremental-constante-incremental, debe añadir el parámetro `-VMBACKUPUPDATEGUID` al mandato `backup vm`. Esta opción actualizará el GUID, en el servidor IBM Spectrum Protect, de modo que el nuevo GUID se asocie a las copias de seguridad almacenadas para la máquina virtual ORION. La cadena de copias de seguridad incrementales se mantiene; no es necesario suprimir las copias de seguridad existentes y sustituirlas por las nuevas copias de seguridad.

### `-PREView`

Esta opción muestra información sobre una máquina virtual, incluidas las etiquetas de los discos duros de la máquina virtual y la información de clase de gestión de una máquina virtual.

Puede utilizar las etiquetas de disco con las palabras clave `:vmdk= o :-vmdk=` para incluir o excluir discos de una operación de copia de seguridad. El texto siguiente es una salida de muestra del parámetro `-preview`:

```
backup vm vml -preview
BACKUP de VM completo de las máquinas virtuales 'VM1'

vmName:vml
VMDK[1]Etiqueta: Disco duro 1
VMDK[1]Nombre: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14.vmdk
VMDK[1]Estado: Incluido
VMDK[2]Etiqueta: Disco duro 2
VMDK[2]Nombre: [ds5k_svt_1] tsmcetlnx14/tsmcetlnx14_1.vmdk
VMDK[2]Estado: Excluido: usuario,independiente,pRDM
```

Este ejemplo de salida de `-preview` muestra que VMDK 2 se ha excluido de la copia de seguridad anterior. Los discos que se han incluido en una copia de seguridad tienen el estado `Included`. Los discos que se han excluido de la copia de seguridad tienen el estado `Excluded`, seguido de un código de razón. Los códigos de razón pueden ser cualquiera de los siguientes:

#### usuario

Indica que el disco se ha omitido porque estaba excluido en una sentencia `domain.vmfull`, en la línea de mandatos, o en el archivo de opciones del cliente.

#### Independiente

Indica que el disco es un disco independiente. Los discos independientes no pueden formar parte de una instantánea, por lo que son excluidos de las operaciones `backup vm`. Asegúrese de que la opción `vmprocessvmwithindependent` esté establecida en `yes` o toda la máquina virtual es omitida por la operación de copia de seguridad si contiene uno o más discos independientes.

#### pRDM

Indica que el disco es un disco pRDM (physical Raw Device Mapped). Los discos pRDM no pueden formar parte de una instantánea, por lo que son excluidos de las operaciones `backup vm`. Asegúrese de que la opción `vmprocessvmwithprdm` esté establecida en `yes` o toda la máquina virtual es omitida por una operación de copia de seguridad si contiene uno o más volúmenes RDM (Raw Device Mapping, asignación de dispositivos en bruto) suministrados en modo de compatibilidad física (pRDM).

La salida del parámetro `-preview` también muestra el nombre de la clase de gestión que está asociada con la máquina virtual, junto con información sobre el lugar en el que se ha definido la clase de gestión. Esta información puede ayudarle a verificar si los valores de dominio y de código se han definido correctamente para la clase de gestión. Por ejemplo:

```
backup vm -preview
BACKUP de VM completo de las máquinas virtuales especificadas en la opción DOMAIN.VMFULL.
```

```
1. vmName: tag_vm_2
   DomainKeyword: all-vm
   toolsRunningStatus: guestToolsNotRunning
   toolsVersionStatus: guestToolsNotInstalled
   consolidationNeeded: No
   Change Block Tracking: On
   managementClassName: STANDARD
   managementClassLocation: Node Default

   VMDK[1]Etiqueta: 'Hard disk 1' (Hard Disk 1)
   VMDK[1]Nombre: '[Raid1-lannds2] tag_vm_2/tag_vm_2.vmdk'
   VMDK[1]Estado: Incluido
...

12. vmName: vm-jean
   DomainKeyword: all-vm
   toolsRunningStatus: guestToolsNotRunning
   toolsVersionStatus: guestToolsNotInstalled
   consolidationNeeded: No
   Change Block Tracking: On
   managementClassName: MGMTCLASS1 (invalid)
   managementClassLocation: VM Tag Management Class (IBM Spectrum Protect)

   VMDK[1]Etiqueta: 'Hard disk 1' (Hard Disk 1)
   VMDK[1]Nombre: '[Raid1-lannds2] vm-jean/vm-jean.vmdk'
   VMDK[1]Estado: Incluido
```

donde:

#### managementClassName

Muestra el nombre de la clase de gestión a la que está vinculada la máquina virtual.

Si aparece la etiqueta "(invalid)" junto al nombre de la clase de gestión, significa que el nombre se ha especificado incorrectamente, que la clase de gestión se ha eliminado del servidor de IBM Spectrum Protect o que no se ha encontrado ningún grupo de copias de seguridad en la clase de gestión en el servidor. Si el nombre de la clase de gestión no es válido, la operación de copia de seguridad de la máquina virtual falla.

#### managementClassLocation

Muestra el lugar en el que se ha definido la clase de gestión. Se permiten las siguientes ubicaciones:

##### Nodo predeterminado

La clase de gestión se ha definido en el dominio predeterminado del nodo del centro de datos de VMware.

##### Opción VMMC

La clase de gestión se ha definido con la opción vmmc.

##### Opción VMCTLMC

La clase de gestión se ha definido con la opción vmctlmc.

##### Opción INCLUDE.VM

La clase de gestión se ha definido con la opción include.vm.

##### VM Tag Management Class (IBM Spectrum Protect)

La clase de gestión se ha definido como un valor de código de la categoría de códigos `Management Class (IBM Spectrum Protect)`. Los valores de los códigos se pueden definir con valores de protección de datos en la Plug-in de cliente de IBM Spectrum Protect vSphere del cliente web de vSphere, o bien utilizando herramientas como VMware vSphere PowerCLI versión 5.5 R2 o posterior.

Importante: Para visualizar la información de la clase de gestión definida por los códigos, debe definir la opción `vmtagdatamover yes` en el archivo de opciones del cliente o debe incluir el parámetro `-vmtagdatamover=yes` cuando ejecute el mandato `dsmc backup vm`. Si no ha establecido la opción `vmtagdatamover` o si se ha establecido en `no`, el cliente pasa por alto cualquier valor de código de clase de gestión y muestra la definición de la clase de gestión establecida en el dominio predeterminado del nodo del centro de datos, en la opción `vmmc` o en la opción `include.vm`.

## Códigos de retorno para operaciones de copia de seguridad de máquinas virtuales

Las operaciones de copia de seguridad para máquinas virtuales pueden completarse con los códigos de retorno que se muestran en la siguiente tabla:

Código de retorno	Descripción
0	Un mandato para realizar una copia de seguridad de una o más máquinas virtuales se ha completado correctamente.
8	Un mandato para realizar una copia de seguridad de varias máquinas virtuales se ha realizado correctamente para algunas de las máquinas virtuales para las que se ha ejecutado el mandato. Examine el archivo de registro para determinar el estado de proceso de cada una de las máquinas virtuales de destino.
12	Indica que se ha producido alguna de las siguientes condiciones de error: <ul style="list-style-type: none"> <li>El mandato de copia de seguridad no ha podido realizar la copia de seguridad de ninguna de las máquinas virtuales que eran destinos de la operación de copia de seguridad.</li> <li>El mandato <code>backup</code> ha fallado y se ha detenido antes de que se inspeccionaran todas las máquinas virtuales que se han especificado.</li> </ul> Examine el archivo de registro para determinar el motivo del error.

## Mandatos de ejemplo de protección de datos de vStorage API

Realizar una copia de seguridad IFIncremental de dos máquinas denominadas `vm3` y `vm4`.

```
dsmc backup vm vm3,vm4 -vmbackuptype=fullvm -mode=ifincremental
```

Realizar una copia de seguridad IFFull de una máquina denominada `vm1`.

```
dsmc backup vm vm1 -vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad de máquina virtual IFFull de una máquina virtual denominada `vm1`, pero incluyendo únicamente el disco duro 1 en la operación de copia de seguridad.

```
dsmc backup vm "vm1:vmdk=Hard Disk 1" -vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad siempre incremental de una máquina virtual llamada `vm1`, pero excluir el disco duro 1 y el disco duro 4 de la operación de copia de seguridad.

```
dsmc backup vm "vm1:-vmdk=Hard Disk 1:-vmdk=Hard Disk 4"  
-vmbackuptype=fullvm -mode=iffull
```

Realizar una copia de seguridad incremental siempre incremental de dos máquinas virtuales llamadas vm1 y vm2. En vm1, realizar una copia de seguridad sólo del disco duro 2 y el disco duro 3. En vm2, realizar una copia de seguridad de todos los discos virtuales.

```
dsmc backup vm "vm1:vmdk=Hard Disk 2:vmdk=Hard Disk 3",  
vm2 -vmbackuptype=fullvm -mode=iffull
```

Realizar copias de seguridad paralelas de tipo completa-constante-incremental de las máquinas virtuales VMware que se han seleccionado para copia de seguridad utilizando los criterios de selección (parámetros de dominio) en la sentencia domain.vmfll. Defina el número máximo de copias de seguridad paralelas en 5 máquinas virtuales y 10 sesiones, y limite las copias de seguridad a 5 máquinas virtuales por host y 5 máquinas virtuales por almacén de datos.

```
dsmc backup vm -vmbackuptype=fullvm -mode=iffull -vmmaxparallel=5  
-vmmaxbackupsessions=10 -vmlimitperhost=5 -vmlimitperdatastore=5
```

 Sistemas operativos Linux  Sistemas operativos Windows

Enlaces relacionados para realizar copias de seguridad de máquinas virtuales VMware

- Query VM
- Restore VM
- Domain.vmfll
- Include.vm
- Mbojrefreshtresh
- Mbpctrefreshtresh
- Mode
- Vmbackdir
- Vmbackuplocation
- Vmbackuptype
- Vmchost
- Vmctlmc
- Vmcpw
- Vmuser
- Vmlimitperdatastore
- Vmlimitperhost
- Vmmc
- Vmmaxbackupsessions
- Vmmaxparallel
- Vmtagdatamover
- Set Vmtags
- Opciones exclude de la máquina virtual
- Opciones include de la máquina virtual

 Sistemas operativos Windows

## Realización de copias de seguridad de máquinas virtuales Hyper-V de Microsoft

Utilice el mandato backup vm para realizar copias de seguridad de máquinas virtuales Hyper-V. Puede realizar una copia de seguridad de los huéspedes de Hyper-V que existen en un disco local, un disco conectado a SAN, un volumen compartido de clúster (CSV) o huéspedes que existen en un recurso compartido de servidor de archivos remoto. Los recursos compartidos de servidor de archivos remoto deben estar en un sistema Windows Server 2012 o posterior.

Especifique la modalidad de copia de seguridad que se utilizará cuando desee realizar una copia de seguridad de una máquina virtual añadiendo el parámetro -mode a la línea de mandatos, o puede establecer la opción mode en el archivo de opciones del cliente. No se puede especificar ninguna de las siguientes modalidades:

### IFFull

Modalidad completa-constante-incremental. En esta modalidad, se realiza una copia de seguridad en el servidor de una instantánea de todos los bloques de utilizados en los discos de una máquina virtual. La copia de seguridad incluye información de configuración, y todos los discos. Debe tener licencia para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta modalidad. Esta modalidad sólo se puede utilizar en clientes Windows en hosts Hyper-V que se ejecutan en entornos Windows Server 2012 o posteriores.

### IFIncremental

Incremental-constante-incremental. En esta modalidad, se crea una instantánea de los bloques que han cambiado desde la última copia de seguridad. La copia de seguridad incluye información de configuración, y todos los discos. Debe tener licencia para IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta modalidad. Esta



```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Si especifica varios discos de máquina virtual a incluir o excluir, la palabra clave vhd= o -vhd= y los valores asociados deben estar separados por dos puntos, sin caracteres de espacio intercalado. Por ejemplo:

```
dsmc backup vm "*: -VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

Si especifica varios nombres de máquina virtual y discos de máquina virtual, el nombre de máquina virtual y los valores asociados deben estar separados por punto y coma, sin caracteres de espacio intercalado. Por ejemplo:

```
dsmc backup vm "vm1:-VHDX=IDE 1 0:-VHDX=SCSI 0 1;vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1"
```

#### -VMBACKUPUPDATEGUID

Tiene que tener licencia de uso de IBM Spectrum Protect for Virtual Environments: Data Protection for Microsoft Hyper-V para utilizar esta opción.

Esta opción actualiza el identificador exclusivo global (GUID) para la máquina virtual de la cual realiza la copia de seguridad. Este parámetro está destinado para utilizar sólo en el siguiente caso de ejemplo:

Desea restaurar una máquina virtual de la cual previamente se ha realizado una copia de seguridad, llamada ORION. Pero, antes de concluir y sustituir la copia de ORION que está ejecutándose en su entorno de producción, desea verificar la configuración de la máquina virtual restaurada antes de utilizarla para sustituir la ORION existente.

1. Restaura la máquina virtual ORION y le asigna un nombre nuevo: `dsmc restore vm Orion -vmname=Orion2`
2. Actualiza y verifica la máquina virtual ORION2 y determina que está preparada para sustituir la máquina virtual existente denominada ORION.
3. Apaga y suprime ORION.
4. Renombra ORION2, de modo que ahora se llama ORION.
5. La próxima vez que realice una copia de seguridad de ORION, utilizando una copia de seguridad incremental-constante-completa, o incremental-constante-incremental, debe añadir el parámetro -VMBACKUPUPDATEGUID al mandato backup vm. Esta opción actualizará el GUID, en el servidor IBM Spectrum Protect, de modo que el nuevo GUID se asocie a las copias de seguridad almacenadas para la máquina virtual ORION. La cadena de copias de seguridad incrementales se mantiene; no es necesario suprimir las copias de seguridad existentes y sustituirlas por las nuevas copias de seguridad.

#### -PREVIEW

Este parámetro muestra información sobre una máquina virtual, incluidas las etiquetas de los discos duros virtuales que se encuentran en la máquina virtual.

Cuando emita la opción -preview, no se iniciará la operación de copia de seguridad. Debe emitir el mandato de copia de seguridad sin la opción -preview para iniciar la operación de copia de seguridad.

Puede utilizar la opción -preview y la opción -detail en el mandato para visualizar información sobre los subdiscos que se incluyen cuando se ejecuta la copia de seguridad. Un subdisco es el archivo AVHDX que se crea cuando se realiza una instantánea de un archivo VHDX.

## Códigos de retorno para operaciones de copia de seguridad de máquinas virtuales

Las operaciones de copia de seguridad para máquinas virtuales pueden completarse con los códigos de retorno que se muestran en la siguiente tabla:

Código de retorno	Descripción
0	Un mandato para realizar una copia de seguridad de una o más máquinas virtuales se ha completado correctamente.
8	Un mandato para realizar una copia de seguridad de varias máquinas virtuales se ha realizado correctamente para algunas de las máquinas virtuales para las que se ha ejecutado el mandato. Examine el archivo de registro para determinar el estado de proceso de cada una de las máquinas virtuales de destino.
12	Indica que se ha producido alguna de las siguientes condiciones de error: <ul style="list-style-type: none"><li>• El mandato de copia de seguridad no ha podido realizar la copia de seguridad de ninguna de las máquinas virtuales que eran destinos de la operación de copia de seguridad.</li><li>• El mandato backup ha fallado y se ha detenido antes de que se inspeccionaran todas las máquinas virtuales que se han especificado.</li></ul> Examine el archivo de registro para determinar el motivo del error.

## Ejemplos de copia de seguridad de Microsoft Hyper-V

Inicie una copia de seguridad incremental constante incremental de una máquina virtual Hyper-V que se denomine "VM1".

```
dsmc backup vm VM1 -mode=ifincremental
```

Inicie una copia de seguridad incremental-constante-incremental de todas las máquinas virtuales Hyper-V que se especifican en la opción domain.vmfull.

```
dsmc backup vm -mode=ifincremental
```

Para los sistemas operativos Windows Server 2016 o posteriores: El mandato siguiente excluye un disco IDE (con el número de controlador 1 y la ubicación de disco 0) y un disco SCSI (con el número de controlador 0 y la ubicación de disco 1) de una copia de seguridad de Hyper-V RCT incremental-constante incremental, "vm2":

```
dsmc backup vm "vm2:-VHDX=IDE 1 0:-VHDX=SCSI 0 1" -mode=ifincremental
```

Para sistemas operativos Windows Server 2016 o posteriores: El mandato siguiente muestra la vista previa de una copia de seguridad de Hyper-V RCT de una máquina virtual, "VM05":

```
dsmc backup vm VM05 -mode=ifincremental -preview
```

En la salida del mandato, el parámetro -preview muestra las etiquetas de VHDX de la máquina virtual. Si se especifica el parámetro -detail con el parámetro -preview, no se muestra información adicional para las copias de seguridad de Hyper-V RCT.

Se ha iniciado el mandato de copia de seguridad de la máquina virtual. Número total de máquinas virtuales a procesar: 1

1. Nombre de VM: VM05

```
Palabra clave de dominio: VM05
Modalidad: Incremental constante - Incremental
Nombre de nodo de destino: NODE14
Nombre de nodo de transportador de datos: NODE14
Recurso de clúster: No
```

```
Disk[1]
Nombre: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05.vhdx
Capacidad: 15,00 GB
Tamaño: 10,91 GB
Estado: incluido
Tipo de disco: VHDX
Número de subdisco: 0
Ubicación del controlador: IDE 0 0
```

```
Disk[2]
Nombre: \\node14\d$\Hyper_V_Virtual_Machine\VM05\Virtual Hard Disks\VM05_Disk2.vhdx
Capacidad: 2,00 GB
Tamaño: 132,00 MB
Estado: incluido
Tipo de disco: VHDX
Número de subdisco: 0
Ubicación del controlador: SCSI 0 1
```

Número total de máquinas virtuales procesadas: 1

Para Windows Server 2012 o 2012 R2: El mandato siguiente inicia una copia de seguridad incremental siempre incremental de una máquina virtual Hyper-V, "VM3":

```
dsmc backup vm VM3 -mode=ifincremental -preview
```

En la salida del mandato, el parámetro -preview muestra las etiquetas de VHDX de la máquina virtual:

Nombre de VM: VM3

```
Palabra clave de dominio: all-vm
Modalidad: Incremental constante - Incremental
Nombre de nodo de destino: NODE1
Nombre de nodo de transportador de datos: NODE1
Recurso de clúster: Sí
```

```
Disk[1]
Nombre: c:\ClusterStorage\Volum1\Hyper-V\VM3\VM3.VHDX
Capacidad: 40.00 GB
Tamaño: 9,09 GB
Copia de seguridad completa: incluida
Copia de seguridad incremental: excluida
Tipo de disco: VHDX
Número de subdisco: 1
```



```

Disk[2]
Nombre: c:\ClusterStorage\Volume3\Hyper-V\VM3\VM3-DISK2.VHDX
Capacidad: 127,00 GB
Tamaño: 4.00 MB
Copia de seguridad completa: incluida
Copia de seguridad incremental: excluida
Tipo de disco: VHDX
Número de subdisco: 1

```

Si se especifica el parámetro -detail con el parámetro -preview, se muestran las etiquetas VHDX y sus subdiscos. La siguiente salida de ejemplo está abreviada para mostrar únicamente información acerca de una máquina virtual y un disco:

Nombre de VM: VM3

```

Palabra clave de dominio: all-vm
Modalidad: Incremental constante - Incremental
Nombre de nodo de destino: NODE1
Nombre de nodo de transportador de datos: NODE1
Recurso de clúster: Sí

```

```

Disk[1]
Nombre: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3.VHDX
Capacidad: 40.00 GB
Tamaño: 9,09 GB
Copia de seguridad completa: incluida
Copia de seguridad incremental: excluida
Tipo de disco: VHDX
Número de subdisco: 1

```

```

Subdisk[1]
Nombre: c:\ClusterStorage\Volume1\Hyper-V\VM3\VM3_9B26166-9C3E.avhdx
Capacidad: 40.00 GB
Tamaño: 1,25 GB
Copia de seguridad completa: incluida
Copia de seguridad incremental: incluida
Tipo de disco: AVHDX

```

## Ejemplos del archivo de opciones de Hyper-V

El siguiente ejemplo especifica las máquinas virtuales individuales en el archivo de opciones de cliente y muestra la opción domain.vmvull.

```
domain.vmfull vm1,vm2,vm5
```

En los ejemplos siguientes, se utiliza la opción domain.vmfull para procesar una máquina virtual específica.

Para sistemas operativos Windows Server 2016 o posteriores: en el ejemplo, siguiente, la opción domain.vmfull se especifica del siguiente modo:

```
domain.vmfull VM04,VM05
```

El mandato siguiente muestra una vista previa de una copia de seguridad Hyper-V RCT de todas las máquinas virtuales especificadas en la opción domain.vmfull. El mandato muestra información previa sobre cada máquina virtual:

```
dsmc backup vm -mode=ifull -preview
```

Se muestra la siguiente salida:

Se ha iniciado el mandato de copia de seguridad de la máquina virtual. Número total de máquinas virtuales para procesar: 2

1. Nombre de VM: VM04

```

Palabra clave de dominio: VM04
Modalidad: Incremental constante - Completa
Nombre de nodo de destino: NODE14
Nombre de nodo de transportador de datos: NODE14
Recurso de clúster: No

```

```

Disk[1]
Nombre: \\node14\d$\Hyper_V_Virtual_Machine\VM04\Virtual Hard Disks\VM04.vhdx
Capacidad: 36,00 GB
Tamaño: 9,16 GB
Estado: incluido
Tipo de disco: VHDX
Número de subdisco: 0

```

Ubicación del controlador: IDE 0 0

2. Nombre de VM: VM05

Palabra clave de dominio: VM05  
Modalidad: Incremental constante - Completa  
Nombre de nodo de destino: NODE14  
Nombre de nodo de transportador de datos: NODE14  
Recurso de clúster: No

Disk[1]  
Nombre: \\node14\d\$\Hyper\_V\_Virtual\_Machine\VM05\Virtual Hard Disks\VM05.vhdx  
Capacidad: 15,00 GB  
Tamaño: 10,91 GB  
Estado: incluido  
Tipo de disco: VHDX  
Número de subdisco: 0  
Ubicación del controlador: IDE 0 0

Disk[2]  
Nombre: \\node14\d\$\Hyper\_V\_Virtual\_Machine\VM05\Virtual Hard Disks\VM05\_Disk2.vhdx  
Capacidad: 2,00 GB  
Tamaño: 132,00 MB  
Estado: incluido  
Tipo de disco: VHDX  
Número de subdisco: 0  
Ubicación del controlador: SCSI 0 1

Número total de máquinas virtuales procesadas: 2

Para Windows Server 2012 o 2012 R2: en el ejemplo, siguiente, la opción domain.vmfull especifica estas máquinas virtuales:

```
domain.vmfull BigVM,myGentoox64,HPV2VM3-OLD,Local10
```

El mandato siguiente muestra una vista previa de una operación de copia de seguridad incremental constante-incremental de todas las máquinas virtuales de Hyper-V: especificadas en la opción domain.vmfull. El mandato muestra información previa sobre cada máquina virtual:

```
dsmc backup vm -mode=iffull -preview
```

Se muestra la siguiente salida:

1. Nombre de máquina virtual: BigVM

Palabra clave de dominio: all-vm  
Modalidad: Incremental constante - Completa  
Nombre de nodo de destino: MSF  
Nombre de nodo de transportador de datos: MSF  
Recurso de clúster: No

Disk[1]  
Nombre: \\lingonberry\c\$\Users\michael\Documents\Storage\BigVM.vhdx  
Capacidad: 5,85 TB  
Tamaño: 5,00 MB  
Copia de seguridad completa: incluida  
Copia de seguridad incremental: excluida  
Tipo de disco: VHDX  
Número de subdisco: 0

2. Nombre de máquina virtual: Gentoox64

Palabra clave de dominio: all-vm  
Modalidad: Incremental constante - Completa  
Nombre de nodo de destino: MSF  
Nombre de nodo de transportador de datos: MSF  
Recurso de clúster: No

3. Nombre de máquina virtual: HPV2VM3-OLD

Palabra clave de dominio: all-vm  
Modalidad: Incremental constante - Completa  
Nombre de nodo de destino: MSF  
Nombre de nodo de transportador de datos: MSF  
Recurso de clúster: No

4. Nombre de máquina virtual: Local10





```
Palabra clave de dominio:    all-vm
Modalidad:                  Incremental constante - Completa
Nombre de nodo de destino:   MSF
Nombre de nodo de transportador de datos: MSF
Recurso de clúster:         No
```

```
Disk[1]
Nombre: \\lingonberry\c$\Users\michael\Documents\Storage\Local10.vhdx
Capacidad:                  127,00 GB
Tamaño:                     4.00 MB
Copia de seguridad completa: incluida
Copia de seguridad incremental: excluida
Tipo de disco:              VHDX
Número de subdisco:         0
```

Número total de máquinas virtuales procesadas: 4  
El código de retorno de ANS1900I es 0.  
El código de retorno más alto de ANS1901I fue 0.

Enlaces relacionados para realizar copias de seguridad de máquinas virtuales Hyper-V

- Detail
- Domain.vmfull
- Mbojrefreshtresh
- Mbpctrefreshtresh
- Mode
- Query VM
- Restore VM
- Vmbackdir
- Vmbackuptype




 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Cancel Process

---

El mandato cancel process visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.

Desde la lista, el usuario de administración puede seleccionar el proceso que desea cancelar. El privilegio de propietario cliente es una autorización suficiente para poder cancelar los procesos de copia de seguridad de imagen o restauración NAS seleccionados.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

---

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Este mandato sólo es válido para los clientes AIX, Linux, y Solaris.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

---

```
>>-Cancel Process-----><
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

Tarea

Cancelar los procesos de copia de seguridad de imagen o restauración NAS actuales.

**Mandato:** cancel process


## Cancel Restore






---

El mandato cancel restore visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor.

Sólo puede cancelar una única sesión de restauración reiniciable al mismo tiempo. Vuelva a ejecutar el mandato cancel restore para cancelar más restauraciones. Para reiniciar sesiones de restauración reiniciables, utilice el mandato restart restore.

Utilice el mandato cancel restore cuando se den las circunstancias siguientes:

- No se puede hacer una copia de seguridad de archivos afectados por una restauración reiniciable.
-  Sistemas operativos Windows Quiere cancelar sesiones de restauración reiniciables.
- Las sesiones de restauración reiniciables bloquean el espacio de archivos del servidor, por lo que los archivos no se pueden traspasar fuera de los volúmenes secuenciales del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Cancel Restore-----<<
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

Tarea

Cancelar una operación de restauración.






```
cancel restore
```

## Delete Access

---

El mandato delete access suprime reglas de autorización para los archivos que están almacenados en el servidor.

Cuando se suprime una regla de autorización, se revoca el acceso de usuario a cualquier archivo o imágenes que se haya especificado en dicha regla.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Delete-- --Access-----<<
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

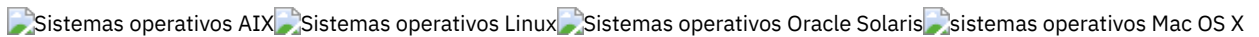
---

Tarea

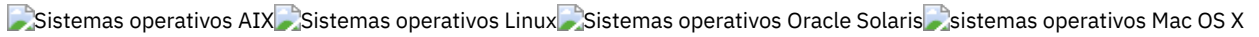
Mostrar una lista de las reglas de autorización actuales y seleccionar las que se deben suprimir.


```
delete access
```

Vea el siguiente ejemplo de pantalla:

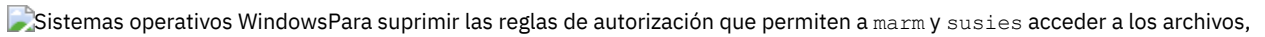


```
Índice Tipo      Nodo      Prop.      Ruta
-----
1      Backup      NODO1     MARTA      home/dev/proja/list/
2      Archive     NODO3     CELIA      home/fin/budg/depta/
3      Backup      NODO4     PILAR      home/plan/exp/deptc/
4      Archive     NODO5     MIGUEL     home/mfg/invn/parta/
Escriba el índice de regla(s) para suprimir, o quit para
cancelar:
```

  
Para suprimir las reglas de autorización que permiten a `luie` y `user2s` acceder a los archivos e imágenes, escriba `2 4` o `2,4` y pulse `Intro`.



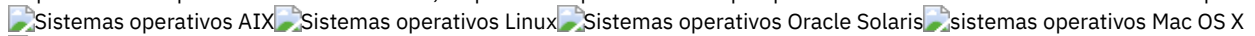

```
Índice Tipo      Nodo      Prop.      Ruta
-----
1      Backup      nodo1     marta     c:\dev\proja\list.c
2      Archive     nodo3     celia     c:\fin\budg\depta.jan
3      Backup      nodo4     pilar     c:\plan\exp\deptc.feb
4      Archive     nodo5     miguel    c:\mfg\invn\parta.wip
Escriba el índice de regla(s) para suprimir, o quit para
cancelar:
```

  
Para suprimir las reglas de autorización que permiten a `marm` y `susies` acceder a los archivos, escriba `2 4` o `2,4`, y pulse `Intro`.

## Delete Archive

El mandato `delete archive` suprime las copias archivadas del almacenamiento del servidor de IBM Spectrum Protect. Su administrador debe concederle la autoridad para suprimir los archivos archivados.

Importante: si suprime archivos archivados, no podrá recuperarlos. Verifique que los archivos están obsoletos antes de suprimirlos.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Delete ARchive--+-+-----+----->
                '- --options-'

>--+- --filespec-----+-----<<
        '- --{--filespecname--}--filespec-'
```

## Parámetros

### filespec


Especifica la vía de acceso y el nombre del archivo que se desea suprimir del almacenamiento. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. También puede utilizar la opción `filelist` para procesar una lista de archivos. El cliente de copia de seguridad y archivado abre el archivo que especifique con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico.

Nota: si indica `filespecname`, no incluya una letra de unidad en la especificación de archivo.

### {filespecname}

Especifica el nombre del espacio de archivos (entre llaves) del servidor que contiene el archivo que se desea suprimir. Es el nombre de la unidad de la estación de trabajo desde la que se archivó el archivo.

Utilice el `filespecname` si el nombre ha cambiado o si desea suprimir copias archivadas de otro nodo cuyas etiquetas de unidad son distintas de las suyas.

 Sistemas operativos Windows Puede especificar un nombre UNC; los nombres de etiqueta de unidad sólo se utilizan para medios extraíbles.










 Sistemas operativos Windows Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. Sólo son válidas las comillas simple en modalidad de bucle. Por ejemplo, {"NTFSDrive"} and {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.









Tabla 1. mandato delete archive: opciones relacionadas

Opción	Dónde se utiliza
dateformat	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
description	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
noprompt	Sólo línea de mandatos.
numberformat	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
pick	Sólo línea de mandatos.
subdir	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.









## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir un archivo denominado budget.









```
dsmc delete archive /user/home/proj1/budget
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir todas las copias archivadas del directorio /user/home/proj1 que tienen la extensión de archivo .txt.



```
dsmc del arch "/user/home/proj1/*.txt"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir todas las copias archivadas del directorio /user/project mediante la utilización de la opción pick para que se visualice una lista de las copias archivadas que coinciden con la especificación de archivo. En esta lista, puede seleccionar las versiones que se desee procesar.



```
dsmc delete archive "/user/project/*" -pick
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir los archivos seleccionados del grupo de copias archivadas que tienen la descripción "Monthly Budgets 2010" y que se encuentran en /user/projects y sus subdirectorios.

```
dsmc delete ar "/user/projects/*" -description="Monthly Budgets 2010" -pick -subdir=yes
```


 Sistemas operativos Windows Tarea  Sistemas operativos Windows  
Suprimir archivos del espacio de archivos abc del directorio proj.

```
dsmc delete archive {"abc"}\proj\*
```

 Sistemas operativos Windows Tarea  Sistemas operativos Windows  
Suprimir un archivo denominado budget.


```
dsmc delete archive c:\plan\proj1\budget.jan
```

## Sistemas operativos Windows Tarea

 Sistemas operativos Windows Suprimir todas las copias archivadas del directorio `c:\plan\proj1` que tienen la extensión de archivo `.txt`.


```
delete archive c:\plan\proj1\*.txt
```

## Sistemas operativos Windows Tarea

 Sistemas operativos Windows Suprimir todas las copias archivadas del directorio `c:\project` mediante la utilización de la opción `pick` para que se visualice una lista de las copias archivadas de coinciden con la especificación de archivo. En esta lista, puede seleccionar las versiones que se desee procesar.

```
dsmc delete archive c:\project\* -pick
```

## Sistemas operativos Windows Tarea

 Sistemas operativos Windows Suprimir los archivos seleccionados del grupo de copias archivadas que tienen la descripción "Monthly Budgets 2013" y que se encuentran en `c:\projects` y sus subdirectorios.

```
dsmc delete ar c:\projects\* -description="Monthly Budgets 2013" -pick -subdir=yes
```





## Delete Backup


---

El mandato `delete backup` suprime archivos, imágenes y máquinas virtuales de las que se ha realizado copia de seguridad en el almacenamiento del servidor de IBM Spectrum Protect. El administrador debe otorgar autorización para suprimir objetos.

Al suprimir archivos, el servidor de IBM Spectrum Protect toma todos los archivos de copia de seguridad que cumplen las opciones `filespec` y `delttype` específicas y las desactiva. El servidor también asigna una fecha de desactivación de *infinite-minus* de forma que los archivos dejan de estar disponibles para la restauración y se depurarán, inmediatamente en la subsiguiente ejecución de caducidad de archivo. El archivo no se elimina físicamente hasta que se ejecuta el proceso de caducidad.

Importante: Después de suprimir las copias de seguridad, no podrá restaurarlas; verifique que los archivos de copia de seguridad ya no sean necesarios antes de suprimirlos. Se le solicitará si desea continuar con la operación de supresión. Si especifica `yes`, los archivos de copia de seguridad especificados se planifican para su supresión y se eliminan del almacenamiento del servidor.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X


 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

 Sistemas operativos Windows

## Sintaxis

---

```
>>-Delete Backup-- +-+-----+-----+-----+-----+----->
                    '+-+filespec-----+-----+-----+-----+-----+'
                    '-{--filespace--}-filespec-'

>-----+-----+-----+-----+-----+----->
| .-objtype=FILE-----+-----+-----+-----+-----+-----|
| '+-----+-----+-----+-----+-----+-----+'
| +-objtype=IMAGE-----+-----+-----+-----+-----+-----+
| '-objtype=VM-----+-----+-----+-----+-----+-----+ vmname-'
| | .-BOTH---. |
| '--FROM --SERVER--+'
| '-LOCAL--'

.-delttype=ACTIVE-----
>-----+-----+-----+-----+-----+-----><
+-+-----+-----+-----+-----+-----+-----+
| '-delttype=INACTIVE-' |
| '+-----+-----+-----+-----+-----+-----+'
| '-delttype=ALL-'
```

## Parámetros

---

*filespace/filespec*

### *filespec*

Especifica la vía de acceso y el nombre del archivo que se desea suprimir del almacenamiento. Para especificar un archivo en otro espacio de archivos, preceda el nombre de archivo con el nombre de espacio de archivos. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Separe las especificaciones de los archivos con un espacio en blanco. También puede utilizar la opción `filelist` para procesar una lista de archivos. El cliente de copia de seguridad y archivado abre el archivo que se ha especificado con esta opción y procesa la lista de archivos que contiene de acuerdo con el mandato específico.

Nota: si indica *filespace*, no incluya una letra de unidad en la especificación de archivo.

Cuando utilice `-deltype=inactive` o `-deltype=active`, haga uso de los caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

Al utilizar `-deltype=all`, especifique un directorio con caracteres comodín.

### *objtype*

Especifica el tipo de objeto que desea eliminar. Puede especificar uno de los valores siguientes:

#### FILE


Especifica que se desea suprimir directorios y archivos. Este valor es el tipo de objeto predeterminado.

#### IMAGE

Especifica que se desea suprimir una copia de seguridad de imagen. Especifica que se desea suprimir una copia de seguridad de imagen. `Objtype=image` no está soportado en Mac OS X.

#### VM *vmname*

Especifica que desea suprimir una o varias versiones de una copia de seguridad de máquina virtual; la máquina virtual se identifica mediante el parámetro variable *vmname*. El nombre de la máquina virtual no puede contener caracteres comodín.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.

Cuando se especifica `objtype=VM`, no se puede utilizar la opción `filelist`. Especificar `objtype=VM` cambia el comportamiento de la opción `-deltype`. Cuando se especifica `objtype=vm`, puede utilizar `-deltype=active` o `-deltype=inactive`. No puede utilizar `-deltype=all`. Al especificar `-deltype=inactive` se muestra una lista de copias de seguridad activas e inactivas. Puede utilizar esta lista para especificar qué copias de seguridad de máquina virtual desea eliminar. Para suprimir copias de seguridad de máquinas virtuales solo activas, utilice `-deltype=active`.

Cuando especifica `-objtype=VM`, este mandato suprime únicamente las copias de seguridad de máquina virtual que se han creado con cualquiera de las siguientes modalidades: FULL, IFINCR e IFFULL. Las copias de seguridad creadas con la modalidad completa o incremental se han creado con el cliente de la versión 7.1 o anterior.

En el caso de copias de seguridad creadas con clientes de la versión 7.1 o anteriores: las copias de seguridad incrementales individuales (copias de seguridad creadas utilizando `MODE=INCR`) que se hayan creado después de ejecutar una copia de seguridad completa no se podrán suprimir con este mandato. Sin embargo, si suprime una copia de seguridad de imagen de máquina virtual completa (creada utilizando `MODE=FULL`), y si el servidor incluye alguna copia de seguridad incremental (`MODE=INCR`) que se creara para esta máquina virtual después de la copia de seguridad completa, al suprimir la copia de seguridad de máquina virtual completa también se suprimen los archivos que se han creado en una copia de seguridad `MODE=INCR`.

Si se suprime una copia de seguridad activa para una máquina virtual, la copia inactiva más reciente pasa a ser la copia de seguridad activa. Si especifica la opción `-pick` o `-inactive`, sólo se suprimirá la copia de seguridad que especifique. Si selecciona una copia de seguridad que se crea mediante `MODE=IFINCR`, sólo se suprimirá la copia de seguridad incremental seleccionada; no se suprimirán otras copias de seguridad incrementales para la máquina virtual.

#### -FROM

Especifica la ubicación o ubicaciones de la copia de seguridad donde se suprimen las copias de seguridad de la máquina virtual. Puede especificar uno de los valores siguientes:

#### SERVER

Las copias de seguridad de máquinas virtuales se suprimen del servidor de IBM Spectrum Protect.

#### LOCAL

Las instantáneas persistentes de máquinas virtuales se suprimen del almacenamiento de hardware.

#### BOTH

Se suprimen las copias de seguridad de máquinas virtuales que se encuentran en el servidor de IBM Spectrum Protect y las instantáneas que se encuentran en el almacenamiento de hardware. Este es el valor predeterminado.

Al especificar este valor, se muestra una lista de ubicaciones de copia de seguridad. En esta lista, puede seleccionar la ubicación de la que desea que se supriman las copias de seguridad de máquina virtual.



## deltypes

Especifica el tipo de supresión. Especifique uno de los valores siguientes:

### ACTIVE

Suprimir sólo los objetos de archivo activos. Los objetos de directorio no se suprimen. Este valor es el tipo de supresión predeterminado.

Nota: Si existe algún objeto inactivo, tras la supresión del objeto activo, el objeto inactivo más actual cambiará de inactivo a activo.

Para suprimir todas las versiones de un archivo, emita en primer lugar el mandato delete backup con `-deltypes=inactive` y, a continuación, especifique el mandato `-deltypes=active`.

### INACTIVE

Suprimir sólo los objetos de archivo inactivos. Los objetos de directorios no se suprimen.

### ALL

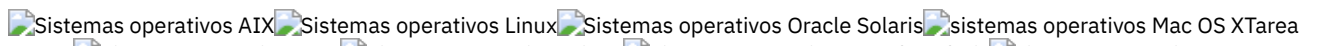
Suprimir todos los objetos activos e inactivos por debajo de un directorio determinado, incluidos todos los subdirectorios y los archivos.

Nota: No se suprime el directorio padre de los archivos y subdirectorios suprimidos. Si especifica `deltypes=ALL`, no puede utilizar la opción pick porque `deltypes=ALL` y la opción pick son mutuamente exclusivos.

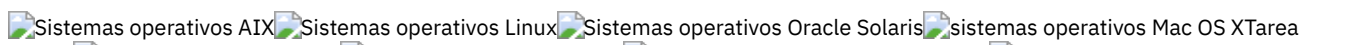
Tabla 1. Mandato Delete Backup: opciones relacionadas

Opción	Dónde se utiliza
description	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
fromdate	Línea de mandatos y en la función de búsqueda de la GUI.
fromtime	Línea de mandatos y en la función de búsqueda de la GUI.
noprompt	Sólo línea de mandatos.
pick	Sólo línea de mandatos.
pitdate	Línea de mandatos y en la función de búsqueda de la GUI.
pittime	Línea de mandatos y en la función de búsqueda de la GUI.
subdir	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
tapeprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
todate	Línea de mandatos y en la función de búsqueda de la GUI.
totime	Línea de mandatos y en la función de búsqueda de la GUI.

## Ejemplos

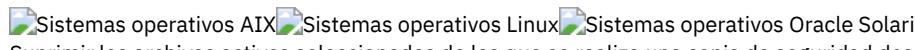
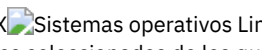
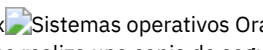
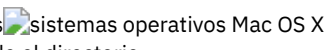
 Suprimir todos los objetos de archivo activos e inactivos denominados budget del directorio /data/plan/proj1.  
Mandatos:

```
delete backup /data/plan/proj1/budget.jan  
-deltypes=inactive  
delete backup /data/plan/proj1/budget.jan  
-deltypes=active
```

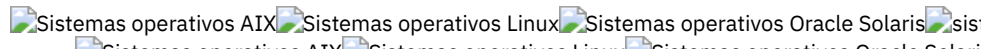
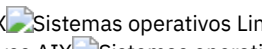
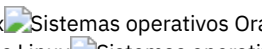
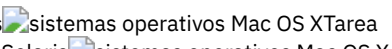
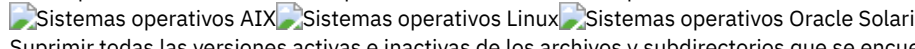
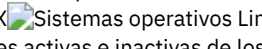
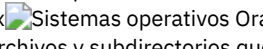
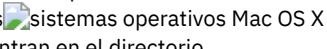
 Suprimir todos los archivos inactivos que tengan una extensión .txt y cuya copia de seguridad se ha realizado desde el directorio /data/plan/proj1 y sus subdirectorios.

Mandato: `delete backup "/data/plan/proj1/*.txt" -deltypes=inactive -subdir=yes`



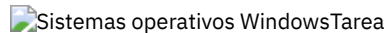
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir los archivos activos seleccionados de los que se realiza una copia de seguridad desde el directorio /home/marymb/project. Utilice la opción -pick para que se visualice una lista de las copias de seguridad que coinciden con la especificación de archivo. En la lista, puede seleccionar qué versiones han de suprimirse.


Mandato: `delete backup "/home/marymb/project/*" -pick`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suprimir todas las versiones activas e inactivas de los archivos y subdirectorios que se encuentran en el directorio /home/storman/myproject. A continuación, suprima todas las versiones activas e inactivas del directorio /user/myproject.

Mandato:

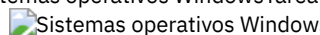
```
delete backup "/home/storman/myproject*"
-deltype=all
```

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir todos los objetos de archivo activos del espacio de archivos abc del directorio proj.

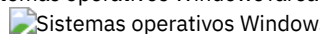
Mandato: `delete backup {abc}\proj\*`

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir todos los archivos inactivos con un nombre que acaba en .txt y cuya copia de seguridad se ha realizado desde el directorio c:\plan\proj1 y sus subdirectorios.

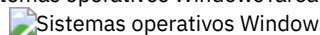
Mandato: `delete backup c:\plan\proj1\*.txt -deltype=inactive -subdir=yes`

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir los archivos activos seleccionados de los que se realiza copia de seguridad desde el directorio c:\project. Utilice la opción -pick para que se visualice una lista de las copias de seguridad que coinciden con la especificación de archivo. En la lista, puede seleccionar qué versiones han de suprimirse.

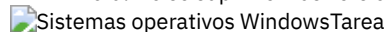
Mandato: `delete backup c:\project\* -pick`


 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir todas las versiones activas e inactivas de los archivos y subdirectorios de c:\user\myproject.

Mandato: `delete backup c:\user\myproject\* -deltype=all`

Nota: No se suprimen las versiones de copia de seguridad del objeto de directorio c:\user\myproject.

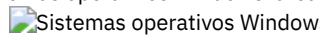
 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir la copia de seguridad activa de una máquina virtual que se denomina vm1.

Mandato: `delete backup -objtype=vm vm1`

Nota: Si existe una o varias de las versiones inactivas de esta copia de seguridad, la más reciente se convertirá en la versión activa.

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsSuprimir una o varias versiones de copia de seguridad de una máquina virtual que se denomina vm\_test.

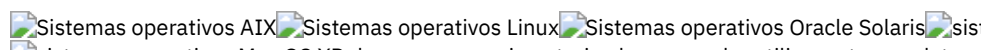
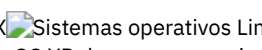
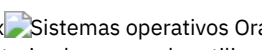
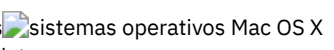
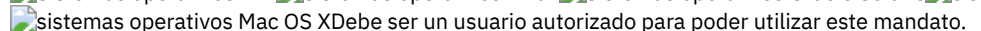
Mandato: `delete backup -objtype=vm -inactive vm_test`

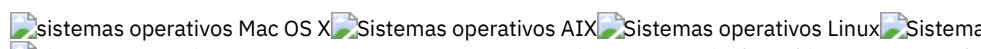
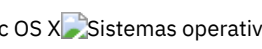
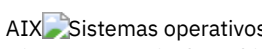
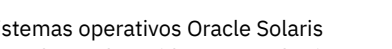
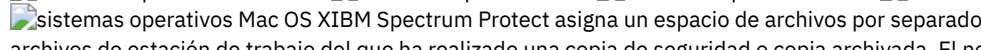
Nota: Todas las versiones de copias de seguridad para este nodo de máquina virtual aparecen en una lista; seleccione las versiones a suprimir.


## Delete Filespace

---

El mandato delete filesystem supprime espacios de archivos del almacenamiento del servidor de IBM Spectrum Protect. Un espacio de archivos es un espacio lógico del servidor que contiene archivos de los que se realizó copia de seguridad o de archivado.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 sistemas operativos Mac OS XDebe ser un usuario autorizado para poder utilizar este mandato.






 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS XIBM Spectrum Protect asigna un espacio de archivos por separado en el servidor para cada sistema de archivos de estación de trabajo del que ha realizado una copia de seguridad o copia archivada. El nombre del espacio de archivos es igual al nombre del sistema de archivos.






 Sistemas operativos Windows IBM Spectrum Protect asigna un espacio de archivos por separado en el servidor para cada sistema de archivos de estación de trabajo del que ha realizado una copia de seguridad o copia archivada. El nombre del espacio de archivos es igual al nombre UNC.

Cuando escribe el mandato delete filespace, se muestra una lista de los espacios de archivos. En dicha lista, seleccione el espacio de archivos que desea suprimir.

El administrador de IBM Spectrum Protect debe otorgar autorización para suprimir un espacio de archivos. Es necesaria una autorización BACKDEL si el espacio de archivos que desea suprimir contiene versiones de copia de seguridad o la autorización ARCHDEL si el espacio de archivos contiene copias archivadas. Si el espacio de archivos contiene ambas, versiones de copia de seguridad y copias archivadas, necesita ambos tipos de autorización.

Importante: cuando se suprime un espacio de archivos, está suprimiendo todas las versiones de copia de seguridad y de copias archivadas que hay en ese espacio de archivos. Cuando suprime un espacio de archivo, **no puede restaurar los archivos**. Verifique que los archivos están obsoletos antes de suprimirlos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows El mandato delete filespace se puede utilizar para suprimir interactivamente espacios de archivos NAS del almacenamiento del servidor. Utilice la opción nasnodename para identificar el nodo del servidor de archivos NAS. Utilice la opción class para especificar la clase del espacio de archivos que se ha de suprimir.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados













































Este mandato es válido para todos los clientes.





## Sintaxis

```
>>-Delete Filespace--+-----+----->>
      '- --options-'
```

## Parámetros

Tabla 1. mandato delete filespace: opciones relacionadas

Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows class	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Sólo línea de mandatos.
detail	Sólo línea de mandatos.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X nasnodename	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema cliente o línea de mandatos.
 Sistemas operativos Windows nasnodename	 Sistemas operativos Windows En el archivo de opciones del cliente o en la línea de mandatos.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrolllines	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema cliente o línea de mandatos.
 Sistemas operativos Windows scrolllines	 Sistemas operativos Windows En el archivo de opciones del cliente o en la línea de mandatos.
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrollprompt	 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema cliente o línea de mandatos.






Opción	Dónde se utiliza
 Sistemas operativos Windows	 Sistemas operativos Windows
 scrollprompt	 Archivo de opciones del sistema cliente o línea de mandatos.






## Ejemplos

### Tarea

Suprimir un espacio de archivos.

**Mandato:** `delete filespace`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

Suprimir los espacios de archivos NAS del servidor de archivos NAS **dagordon** que hay almacenados en el servidor.

**mandato:** `delete filespace -nasnodename=dagordon -class=nas`





## Delete Group

Utilice el mandato `delete group` para suprimir una copia de seguridad de grupo en el servidor de IBM Spectrum Protect.




Después de suprimir un grupo, el líder del grupo (`virtualfsname`) permanece en el servidor de IBM Spectrum Protect. No contiene miembros (archivos ni directorios) pero se notifica en un mandato `query filespace` subsiguiente. No habrá archivos listados si se agrega la opción `showmembers`. Al suprimir un grupo no se suprime el espacio de archivos en el que reside porque es posible que éste contenga otros grupos. Utilice `delete filespace` si desea eliminar el espacio de archivos y todos los datos que contiene.

### Nota:

1. Utilice la opción `inactive` para visualizar las versiones de copia de seguridad de grupo activas y también inactivas. De forma predeterminada, el cliente muestra las versiones activas.
2. Utilice la opción `pick` para seleccionar un grupo específico con el fin de suprimirlo del servidor de IBM Spectrum Protect.
3. Utilice la opción `noprompt` si desea eliminar la solicitud de confirmación que normalmente aparece antes de que suprima una versión de copia de seguridad de grupo. De forma predeterminada, el cliente le solicitará confirmación antes de suprimir la copia de seguridad de grupo. Al utilizar esta opción se acelera el procedimiento de supresión. Sin embargo, también aumenta el riesgo de suprimir accidentalmente una versión de copia de seguridad de grupo que desea guardar. Utilice esta opción con precaución.
4. Utilice el mandato `query filespace` para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Este mandato es válido para todos los clientes UNIX y Linux, a excepción de Mac OS X.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

```
>>-Delete GGroup-- --filespec-+-----+----->>
                        '- --options-'
```

## Parámetros

### filespec

Especifica el nombre del espacio de archivos virtual y el nombre de grupo que desea suprimir del almacenamiento del servidor.

Tabla 1. mandato `delete group`:  
opciones relacionadas

Opción	Dónde se utiliza
--------	------------------

Opción	Dónde se utiliza
inactive	Sólo línea de mandatos.
noprompt	Sólo línea de mandatos.
pick	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.

## Ejemplos

Tarea  
 Suprimir la versión activa actual del grupo /virtfs/group1.

**Mandato:**

```
delete group /virtfs/group1
```

Tarea  
 Suprimir la versión activa actual del grupo virtfs\group1.

**Mandato:**

```
delete group {virtfs}\group1
```

Tarea  
 Suprimir una versión de copia de seguridad del grupo /virtfs/group1 de una lista de versiones activas e inactivas.

**Mandato:**

```
delete group /virtfs/group1 -inactive -pick
```

Tarea  
 Suprimir una versión de copia de seguridad del grupo virtfs\group1 de una lista de versiones activas e inactivas.

**Mandato:**

```
delete group {virtfs}\group1 -inactive -pick
```

## Expire

El mandato expire desactiva los objetos de copia de seguridad que especifica en la especificación de archivos o con la opción filelist. Puede especificar un archivo individual para que caduque, o un archivo que contiene una lista de archivos que caducarán. Si OBJTYPE=VM, este mandato desactivará la copia de seguridad actual para una máquina virtual.

Cuando se trabaja en modalidad interactiva, una solicitud le notificará si los archivos han caducado.

El mandato expire no suprime los archivos de estación de trabajo. Si caduca un archivo o directorio que todavía existe en la estación de trabajo, se vuelve a realizar una copia de seguridad del archivo o directorio de éste en la siguiente copia de seguridad incremental excepto en el caso de que el objeto se excluya mediante un proceso de inclusión/exclusión.

Si caduca un directorio que contiene archivos activos, estos archivos no se muestran en una consulta posterior de la GUI. Sin embargo, estos archivos se muestran en la línea de mandatos, si especifica la consulta correcta con un carácter comodín para el directorio.

Nota:  
Dado que el mandato expire cambia la imagen del servidor del sistema de archivos cliente sin cambiar el sistema de archivos cliente, el mandato expire no está permitido en archivos ubicados en un sistema de archivos que está supervisado por el daemon de registro por diario IBM Spectrum Protect.


Nota: Dado que el mandato expire cambia la imagen del servidor del sistema de archivos cliente sin cambiar el sistema de archivos cliente, el mandato expire no está permitido en archivos ubicados en un sistema de archivos que está supervisado por el servicio de registro por diario IBM Spectrum Protect.


## Clientes soportados

Este mandato es válido para todos los clientes.











Mandato: `expire "/home/letter1.txt"`


 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Desactive el archivo `letter1.txt` del directorio `home`.

Mandato: `expire c:\home\letter1.txt`









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Desactive todos los archivos del directorio `/admin/mydir`.

Mandato: `expire /admin/mydir/*`


 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Desactive todos los archivos del directorio `admin\mydir`.

Mandato: `expire c:\admin\mydir\*`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Desactive todos los archivos que se denominan en el archivo `/home/avi/filelist.txt`.


Mandato: `expire -filelist=/home/avi/filelist.txt`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Desactive todos los archivos que se denominan en el archivo `c:\avi\filelist.txt`.

Mandato: `expire -filelist=c:\avi\filelist.txt`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Desactivar la copia de seguridad actual de la máquina virtual que se denomina `vm_test`.






Mandato: `expire -objtype=VM vm_test`

## Help

---

Utilice el mandato `help` para visualizar información acerca de mandatos, opciones y mensajes.

Consejo: si utiliza el mandato `help` en la línea de mandatos inicial, no se establecerá ningún contacto con el servidor y no se necesitará ninguna contraseña.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Ayuda--+-----+-----><
      +-nombre-mandato [nombre-submandato]-----+
      +-nombre de la opción-----+
      +-número de sección de la tabla de contenido--+
      '-[ANS] número-mensaje-----'
```

Si especifica el mandato `help` sin ningún argumento, la ayuda mostrará toda la tabla de contenido. Ya sea con el mandato inicial o cuando `HELP` muestre un indicador de solicitud, puede especificar los parámetros siguientes.

## Parámetros

---

`nombre-mandato [nombre-submandato]`

Especifica un nombre de mandato y, opcionalmente, un nombre de submandato o su nombre abreviado, por ejemplo: `backup image`, o `b i`. En este caso, la combinación debe ser exclusiva. Los nombres abreviados no exclusivos producen la visualización de la primera sección de todo el archivo de ayuda que coincide con el nombre abreviado. Este parámetro es opcional.

`nombre-opción`

Especifica el nombre de la opción, por ejemplo: `domain` o `do`. Este parámetro es opcional.

número-sección-TOC

Especifica un número de sección de la tabla de contenido, por ejemplo: 1.5.3. Este parámetro es opcional.

[ANS]número-mensaje

Especifica un número de mensaje con o sin su prefijo, por ejemplo: ans1036 o 1036. Este parámetro es opcional. El código de gravedad no es nunca necesario. Si introduce ans1036E obtendrá como resultado "respuesta no encontrada".

Importante: Si especifica argumentos que no se ajusten a estas descripciones, puede provocar que se visualicen resultados no esperados (o ningún resultado). Si introduce más de dos argumentos, se rechazará su solicitud de ayuda. Cuando un nombre de mandato y un nombre de opción coinciden, por ejemplo: incremental (mandato) e incremental (opción), puede obtener ayuda sobre la opción mediante la especificación del número de sección de la tabla de contenido.

El texto de la ayuda solicitada se visualizará en una o más secciones, en función del número de líneas de visualización disponibles en la ventana del mandato. Cuando se muestran suficientes líneas para llenar el espacio de visualización, o cuando se muestre el final del texto de la ayuda solicitada, verá un indicador de solicitud junto con instrucciones sobre lo que se puede especificar en este indicador de solicitud. Para continuar visualizando el texto para la selección actual, pulse Intro o la tecla 'd' para desplazarse hacia abajo. Para desplazarse hacia arriba en la selección actual, pulse la tecla 'u' e Intro. Es posible que se presenten otras opciones, por lo que debe leer las instrucciones del indicador de solicitud.

La visualización correcta del texto de ayuda requiere un ancho de pantalla utilizable de 72 caracteres. Una anchura de visualización menor de 72 caracteres hace que las frases que tienen 72 caracteres de ancho se pasen a la línea siguiente. Esto puede hacer que el texto de ayuda desplegado comience en algún lugar dentro de la sección en lugar de al principio. Se pueden visualizar las líneas no desplegadas utilizando la función de desplazamiento del terminal para moverse hacia arriba.

## Ejemplos

---

Tarea

Visualizar la tabla de contenido de los temas de ayuda.

**Mandato:** `dsmc help`

Tarea

Visualizar la información en el tema de la ayuda 2.1.2

**Mandato:** `dsmc help 2.1.2`

Tarea

Visualizar información de ayuda sobre el mandato archive.

**Mandato:** `dsmc help archive`

Tarea

Visualizar información de ayuda sobre el mensaje ANS1036.






**Mandato:** `dsmc help 1036`

**Mandato:** `dsmc help ANS1036`


## Incremental

---






El mandato incremental realiza la copia de seguridad de todos los datos nuevos o modificados de las ubicaciones que especifique, a menos que los excluya de los servicios de copia de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Puede realizar una copia de seguridad de todos los archivos o directorios nuevos o cambiados del dominio del cliente predeterminado o de los sistemas de archivos, directorios o archivos.

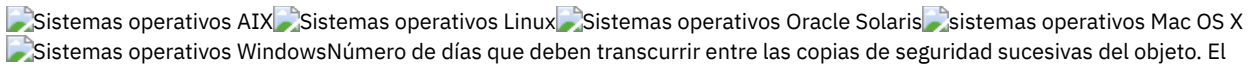
Para hacer copias de seguridad incrementales de archivos o directorios seleccionados, proporcione la especificación de archivo en el mandato. Si no proporciona una especificación de archivo, el valor predeterminado es realizar una copia de seguridad de los archivos o directorios del dominio predeterminado.

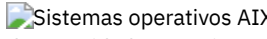
 Sistemas operativos AIX Sólo AIX: puede activar la copia de seguridad incremental basada en instantáneas mediante la utilización de la opción `snapshotproviderfs=JFS2`.


Los siguientes atributos de la clase de gestión asignada al archivo o directorio determinan si se va a realizar la copia de seguridad de los datos:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Frecuencia



 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows. Número de días que deben transcurrir entre las copias de seguridad sucesivas del objeto. El atributo frequency sólo se aplica a una copia de seguridad incremental completa.

 Sistemas operativos AIX, Sistemas operativos Linux. Este atributo de clase de gestión no se tiene en cuenta durante una copia de seguridad con registro por diario.

 Sistemas operativos Windows. Este atributo de clase de gestión no se tiene en cuenta durante una copia de seguridad con registro por diario.

#### Modalidad

Especifica si los cambios desde la última operación de copia de seguridad afectan al procesamiento. Si `mode=modified`, solo se procesan los objetos que han cambiado desde la última operación de copia de seguridad. Si `mode=absolute`, se procesan todos los objetos, independientemente de si el objeto ha cambiado desde la última operación de copia de seguridad.

Si la modalidad del grupo de copia está establecida en modificada, puede alterarse temporalmente mediante la opción `absolute` del cliente. Para obtener más información sobre la opción `absolute`, consulte `Absolute`.


#### Serialización

Permite o deniega la copia de seguridad de archivos o directorios en función los valores siguientes:

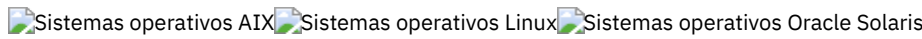
- **estática:** para que se haga copia de seguridad de los mismos, los datos no deben haberse modificado durante la copia de seguridad o archivado.
- **Estática compartida:** si los datos del archivo o del directorio se modifican durante cada uno de los intentos permitidos de incluirlos en una operación de copia de seguridad o de archivado, no se incluyen. El valor de la opción `changingretries` determina el número de intentos realizados. El valor predeterminado es 4.
- **Dinámica:** el objeto se incluye en la operación de copia de seguridad o de archivado en el primer intento, sin tener en cuenta si los datos se modifican durante el proceso.
- **Dinámica compartida:** el objeto se incluye en la operación de copia de seguridad o de archivado en el último intento, aunque los datos se modifiquen durante el proceso.


Utilizando la opción `include` de la lista de inclusión/exclusión puede modificar la clase de gestión predeterminada para un archivo o grupo de archivos.

Puede realizar una copia de seguridad incremental completa o una copia de seguridad incremental por fecha. El valor predeterminado es una operación de copia de seguridad incremental completa.

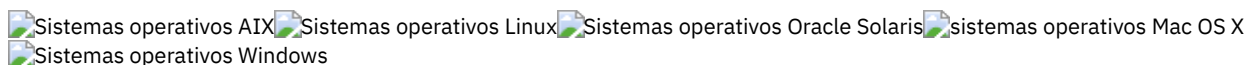
 Sistemas operativos AIX, Sistemas operativos Windows, Sistemas operativos Linux. Si está registrando por diario un sistema de archivos y el diario es válido, la copia de seguridad incremental completa realizará una copia de seguridad con registro por diario. Puede iniciarse más de una sesión de copia de seguridad con registro por diario, pero sólo puede continuar una de las sesiones. Todas las demás sesiones de copia de seguridad con registro por diario que necesiten acceso al mismo espacio de archivos deben esperar hasta que la sesión actual de copia de seguridad con registro por diario haya finalizado antes de que la siguiente sesión pueda continuar. Es posible realizar una copia de seguridad incremental completa sin diario utilizando la opción `nojournal`.

También puede utilizar el mandato `selective` para llevar a cabo una copia de seguridad que sólo realizará la copia de seguridad de los archivos, directorios o directorios vacíos especifique, con independencia de si se habían modificado.





































































 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X. Una copia de seguridad incremental completa hace copia de seguridad de todos los archivos y directorios que sean nuevos o que hayan sido modificados desde la última copia de seguridad incremental. Durante una copia de seguridad incremental completa, el cliente consulta al servidor. IBM Spectrum Protect utiliza esta información cuando realiza las siguientes acciones:





























































 Sistemas operativos Windows. Una copia de seguridad incremental completa hace copia de seguridad de todos los archivos y directorios que sean nuevos o que hayan sido modificados desde la última copia de seguridad incremental. Durante la realización de una copia de seguridad incremental completa, el cliente consulta al servidor o a la base de datos de registro por diario. IBM Spectrum Protect utiliza esta información cuando realiza las siguientes acciones:





















- Hacer una copia de seguridad de archivos o directorios nuevos.
- Hacer una copia de seguridad de archivos o directorios cuyo contenido se ha modificado desde la copia de seguridad anterior.
- Marcar las versiones de copia de seguridad inactivas en el servidor para los archivos y directorios que se hayan eliminado de la estación de trabajo.
- Volver a vincular versiones de copia de seguridad con clases de gestión, si se han modificado las asignaciones de la clase de gestión.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows.











Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X changingretries	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo dsm.sys o línea de mandatos.
 Sistemas operativos Windowscompressalways	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compressalways	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windowscompression	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compression	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo dsm.sys de una stanza del servidor o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windowsdetail	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Windows Sólo línea de mandatos.
 Sistemas operativos Linux  Sistemas operativos Windowsdiffsnapshot	 Sistemas operativos Linux  Sistemas operativos Windows Sólo línea de mandatos.
dironly	Sólo línea de mandatos.
 Sistemas operativos Windowsdominio	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dominio	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Sólo archivo dsm.sys o archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X encryptiontype	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.
 Sistemas operativos Windowsencryptiontype	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt).
 Sistemas operativos Windowsencryptkey	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt).
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X encryptkey	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del sistema (dsm.sys) dentro de una stanza de servidor.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.





Opción	Dónde se utiliza
incrbydate	Sólo línea de mandatos.
 Sistemas operativos Windowsmemoryefficientbackup	 Sistemas operativos WindowsEn el archivo de opciones del cliente (dsm.opt), en el servidor o en la línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X memoryefficientbackup	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XArchivo de opciones del usuario cliente (dsm.opt), archivo de opciones del sistema cliente (dsm.sys), servidor o línea de mandatos.
 Sistemas operativos Windowsnojournal	 Sistemas operativos WindowsSólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linuxnojournal	 Sistemas operativos AIX  Sistemas operativos LinuxSólo línea de mandatos.
 Sistemas operativos Windowspostsnapshotcmd	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X preservelastaccessdate	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XArchivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windowspreservelastaccessdate	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windowspresnapshotcmd	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS Xremoveoperandlimit	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS XSólo línea de mandatos.
 Sistemas operativos Windowsresetarchiveattribute	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt).
 Sistemas operativos Windowsskipntpermissions	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windowsskipntsecuritycrc	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Linux  Sistemas operativos Windowssnapdiff	 Sistemas operativos Linux  Sistemas operativos WindowsSólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linuxsnapshotcachesize	 Sistemas operativos AIX  Sistemas operativos LinuxArchivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Windowssnapshotproviderfs	 Sistemas operativos AIX  Sistemas operativos WindowsArchivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.
 Sistemas operativos Windowssnapshotproviderimage	 Sistemas operativos WindowsArchivo de opciones del cliente (dsm.opt) o con la opción include.image.
snapshotroot	Sólo línea de mandatos.

Opción	Dónde se utiliza
 Sistemas operativos Windows subdir	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X subdir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows tapeprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X tapeprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.



## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Ejecutar una copia de seguridad incremental del dominio de cliente que se ha especificado en el archivo de opciones de usuario del cliente (dsm.opt).


```
Incremental
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Ejecutar una copia de seguridad incremental que haya una copia de seguridad de todos los archivos del dominio, con independencia de si éstos se han modificado desde la última copia de seguridad.



```
Incremental -absolute
```

 Sistemas operativos Windows  
 Sistemas operativos Windows  
Ejecutar una copia de seguridad incremental del dominio de cliente predeterminado que se ha especificado en el archivo de opciones del cliente (dsm.opt).



```
Incremental
```

 Sistemas operativos Windows  
Ejecutar una copia de seguridad incremental del dominio que se ha especificado en el archivo de opciones de usuario del cliente. Si se añade la opción -absolute, se impone una copia de seguridad de todos los archivos del dominio, aunque no se hayan modificado desde la última copia de seguridad incremental.









```
Incremental -absolute
```

 Sistemas operativos Windows  
 Sistemas operativos Windows  
Ejecutar una copia de seguridad incremental de las unidades C, D y E.









```
incremental c: d: e:
```

 Sistemas operativos Windows  
 Sistemas operativos Windows  
Ejecutar una copia de seguridad incremental del directorio \home\ngai y de su contenido en la unidad actual.

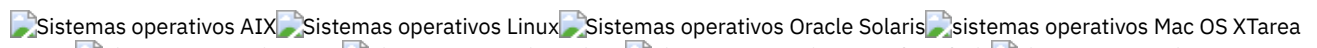
```
i \home\ngai\
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Ejecutar una copia de seguridad incremental para los sistemas de archivos /home, /usr y /proj.

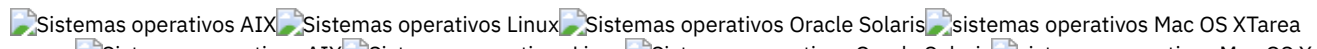
```
Incremental /home /usr /proj
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Ejecutar una copia de seguridad incremental para el directorio /proj/test.

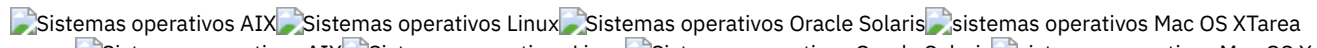
```
Incremental /proj/test/
```

 Ejecutar una copia de seguridad incremental por fecha para el sistema de archivos /home.

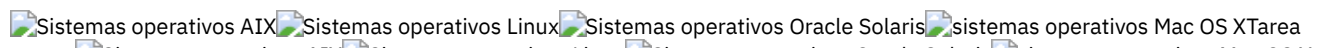
```
Incremental -incrbydate /home
```

 Ejecutar una copia de seguridad incremental del archivo abc en el directorio /fs/dir1.

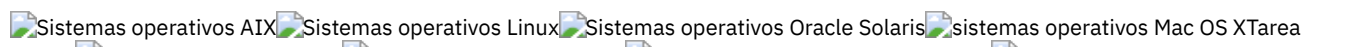
```
Incremental -subdir=yes /fs/dir1/abc
```

 Ejecutar una copia de seguridad incremental del objeto de directorio /fs/dir1, pero no de los archivos del directorio /fs/dir1.


```
Incremental /fs/dir1
```

 Ejecutar una copia de seguridad incremental del objeto de directorio /fs/dir1, de todos los archivos del directorio fs/dir1 y de todos los archivos y subdirectorios de /fs/dir1.


```
Incremental -subdir=yes /fs/dir1/
```

 Ejecutar una copia de seguridad incremental, dándose por supuesto que ha iniciado una instantánea del sistema de archivos /usr y que ha montado la instantánea como /snapshot/day1, de todos los archivos y directorios de la instantánea local y gestionar éstos en el servidor de IBM Spectrum Protect, en el nombre de espacio de archivos /usr.


```
dsmc inc /usr -snapshotroot=/snapshot/day1
```

 Suponiendo que haya iniciado una instantánea de la unidad C y que haya montado la instantánea como \\florence\c\$\snapshots\snapshot.0, ejecute una copia de seguridad incremental de todos los archivos y directorios de la instantánea local y gestiónelos en el servidor de IBM Spectrum Protect en el nombre de espacio de archivos de la unidad C:\.


```
dsmc inc c: -snapshotroot=\\florence\c$\snapshots\snapshot.0
```

 Ejecutar una copia de seguridad incremental para el sistema de archivos /home utilizando la opción snapdiff y especificar la opción para crear la instantánea de diferencias. En el siguiente ejemplo, /home representa el punto de montaje de NFS para un volumen de archivador de NAS/N-Series.


```
incremental /home -snapdiff -diffsnapshot=create
```

 Ejecutar una copia de seguridad incremental del sistema de archivos /proj mediante la opción snapdiff. Especificar la opción para utilizar la instantánea más reciente en el archivador como la instantánea de diferencia. En el siguiente ejemplo, /proj representa el punto de montaje de NFS para un volumen de archivador de NAS/N-Series.






```
incremental /proj -snapdiff -diffsnapshot=latest
```

 Ejecutar una copia de seguridad incremental snapdiff a partir de una instantánea tomada de una unidad compartida de red //homestore.example.com/vol1 montada en la unidad H, donde homestore.example.com es un servidor de archivos.

```
incremental -snapdiff H:
```

 Ejecutar una copia de seguridad incremental snapdiff a partir de una instantánea tomada de una unidad compartida de red //homestore.example.com/vol1 montada en la unidad H, donde homestore.example.com es un servidor de archivos. El valor de la opción -diffsnapshot de LATEST significa que la operación utiliza la última instantánea (la instantánea activa) para el volumen H.

```
incremental -snapdiff H: -diffsnapshot=LATEST
```

-  Sistemas operativos Windows Soporte de archivos abiertos  
Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).
-  Sistemas operativos Windows Copia de seguridad con registro por diario  
Si se ha instalado y está en ejecución el servicio de motor de registro por diario, el mandato incremental, de forma predeterminada, realizará una copia de seguridad con registro por diario en los sistemas de archivos que supervisa el servicio de motor de registro por diario.
-  Sistemas operativos AIX  Sistemas operativos Linux Copia de seguridad con registro por diario  
Una copia de seguridad de un sistema de archivos concreto se basa en registro por diario cuando el daemon de registro por diario de IBM Spectrum Protect se instala y se configura para registrar por diario el sistema de archivos y se ha establecido un registro por diario válido.
- Copia de seguridad de puntos de montaje de volúmenes NTFS o ReFS  
Si realiza una copia de seguridad incremental de un sistema de archivos en el que existe un punto de montaje de volumen, IBM Spectrum Protect realiza una copia de seguridad del directorio (punto de unión) en el que está montado el volumen, pero no recorre los datos del volumen montado ni realiza una copia de seguridad de éstos.
-  Sistemas operativos Windows Copia de seguridad de la raíz Dfs de Microsoft  
Si realiza una copia de seguridad incremental de la raíz de Dfs de Microsoft especificando `dfsbackupmntpnt=yes`, el cliente de copia de seguridad y archivado sólo realizará la copia de seguridad de los puntos de unión, *no* del subárbol situado debajo de los puntos de unión.
- Incremental por fecha  
Una copia de seguridad incremental por fecha realiza copia de seguridad de los archivos nuevos o modificados cuya fecha de modificación sea posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que los archivos se excluyan de la copia de seguridad mediante una sentencia **exclude**.
- Asociación de una instantánea local a un espacio de archivos del servidor  
Utilice la opción `snapshotroot` con el mandato incremental junto con una aplicación suministrada por otro proveedor que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

 Sistemas operativos Windows

## Soporte de archivos abiertos

---

Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).

Utilice VSS como el proveedor de instantáneas; establezca `snapshotproviderimage` o `snapshotproviderfs` en VSS.

Nota:

1. Puede utilizar la opción `include.fs` para establecer opciones de instantánea para cada sistema de archivos.
2. El soporte de archivos abiertos solo se admite en volúmenes fijos locales, (montados en letras de unidad o en puntos de montaje de volúmenes) con formato de sistemas de archivos NTFS. Este soporte incluye los volúmenes conectados con la SAN que satisfacen estos requisitos.
3. Si el cliente no puede crear una instantánea, se produce una recuperación de error en una copia de seguridad no OFS; el mismo soporte de copia de seguridad se realiza si la característica OFS no estuviera configurada.
4. Para activar el soporte de archivos abiertos en un entorno de clúster, todos los sistemas del clúster deberán tener configurada la característica OFS.

 Sistemas operativos Windows

## Copia de seguridad con registro por diario

---

Si se ha instalado y está en ejecución el servicio de motor de registro por diario, el mandato incremental, de forma predeterminada, realizará una copia de seguridad con registro por diario en los sistemas de archivos que supervisa el servicio de motor de registro por diario.

El cliente de copia de seguridad y archivado no utiliza el recurso del registro por diario propio de los sistemas de archivos NTFS o ReFS de Windows ni de ningún otro sistema de archivos de registro por diario.

El servicio de motor con registro por diario registra cambios de un objeto o de sus atributos en una base de datos de diario. Durante una copia de seguridad con registro por diario, el cliente obtiene una lista de archivos que pueden utilizarse para realizar la copia de seguridad de la base de datos de diario. Si se realizan copias de seguridad con regularidad, se mantiene el tamaño del registro por diario.

Una copia de seguridad con registro por diario puede aumentar el rendimiento de la operación de copia de seguridad. Con una copia de seguridad con registro por diario, el cliente no explora el sistema de archivos local ni obtiene información del servidor para determinar los archivos que debe procesar. La copia de seguridad con registro por diario también reduce el tránsito en la red entre el cliente y el servidor.

El cliente filtra la lista utilizando la lista de inclusión/exclusión actual. IBM Spectrum Protect procesa, caduca y actualiza los archivos resultantes según las restricciones de política, como por ejemplo la serialización. El atributo de frecuencia de copia de clase de gestión se pasa por alto en la copia de seguridad con registro por diario.

El servicio de motor de registro por diario excluye archivos del sistema específicos (archivo de páginas, registro, etc.) para que los cambios no se registren en el registro por diario. Como los cambios de estos archivos no se registran por diario, el cliente no hace una copia de seguridad de estos archivos. Consulte el archivo de configuración del servicio de diario tsmjbbd.ini que se encuentra en el directorio de instalación del cliente de copia de seguridad y archivado para ver los archivos del sistema específicos que se excluyen.

Para dar soporte a la copia de seguridad con registro por diario, debe instalar el servicio de motor con registro por diario. Instale este servicio mediante la utilización del mandato dsmcutil o del asistente para la instalación de la GUI.

Si la especificación de archivo del mandato incremental es un espacio de archivos, el cliente procesará cualquier entrada de diario para el espacio de archivos. El cliente procesa del mismo modo los directorios y especificaciones de archivo que contienen caracteres comodín. Si no define ninguna especificación de archivo, el cliente utiliza la lista de dominios.

Nota: Es posible que la copia de seguridad con registro por diario no se realice como la copia de seguridad incremental tradicional si el dominio de políticas de su nodo se ha modificado en el servidor, dependiendo de cuándo se ha actualizado por última vez el juego de políticas de su dominio y de la fecha de la última copia de seguridad incremental. En este caso, deberá forzar una copia de seguridad incremental completa del modo tradicional para volver a vincular los archivos con el dominio nuevo. Utilice la opción nojournal con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional, en lugar de la copia de seguridad basada en el registro por diario predeterminada.

Cuando un usuario suprime un archivo con un nombre largo, el sistema operativo Windows puede ofrecer un nombre corto (comprimido) al servicio de motor con registro por diario. Después de haberse suprimido el objeto, el nombre comprimido podrá volver a utilizarse y el aviso de supresión ya no podrá identificar a un objeto exclusivo. Durante una copia de seguridad incremental con diario, dará error el intento de caducidad del archivo porque el servidor desconoce el nombre comprimido. Cuando se produce este error, se coloca un registro en el diario que indica que el directorio actual no está representado exactamente en el servidor. Utilice la opción incrthreshold para especificar qué acción se ha de llevar a cabo cuando suceda esto.

La base de datos de diario se considera no válida y el cliente recupera la copia de seguridad incremental completa tradicional cuando se produce alguno de estos sucesos:

- Se ha modificado el nombre del espacio de archivos registrado por diario.
- El nombre de un nodo cliente cambia.
- El cliente se pone en contacto con un servidor distinto para realizar la copia de seguridad.
- Se ha modificado una política (activación de un nuevo conjunto de políticas).
- El diario está dañado (condición de falta de espacio, error de disco).
- El servicio de diario no funciona.
- El servicio de diario se ha detenido o se ha iniciado por cualquier motivo, incluso si se reinicia porque se reinicia el sistema.

La copia de seguridad con registro por diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- IBM Spectrum Protect no impone frecuencias de copia no predeterminadas (distintas de 0).
- Si se realizan cambios en los atributos de un objeto, es necesario realizar una copia de seguridad del objeto completo.

Puede utilizar la opción nojournal con el mandato incremental para especifica que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario que se realiza de forma predeterminada.


Es posible disponer de varias sesiones de copia de seguridad con registro por diario.

 Sistemas operativos AIX  Sistemas operativos Linux


## Copia de seguridad con registro por diario

---

Una copia de seguridad de un sistema de archivos concreto se basa en registro por diario cuando el daemon de registro por diario de IBM Spectrum Protect se instala y se configura para registrar por diario el sistema de archivos y se ha establecido un registro por diario válido.

 Sistemas operativos AIX La copia de seguridad basada en registro por diario se admite en clientes de copia de seguridad/archivado AIX para sistemas de archivos JFS y JFS2.



 Sistemas operativos Linux La copia de seguridad basada en el diario se admite en el cliente de archivado y copia de seguridad Linux en Ext2, Ext3, Ext4; XFS, ReiserFS, JFS, VxFS y NSS. GPFS no se admite para las copias de seguridad basadas en el diario en Linux.

Si se ha instalado y está en ejecución el daemon de registro por diario, el mandato incremental, de forma predeterminada, realizará una copia de seguridad con registro por diario en los sistemas de archivos que supervisa el daemon de motor de registro por diario. Se deben cumplir las condiciones siguientes para que se efectúe satisfactoriamente una copia de seguridad basada en registro por diario:

- Se debe configurar el daemon de registro por diario para que supervise el sistema de archivos que contiene los archivos y directorios de los que se hace una copia de seguridad.
- Una copia de seguridad incremental completa debe haberse ejecutado satisfactoriamente al menos una vez en el sistema de archivos del que se hace una copia de seguridad.
- Un mandato administrativo no puede haber modificado la imagen del espacio de archivos del sistema de archivos en el servidor desde la última copia de seguridad completa incremental.
- La política de gestión de almacenamiento para los archivos de los que se hace copia de seguridad no se puede haber actualizado desde la última copia de seguridad incremental completa.

El daemon de registro por diario registra en una base de datos de diario los cambios que se han producido en un objeto o en sus atributos. Durante una copia de seguridad con registro por diario, el cliente obtiene una lista de archivos que pueden utilizarse para realizar la copia de seguridad de la base de datos de diario. La copia de seguridad con registro por diario puede aumentar el rendimiento de la copia de seguridad porque el cliente no explora el sistema de archivos local ni se pone en contacto con el servidor para determinar qué archivos se deben procesar. La copia de seguridad con registro por diario también reduce el tránsito en la red entre el cliente y el servidor.


El cliente de copia de seguridad y archivado filtra la lista basándose en la lista de exclusión/inclusión actual y procesa, caduca y actualiza los archivos resultantes según las restricciones de política, como por ejemplo la serialización. Sin embargo, el cliente ignora el atributo de frecuencia del servidor durante una copia de seguridad con registro por diario. El motivo de esto es que una copia de seguridad con registro por diario elimina la consulta de la versión de la copia de seguridad al servidor; por ello, el cliente no sabe cuántos días han pasado desde la última copia de seguridad del archivo.

El daemon de registro por diario no registra los cambios en los archivos especiales de UNIX.

El daemon de registro por diario excluye archivos específicos del sistema para que los cambios no se registren en el registro por diario. Como los cambios de estos archivos no se registran por diario, el cliente no hace una copia de seguridad de estos archivos. Consulte el archivo de configuración del daemon de diario `tsmjbbd.ini` que se encuentra en el directorio de instalación del cliente de copia de seguridad y archivado para ver los archivos específicos del sistema que se excluyen.

Nota:

1. Al utilizar un programa antivirus, hay limitaciones en la copia de seguridad con registro por diario. Algunos programas antivirus pueden generar incorrectamente notificaciones de cambios en el servicio de diario de IBM Spectrum Protect, lo que hace que se produzcan anomalías en el proceso de la copia de seguridad basada en el registro por diario de los archivos que no se han modificado. Para evitar estos problemas, utilice Norton Anti-Virus Corporate Edition 8.0 y superior.
2. Es posible que una copia de seguridad con registro por diario no se realice como la copia de seguridad incremental tradicional si el dominio de políticas de su nodo se ha modificado en el servidor. Esto depende de cuándo se ha actualizado por última vez el juego de políticas de su dominio y de la fecha de la última copia de seguridad incremental. En este caso, deberá forzar una copia de seguridad incremental completa del modo tradicional para volver a vincular los archivos con el dominio nuevo. Utilice la opción `nojournal` con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario predeterminada.

 Sistemas operativos AIX Añada una sentencia de instantánea de exclusión al archivo `tsmjbbd.ini` para AIX 6.1 (o posterior) para evitar que el daemon de copia de seguridad basada en el diario supervise los directorios de instantánea interna JFS2. Si excluye los directorios de instantáneas, los archivos en ellos serán incluidos en la copia de seguridad Copiar los directorios de instantánea es redundante y desperdicia espacio de servidor.

En las siguientes situaciones, cuando la base de datos de diario no es válida y el cliente realiza la copia de seguridad incremental completa tradicional:


- Se ha modificado el nombre del espacio de archivos registrado por diario.
- Se ha modificado el nombre del nodo cliente.
- El cliente se pone en contacto con un servidor distinto para que haga la copia de seguridad.
- Se han producido modificaciones en la política (se ha activado un nuevo juego de políticas).
- El diario está dañado (condición de falta de espacio, error de disco).
- El diario no funciona.

La copia de seguridad con registro por diario se diferencia de la copia de seguridad incremental completa tradicional en los siguientes aspectos:

- IBM Spectrum Protect no fuerza frecuencias de copia no establecidas de forma predeterminada (distintas de 0).

- Los cambios realizados en archivos especiales de UNIX no se detectan.

Puede utilizar la opción `nojournal` con el mandato incremental para especifica que desea realizar una copia de seguridad incremental completa tradicional en lugar de la copia de seguridad con registro por diario que se realiza de forma predeterminada.

 Sistemas operativos Windows

## Copia de seguridad de puntos de montaje de volúmenes NTFS o ReFS

Si realiza una copia de seguridad incremental de un sistema de archivos en el que existe un punto de montaje de volumen, IBM Spectrum Protect realiza una copia de seguridad del directorio (punto de unión) en el que está montado el volumen, pero no recorre los datos del volumen montado ni realiza una copia de seguridad de éstos.

Por ejemplo, si `C:\mount` es un punto de montaje, una copia de seguridad incremental de la unidad `C:\` realiza una copia de seguridad sólo del punto de unión (`C:\mount`), y no de los datos en `C:\mount`.

- Copia de seguridad de datos en volúmenes montados NTFS o ReFS  
Realizar la copia de seguridad de un volumen desde un punto de montaje es especialmente útil para los volúmenes que no tienen asignada una letra de unidad. Si la letra de unidad también puede hacer referencia al volumen montado en el punto de montaje, no tiene que realizarse la copia de seguridad del volumen sobre el punto de montaje.

### Conceptos relacionados:

Restauración de puntos de montaje de volúmenes NTFS o ReFS

Restauración de datos en volúmenes montados NTFS

Copia de seguridad de datos en volúmenes montados NTFS o ReFS

 Sistemas operativos Windows

## Copia de seguridad de la raíz Dfs de Microsoft

Si realiza una copia de seguridad incremental de la raíz de Dfs de Microsoft especificando `dfsbackupmntpnt=yes`, el cliente de copia de seguridad y archivado sólo realizará la copia de seguridad de los puntos de unión, *no* del subárbol situado debajo de los puntos de unión.


Si desea recorrer el árbol de Dfs y realizar la copia de seguridad de los archivos y subdirectorios de cualquier punto de unión que éste encuentre, especifique la opción `dfsbackupmntpnt=no`. Si desea realizar la copia de seguridad de la estructura de árbol de Dfs y de los datos contenidos en el árbol de Dfs, deberá ejecutar dos copias de seguridad: una con `dfsbackupmntpnt=yes` y otra con `dfsbackupmntpnt=no`.





Esta opción no tiene efecto si está realizando copia de seguridad de puntos de unión individuales. El comportamiento de la opción **`exclude.dir`** para los puntos de unión Dfs es igual al de los volúmenes virtuales montados.

Nota: Si se agrega o modifica una raíz de DFS, el cliente no realizará la copia de seguridad de la misma. Debe especificar la raíz de DFS en la opción `domain` del archivo de opciones del cliente (`dsm.opt`) independientemente de si se ha especificado `DOMAIN ALL-LOCAL`.

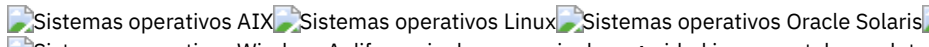
## Incremental por fecha

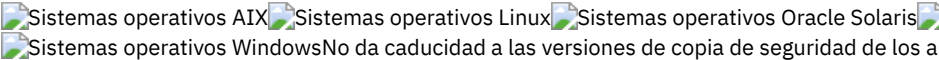
Una copia de seguridad incremental por fecha realiza copia de seguridad de los archivos nuevos o modificados cuya fecha de modificación sea posterior a la fecha de la última copia de seguridad incremental almacenada en el servidor, a menos que los archivos se excluyan de la copia de seguridad mediante una sentencia **`exclude`**.

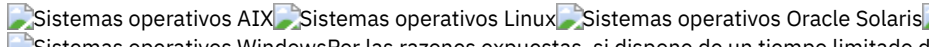
 Sistemas operativos Windows Si se ejecuta una copia incremental por fecha sólo en parte de un sistema de archivos, no se actualizará la fecha de la última copia incremental completa, y la próxima copia incremental por fecha volverá a efectuar copia de seguridad de estos archivos. Utilice el mandato `query filespace` para determinar la fecha y la hora de la última copia de seguridad incremental de todo el sistema de archivos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si se ejecuta una copia incremental por fecha sólo en parte de un sistema de archivos, no se actualizará la fecha de la última copia incremental completa, y la próxima copia incremental por fecha volverá a efectuar copia de seguridad de estos archivos. Los cambios en las listas de control de accesos (ACL) o en los atributos ampliados no hacen que se lleven a cabo copias de seguridad de los archivos durante una copia de seguridad incremental por fecha. Utilice el mandato `query filespace` para determinar la fecha y la hora de la última copia de seguridad incremental de todo el sistema de archivos.

Para realizar una copia de seguridad incremental por fecha, utilice la opción `incrbydate` con el mandato incremental.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows. A diferencia de una copia de seguridad incremental completa, una copia de seguridad incremental por fecha no conserva el almacenamiento del servidor actual de *todos* los archivos de la estación de trabajo por los motivos siguientes:

-  Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows. No da caducidad a las versiones de copia de seguridad de los archivos que se han suprimido de la estación de trabajo.
- No revincula versiones de copia de seguridad con una nueva clase de gestión si ésta ha cambiado.
- No efectúa copias de seguridad de archivos cuyos atributos han cambiado, a no ser que se hayan modificado también la fecha y la hora.
- No tiene en cuenta el atributo de frecuencia de grupo de copia de las clases de gestión.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows. Por las razones expuestas, si dispone de un tiempo limitado durante la semana para realizar las copias de seguridad, pero dispone de tiempo adicional los fines de semana, puede realizar una copia de seguridad incremental por fecha durante la semana y una copia de seguridad incremental completa los fines de semana para conservar el almacenamiento del servidor actual de los archivos de la estación de trabajo.

Si vuelve a emitirse el mandato incremental por haberse producido una anomalía en las comunicaciones o una pérdida de la sesión, las estadísticas de la transferencia visualizarán el número de bytes que el cliente intenta transferir durante todos los intentos de ejecución del mandato. Por ello, es posible que las estadísticas de bytes transferidos no coincidan con las estadísticas de archivos, como las relativas al tamaño de archivo.

## Asociación de una instantánea local a un espacio de archivos del servidor

Utilice la opción `snapshotroot` con el mandato incremental junto con una aplicación suministrada por otro proveedor que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect.

La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.


## Loop

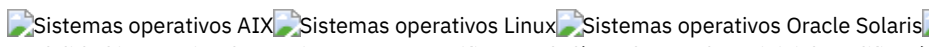
El mandato `loop` inicia una sesión de línea de mandatos interactiva que se mantiene hasta que el usuario escribe `quit`.

Si debe especificar una contraseña, se le solicitará antes de que aparezca el indicador de modalidad de bucle.

Nota: no es posible entrar en modalidad de bucle sin un contacto de servidor. Una de las consecuencias de ello es que algunos mandatos, como `restore backupset -location=file`, sólo se aceptan en la línea de mandatos inicial cuando no hay un servidor válido disponible.





En una sesión de línea de mandatos interactiva, no es necesario que cada nombre de mandato vaya precedido de **dsmc** y la contraseña, si procede.

 Sistemas operativos Windows. En la modalidad interactiva, las opciones que especifique en la línea de mandatos inicial modificarán temporalmente el valor que ha especificado en el archivo de opciones del cliente (`dsm.opt`). Este valor seguirá aplicándose durante toda la sesión interactiva a menos que un valor distinto lo modifique en un mandato interactivo determinado. Por ejemplo, si establece la opción `subdir` en `yes` en el archivo de opciones del cliente (`dsm.opt`) y especifica `-subdir=no` en la línea de mandatos inicial, el valor `-subdir=no` seguirá en vigor durante la totalidad de la sesión interactiva a menos que lo modifique temporalmente mediante el valor `-subdir=yes` en un mandato interactivo determinado. Sin embargo, el valor `subdir=yes` sólo afectará al mandato en el que se especifique éste. Cuando ese mandato se haya completado, el valor volverá a establecerse en `subdir=no`, el valor que tenía al inicio de la sesión interactiva.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X. En la modalidad interactiva, las opciones que especifique en la línea de mandatos inicial modificarán temporalmente el valor que ha especificado en el archivo de opciones de usuario del cliente (`dsm.opt`) o el archivo `dsm.sys`. Este valor seguirá aplicándose durante toda la sesión interactiva a menos que un valor distinto lo modifique en un mandato interactivo determinado. Por ejemplo, si establece la opción `subdir` en `yes` en el archivo de opciones del usuario cliente (`dsm.opt`) y especifica `-subdir=no` en la línea de mandatos inicial, el valor `-subdir=no` seguirá en vigor durante la totalidad de la sesión interactiva a menos que lo modifique temporalmente mediante el valor `-subdir=yes` en un mandato interactivo determinado. Sin embargo, el valor `subdir=yes` sólo afectará al mandato en el que se especifique éste. Cuando ese mandato se haya completado, el valor volverá a establecerse en `subdir=no`, el valor que tenía al inicio de la sesión interactiva.

En la modalidad interactiva, puede especificar todos los mandatos válidos, *excepto* los mandatos `schedule` y `loop`.

Algunas opciones no pueden utilizarse en la sesión interactiva creada por el mandato loop y se indican en la descripción de opciones de la siguiente forma: *Esta opción sólo es válida en la línea de mandatos inicial. No es válida en la modalidad interactiva.*

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota:

1. En la modalidad de bucle, después de una operación de restauración directamente desde cinta, el punto de montaje no se libera por si se realizan solicitudes de restauración adicionales de dicho volumen. Si solicita una operación de copia de seguridad en la misma sesión y dicho punto de montaje es el único que está disponible, la operación de copia de seguridad se interrumpirá con el mensaje siguiente:

```
Esperando a que se monte un medio fuera de línea.
```

En este caso, el punto de montaje no se libera hasta que se cumple una de las siguientes condiciones:

- Se satisface el límite MOUNTRETENTION de la clase de dispositivo.
  - Se satisface el período de inactividad (idletimeout) del cliente.
  - La sesión de bucle dsmc se cierra una vez que ha finalizado la operación de restauración, lo que permite iniciar otra sesión en modalidad de bucle para realizar la operación de copia de seguridad.
2. En la modalidad interactiva, no se puede introducir una especificación de archivo que contenga caracteres específicos del idioma nacional. Si un mandato contiene caracteres de este tipo, procese el mandato en modalidad por lotes, especificando el nombre del programa ejecutable **dsmc** antes del nombre del mandato.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-LOOP-----<<
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---





Tarea





Iniciar una sesión de línea de mandatos interactiva.

**Mandato:** dsmc




En el indicador de mandatos `Protect>`, especifique un mandato.


 Sistemas operativos Windows Para finalizar una sesión interactiva, especifique `quit`.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Existen dos métodos para finalizar una sesión interactiva:

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

- Especifique `quit`.
- Si ha establecido `editor=yes`, puede realizar lo siguiente:
  1. Pulse la tecla de escape (Esc).
  2. Escriba una Q y pulse la tecla Intro.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

 sistemas operativos Mac OS X Nota: El valor predeterminado es `editor=yes`.

Nota: Para interrumpir un mandato dsmc antes de que el cliente haya terminado el proceso, especifique QQ en la consola de IBM Spectrum Protect. En la mayoría de los casos, no en todos, ello interrumpirá el mandato.






## Macro

---

El mandato macro ejecuta una serie de mandatos que se especifican en un archivo de macros.

Mediante la inclusión de los mandatos macro dentro de un archivo de macro, pueden anidarse hasta diez niveles de mandatos.

Las líneas de comentarios no se pueden utilizar en el archivo de macro especificado para el mandato macro.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-MAcro-- --macroname-----<<
```

## Parámetros

---

**nombremacro**  
Especifica el nombre completo del archivo que contiene los mandatos.
















## Ejemplos






---





A continuación, se muestra un ejemplo de cómo utilizar el mandato macro.

### Tarea

Realizar una copia de seguridad selectiva de los archivos de los siguientes directorios:

-  Sistemas operativos Windows c:\devel\project\proja
-  Sistemas operativos Windows c:\devel\project\projb
-  Sistemas operativos Windows c:\devel\project\projc
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X/devel/project/proja
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X/devel/project/projb
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X/devel/project/projc





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows **Mandato:**macro backabc.mac

Donde backabc.mac contiene las sentencias siguientes:  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X

```
Selective /devel/project/proja/  
Selective /devel/project/projb/  
Selective /devel/project/projc/
```

 Sistemas operativos Windows

```
selective c:\devel\project\proja\*.*  
selective c:\devel\project\projb\*.*  
selective c:\devel\project\projc\*.*
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Monitor Process


---


El mandato monitor process visualiza una lista de los procesos actuales de copia de seguridad de imagen y de restauración NAS (si se ha activado el soporte de NDMP) para los que el usuario de administración dispone de autorización. Se le solicitará el ID de administrador de IBM Spectrum Protect.

El usuario de administración puede seleccionar el proceso que desea supervisar. El privilegio de propietario cliente es una autorización suficiente para poder supervisar los procesos de copia de seguridad de imágenes o restauración NAS seleccionados.

## Clientes soportados

---

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris Este mandato sólo es válido para los clientes AIX, Linux, y Solaris.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

---

```
>>-MONitor Process-----<<
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

Tarea

Supervisar los procesos de copia de seguridad de imagen o restauración NAS actuales.

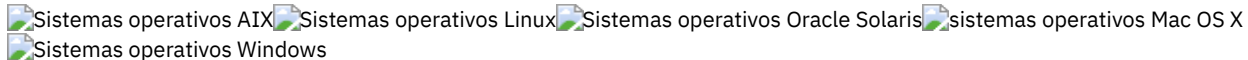
 **Mandato:** monitor process

## Preview Archive

---

El mandato preview archive simula un mandato de copia de seguridad sin enviar los datos al servidor.

El mandato preview genera un archivo de texto delimitado por tabuladores que se puede importar a un programa de hojas de cálculo. La vista preliminar contiene información, por ejemplo, sobre si el archivo está excluido o incluido. Si el archivo está excluido, se mostrará el patrón o motivo por el que se ha excluido el archivo, junto con el origen del patrón.

 Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
                                .- -filter=ALL--.
>>-PREview--Archive--filespec--+ -filter=INCL-+----->
                                '- -filter=EXCL-'
>--+-----+-----+-----+----->
  '- -FILENAME= filename-' '- -CONsole-'
                                .- -TRaverse=Yes-.
>--+-----+-----+-----+----->
  '- -TRaverse=No--'
```

## Parámetros

---

filespec

Especifica la vía de acceso y el nombre del archivo que se desea archivar. Utilice caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio.

-filter

Especifica la salida que se debe visualizar. Puede visualizar objetos incluidos, objetos excluidos o ambos.

ALL

Muestra la salida para los objetos incluidos y excluidos. Éste es el valor predeterminado.

INCLuded

Muestra la salida sólo para los objetos incluidos.

EXCLuded

Muestra la salida sólo para los objetos excluidos.






- FILENAME=
  - Especifica el nombre de archivo en el que se debe grabar la salida delimitada por tabuladores. El valor predeterminado es dsmprev.txt.
- CONsole
  - La salida se graba en la consola y en el archivo.
- TRaverse
  - Previsualiza el directorio actual y sus subdirectorios.
- Yes
  - Previsualiza los directorios actuales y sus subdirectorios. Éste es el valor predeterminado.
- No
  - Sólo previsualiza el directorio actual, sin subdirectorios.

Importante: la especificación de **-traverse** no ofrece una previsualización de los directorios que se han excluido mediante la utilización de la opción `exclude.dir`.

## Previsualizar copia de seguridad

El mandato `preview` simula un mandato de copia de seguridad sin enviar los datos al servidor.

El mandato `preview` genera un archivo de texto delimitado por tabuladores que se puede importar a un programa de hojas de cálculo. La vista preliminar contiene información, por ejemplo, sobre si el archivo está excluido o incluido. Si el archivo está excluido, se mostrará el patrón o motivo por el que se ha excluido el archivo, junto con el origen del patrón.

 Sistemas operativos AIX
  Sistemas operativos Linux
  Sistemas operativos Oracle Solaris
  sistemas operativos Mac OS X
  Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```

      .- -filter=ALL--.
>>-PREview--backup--filespec--+- -filter=INCL+----->
      '- -filter=EXCL-'

>+-----+-----+-----+----->
  '- -FILENAME= filename-' '- -CONsole-'

      .- -TRaverse=Yes-.
>+-----+-----+-----+-----><
  '- -TRaverse=No--'
```

## Parámetros

### filespec

Especifica la vía de acceso y el nombre del archivo del que se desea realizar la copia de seguridad. Utilice caracteres comodín para seleccionar un grupo de archivos o todos los archivos de un directorio.

### -filter

Especifica la salida que se debe visualizar. Puede visualizar objetos incluidos, objetos excluidos o ambos.

#### ALL

Muestra la salida para los objetos incluidos y excluidos. Éste es el valor predeterminado.

#### INCLuded

Muestra la salida sólo para los objetos incluidos.

#### EXCLuded

Muestra la salida sólo para los objetos excluidos.

### -FILENAME=

Especifica el nombre de archivo en el que se debe grabar la salida delimitada por tabuladores. El valor predeterminado es `dsmprev.txt`.

### -CONsole

La salida se graba en la consola y en el archivo.

### -TRaverse

Previsualiza el directorio actual y sus subdirectorios.

Yes

Previsualiza los directorios actuales y sus subdirectorios. Éste es el valor predeterminado.

No

Sólo previsualiza el directorio actual, sin subdirectorios.

Importante: la especificación de **-traverse** no ofrece una previsualización de los directorios que se han excluido mediante la utilización de la opción `exclude.dir`.





## Query Access

---

El mandato `query access` muestra los usuarios a los que ha otorgado acceso a las versiones de copia de seguridad o copias archivadas de archivos específicos.

El cliente de copia de seguridad y archivado muestra una lista de las reglas de autorización que ha definido con el mandato `set access` o con el menú Programas de utilidad > Lista de acceso a nodo de la interfaz gráfica de usuario (GUI) del cliente de copia de seguridad y archivado.

A continuación se indica la información incluida:

- Autorización que ha otorgado a un usuario para restaurar versiones de copia de seguridad o para recuperar copias archivadas.
- El nombre de nodo del usuario al que se otorga autorización.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X El identificador del usuario de dicho nodo al que se ha otorgado autorización.
- Los archivos para los que el usuario dispone de acceso.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Query ACcess-----><
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

Tarea

Visualizar una lista de los usuarios que tienen acceso a sus archivos.

**Mandato:** `query access`

 Sistemas operativos Windows

## Query Adobjects

---

Utilice el mandato `query adobjects` para mostrar información acerca de los objetos suprimidos ubicados en el dominio local de Active Directory.

En clientes de sistema operativo Windows Server, la información de objetos de Active Directory también se puede visualizar desde las copias de seguridad completas de estado de sistema en el servidor.

## Clientes soportados

---

Este mandato es válido para clientes de sistema operativo Windows Server solamente.

## Sintaxis

---



```
>>-Query ADOBJects--+-----+-----+-----+-----><
      '- --sourcepathspec-' '-options-'
```

## Parámetros

### sourcepathspec

Especifica el objeto o contenedor de Active Directory que desea consultar. Puede especificar un asterisco (\*) como carácter comodín. Puede especificar el nombre distinguido completo de un objeto o un contenedor o sólo el atributo del nombre (cn o bien ou), donde es posible utilizar el comodín. También puede especificar el GUID de objeto incluido entre llaves ({}). Los siguientes caracteres especiales requieren un carácter de escape, la barra inclinada invertida, (\), si alguno está incluido en el nombre:

- \
- #
- +
- =
- <
- >

Por ejemplo, "cn=test#" se especificará como "cn=test\#".

El cliente no puede mostrar nombres de objetos que contengan un asterisco (\*) como parte del nombre.

Tabla 1. Mandato Query Aobjects: opciones relacionadas

Opción	Dónde se utiliza
adlocation	Sólo línea de mandatos.
fechaformato	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
detail	Sólo línea de mandatos.
pitdate (la opción se ignora si no se ha especificado adlocation)	Sólo línea de mandatos.
pitime (la opción se ignora si no se ha especificado adlocation)	Sólo línea de mandatos.
scrolllines	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
scrollprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

## Ejemplos

### Tarea

Consultar todos los objetos suprimidos locales.

**Mandato:** query aobjects

### Tarea

Consultar todos los objetos suprimidos locales de un usuario cuyo nombre empieza por Fred.

**Mandato:** query aobjects "cn=Fred\*" -detail

### Tarea

Consultar todos los objetos ubicados en el contenedor Users del dominio bryan.test.example.com del servidor.

**Mandato:** query aobjects "cn=Users,DC=bryan,DC=test,DC=ibm,DC=com" -adloc=server

### Tarea

Consultar todos los objetos suprimidos locales de la unidad organizativa testou.

**Mandato:** query aobjects "ou=testou"

### Tarea



















Consultar el objeto local suprimido cuyo GUID es E079130D-3451-4C69-8349-31747E26C75B.

**Mandato:** query adobjects {E079130D-3451-4C69-8349-31747E26C75B}





## Query Archive

El mandato query archive muestra una lista de las copias archivadas y la siguiente información acerca de cada archivo: tamaño de archivo, fecha de archivado, especificación de archivo, fecha de caducidad y descripción de archivado.

Si utiliza la opción detail con el mandato query archive, el cliente visualizará la información adicional siguiente:

- Fecha de última modificación
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Fecha de último acceso
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Fecha de último cambio de atributos de archivo (inode)
-  Sistemas operativos Windows Fecha de creación
- Tipo de compresión
- Tipo de cifrado
-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows Deduplicación de datos del lado del cliente
- Iniciación de retención
- Si el archivo está en espera
-  Sistemas operativos AIX  Sistemas operativos Linux Tamaño de metadatos de ACL (IBM Spectrum Scale), para clientes AIX y Linux
-  Sistemas operativos AIX  Sistemas operativos Linux Información de almacenamiento del servidor (clase de medios, ID de volumen y orden de restauración), para clientes AIX y Linux

En el siguiente ejemplo se muestra un ejemplo de la salida del mandato query archive con la opción detail:

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris

```
Tamaño  Fecha - Hora archivado - Caducidad archivo - Descripción
-----
219 B 08/15/2016 09:32:13 /Volumes/Data/info.txt 08/16/2016
Archive Date: 08/16/2016
RetInit:STARTED Obj
Held:NO
Modificado: 03/02/2016 19:43:00 Accedido: 03/03/2016 09:31:23 Inode cambiado: 03/02/2016 19:43:00
Tipo compresión: LZ4 Tipo cifrado: Ninguno Deduplicado por cliente: YES
ACL Size: 0 Media Class: Fixed Volume ID: 0008 Restore Order: 00000000-0000001F-00000000-00600774
```

 Sistemas operativos Windows

```
Tamaño  Fecha - Hora archivado - Caducidad archivo - Descripción
-----
219 B 03/03/2016 09:32:13 \\halley\m$\tsm620c.0901fa\debug\bin\
winnt_unicode\dsm.opt 03/03/2016
Fecha archivado: 03/03/2016
RetInit:STARTED Obj
Held:NO
Modificado: 03/03/2016 19:43:00 Creado: 03/01/2016 15:31:23
Tipo compresión: LZ4 Tipo cifrado: Ninguno Deduplicado por cliente: YES
```

Para obtener más información sobre el tipo de compresión, consulte el apartado Compression.

## Clientes soportados









Este mandato es válido para todos los clientes.



## Sintaxis


```
>>-Query ARchive--+-+-----+----->
                '- --options-'

>--+- --filespec-----+--+ --filespec---+-----><
                '- --{--filespecname--}--filespec-' '- --"filespec"-'
```

## Parámetros


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Si utiliza caracteres comodín, incluya la especificación de archivo entre comillas. Especifique un asterisco (\*) para consultar todas las copias archivadas del directorio actual.

 Sistemas operativos Windows  filespec

 Sistemas operativos Windows  
Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

Si incluye filespace, no incluya una letra de unidad en la especificación de archivo. Los nombres de la etiqueta de unidad sólo se utilizan para medios extraíbles.

































 Sistemas operativos Windows {filespace}







































 Sistemas operativos Windows  
Especifica el espacio de archivos (entre llaves) del servidor que contiene el archivo que desea consultar. El espacio de archivos es el nombre de la unidad de la estación de trabajo desde la que se archivó el archivo. El siguiente ejemplo es válido para especificar un nombre UNC: {"\\machine\C\$"}.

Utilice filespace si el nombre ha cambiado o si está consultando copias que se archivaron desde otro nodo cuyas etiquetas de unidad son distintas de las suyas.









Nota: debe especificar un filespace entre comillas dentro de llaves; por ejemplo, {"NTFSDrive"}. En la modalidad de bucle se pueden utilizar indistintamente comillas dobles o comillas simples. Por ejemplo, {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples.

Tabla 1. Mandato query archive: opciones relacionadas



Opción	Dónde se utiliza
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dateformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
description	Sólo línea de mandatos.
detail	Sólo línea de mandatos.
dironly	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
fromdate	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X Sólo línea de mandatos.
fromtime	Sólo línea de mandatos.
 Sistemas operativos Windows numberformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X numberformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
querysummary	Sólo línea de mandatos.
 Sistemas operativos Windows scrolllines	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrolllines	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrollprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrollprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows subdir	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X subdir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X timeformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
todate	Sólo línea de mandatos.
totime	Sólo línea de mandatos.









## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Visualizar una lista de todas las copias archivadas del directorio de trabajo actual.



**Mandato:** q archive "\*"

 Sistemas operativos Windows Tarea  
 Sistemas operativos Windows Visualizar una lista de todas las copias archivadas del directorio c:\proj.









**Mandato:** q ar c:\proj\\*

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Visualizar una lista de todas las copias archivadas del directorio /devel y de todos sus subdirectorios.

**Mandato:** query archive "/devel/\*" -subdir=yes


 Sistemas operativos Windows Tarea  
 Sistemas operativos Windows Visualizar una lista de todas las copias archivadas de la unidad c: que tienen la descripción "January Ledgers".

**Mandato:** query archive c:\ -su=y -descr="Contabilidad general de enero"









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Visualizar una lista de todas las copias archivadas del directorio actual. Utilice las opciones dateformat y timeformat para volver a formatear las fechas y las horas.

**Mandato:** q ar -date=5 -time=1 "\*"

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Visualizar una lista de todas las copias archivadas del directorio `c:\proj`. Utilice las opciones `dateformat` y `timeformat` para volver a formatear las fechas y las horas.

**Mandato:** `q ar -date=5 -time=4 c:\proj\*`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Visualizar una lista de todas las copias archivadas del directorio actual. Utilice la opción `detail` para que se visualicen la última fecha de modificación y la última fecha de acceso de cada archivo.


**Mandato:** `q ar -detail "*"`

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Visualizar una lista de todas las copias archivadas del directorio `c:\dir1`. Utilice la opción `detail` para que se visualicen la última fecha de modificación y la fecha de creación de cada archivo.


**Mandato:** `q ar -detail c:\dir1\*`

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Visualizar una lista de todas las copias archivadas del directorio `c:\proj` que contengan la extensión de archivo `.dev`. Utilice las opciones `dateformat` y `timeformat`.


**Mandato:** `q ar -date=5 -time=4 c:\proj\*.dev`

 Sistemas operativos Windows Tarea









 Sistemas operativos Windows Recientemente cambió la etiqueta de la unidad `c:\` para `store` y realizó el archivado de varios archivos. A continuación, ayer la etiqueta se cambió a `dev` y se archivaron unos archivos más. Visualizar una lista de todos los archivos que se archivaron del directorio `c:\proj` cuando la etiqueta era `store`.

**Mandato:** `q ar {store}\proj\*`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Recientemente, se archivaron copias desde un disquete con la etiqueta `docs`. Mostrar una lista de todas las copias archivadas.

**Mandato:** `q ar {docs}\*`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Visualizar una lista de todas las copias archivadas del directorio `/home/proj` cuyos cuatro primeros caracteres del nombre del archivo empecen por `proj`.

**Mandato:** `q ar "/home/proj/proj*"`

## Query Backup










---

El mandato `query backup` muestra una lista de versiones de copia de seguridad de los archivos almacenadas en el servidor de IBM Spectrum Protect, o del interior de un juego de copias de seguridad del servidor cuando se especifica la opción `backupsetname`.

El mandato muestra la siguiente información adicional:

- Especificación de archivo
- Tamaño del archivo
- Fecha de la copia de seguridad
- Si el archivo está activo o inactivo
- La clase de gestión asignada al archivo. En el nombre de la clase de gestión únicamente se muestran los 10 diez caracteres.

Si utiliza la opción `detail` con el mandato `query backup`, el cliente visualizará la información adicional siguiente:

- Fecha de última modificación
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Fecha de último acceso
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Última fecha de cambio de atributos de archivo (inode)
-  Sistemas operativos Windows Fecha de creación
- Tipo de compresión
- Tipo de cifrado

- Deduplicación de datos del lado del cliente
- Indica si el archivo ha migrado o premigrado. Un valor de *Yes* significa que el archivo ha migrado o premigrado. Un valor de *No* indica que el archivo no ha migrado o premigrado.
- Número de inodo de archivo
- Tamaño de metadatos de ACL (IBM Spectrum Scale)
- Información de almacenamiento del servidor (clase de medios, ID de volumen y orden de restauración)

En el siguiente ejemplo se muestra un ejemplo de la salida del mandato `query backup` con la opción `detail`:

Tamaño	Fecha copia seg.	Clase gest.	Archivo A/I
1,500,000 B	08/15/2016 16:01:25	DEFAULT	A /home/test/mydir/myfile1.txt
Modified: 08/15/2016 16:00:10 Accessed: 08/16/2016 15:31:23 Inode changed: 08/15/2016 16:00:10			
Compression Type: LZ4 Encryption Type: None Client-deduplicated: YES Migrated: NO Inode#: 22691			
ACL Size: 0 Media Class: Fixed Volume ID: 0008 Restore Order: 00000000-0000001F-00000000-00600774			

Tamaño	Fecha copia seg.	Clase gest.	Archivo A/I
1,000,000 B	03/15/2016 14:33:17	DEFAULT	A \\eighth\n\$\testdir\myfile1.txt
Modificado: 03/15/2016 14:31:42 Creado: 03/15/2016 14:31:41			
Tipo compresión: LZ4 Tipo cifrado: Ninguno Deduplicado por cliente: YES			

Para obtener más información sobre el tipo de compresión, consulte el apartado [Compression](#).

## Cientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Query Backup--+-+-----+----->
                '- --options-'

>--+ --filespec-----+--+ --filespec---+----><
                '- --{--filespecname--}--filespec-' '- --"filespec"-'
```

## Parámetros

`filespec`  
 Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. Si utiliza caracteres comodín, incluya la especificación de archivo entre comillas. Especifique un asterisco (\*) para ver información acerca de las versiones de copia de seguridad de todos los archivos del directorio actual. No utilice caracteres comodín cuando consulte las imágenes del sistema de archivos NAS con la opción `-class=nas`.

`filespec`

Especifica la vía de acceso y el nombre del archivo que se desea consultar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio. No utilice caracteres comodín cuando consulte las imágenes del sistema de archivos NAS con la opción `-class=nas`.

Si incluye `filespecname`, no incluya una letra de unidad en la especificación de archivo. Los nombres de la etiqueta de unidad sólo se utilizan para medios extraíbles.

También puede utilizar el siguiente valor para `filespec`:

`systemstate`

Visualiza la lista de versiones de copia de seguridad del estado del sistema Windows .



















































`{filespecname}`

Especifica el espacio de archivos, entre llaves, del servidor que contiene el archivo que desea consultar. Es el nombre de etiqueta de la unidad o el nombre UNC de la unidad de la estación de trabajo desde la que se realizó copia de seguridad del archivo. El siguiente ejemplo muestra cómo especificar un nombre UNC: `{ '\\\machine\C$' }`.

Utilice el *filespace* si el nombre se ha modificado o si desea consultar archivos cuyas copias de seguridad se realizaron desde otro nodo con nombres de etiqueta de unidad diferentes de los suyos.

Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. En la modalidad de bucle se pueden utilizar indistintamente comillas dobles o comillas simples. Por ejemplo: {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples.

Tabla 1. mandato query backup: opciones relacionadas

Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windowsclass	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Sólo línea de mandatos.
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dateformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
detail	Sólo línea de mandatos.
dironly	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
fromdate	Sólo línea de mandatos.
fromowner	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X Sólo línea de mandatos.
fromtime	Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X nasnodename	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows nasnodename	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows numberformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X numberformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
querysummary	Sólo línea de mandatos.

Opción	Dónde se utiliza
Sistemas operativos Windows scrolllines	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X scrolllines	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows scrollprompt	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X scrollprompt	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows subdir	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X subdir	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows timeformat	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X timeformat	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
todate	Sólo línea de mandatos.
totime	Sólo línea de mandatos.

## Ejemplos

Sistemas operativos Windows  
dsmc query backup c:\\* -subdir=yes -querysummary

Sistemas operativos Windows  
dsmc query archive c:\\* -subdir=yes -querysummary

Sistemas operativos Windows  
Tarea

Sistemas operativos Windows  
Consultar archivos del directorio `proj` del espacio de archivos `abc`.

```
dsmc query backup {"abc"}\proj\*.*
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Tarea  
Visualizar una lista de todas las versiones de copia de seguridad activas o inactivas que se realizaron de los archivos del directorio actual.

```
dsmc query backup -inactive ""
```

Sistemas operativos Windows  
Tarea

Sistemas operativos Windows  
Visualizar una lista de todas las versiones de copia de seguridad activas o inactivas cuyas copias de seguridad se han realizado desde el directorio `c:\proj`.


```
dsmc q backup -ina c:\proj\*
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Tarea  
Visualizar una lista de todas las copias de seguridad del directorio actual. Utilice la opción `detail` para que se visualicen la última fecha de modificación y la última fecha de acceso de cada archivo.

```
dsmc q backup -detail ""
```




#### Sistemas operativos WindowsTarea

 Sistemas operativos WindowsVisualizar una lista de todas las copias de seguridad del directorio `c:\dir1`. Utilice la opción `detail` para que se visualicen la última fecha de modificación y la fecha de creación de cada archivo.





```
dsmc q backup -detail c:\dir1\*
```

#### Sistemas operativos WindowsTarea

 Sistemas operativos WindowsVisualizar una lista de todas las versiones de copia de seguridad activas o inactivas cuyas copias de seguridad se han realizado desde el directorio `c:\proj`. Utilice las opciones `dateformat` y `timeformat` para volver a formatear las fechas y las horas.





```
dsmc q b -date=5 -time=4 -ina c:\proj\*
```

#### Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Visualizar una lista de los archivos cuya copia de seguridad se ha realizado desde el directorio `/home/proj` y cuyos nombres de archivos empiezan por `proj`.


```
dsmc q b "/home/proj/proj*"
```

#### Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Visualizar una lista de las versiones de archivos de copia de seguridad activos e inactivos del sistema de archivos `/home`.




```
dsmc q b -ina -su=yes /home/
```

#### Sistemas operativos WindowsTarea

 Sistemas operativos WindowsLa semana pasada, se realizaron copias de seguridad de archivos desde un disquete con la etiqueta **docs**. Mostrar una lista de dichos archivos.


```
dsmc q b {docs}\*
```

#### Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle SolarisTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle SolarisConsultar imágenes de sistemas de archivos del servidor de archivos NAS `nas2`.


```
dsmc query backup -nasnodename=nas2 -class=nas
```

#### Sistemas operativos WindowsTarea

 Sistemas operativos WindowsConsultar imágenes de sistemas de archivos del servidor de archivos NAS `nas2`.


```
dsmc query backup -nasnodename=nas2 -class=nas
```

#### Sistemas operativos WindowsTarea






 Sistemas operativos WindowsVisualizar una lista de todos los archivos de la unidad `c` que están contenidos en el conjunto de copias de seguridad llamado `weekly_accounting_data.32145678`.

```
dsmc query backup c:\* -subdir=yes -backupsetname=weekly_accounting_data.32145678
```

#### Sistemas operativos WindowsTarea

 Sistemas operativos WindowsVisualiza información acerca de las versiones de copia de seguridad activa e inactiva de estado del sistema en el servidor.

```
dsmc query backup -ina systemstate
```

-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos WindowsConsultar imágenes de sistemas de archivos NAS  
Puede utilizar el mandato `query backup` para mostrar información acerca de las imágenes del sistema de archivos de un servidor de archivos NAS de las que se ha hecho una copia de seguridad. El cliente le solicita un ID de administrador.

## Query Backupset

---

El mandato `query backupset` consulta un juego de copias de seguridad de un archivo local, de un dispositivo de cinta (si es aplicable) o del servidor de IBM Spectrum Protect.

Este mandato muestra el nombre del juego de copias de seguridad, la fecha de generación, la retención (para un juego de copias de seguridad en el servidor de IBM Spectrum Protect) y una descripción proporcionada por el usuario.

## Cientes soportados

---

Este mandato es válido para todos los clientes.

El soporte para cintas solo está disponible en clientes de AIX y Oracle Solaris.

## Sintaxis

```
>>-Query BACKUPSET--+-+-----+--BACKUPSETName=----->
      '-options-'

>--+-backupsetname-+-+-----+-----><
+-localfilename+  '-LOCation=--+-server--+'
'-tapedevice----'      +-file----+
                        '-tape----'
```

## Parámetros

### BACKUPSETName=

Especifica el nombre de un juego de copias de seguridad que desea consultar. Puede utilizar caracteres comodín para especificar el nombre del juego de copias de seguridad. Si utiliza caracteres comodín o no especifica ningún nombre de juego de copias de seguridad, se visualizarán todos los juegos de copias de seguridad que posea. Este parámetro es obligatorio.

Cuando se crea un juego de copias de seguridad, el servidor designa al usuario root como el propietario del juego de copias de seguridad. Al consultar un juego de copias de seguridad en el servidor, un usuario que no sea root no podrá ver el juego de copias de seguridad listado, incluso aunque conozca el nombre del juego de copias de seguridad y lo utilice en la consulta.

El valor de backupsetname depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de estas tres opciones:

#### backupsetname

Especifica el nombre del juego de copias de seguridad del servidor. Si se especifica el parámetro location, debe establecer `-location=server`.

#### localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer `-location=file`.

#### tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo nativo de Windows, no el controlador de dispositivo proporcionado por IBM. Debe establecer `-location=tape`.

### LOCation=

Especifica dónde ha de buscar el cliente de copia de seguridad y archivado el juego de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect.

#### server

Especifica que el cliente buscará el juego de copias de seguridad del servidor. Esta ubicación es el valor predeterminado.

#### file



















Especifica que el cliente buscará el juego de copias de seguridad en un archivo local.

#### tape

Especifica que el cliente buscará el juego de copias de seguridad en un dispositivo de cinta local.

Tabla 1. mandato query backupset: opciones relacionadas

Opción	Dónde se utiliza
 description	 Sólo línea de mandatos.
 description	 Sólo línea de mandatos.
 scrolllines	 Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris scrolllines	 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrollprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris scrollprompt	 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.

## Ejemplos

### Tarea









Consultar todos los juegos de copias de seguridad del servidor de IBM Spectrum Protect.

**Mandato:** `query backupset -backupsetname=*`


### Tarea


Consultar un juego de copias de seguridad denominado `monthly_financial_data` desde el servidor IBM Spectrum Protect.

**Mandato:** `query backupset -backupsetname=monthly_financial_data.12345678`









 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Consultar el juego de copias de seguridad en el archivo `/home/budget/weekly_budget_data.ost`.

**mandato:** `dsmc query backupset -backupsetname="/home/budget/weekly_budget_data.ost" -loc=file`

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Consultar el juego de copias de seguridad en el archivo  
`c:\budget\weekly_budget_data.ost`.

**mandato:** `query backupset -backupsetname=c:\budget\weekly_budget_data.ost loc=file`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Consultar el juego de copias de seguridad del dispositivo de cinta `/dev/rmt0`.

**Mandato:** `dsmc query backupset -backupsetname=/dev/rmt0 -loc=tape`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Consultar el juego de copias de seguridad del dispositivo de cinta `\\.\tape0`.

**Mandato:** `dsmc query backupset -backupsetname=\\.\tape0 -loc=tape`


- `query Backupset` sin el parámetro `backupsetname`  
 El mandato `query backupset` se puede utilizar sin el parámetro `backupsetname`.






## Query Filespace

El mandato `query filespace` muestra una lista de espacios de archivos para un nodo. Los espacios de archivos se almacenan en el servidor de IBM Spectrum Protect o en el interior de un juego de copias de seguridad del servidor cuando se especifica la opción `backupsetname`. También puede especificar un único nombre de espacio de archivos para su consulta.

Un *espacio de archivos* es un espacio lógico del servidor que contiene archivos de los que se realizó copia de seguridad o de archivado. Se asigna un espacio de archivos por separado en el servidor para cada nodo de la estación de trabajo de la que ha realizado una copia de seguridad o ha archivado archivos.

Se asigna un espacio de archivos por separado en el servidor para cada sistema de archivos de la estación de trabajo de la que ha realizado una copia de seguridad o ha archivado archivos. El nombre del espacio de archivos es igual al nombre del sistema de archivos.

 Sistemas operativos Windows Puede que un nombre de espacio de archivos Unicode no se visualice correctamente si el servidor no puede visualizar el nombre Unicode. En este caso, utilice el identificador (identificador de espacio de archivos) para identificar estos espacios de archivos en el servidor. Utilice el mandato query filespace con la opción detail para determinar el ID de espacio de archivos de un espacio de archivos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Cientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis




























```
>>-Query Filespace--+-+-----+-----+-----+-----<<
                    '- --filespace-name-' '- --options-'
```





























## Parámetros

filespace-name






Especifica una serie de caracteres opcional que puede incluir caracteres comodín. Utilice este argumento para especificar un subconjunto de espacios de archivos. El valor predeterminado es la visualización de todos los espacios de archivos.

Tabla 1. Mandato query filespace: opciones relacionadas





Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
 Sistemas operativos Windows  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS Xclass	 Sistemas operativos Windows  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XSólo línea de mandatos.
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dateformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
detail	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS XSólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X nasnodename	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows nasnodename	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrolllines	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrolllines	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrollprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrollprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X timeformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.





## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows Visualizar los espacios de archivos. Utilice las opciones `dateformat` y `timeformat` para volver a formatear las fechas y las horas.






```
query filespace -date=5 -time=4
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Visualizar el espacio de archivos `/home`.

```
query filespace /home
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Visualizar los nombres de espacio de archivos que incluyen el patrón `smith`.


```
query filespace "*smith*"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows Consultar un espacio de archivos del servidor de archivos NAS `nas2`.


```
query filespace -nasnodename=nas2 -class=nas
```

 Sistemas operativos Windows Visualizar el espacio de archivos `\\florence\c$`.

```
query filespace \\florence\c$
```

 Sistemas operativos Windows Visualizar todos los nombres de espacios de archivos del servidor cuyos nombres de espacios de archivos finalicen por `'$'` y que pertenezcan al sistema denominado `florence`.

```
query filespace \\florence\*$
```

 Sistemas operativos Windows Visualizar espacios de archivos en el juego de copias de seguridad denominado `monthly_accounting.23456789`.

```
query filespace -backupsetname=monthly_accounting.23456789
```

Visualizar información detallada acerca del espacio de archivos que muestra el estado de réplica durante una migración tras error.

Mandato:

```
query filespace -detail
```

Salida:

#	Fecha último	Incr	Tipo	fsID	Unicode	Réplica	Espacio archivos
----	-----	-----	----	-----	-----	-----	-----
1	00/00/0000	00:00:00	HFS	3	Sí	Actual	/

Fecha últ. alm.	Servidor	Local
Datos cop. seg.: 04/29/2013 16:49:55		04/29/2013 16:49:55
Datos archivado: Ninguna fecha disponible		Ninguna fecha disponible

- Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, sistemas operativos Mac OS X, Sistemas operativos Windows

Consulta de espacios de archivos NAS  
 Utilice la opción nasnodename para identificar el servidor de archivos NAS que se debe consultar. Cuando se utilice una sesión de línea de mandatos interactiva con un ID que no es un ID de administración, el cliente solicitará un ID de administrador.

## Query Group

Utilice el mandato query group para que se visualice información acerca de una copia de seguridad de grupo y sus miembros.

Nota:

- Utilice la opción showmembers para visualizar y seleccionar los miembros individuales del grupo que desea consultar. La opción showmembers no es válida con la opción inactive. Si desea visualizar los miembros de un grupo que actualmente no están activos, utilice las opciones pitdate y pittime para especificar la fecha y la hora de copia de seguridad del miembro que desea consultar.
- Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris, Sistemas operativos Windows  
 Utilice el mandato query filespace para visualizar nombres de espacios de archivos virtuales para el nodo que se almacenan en el servidor de IBM Spectrum Protect.
- Si realiza una copia de seguridad de grupo completa y diferencial, una consulta de este grupo en la que se utilice la opción -inactive visualizará dos copias de seguridad activas con el mismo nombre, una de tipo FULL (completa) y otra de tipo DIFF (diferencial).

Estas copias de seguridad desactivan las copias de seguridad completas y diferenciales anteriores:

Sistemas operativos Windows

```
Protect> q group {\fs}\v1 -inactive
```

Tamaño	Fecha copia seg.	Clase gest	Grupo A/I
978 B	06/02/2007 11:57:04	DEFAULT	A FULL \fs\v1
32 B	06/05/2007 13:52:04	DEFAULT	A DIFF \fs\v1

Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris

```
Protect> q group {/fs}/v1 -inactive
```

Tamaño	Fecha copia seg.	Clase gest	Grupo A/I
978 B	06/02/2007 11:57:04	DEFAULT	A FULL /fs/v1
32 B	06/05/2007 13:52:04	DEFAULT	A DIFF /fs/v1

Si consulta una copia de seguridad de grupo sin la opción -inactive, la consulta sólo visualizará la última copia de seguridad de grupo, tanto si es de tipo FULL (completa) como de tipo DIFF (diferencial):

Sistemas operativos Windows

```
Protect> q group {\fs}\v1
```

Tamaño	Fecha copia seg.	Clase gest	Grupo A/I
32 B	06/05/2007 13:52:04	DEFAULT	A DIFF \fs\v1

Sistemas operativos AIX, Sistemas operativos Linux, Sistemas operativos Oracle Solaris

```
Protect> q group {/fs}/v1
```

Tamaño	Fecha copia seg.	Clase gest	Grupo A/I
32 B	06/05/2007 13:52:04	DEFAULT	A DIFF /fs/v1

## Clientes soportados

Este mandato es válido para todos los clientes, a excepción de Mac OS X.

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Query GRoup-- --filespec--+-+-----+----->>
                               '- --options-'
```

## Parámetros

filespec

Especifica el nombre del espacio de archivos virtual (entre llaves) y el nombre del grupo que desea consultar en el servidor.

filespec

Especifica el nombre del espacio de archivos virtual y el nombre del grupo que desea consultar en el servidor.

Tabla 1. Mandato query group: opciones relacionadas

Opción	Dónde se utiliza
fromnode	Sólo línea de mandatos.
fromowner	Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
showmembers (no se aplica a Mac OS X)	Sólo línea de mandatos.

## Ejemplos

Tarea

Visualizar todos los grupos del espacio de archivos /virtfs.

**Mandato:**

```
query group /virtfs/*
```

Tarea

Visualizar todos los grupos del espacio de archivos virtfs.

**Mandato:**

```
query group {virtfs}\*
```

Tarea

Visualizar las versiones activas e inactivas del espacio de archivos /virtfs/group1.

**Mandato:**

```
query group /virtfs/group1 -inactive
```

Tarea

Visualizar las versiones activas e inactivas del espacio de archivos virtfs\group1.

**Mandato:**

```
query group {virtfs}\group1 -inactive
```

Tarea  
 Visualizar el espacio de archivos /virtfs/group1. Utilice la opción showmembers para que se visualice una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea consultar.

**Mandato:**

```
query group /virtfs/group1 -showmembers
```

Tarea  
 Visualizar el espacio de archivos virtfs\group1. Utilice la opción showmembers para que se visualice una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea consultar.

**Mandato:**

```
query group {virtfs}\group1 -showmembers
```

## Query Image

---

El mandato query image muestra información sobre las imágenes del sistema de archivos que se almacenan en el servidor de IBM Spectrum Protect, o en el interior de un juego de copias de seguridad del servidor de IBM Spectrum Protect, cuando se especifica la opción backupsetname.

Se visualizará la siguiente información acerca de las imágenes del sistema de archivo:

- Tamaño de imagen - El tamaño del volumen del que se ha realizado la copia de seguridad.
- Tamaño almacenado - El tamaño de imagen real almacenado en el servidor. La imagen almacenada en el servidor de IBM Spectrum Protect tiene un tamaño que equivale a la capacidad del volumen. Para las copias de seguridad de imágenes en línea basadas en instantáneas, la imagen almacenada puede ser más grande que el sistema de archivos, basándose en el tamaño de los archivos de la caché. La imagen almacenada en el servidor tiene un tamaño que equivale a la capacidad del volumen.
- Tamaño almacenado - El tamaño de imagen real almacenado en el servidor. Puesto que la copia de seguridad de imágenes le permite realizar la copia de seguridad únicamente de los bloques utilizados en un sistema de archivos, el tamaño almacenado de la imagen en el servidor de IBM Spectrum Protect podría ser más pequeño que el tamaño del volumen. Para las copias de seguridad de imágenes en línea, la imagen almacenada puede ser más grande que el sistema de archivos, en función del tamaño de los archivos de la caché.
- Tipo de sistema de archivos
- Fecha y hora de la copia de seguridad
- Clase de gestión que se asigna a la copia de seguridad de imágenes
- Si la copia de seguridad de imágenes es una copia activa o inactiva
- El nombre de la imagen

Nota: La API de IBM Spectrum Protect debe estar instalada para utilizar el mandato query image.

## Clientes soportados

---

Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Este mandato es válido para todos los clientes Windows.

## Sintaxis

---

```
>>-Query Image-+-----+--+ --logicalvolumename-+----->>  
      '- --options-' '- --filespaceName-----'
```

## Parámetros

---

nombrevolumenlógico

El nombre de un volumen lógico que desea consultar. Debe especificarse el nombre exacto de la imagen. No puede utilizar caracteres comodín. El valor predeterminado son todas las imágenes activas (a menos que se limiten mediante una o varias opciones).

filespaceName



Especifica el nombre del espacio de archivos que desea consultar.

Si omite *nombrevolumenlógico* y *nombreespacioarchivos*, se visualizarán todas las imágenes.

Tabla 1. Mandato query image: opciones relacionadas







Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris dateformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
fromnode	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris numberformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows numberformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris scrolllines	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrolllines	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris scrollprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrollprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris timeformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

## Ejemplos







### Tarea

Mostrar todas las imágenes de las que se ha realizado copia de seguridad.



**Mandato:** q image

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Mostrar todas las imágenes de las que se ha realizado copia de seguridad propiedad de *kutras* en el nodo *avalon*.

**Mandato:** query image -fromnode=avalon -fromowner=kutras

   Tarea  
   Visualizar las versiones activas e inactivas de la imagen /usr.

**Mandato:** q i /usr -inactive

 Tarea  
 Visualizar las versiones activas e inactivas de la imagen h:.

**Mandato:** q im h: -inactive

Tarea

Mostrar todas las imágenes que están contenidas en el juego de copias de seguridad llamado weekly\_backup\_data.32145678.

**Mandato:** query image -backupsetname=weekly\_backup\_data.32145678


## Query Inclexcl

El mandato query inclexcl visualiza una lista de sentencias de inclusión/exclusión en el orden en que se procesan durante las operaciones de copia de seguridad/archivado. La lista visualiza el tipo de opción, el ámbito de la opción (archive, all, etc.), y el nombre del archivo fuente.

El cliente de archivado y copia de seguridad excluye algunos archivos de las operaciones de copia de seguridad y restauración del sistema de archivos. Puede utilizar el mandato query inclexcl para visualizar una lista de estos archivos. En la salida del mandato, estos archivos tienen Sistema operativo junto a la vía de acceso.

Puede comprobar la validez de los patrones que desea utilizar en la lista de inclusión/exclusión antes de insertarlos realmente en el archivo de opciones. Consulte la explicación sobre *el patrón de prueba*.


Utilice la opción detail para que se visualice la clase de gestión que se asocia a una sentencia de inclusión/exclusión.

 Utilice la opción display para visualizar los archivos incluidos en o excluidos de una operación de copia de seguridad del sistema de archivos.


## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Query INCLexcl-- --+-----+-----+-----+-----><
                        '-test pattern-' '- -DETail-'
```



```
>>-Query INCLexcl--++-----+-----+-----+-----+-----+><
                        '-patrón prueba-' '- -DETail-' |                .-básica--. |
                                                '--DISPLAY=--+vssexcl+--'
                                                '-all-----'
```

## Parámetros

test pattern

Se utiliza para comprobar la validez de los patrones que desea utilizar en la lista de inclusión/exclusión. Cuando utilice un patrón de prueba con este mandato, ocurre lo siguiente:


- No se muestra la lista de inclusión/exclusión interna.
- El patrón se procesa como si se hubiera originado en una sentencia de inclusión/exclusión, incluyendo toda la comprobación de errores habitual
- El patrón se muestra tal y como aparecería en la lista de inclusión/exclusión

Si el patrón de prueba no contiene errores, el resultado del patrón compilado es el mismo que el del patrón de prueba.

-DEtail


Visualiza la clase de gestión que se asocia a cada sentencia.


 Sistemas operativos Windows-DISPLAY=basic | vssexcl | all

 Sistemas operativos Windows-DISPLAY=basic muestra los archivos y directorios incluidos o excluidos mediante uno de los métodos siguientes:

- Los objetos incluidos o excluidos en el archivo de opciones del cliente.
- Los objetos incluidos o excluidos en un conjunto de opciones del cliente del lado del servidor.
- Los objetos han sido excluidos por el sistema operativo porque están contenidos en la clave de registro de HKEY\_LOCAL\_MACHINES\SYSTEM\CurrentControlSet\BackupRestore\FilesNotToBackup.
- Los objetos han sido excluidos explícitamente por el cliente.

Éste es el valor predeterminado si no se ha especificado un valor de visualización.

 Sistemas operativos Windows-DISPLAY=vssexcl muestra una lista de archivos excluidos de una copia de seguridad del sistema de archivos porque están incluidos cuando se realiza una copia de seguridad de estado del sistema. Los archivos de los que se ha hecho copia de seguridad mediante una operación backup systemstate están protegidos por el grabador de VSS; no se puede incluir estos archivos en una copia de seguridad del sistema de archivos añadiéndolos a una sentencia de inclusión en el archivo dsm.opt, o el conjunto de opciones de cliente.

 Sistemas operativos Windows-DISPLAY=all muestra todos los archivos incluidos o excluidos durante una copia de seguridad del sistema de archivos.

## Ejemplos

---

Tarea


Excluir un archivo de la eliminación de duplicados excluyéndolo del archivo de opciones de cliente:


```
Exclude Dedup *\...\file2
```

Tarea

Visualiza una lista básica de sentencias de inclusión/exclusión. Mandato:

```
query inclexcl
```

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsVisualizar una lista de los archivos excluidos de las copias de seguridad del sistema de archivos porque el grabador de VSS los incluye en las copias de seguridad de estado del sistema.





```
query inclexcl -display=vssexcl
```

Tarea

Visualizar una lista de sentencias de inclusión/exclusión. Visualiza la clase de gestión que se asocia con cada sentencia.

```
query inclexcl -detail
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Comprobar la validez de este patrón: /.../?x?/\*.log

```
query inclexcl /.../?x?/*.log
```

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsComprobar la validez de este patrón: ..\?x?\\*.log


```
query inclexcl ..\?x?\*.log
```

## Query Mgmtclass

---

El mandato query mgmtclass visualiza la información sobre las clases de gestión disponibles en el conjunto de políticas activo.

El administrador define clases de gestión que contienen atributos que controlan si un archivo es elegible para los servicios de copias de seguridad o archivado. Las clases de gestión también determinan el modo en que se gestionan las copias de seguridad y las copias archivadas en el servidor.

 Sistemas operativos WindowsEl conjunto de políticas activo contiene una clase de gestión predeterminada; puede contener cualquier número de clases de gestión adicionales. Puede asignar clases de gestión específicas a los archivos mediante la utilización de las opciones include que se encuentran en el archivo de opciones del cliente (dsm.opt). Si no asigna una clase de gestión a un archivo, se utiliza la clase de gestión predeterminada.

El conjunto de políticas activo contiene una clase de gestión predeterminada; puede contener cualquier número de clases de gestión adicionales. Puede asignar clases de gestión específicas a los archivos mediante la utilización de las opciones include que se encuentran en el archivo de opciones de usuario del cliente (dsm.opt). Si no asigna una clase de gestión a un archivo, se utiliza la clase de gestión predeterminada.

Si realiza una copia archivada, podrá modificar temporalmente la clase de gestión asignada utilizando la opción archmc.

## Cientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Query Mgmtclass--+-+-----+-----<<
                    '- --options-'
```

## Parámetros

Tabla 1. Mandato query mgmtclass: opciones relacionadas

Opción	Dónde se utiliza
detail	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.

## Ejemplos

Tarea  
 Mostrar las clases de gestión predeterminadas y disponibles.

**Mandato:** query mgmtclass

## Query Node

El mandato query node muestra todos los nodos en los que un identificador de usuario de administración dispone de autorización para realizar operaciones. Se le solicitará el ID de administrador de IBM Spectrum Protect.

Idealmente, el ID de usuario de administración tiene como mínimo autorización de propietario de cliente sobre el nodo de estación de trabajo de cliente que utiliza desde la línea de mandatos o desde la Web.

Utilice la opción type para especificar el tipo de nodo que se ha de filtrar. Los valores válidos son los siguientes:

- nsas
- client
- servidor
- any

El valor predeterminado es any.

Nota: Cuando se instala el archivo de licencia de IBM Spectrum Protect for Virtual Environments: Data Protection for VMware en un servidor de copia de seguridad vStorage, la serie de la plataforma almacenada en el servidor IBM Spectrum Protect se establece en "TDP VMware" para todos los nombres de nodo utilizados en esa máquina. La serie de la plataforma puede utilizarse en el contexto de los cálculos de PVU. Si un nodo se está utilizando para realizar una copia de seguridad de la máquina con funciones de cliente con copia de seguridad-archivado estándar (por ejemplo, a nivel de archivo o copia de seguridad de imágenes), esta serie de plataforma debe interpretarse como un "cliente" para los cálculos de PVU.

Para obtener más información sobre unidades de valor del procesador, consulte *Estimación de unidades de valor de procesador (PVU)* en la documentación del servidor de IBM Spectrum Protect.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-Query Node-----+-----><
      '- --options-'
```

## Parámetros

Tabla 1. Mandato query node: opciones relacionadas

Opción	Dónde se utiliza
type	Sólo línea de mandatos.
scrolllines	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
scrolllines	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
scrollprompt	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
scrollprompt	Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

## Ejemplos

Tarea  
 Mostrar todos los nodos NAS.

**Mandato:** query node -type=nas

Tarea  
 Visualizar todos los nodos cliente que son clientes de copia de seguridad/archivado.

**Mandato:** query node -type=client

## Query Options

Utilice el mandato query options para que se visualicen todas o parte de las opciones y sus valores actuales relacionados con el cliente de línea de mandatos.

## Clientes soportados

Este mandato es válido para todos los clientes.





















```
>>-Query Options--+-----+----- --pattern-----><
                '- --options-'
```

## Parámetros

### patrón

Serie de caracteres opcional que puede incluir comodines. Utilice este argumento para especificar un subconjunto de opciones. El valor predeterminado consiste en visualizar todas las opciones.

Tabla 1. Mandato query options: opciones relacionadas

Opción	Dónde se utiliza
 Sistemas operativos Windows scrolllines	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrolllines	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows scrollprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X scrollprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

## Ejemplos

### Tarea

Visualizar todas las opciones y sus valores.

```
query options
```

### Tarea

Visualizar sólo las opciones que empiezan por *comm*.

```
query options comm*
```

### Tarea

Visualiza el valor de la opción sustituir.

```
query options replace
```

### Tarea

Emita el mandato para visualizar todas las opciones y sus valores. Se visualizará la información de estado de migración tras error.

```
query options
```






### Salida:

```
MYPRIMARYSERVERNAME: SERVER1
MYREPLICATIONSERVER: TARGET
REPLSERVERNAME: TARGET
    Address: 192.0.2.9
    Port: 1501
    SSLPort: 1502
    GUID: 39.5a.da.d1.ae.92.11.e2.82.d3.00.0c.29.2f.07.d3
    Used: yes
```

## Query Restore

El mandato query restore visualiza una lista de las sesiones de restauración reiniciables de la base de datos del servidor. La lista contiene los siguientes campos: owner, replace, subdir, preservepath, source y destination.

Se crea una sesión de restauración reiniciable cuando un mandato restore no se ejecuta correctamente debido a una anomalía en la red, en el cliente, en el servidor o cualquier otro problema parecido. Cuando se produce una anomalía, se bloquea el espacio de archivos del servidor por lo que no se pueden traspasar los archivos fuera de los volúmenes secuenciales. Para desbloquear el espacio de archivos, reinicie la restauración hasta que finalice (mandato query restore), o cancele la restauración (mandato cancel restore). Utilice query restore para determinar si hay sesiones de restauración reiniciables y qué espacios de archivos se ven afectados.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Query Restore-----<<
```


## Parámetros


---

No hay parámetros para este mandato.

## Ejemplos

---

 Tarea

 El siguiente ejemplo muestra la salida que se obtiene cuando se utiliza query restore:






```
---
Información de restauración reiniciable ---
Sesión reiniciable : 1
  Fecha/hora inicio: 10/17/2001 15:18:22
  Origen : {"\\ers\c$"}\data\proposals\*
  Destino: - no especificado por el usuario -

Sesión reiniciable : 2
  Fecha/hora inicio: 10/17/2001 15:20:01
  Origen: {"\\ers\c$"}\data\spreadsheets\*
  Destino: - no especificado por el usuario -
```

     
 Tarea

     
 Mostrar la sesión de restauración reiniciable en la base de datos del servidor.

**Mandato:** query restore

## Query Schedule

---

El mandato query schedule visualiza los sucesos planificados de su nodo. El administrador puede establecer planificaciones para realizar operaciones de copia de seguridad/archivado de forma automática. A fin de planificar el trabajo, utilice este mandato para determinar cuándo van a ocurrir los siguientes sucesos planificados.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Query Schedule-----<<
```

## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

Tarea






Mostrar los sucesos planificados.

**Mandato:** query schedule

## Query Session

---

El mandato query session muestra información acerca de la sesión como, por ejemplo, el nombre de nodo actual, cuándo se ha establecido la sesión, información del servidor e información de conexión del servidor.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-Query SEssion-----><
```











## Parámetros

---

No hay parámetros para este mandato.

## Ejemplos

---

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows Mostrar información acerca de la sesión.

**Mandato:** query session







A continuación, se muestra una pantalla query session de ejemplo:

```
Nombre de servidor.....: HALLEY_SERVER1
Tipo de servidor.....: Windows
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 2, Niv. 0.0
Fecha último acceso.....: 09/03/2009 09:08:13
Suprimir archivos copia seg....: "No"
Suprimir copias archivadas.....: "Sí"
Deduplicación.....: "Sólo servidor"
```

```
Nombre de nodo.....: HALLEY
Nombre de usuario.....:
```

Valores posibles de eliminación de duplicados de parte del cliente:

- Ninguna
  - Se visualizará al conectarse a un servidor IBM Spectrum Protect anterior a V6.1
- Sólo servidor
- Cliente o Servidor

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris



A continuación, se muestra una pantalla query session con Activar sin LAN activado de ejemplo:

```
Información de conexión de IBM Spectrum Protect Server

Nombre de servidor.....: TEMPLAR
Tipo de servidor.....: AIX
Protección de archivo de retención..: "No"
Versión de servidor.....: Ver. 6, Rel. 1, Niv. 4.0
Fecha último acceso.....: 08/12/10 22:10:15
Suprimir archivos copia seg....: "No"
Suprimir copias archivadas.....: "Sí"

Nombre de nodo.....: LAN2
Nombre de usuario.....: root






Nombre agente almacenamiento...: TEMPLAR_STA
Tipo agente almacenamiento.....: AIX
Versión agente almacenamiento..: Ver. 6, Rel. 1, Niv. 3.3
```

## Query Systeminfo

Utilice el mandato query systeminfo para recopilar información y enviar esta información a un archivo o a la consola.

La finalidad principal de este mandato es ayudar al soporte de IBM® en el diagnóstico de problemas. Sin embargo, los usuarios que estén familiarizados con los conceptos relacionados con esta información también podrían encontrarlo de utilidad.

Si utiliza la opción console, no se realiza ningún formato especial de la salida para ajustarla a la altura o anchura de la pantalla. Por consiguiente, es posible que la salida de la consola sea difícil de leer debido a la longitud y a la acomodación de líneas. Si la salida de la consola es difícil de leer, utilizar la opción filename con el mandato query systeminfo. Esta combinación permite que la salida se grabe en un archivo que puede enviarse al soporte de IBM.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```











      .----- .
      v         |
>>-Query SYSTEMInfo----- --elemento-----+-----><
                                   '- --options-'
```

## Parámetros

elemento


Especifica el elemento o elementos de los que desea recopilar información y que la información debe enviarse al nombre de archivo que ha especificado con la opción filename o a la consola. El valor predeterminado consiste en reunir todos los elementos.

Puede recopilar información acerca de uno o varios de los elementos siguientes:

- DSMOPTFILE - El contenido del archivo dsm.opt.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
DSMSYSFILE - El contenido del archivo dsm.sys.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows ENV - Variables de entorno.
- ERRORLOG - El archivo de anotaciones de errores del cliente.
- FILE - Atributos para el nombre de archivo que especifique.
-  Sistemas operativos Windows FILESNOTTOBACKUP: enumeración de la clave de registro de Windows:















```
HKEY_LOCAL_MACHINE\
  SYSTEM\
    CurrentControlSet\
      BackupRestore\
        FilesNotToBackup
```

Esta clave especifica los archivos que no tienen copia de seguridad. El mandato query inclexcl indicará que el sistema operativo excluirá dichos archivos.




- INCLEXCL - Compila una lista de sentencias de inclusión/exclusión en el orden en el que se procesan durante las operaciones de copia de seguridad y archivado.
-  Sistemas operativos WindowsKEYSNOTTORESTORE: enumeración de la clave de registro de Windows:

```
HKEY_LOCAL_MACHINE\
  SYSTEM\
    ControlSet001\
      BackupRestore\
        KeysNotToRestore
```

Esta clave especifica las claves de registro de Windows que no se deberían restaurar.

-  Sistemas operativos WindowsMSINFO: información del sistema Windows (salida de MSINFO32.EXE).
- OPTIONS - Opciones compiladas.
-  Sistemas operativos WindowsOSINFO - Nombre y versión del sistema operativo cliente
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X OSINFO - Nombre y versión del sistema operativo cliente (incluye la información ULIMIT para UNIX).
- POLICY - Volcado de conjunto de políticas.
-  Sistemas operativos WindowsREGISTRY - Entradas de registro de Windows relacionadas con IBM Spectrum Protect.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos WindowsSCHEDLOG - Contenido del registro de planificación (por lo general, dsmsched.log).
-  Sistemas operativos WindowsSFP - Lista de los archivos protegidos mediante la característica de Protección de archivos del sistema de Windows y, para cada archivo, indica ese archivo existe. Se hace una copia de seguridad de estos archivos como parte del objeto del sistema SYSFILES.
-  Sistemas operativos WindowsSFP=<nombre\_archivo> - Indica si el archivo especificado (<nombre\_archivo>) se ha protegido mediante la Protección de archivos del sistema de Windows. Por ejemplo:

```
SFP=C:\WINNT\SYSTEM32\MSVCRT.DLL
```

-  Sistemas operativos WindowsSYSTEMSTATE: información de estado del sistema de Windows.
-  Sistemas operativos AIXCLUSTER - Información de clústeres de AIX.
-  Sistemas operativos WindowsCLUSTER - Información de clústeres de Windows.
- ENCRYPT - Métodos de cifrado disponibles.

Nota:






1.  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice la opción filename para especificar un nombre de archivo en el que almacenar la información que se ha recopilado a partir de los elementos que ha especificado. Si no especifica un nombre de archivo, la información se almacenará, de forma predeterminada, en el archivo /Library/Application Support/tivoli/tsm/client/ba/bin/dsminfo.txt (para Mac OS X) o en el archivo dsminfo.txt (para otros sistemas UNIX y Linux).
2.  Sistemas operativos WindowsUtilice la opción filename para especificar un nombre de archivo en el que almacenar la información que se ha recopilado a partir de los elementos que ha especificado. Si no especifica un nombre de archivo, la información se almacenará, de forma predeterminada, en el archivo dsminfo.txt.
3. Utilice la opción console si desea que la información se muestre en la consola.

Tabla 1. mandato query systeminfo: opciones relacionadas

Opción	Dónde se utiliza
console	Sólo línea de mandatos.
filename	Sólo línea de mandatos.

## Ejemplos

Tarea

Recopilar y almacenar el contenido del archivo dsm.opt y del archivo de anotaciones de error de IBM Spectrum Protect en el archivo tsminfo.txt.

**Mandato:** query systeminfo dsmsoptfile errorlog -filename=tsminfo.txt

## Query Systemstate

Utilice el mandato query systemstate para visualizar información sobre la copia de seguridad del estado del sistema en el servidor de IBM Spectrum Protect, o en el estado del sistema en un conjunto de copias de seguridad de un servidor de IBM Spectrum Protect, cuando se especifica la opción backupsetname.

La salida indica si el objeto está activo ("A") o inactivo ("I"). Sólo aparecerán en la lista los objetos activos a menos que se especifique la opción inactive con el mandato. El cliente de copia de seguridad y archivado de Windows admite el formato estándar y detallado.

### Clientes soportados

Este mandato sólo es válido para los mandatos Windows soportados.

### Sintaxis

```
>>-Query SYSTEMState--+-+-----+-----><
                        '- options-'
```

### Parámetros

Tabla 1. mandato Query Systemstate: opciones relacionadas

Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
dateformat	En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
inactive	Sólo línea de mandatos.
numberformat	En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
showmembers	Sólo línea de mandatos.
timeformat	En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
detail	Sólo línea de mandatos.

### Ejemplos

Tarea

Visualizar información acerca de la copia de seguridad activa del estado del sistema en el servidor de IBM Spectrum Protect.

**Mandato:** query systemstate

Tarea

Visualizar información acerca de la copia de seguridad activa del estado del sistema en el servidor de IBM Spectrum Protect.

**Mandato:** query systemstate -detail

Tarea

Mostrar información sobre la copia de seguridad activa del estado del sistema contenida en el conjunto de copias de seguridad llamado daily\_backup\_data.12345678.

**Mandato:** query systemstate -backupsetname=daily\_backup\_data.12345678


Tarea

Para mostrar información acerca de Active Directory, especifique el siguiente mandato: query systemstate -detail.


Localice la información relacionada con Active Directory en la salida.

## Query VM

Utilice el mandato query VM para listar y verificar las copias de seguridad correctas de las máquinas virtuales (VM).

 Sistemas operativos Windows

El mandato query VM se puede utilizar para determinar a qué máquinas virtuales Microsoft Hyper-V y máquinas virtuales VMware se ha realizado la copia de seguridad en el servidor. La información para cada hipervisor se presenta en su propia sección. Si está consultando las copias de seguridad de las máquinas virtuales Hyper-V, puede saltarse el texto *Query VM para máquinas virtuales VMware*. Si está consultando las copias de seguridad de las máquinas virtuales VMware, no necesita leer el texto *Query VM para máquinas virtuales Hyper-V*.


 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.


 Sistemas operativos Linux  Sistemas operativos Windows

## Query VM para máquinas virtuales VMware

Utilice el mandato query vm para determinar de qué máquinas virtuales VMware se ha realizado una copia de seguridad.

## Clientes soportados

 Sistemas operativos Linux Este mandato es válido en clientes Linux instalados en un servidor de copia de seguridad vStorage.

 Sistemas operativos Windows Este mandato es válido en clientes Windows instalados en un servidor de copia de seguridad vStorage.

## Sintaxis

```
>>-Query VM-- --vmname-----+-----+-----+----->>
|           .-BOTH---. | '-options-'
| --FROM --SERVER-- |
| '-LOCAL--' |
```

## Parámetros

vmname

Especifica el nombre de host de máquina virtual que desea consultar. Si omite el nombre de la máquina virtual, el mandato muestra todas las copias de seguridad de máquina virtual en el servidor IBM Spectrum Protect.

-FROM

Especifica la ubicación o las ubicaciones de copia de seguridad que consultar. Puede especificar uno de los valores siguientes:

SERVER

La consulta está limitada a las copias de seguridad que se encuentran en el servidor de IBM Spectrum Protect.


LOCAL

La consulta está limitada a las instantáneas persistentes que se encuentran en el almacenamiento de hardware.

BOTH

La consulta lista información para las copias de seguridad que se encuentran en el servidor de IBM Spectrum Protect y para las instantáneas que se encuentran en el almacenamiento de hardware. Este es el valor predeterminado.

Tabla 1. Mandato Query VM: opciones relacionadas para consultas de la máquina virtual VMware.





Opción	Dónde se utiliza
detail Válido para vmbackuptype=fullvm  Sistemas operativos Windows Válido para -vmrestoretype	Línea de mandatos.
inactive Válido para vmbackuptype=fullvm	Línea de mandatos.

Opción	Dónde se utiliza
pitdate Válido para vmbackuptype=fullvm	Línea de mandatos.
pittime Válido para vmbackuptype=fullvm	Línea de mandatos.
vmbackuptype	Línea de mandatos o archivo de opciones del cliente.
vmchost	Línea de mandatos o archivo de opciones del cliente.
vmcpw	Línea de mandatos o archivo de opciones del cliente.
vmcuser	Línea de mandatos o archivo de opciones del cliente.

 Sistemas operativos Linux  Sistemas operativos Windows

## Ejemplos de Query VM (VMware)

A continuación figuran ejemplos de uso del mandato query VM y del mandato con la -detail.





 Sistemas operativos Linux  Sistemas operativos Windows Máquina virtual completa  
 Sistemas operativos Linux  Sistemas operativos Windows

```
q vm devesx04-24 -ina
```

Consultar máquina virtual para copia completa de máquina virtual

#	Fecha copia seg.	Clase gest.	Tamaño	Tipo	Ubic A/I	Máquina virtual
1	12/07/2016 14:45:24	DDMGMT	47.85 GB	IFFULL	I SERVER	devesx04-24
2	12/14/2016 17:38:05	DDMGMT	47.85 GB	IFINCR	A SERVER	devesx04-24
3	01/23/2017 14:07:44	DDMGMT	47.85 GB	SNAPSHOT	I LOCAL	devesx04-24
4	02/01/2017 08:59:52	DDMGMT	47.85 GB	SNAPSHOT	A LOCAL	devesx04-24

El código de retorno de ANSI900I es 0.

 Sistemas operativos Linux  Sistemas operativos Windows VM completa con opción -detail  
 Sistemas operativos Linux  Sistemas operativos Windows

```
q vm devesx04-24 -ina -detail
```


Consultar máquina virtual para copia completa de máquina virtual

#	Fecha copia seg.	Clase gest.	Tamaño	Tipo	Ubic A/I	Máquina virtual
1	12/07/2016 14:45:24	DDMGMT	47.85 GB	IFFULL	I SERVER	devesx04-24
El tamaño de esta copia de seguridad incremental : n/d El número de copias de seguridad incrementales desde última completa: 0 La cantidad de datos adicionales: 0 Fragmentación de objetos de IBM Spectrum Protect: 0 Copia de seguridad representada por: 79 objetos TSM Tipo de protección de aplicaciones: VMware Tipo de instantánea: VMware Tools Disco[1]Etiqueta: Disco duro 1 Disco[1]Nombre: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24-000003.vmdk Disco[1]Estado: Protegido Disco[2]Etiqueta: Disco duro 2 Disco[2]Nombre: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_1-000003.vmdk Disco[2]Estado: Protegido Disco[3]Etiqueta: Disco duro 3 Disco[3]Nombre: [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204 af/devesx04-24_2-000003.vmdk Disco[3]Estado: Protegido						
2	12/14/2016 17:38:05	DDMGMT	47.85 GB	IFINCR	A SERVER	devesx04-24
El tamaño de esta copia de seguridad incremental: 186,43 MB El número de copias de seguridad incrementales desde última completa: 1 La cantidad de datos adicionales: 0 Fragmentación de objetos de IBM Spectrum Protect: 2 Copia de seguridad representada por: 119 objetos TSM Tipo de protección de aplicaciones: VMware Tipo de instantánea: VMware Tools Disco[1]Etiqueta: Disco duro 1						



```

Disco[1]Nombre:      [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24-000006.vmdk
Disco[1]Estado:    Protegido
Disco[2]Etiqueta:   Disco duro 2
Disco[2]Nombre:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_1-000006.vmdk
Disco[2]Estado:    Protegido
Disco[3]Etiqueta:   Disco duro 3
Disco[3]Nombre:     [TSMXIV11:vVOL_JOANNE] rfc4122.750c6a3a-9c65-4a1f-9ed7-1b531aa204
af/devesx04-24_2-000006.vmdk
Disco[3]Estado:    Protegido
 3 01/23/2017 14:07:44 DDMGMT          47.85 GB SNAPSHOT I LOCAL      devesx04-24
El tamaño de esta copia de seguridad incremental : n/d
El número de copias de seguridad incrementales desde última completa: 0
La cantidad de datos adicionales: 0
Fragmentación de objetos de IBM Spectrum Protect: 0
Copia de seguridad representada por: 0 objetos TSM
Tipo de protección de aplicaciones: VMware
Tipo de instantánea: VMware Tools
 4 02/01/2017 08:59:52 DDMGMT          47.85 GB SNAPSHOT A LOCAL      devesx04-24
El tamaño de esta copia de seguridad incremental : n/d
El número de copias de seguridad incrementales desde última completa: 0
La cantidad de datos adicionales: 0
Fragmentación de objetos de IBM Spectrum Protect: 0
Copia de seguridad representada por: 0 objetos TSM
Tipo de protección de aplicaciones: VMware
Tipo de instantánea: VMware Tools
-----
Todos los valores promedios se calculan sólo para las copias de seguridad
incrementales-constantes mostradas anteriormente.
El tamaño medio de la copia de seguridad incremental: 186,43 MB
El número medio de copias de seguridad incrementales desde última completa: 1
La sobrecarga media de datos adicionales: 0
La fragmentación media de objetos: 0
El número medio de objetos por copia de seguridad: 49
El código de retorno de ANS1900I es 0.

```

 Sistemas operativos Windows El mandato siguiente devuelve una lista de máquinas virtuales que ejecutan una operación de restauración instantánea.

```
q vm * -vmrestoretype=instantrestore
```

 Sistemas operativos Linux  Sistemas operativos Windows Consultar todas las máquinas virtuales VMware de las que se hizo copia de seguridad utilizando -vmbacktype=fullvm:

```
q vm * -vmbacktype=fullvm
```

 Sistemas operativos Windows

## Máquinas virtuales de Query VM for Microsoft Hyper-V

Utilice el mandato query vm para determinar de qué máquinas virtuales Hyper-V se ha realizado una copia de seguridad.

## Cientes soportados

Este mandato es válido en clientes Windows instalados en un sistema de host Hyper-V.

## Sintaxis

```
>>-Query VM-- --vmname-----+-----<<
                    '-opciones-'
```

## Parámetros

vmname

Especifica el nombre de host de máquina virtual que desea consultar. El nombre de la máquina virtual distingue entre mayúsculas y minúsculas. Si especifica un nombre de máquina virtual en el mandato, el nombre no puede contener caracteres comodín.

Si omite el nombre de la máquina virtual, el mandato muestra todas las copias de seguridad de máquina virtual en el servidor IBM Spectrum Protect.

Tabla 2. Mandato Query VM: opciones relacionadas para consultas de la máquina virtual Hyper-V.

Opción	Dónde se utiliza
detail	Línea de mandatos. Muestra los detalles de cada disco (etiqueta, nombre) y su estado (protegido o excluido), las estadísticas de rendimiento de copia de seguridad incremental-constante.
inactive	Línea de mandatos.
pitdate	Línea de mandatos.
pittime	Línea de mandatos.

## Ejemplos

### Tarea

Listar todas las máquinas virtuales de las que el Data Protection for Microsoft Hyper-V ha realizado copia de seguridad en el host Hyper-V.

```
dsmc query vm
```

## Ejemplos de Query VM (Hyper-V)

El ejemplo siguiente muestra un mandato query VM que muestra información de resumen sobre todas las máquinas virtuales Hyper-V de las que se ha realizado copia de seguridad.

```
dsmc query vm
```

Consultar máquina virtual para copia completa de máquina virtual

#	Fecha copia seg.	Clase gest.	Tamaño	Tipo	Ubic A/I	Máquina virtual
1	03/19/2017 17:54:34	STANDARD	17.00 GB	IFFULL	A SERVER	DeptA_VM05
2	03/20/2017 01:51:34	STANDARD	15.00 GB	IFINCR	A SERVER	DeptA_VM_W2k08R2
3	03/20/2017 01:46:19	STANDARD	36.00 GB	IFFULL	A SERVER	DeptA_VM04

El siguiente mandato query VM con la opción -detail muestra información detallada acerca de las VM Hyper-V de las que se ha realizado copia de seguridad. El resultado detallado incluye el tipo de copia de seguridad que se ha realizado, el tamaño de la máquina virtual, información sobre sus discos, y las estadísticas.

```
dsmc query vm -detail
```

Consultar máquina virtual para copia completa de máquina virtual

#	Fecha copia seg.	Clase gest.	Tamaño	Tipo	Ubic A/I	Máquina virtual
1	03/19/2017 17:54:34	STANDARD	17.00 GB	IFFULL	A SERVER	DeptA_VM05

El tamaño de esta copia de seguridad incremental : n/d  
 El número de copias de seguridad incrementales desde última completa: 0  
 La cantidad de datos adicionales: 0  
 Fragmentación de objetos de IBM Spectrum Protect: 0  
 Copia de seguridad representada por: 99 objetos de IBM Spectrum Protect  
 Tipo de protección de aplicaciones: n/a  
 La copia de seguridad está comprimida: No  
 La copia de seguridad tiene los duplicados eliminados: No  
 Tipo de instantánea: Hyper-V RCT Coherente con la aplicación  
 Disco[1]Nombre: DeptA\_VM05.vhdx  
 Disco[1]Ubicación: IDE 0 0  
 Disco[1]Estado: Protegido  
 Disco[2]Nombre: DeptA\_VM05\_Disk2.vhdx  
 Disco[2]Ubicación: SCSI 0 1  
 Disco[2]Estado: Protegido  
 Disco[3]Nombre: Disk 7 2.00 GB Bus 0 Lun 4 Target 0  
 Disco[3]Ubicación: SCSI 0 0  
 Disco[3]Estado: Omitido: Disco físico  
 Disco[4]Nombre: Disk 8 2.50 GB Bus 0 Lun 5 Target 0

```

Disco[4]Ubicación: SCSI 0 2
Disco[4]Estado: Omitido: Disco físico
2 03/20/2017 01:51:34 STANDARD 15.00 GB IFINCR A SERVER DeptA_VM_W2k08R2
El tamaño de esta copia de seguridad incremental: 544,00 KB
El número de copias de seguridad incrementales desde última completa: 1
La cantidad de datos adicionales: 0
Fragmentación de objetos de IBM Spectrum Protect: 2
Copia de seguridad representada por: 37 objetos de IBM Spectrum Protect
Tipo de protección de aplicaciones: n/a
La copia de seguridad está comprimida: No
La copia de seguridad tiene los duplicados eliminados: No
Tipo de instantánea: Hyper-V RCT Coherente con respecto a bloqueos
Disco[1]Nombre: DeptA_VM_W2k08R2.vhdx
Disco[1]Ubicación: IDE 0 0
Disco[1]Estado: Protegido
3 03/20/2017 01:46:19 STANDARD 36.00 GB IFFULL A SERVER DeptA_VM04
El tamaño de esta copia de seguridad incremental : n/d
El número de copias de seguridad incrementales desde última completa: 0
La cantidad de datos adicionales: 0
Fragmentación de objetos de IBM Spectrum Protect: 0
Copia de seguridad representada por: 79 objetos de IBM Spectrum Protect
Tipo de protección de aplicaciones: n/a
La copia de seguridad está comprimida: No
La copia de seguridad tiene los duplicados eliminados: No
Tipo de instantánea: Hyper-V RCT Coherente con la aplicación
Disco[1]Nombre: DeptA_VM04.vhdx
Disco[1]Ubicación: IDE 0 0
Disco[1]Estado: Protegido

```

```

-----
Todos los valores promedios se calculan sólo para las copias de seguridad
incrementales-constantas mostradas anteriormente.
El tamaño medio de la copia de seguridad incremental: 544,00 KB
El número medio de copias de seguridad incrementales desde última completa: 0
La sobrecarga media de datos adicionales: 0
La fragmentación media de objetos: 0
El número medio de objetos por copia de seguridad: 71

```

La salida detallada también incluye el tipo de instantánea e información de disco como la siguiente:

#### Tipo de instantánea

El tipo de instantánea tomada durante la operación de copia de seguridad de la VM:

##### Hyper-V RCT Coherente con la aplicación

Una instantánea inmovilizada que se ha creado con Hyper-V RCT (Resilient change Tracking) en Windows Server 2016.

##### Hyper-V RCT Coherente con respecto a bloqueos

Una instantánea no inmovilizada que se ha creado con Hyper-V RCT en Windows Server 2016.

##### Hyper-V VSS

Una instantánea que se ha creado con VSS (Volume Shadow Copy Service) en Windows Server 2012 o Windows Server 2012 R2.

#### Disco[n]Ubicación

La ubicación de disco del disco de VM *n*, donde *n* es un número. La ubicación de disco consta del tipo de controlador de disco, "IDE" o "SCSI", seguido del número de controlador y el número de ubicación de dispositivo.

#### Disco[n]Estado

El estado de copia de seguridad del disco de VM *n*, donde *n* es un número.

##### Protegido

Indica que se ha hecho copia de seguridad de los datos del disco de la VM.

##### Omitido: Excluido por el usuario

Indica que el disco de la VM se ha excluido durante las operaciones de copia de seguridad según lo especificado por la opción `exclude.vmdisk`. Para obtener más información, consulte `Exclude.vmdisk`.

##### Omitido: Disco físico

Indica que el disco de la VM es un disco físico (disco de paso a través) y no se ha realizado copia de seguridad de sus datos. Sólo se efectúa copia de seguridad de la información de configuración de disco. Para obtener más información, consulte `Vmprocessvmwithphysdisks`.

El siguiente ejemplo muestra la sintaxis que debe utilizarse para listar la salida detallada de una máquina virtual específica denominada `DeptA_VM_W2k08R2`.

```
dsmc query vm DeptA_VM_W2k08R2 -detail
```

Consultar máquina virtual para copia completa de máquina virtual



#	Fecha copia seg.	Clase gest.	Tamaño	Tipo	Ubic A/I	Máquina virtual
1	03/20/2017 01:51:34	STANDARD	15.00 GB	IFINCR	A SERVER	DeptA_VM_W2k08R2

El tamaño de esta copia de seguridad incremental: 544,00 KB  
El número de copias de seguridad incrementales desde última completa: 1  
La cantidad de datos adicionales: 0  
Fragmentación de objetos de IBM Spectrum Protect: 2  
Copia de seguridad representada por: 37 objetos de IBM Spectrum Protect  
Tipo de protección de aplicaciones: n/a  
La copia de seguridad está comprimida: No  
La copia de seguridad tiene los duplicados eliminados: No  
Tipo de instantánea: Hyper-V RCT Coherente con respecto a bloqueos  
Disco[1]Nombre: Jimmy\_VM\_Windows2008R2.vhdx  
Disco[1]Ubicación: IDE 0 0  
Disco[1]Estado: Protegido

---

Todos los valores promedios se calculan sólo para las copias de seguridad incrementales-constantas mostradas anteriormente.  
El tamaño medio de la copia de seguridad incremental: 544,00 KB  
El número medio de copias de seguridad incrementales desde última completa: 1  
La sobrecarga media de datos adicionales: 0  
La fragmentación media de objetos: 2  
El número medio de objetos por copia de seguridad: 37

## Restart Restore

El mandato restart restore visualiza una lista de las sesiones de restauración reiniciables en la base de datos del servidor.






Sólo puede reiniciar una única sesión de restauración reiniciable al mismo tiempo. Vuelva a ejecutar el mandato restart restore para reiniciar más restauraciones.

La restauración reiniciada utiliza las mismas opciones que se usaron en la restauración que no se pudo ejecutar. La restauración reiniciada continúa a partir del punto en que se detuvo la restauración anterior.

Para cancelar sesiones de restauración reiniciables, utilice el mandato cancel restore. Utilice el mandato restart restore cuando:

- Las sesiones de restauración reiniciables bloquean el espacio de archivos del servidor, por lo que los archivos no se pueden traspasar fuera de los volúmenes secuenciales del servidor.
- No se puede hacer una copia de seguridad de archivos afectados por una restauración reiniciable.

Las opciones de la sesión que no se pudo ejecutar sustituyen a las opciones nuevas o modificadas de la sesión reiniciada.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-REStArt Restore-----<<
```

## Parámetros

No hay parámetros para este mandato.

## Ejemplos

Tarea





Reiniciar una restauración.

**Mandato:** restart restore

## Restore

El mandato restore obtiene copias de versiones de las copias de seguridad de los archivos del servidor de IBM Spectrum Protect o en el interior de un conjunto de copias de seguridad.

Para restaurar los archivos, especifique los directorios o los archivos seleccionados o seleccione los archivos en una lista. Puede restaurar los archivos en el directorio desde donde se realizó la copia de seguridad o en otro directorio. El cliente de copia de seguridad y archivado utiliza la opción preservepath con el valor subtree como valor predeterminado para restaurar los archivos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Nota:

1. En los sistemas UNIX y Linux, cuando se ha creado un enlace simbólico, la hora de modificación de éste se establece en la hora actual del sistema y no puede cambiarse. De esta manera, cuando se restaura un vínculo simbólico, su fecha y hora de modificación se establecen en la fecha y la hora de la restauración y no en la fecha y la hora en que se hizo copia de seguridad del vínculo. Como resultado, el cliente hará copia de seguridad del vínculo simbólico durante la siguiente copia de seguridad incremental, puesto que su hora de modificación ha cambiado desde la última copia de seguridad.





 Sistemas operativos Windows Nota:

1. Cuando se restaura un directorio, la fecha y la hora de modificación de éste se establecen en la fecha y la hora de la restauración, no en la fecha y la hora que tenía el directorio cuando se realizó la copia de seguridad de éste. Esto se debe a que el cliente restaura primero los directorios y, a continuación, añade los archivos a los directorios.
2. Si se intenta restaurar un archivo cuyo nombre es el mismo que el nombre abreviado de un archivo ya existente se producirá un error. Por ejemplo, si se quiere restaurar un archivo cuyo nombre específico es ABCDEF~1.DOC en el mismo directorio en el que se encuentra un archivo llamado abcdefghijk.doc, la restauración falla porque el sistema operativo Windows convierte el nombre del archivo llamado abcdefghijk.doc en el nombre abreviado ABCDEF~1.DOC. La función de restauración trata este caso como una duplicación de archivos.





Si se produce este error, ejecute cualquiera de las acciones siguientes para corregirlo:

- Restaurar el archivo con el nombre abreviado pero colocándolo en un sitio distinto.
- Detener la operación de restauración y cambiar el nombre del archivo ya existente.
- Desactivar el soporte de nombres de archivos abreviados en Windows.
- No utilizar nombres de archivos que entren en conflicto con el convenio de nombres de archivos abreviados; por ejemplo, no utilizar el nombre ABCDEF~1.DOC.





Si establece la opción subdir en yes al restaurar una vía de acceso y un archivo específicos, el cliente restaura de forma recursiva todos los subdirectorios bajo esa vía de acceso y las instancias del archivo especificado que existan en los subdirectorios.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si restaura un directorio o un árbol de directorios completo y no especifica las opciones inactive, latest, pick, todote y fromdate en el mandato restore, el cliente hace un seguimiento de los objetos que se restauran. Si, por alguna razón, el proceso de restauración se interrumpe, puede reiniciar la restauración en el punto de interrupción emitiendo el mandato restart restore. Se pueden crear varias sesiones de restauración reiniciables. Las restauraciones sólo son reiniciables si la especificación de archivo consta sólo de caracteres comodín. Por ejemplo, para una restauración reinicialable, emita:


```
dsmc rest /home/* -sub=yes
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Para una restauración que no sea reinicialable, emita:






```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Utilice el mandato query restore para visualizar una lista de las sesiones de restauración reiniciables en la base de datos del servidor. No podrán realizarse copias de seguridad del sistema de archivos adicionales, a menos que la restauración reinicialable se complete mediante la utilización del mandato restart restore o se cancele mediante la utilización del mandato cancel restore.

```
dsmc rest "/Users/user1/file?.c" -sub=yes
```

 Sistemas operativos Windows Para obtener más información, consulte el artículo de Microsoft Knowledge Base Q121007, titulado *How to Disable the 8.3 Name Creation on NTFS Partitions*.

 Sistemas operativos Windows Si es necesario volver a emitir el mandato restore porque se ha producido un error en las comunicaciones o se ha perdido la sesión, en las estadísticas se visualizarán los bytes que el cliente ha intentado transferir en todos los intentos del mandato. Por lo tanto, puede que las estadísticas de los bytes transferidos no coincidan con las estadísticas de los archivos, como las correspondientes al tamaño del archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
.- --FILE-.
>>-REStore--+-+-----+----->
                '- --options-'
>--+- --sourcefilespec-----+----->
    '- --{--filespaceName--}--sourcefilespec-'
>--+- --sourcefilespec-----+-----+----->
    '- --"sourcefilespec"- ' '- --destinationfilespec-'
>+-----+-----+----->
    '-BACKUPSETName=--+--backupsetname--+-'
                +-localfilename--+
                '-tapeDevice----'
>+-----+-----<
    '-LOcation=--+--server--+-'
                +-file----+
                '-tape----'
```


## Parámetros

### file

Este parámetro especifica que el nombre del archivo origen es un nombre de archivo explícito. Este parámetro es necesario cuando se restaura un nombre de archivo desde la vía de acceso actual, cuando no se especifica una vía de acceso relativa o absoluta y cuando el nombre de archivo entra en conflicto con una de las palabras clave reservadas del mandato restore, como restore backupset.


### sourcefilespec

Especifica la vía de acceso y el nombre del archivo del almacenamiento que desea restaurar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

 **Sistemas operativos Windows**Nota: si incluye el filespaceName, no incluya una letra de unidad en la especificación de archivo.

### {filespaceName}

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación de trabajo desde la que realizó la copia de seguridad de los archivos. Especifique el nombre del espacio de archivos si el nombre de etiqueta de unidad ha sido modificado o si está restaurando archivos cuyas copias de seguridad se realizaron desde otro nodo con nombres de etiqueta de unidad diferentes de los suyos.

 **Sistemas operativos Windows**Nota: Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. En la modalidad de bucle se pueden utilizar indistintamente comillas dobles o comillas simples. Por ejemplo, {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.





### destinationfilespec

Indica la vía de acceso y el nombre de archivo donde desea colocar los archivos restaurados. Si no especifica un destino, el cliente restaura los archivos en la vía de acceso de origen inicial.

 **Sistemas operativos Windows**Cuando especifique destinationfilespec, tenga en cuenta los puntos siguientes:

- Si sourcefilespec especifica un único archivo, destinationfilespec puede ser un archivo o un directorio. Si está restaurando un único archivo, tiene la opción de terminar la especificación con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo.
- Si sourcefilespec contiene caracteres comodín o se especifica `subdir=yes`, destinationfilespec debe ser un directorio y debe terminar con un delimitador de directorio (\).

Nota: Si la vía de acceso de destino o cualquier parte de ella no existe, el cliente creará una vía de acceso.

 **Sistemas operativos AIX**  **Sistemas operativos Linux**  **Sistemas operativos Oracle Solaris**  **sistemas operativos Mac OS X**  
Nota: si no especifica un destino, el cliente determina si puede accederse al sistema de archivos original. Si no es posible acceder al sistema de archivos original, el cliente no restaurará el archivo. En este caso, puede especificar un destino distinto y volver a intentar el mandato.

### BACKUPSETName=

Especifica el nombre de un juego de copias de seguridad. Este parámetro es opcional. Si especifica el parámetro backupsetname con el mandato restore, no puede utilizar la opción pick.

El valor de backupsetname depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de las opciones siguientes:

**backupsetname**

Especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect. Si se especifica el parámetro location, debe establecer `-location=server`. Si el conjunto de copias de seguridad está ubicado en el almacenamiento del servidor de IBM Spectrum Protect, el juego de copias de seguridad debe tener una tabla de contenido.

**localfilename**

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer `-location=file`.

**tapedevice**

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer `-location=tape`.

**LOCation=**

Especifica dónde ha de buscar el cliente el juego de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect.

**servidor**

Especifica que el cliente buscará el juego de copias de seguridad del servidor. Se trata de la ubicación predeterminada.

**file**























































Especifica que el cliente buscará el juego de copias de seguridad en un archivo local.

**tape**



Especifica que el cliente buscará el juego de copias de seguridad en un dispositivo de cinta local.

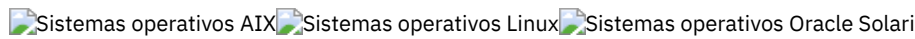
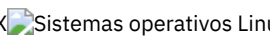
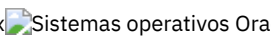
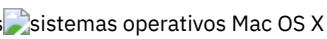
Tabla 1. mandato Restore: opciones relacionadas

Opción	Dónde se utiliza
Sistemas operativos Windows asrmode	Sistemas operativos Windows Sólo línea de mandatos.
Sistemas operativos Windows dateformat	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X dateformat	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
dironly	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X followsymbolic	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
fromdate	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X sistemas operativos Mac OS X fromowner	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  sistemas operativos Mac OS X Sólo línea de mandatos.
fromtime	Sólo línea de mandatos.
ifnewer	Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
latest	Sólo línea de mandatos.

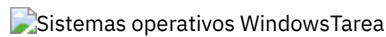
Opción	Dónde se utiliza
 Sistemas operativos Windows numberformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X numberformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
pick Nota: Si especifica el parámetro backupsetname con el mandato restore, no puede utilizar la opción pick.	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
preservepath	Sólo línea de mandatos.
 Sistemas operativos Windows replace	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X replace	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows skipntpermissions	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows skipntsecuritycrc	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows subdir	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X subdir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows tapeprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X tapeprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X timeformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
todate	Sólo línea de mandatos.
totime	Sólo línea de mandatos.

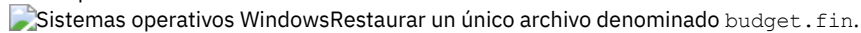
## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea

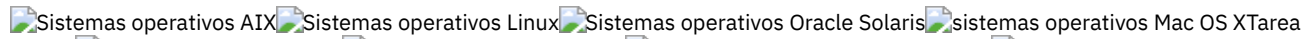
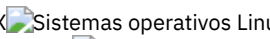
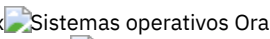
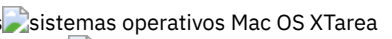
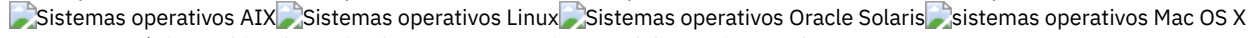
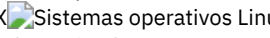
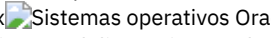
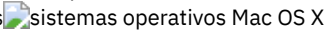
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Restaurar un único archivo denominado `budget` en el directorio `/Users/user1/Documents`.

```
restore /home/devel/projecta/budget
```

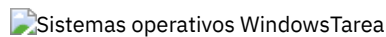
 Sistemas operativos WindowsTarea

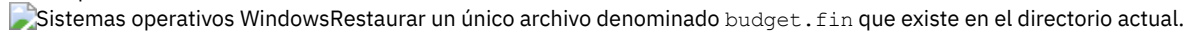
 Sistemas operativos WindowsRestaurar un único archivo denominado `budget.fin`.

```
restore c:\devel\projecta\budget.fin
```

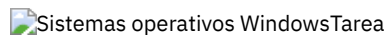
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Restaurar un único archivo denominado `budget` que existe en el directorio actual.

```
restore file budget
```

 Sistemas operativos WindowsTarea

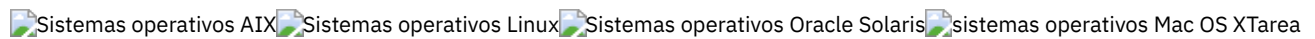
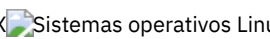
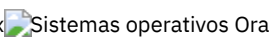
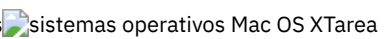
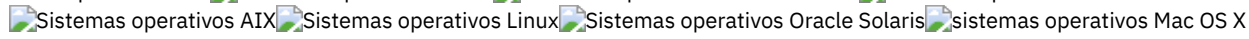
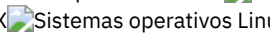
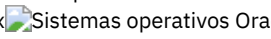
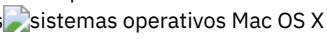
 Sistemas operativos WindowsRestaurar un único archivo denominado `budget.fin` que existe en el directorio actual.

```
restore file budget.fin
```

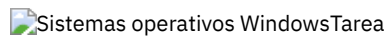
 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsRestaurar los archivos del directorio `proj` del espacio de archivos `abc`.

```
rest {"abc"}\proj\*.*
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Restaurar todos los archivos que tienen la extensión de archivo `.c` del directorio `/home/devel/projecta`.

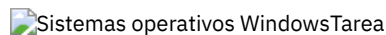
```
restore "/home/devel/projecta/*.c"
```

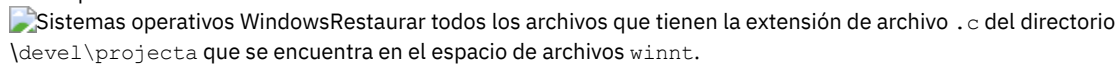
 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsRestaurar todos los archivos que tienen la extensión de archivo `.c` del directorio

```
c:\devel\projecta.
```

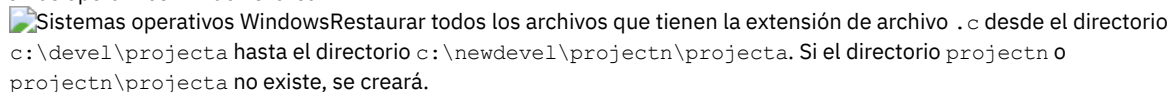
```
rest c:\devel\projecta\*.c
```

 Sistemas operativos WindowsTarea

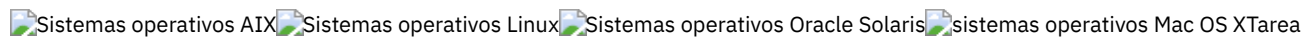
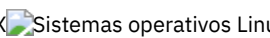
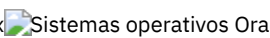
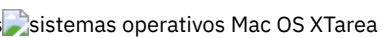
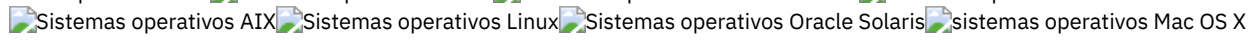
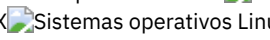
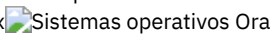
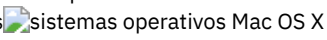
 Sistemas operativos WindowsRestaurar todos los archivos que tienen la extensión de archivo `.c` del directorio `\devel\projecta` que se encuentra en el espacio de archivos `winnt`.

```
rest {winnt}\devel\projecta\*.c
```

 Sistemas operativos WindowsTarea

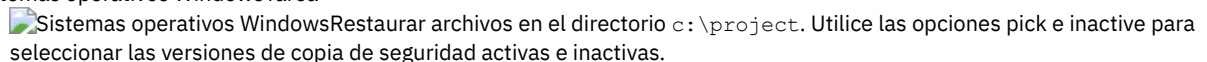
 Sistemas operativos WindowsRestaurar todos los archivos que tienen la extensión de archivo `.c` desde el directorio `c:\devel\projecta` hasta el directorio `c:\newdevel\projectn\projecta`. Si el directorio `projectn` o `projectn\projecta` no existe, se creará.

```
restore c:\devel\projecta\*.c c:\newdevel\projectn\
```


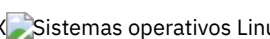
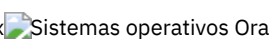
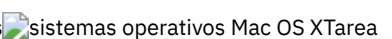
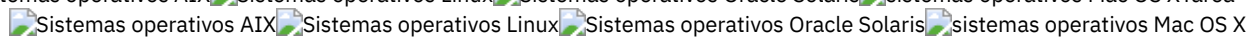
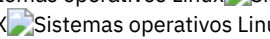
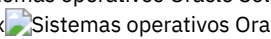
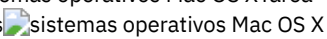
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Restaurar archivos en el directorio `/user/project`. Utilice las opciones `pick` e `inactive` para seleccionar las versiones de copia de seguridad activas e inactivas.

```
restore "/user/project/*" -pick -inactive
```

 Sistemas operativos WindowsTarea

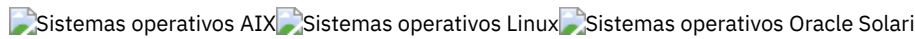
 Sistemas operativos WindowsRestaurar archivos en el directorio `c:\project`. Utilice las opciones `pick` e `inactive` para seleccionar las versiones de copia de seguridad activas e inactivas.

```
restore c:\project* -pi -ina
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Restaurar todos los archivos del directorio `/home/devel/projecta` que finalizan con el carácter `.c` en el directorio `/home/newdevel/projectn/projecta`. Si el directorio `projectn` o `projectn/projecta` no existe, se creará.

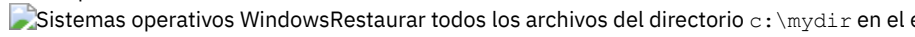
```
restore "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XTarea

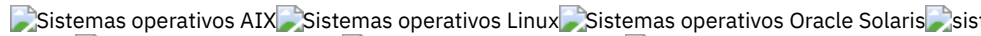
 Restaurar todos los archivos del directorio `/home/mydir` en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.

```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```


 Restaurar todos los archivos del directorio `c:\mydir` en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.

 Restaurar todos los objetos en el directorio `/home/myid/`. Puesto que esta operación de restauración se especifica sólo con caracteres comodín, si el proceso se interrumpiera, se crearía una sesión de restauración reinicializable.


```
restore -pitd=8/17/2002 -pitt=13:00:00 c:\mydir\
```

 Restaurar un archivo desde el espacio de archivos renombrado `\\nodo\h$\_OLD` hasta su ubicación original. Entre el origen y el destino como se indica a continuación:


```
res "/home/myid/*"
```

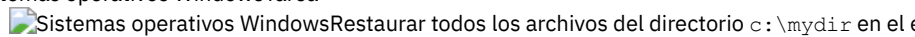
 Restaurar un archivo desde el espacio de archivos renombrado `\\your-node\h$\_OLD\docs\myresume.doc` hasta su ubicación original. Entre el origen y el destino como se indica a continuación:

```
res \\your-node\h$\_OLD\docs\myresume.doc h:\docs\
```







 Restaurar todos los archivos del directorio `/home/mydir` en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.


```
restore -pitd=8/17/2002 -pitt=13:00:00 /home/mydir/
```

 Restaurar todos los archivos del directorio `c:\mydir` en el estado que éstos tenían a las 13:00 horas del día 17 de agosto de 2002.

 Restaurar un único archivo denominado `budget.fin` que reside en el conjunto de copias de seguridad denominado `daily_backup_data.12345678`.

```
restore c:\projecta\budget.fin -backupsetname=daily_backup_data.12345678 -location=server
```

- Restauración de puntos de montaje de volúmenes NTFS o ReFS  
Cuando restaure un sistema de archivos que contenga un punto de montaje de volumen, solo se restaura el punto de montaje (directorio). Los datos del volumen montado en el directorio no se restauran.
-  Restauración de puntos de unión Dfs de Microsoft  
Para restaurar puntos de unión Dfs de Microsoft, debe restaurar la raíz Dfs de Microsoft.
-  Restauración de archivos activos  
Si se restauran versiones activas e inactivas del mismo archivo utilizando la opción `replace`, únicamente se sustituye el archivo restaurado más recientemente.
-  Restauraciones de Convenio de denominación universal  
El cliente almacena archivos en el servidor de IBM Spectrum Protect mediante la utilización del Convenio de denominación universal (UNC) de Windows, no de la letra de unidad. El nombre UNC es el nombre de red para el archivo. El nombre del sistema forma parte del nombre UNC. Por ejemplo, si el nombre del sistema es `STAR` y tiene un archivo denominado `c:\doc\h2.doc`, el nombre UNC es `\\star\c$\doc\h2.doc`.
-  Restauración desde espacios de archivos que no están activados para Unicode  
Si desea realizar una restauración desde espacios de archivos que no están activados para Unicode, debe especificar el origen en el servidor y un destino en el cliente, antes de instalar el cliente activado para Unicode.
-  Restauración de corrientes designadas  
El cliente de copia de seguridad y archivado restaura las corrientes designadas sólo en términos de archivo.
-  Restauración de archivos esparcidos  
Al restaurar archivos esparcidos en un sistema de archivos que no sea NTFS ni ReFS, establezca el valor del tiempo de espera de comunicación (`idletimeout`) del servidor de IBM Spectrum Protect en un valor máximo de 255 para evitar que se exceda el tiempo de espera de la sesión del cliente.



## Restauración de puntos de montaje de volúmenes NTFS o ReFS

---

Cuando restaure un sistema de archivos que contenga un punto de montaje de volumen, solo se restaura el punto de montaje (directorio). Los datos del volumen montado en el directorio no se restauran.

Un punto de montaje también se puede restaurar de forma individual. Por ejemplo, C:\mount es un punto de montaje y se ha realizado copia de seguridad como parte de la unidad C:\ del sistema denominado STORMAN. El mandato siguiente se puede utilizar para restaurar este punto de montaje:

```
dsmc restore {\\storman\c$}\mount
```

Las llaves ({ y }) son necesarias si también ha realizado una copia de seguridad de los datos del volumen montado desde el punto de montaje. Sin las llaves, el cliente restaura datos del espacio de archivos con el nombre más largo que coincide con la especificación de archivo. Si realizó la copia de seguridad de los datos a través del punto de montaje, las copias de seguridad se almacenan en un espacio de archivos llamado \\storman\c\$\mount. Las llaves se utilizan para especificar que los datos se restaurarán desde el espacio de archivos \\storman\c\$.

El punto de montaje no se puede restaurar si cualquiera de las condiciones siguientes es verdadera:


- El punto de montaje ya existe.
- Existe un directorio que no está vacío con el nombre del punto de montaje.
- Existe un archivo con el nombre del punto de montaje.
- Restauración de datos en volúmenes montados NTFS  
El punto de montaje debe existir para que los datos del volumen montado se puedan restaurar en una ubicación original.

### Conceptos relacionados:

Restauración de datos en volúmenes montados NTFS

Copia de seguridad de puntos de montaje de volúmenes NTFS o ReFS

Copia de seguridad de datos en volúmenes montados NTFS o ReFS

 Sistemas operativos Windows

## Restauración de puntos de unión Dfs de Microsoft

---

Para restaurar puntos de unión Dfs de Microsoft, debe restaurar la raíz Dfs de Microsoft.

Si selecciona el propio punto de unión, el cliente de copia de seguridad y archivado restaura los datos bajo el punto de unión, pero no el punto de unión propiamente dicho. Si selecciona un punto de unión que ya no existe en la raíz Dfs, el cliente crea un directorio local en la raíz Dfs con el mismo nombre que tenía el punto de unión antes de realizar la restauración de los datos.

 Sistemas operativos Windows

## Restauración de archivos activos

---

Si se restauran versiones activas e inactivas del mismo archivo utilizando la opción `replac`, únicamente se sustituye el archivo restaurado más recientemente.

 Sistemas operativos Windows

## Restauraciones de Convenio de denominación universal

---

El cliente almacena archivos en el servidor de IBM Spectrum Protect mediante la utilización del Convenio de denominación universal (UNC) de Windows, no de la letra de unidad. El nombre UNC es el nombre de red para el archivo. El nombre del sistema forma parte del nombre UNC. Por ejemplo, si el nombre del sistema es STAR y tiene un archivo denominado c:\doc\h2.doc, el nombre UNC es \\star\c\$\doc\h2.doc.

Cuando restaura archivos en el mismo sistema desde el que se ha realizado la copia de seguridad de éstos, puede utilizar la letra de unidad local o el nombre UNC para hacer referencia al archivo. Por ejemplo, se puede restaurar c:\doc\h2.doc en su ubicación original de las siguientes formas:

```
dsmc restore c:\doc\h2.doc  
dsmc restore \\star\c$\doc\h2.doc
```

Cuando restaura archivos en un sistema que tiene un nombre distinto, debe utilizar el nombre UNC para hacer referencia al archivo. Ello también tendrá aplicación cuando realice la restauración en el mismo sistema físico y el nombre del sistema haya cambiado desde que tuvo lugar la realización de la copia de seguridad.



Por ejemplo, si ha realizado la copia de seguridad de c:\doc\h2.doc en el sistema STAR y desea restaurar el archivo en el sistema METEOR, deberá utilizar el nombre UNC para hacer referencia al archivo. También deberá especificarse una ubicación de restauración de destino. Esto se debe a que el comportamiento predeterminado consiste en restaurar el archivo en su ubicación original, que sería el sistema STAR. Para restaurar el archivo en el sistema METEOR, se puede ejecutar uno de los siguientes mandatos en METEOR:


```
dsmc restore \\star\c$\doc\h2.doc c:\
dsmc restore \\star\c$\doc\h2.doc \\meteor\c$\
```


 sistemas operativos Mac OS X  Sistemas operativos Windows


## Restauración desde espacios de archivos que no están activados para Unicode

---


Si desea realizar una restauración desde espacios de archivos que no están activados para Unicode, debe especificar el origen en el servidor y un destino en el cliente, antes de instalar el cliente activado para Unicode.


 sistemas operativos Mac OS X Nota: Esta sección acerca de Unicode sólo se aplica a Mac OS X.

 Sistemas operativos Windows Si desea realizar una restauración desde espacios de archivos que no están activados para Unicode, debe especificar el origen en el servidor y un destino en el cliente. Por ejemplo, ha realizado la copia de seguridad del disco H denominado \\nodo\h\$ antes de instalar el cliente activado para Unicode. Después de la instalación, emita el mandato siguiente para una copia de seguridad selectiva:


 Sistemas operativos Windows

```
sel h:\logs\*.log
```

 sistemas operativos Mac OS X Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que ha realizado la copia de seguridad de todos los archivos .log en el directorio /Users/user5/Documents. Antes de que se produzca la operación de copia de seguridad, el servidor cambia el nombre del espacio de archivos por Jaguar\_OLD. La operación de copia de seguridad coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado /. Ahora, el nuevo espacio de archivos activado para Unicode sólo contiene el directorio /Users/user5/Documents y los archivos \*.log especificados en la operación.

 sistemas operativos Mac OS X Si desea restaurar un archivo del espacio de archivos *nombre cambiado* (old) en su ubicación original, deberá especificar el origen y el destino de la forma siguiente:

```
restore Jaguar_OLD/Users/user5/Documents
/mylog.log /Users/user5/Documents/
```

 Sistemas operativos Windows Antes de que tenga lugar la copia de seguridad, el servidor cambiará el nombre del espacio de archivos por \\nodo\h\$\_OLD. La operación de copia de seguridad coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado \\nodo\h\$. Ahora, ese espacio de archivos sólo contiene el directorio \logs y los archivos \*.log. Si desea restaurar un archivo del espacio de archivos *renombrado* (old) a su ubicación original, debe entrar el origen y el destino como se indica a continuación:

```
restore \\nodo\h$_OLD\docs\informe.doc h:\docs\
```

 Sistemas operativos Windows

## Restauración de corrientes designadas

---

El cliente de copia de seguridad y archivado restaura las corrientes designadas sólo en términos de archivo.

Los directorios de Windows pueden contener corrientes designadas. Durante una operación de restauración, las corrientes designadas asociadas a un directorio siempre se modificarán (independientemente del valor de la opción prompt).

 Sistemas operativos Windows

## Restauración de archivos esparcidos

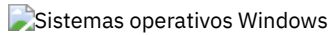
---

Al restaurar archivos esparcidos en un sistema de archivos que no sea NTFS ni ReFS, establezca el valor del tiempo de espera de comunicación (idletimeout) del servidor de IBM Spectrum Protect en un valor máximo de 255 para evitar que se exceda el tiempo de espera de la sesión del cliente.

El cliente de copia de seguridad y archivado está limitado a restaurar archivos esparcidos de tamaño inferior a 4 gigabytes.

Si se restauran más datos de los que permite la cuota de disco de Microsoft, puede que ocurra lo siguiente:

- Si el usuario que realiza la restauración dispone de una cuota de disco (por ejemplo, el usuario pertenece al grupo de operadores de copia de seguridad), el cliente no restaura los datos que sobrepasen la cuota de disco del usuario de restauración y muestra el mensaje "Disco lleno".
- Si el usuario que realiza la restauración no dispone de una cuota de disco (por ejemplo, pertenece al grupo de administradores), el cliente restaura todos los datos y transfiere la propiedad de los archivos que sobrepasen la cuota de disco del propietario original al usuario que realiza la restauración (en este caso, el administrador).



## Restore Adobjects

Utilice el mandato restore adobjects para restaurar objetos de Active Directory individuales del contenedor de objetos suprimidos local.

Los clientes de copia de seguridad y archivado que se ejecutan en plataformas Windows Server pueden restaurar objetos individuales de Active Directory de las copias de seguridad completas de estado de sistema almacenadas en el servidor de IBM Spectrum Protect.

## Clientes soportados

Este mandato es válido para clientes de sistema operativo Windows Server .

## Sintaxis

```
>>-Restore ADOBJects--+-+-----+-----+-----+----->
                        '-especificación_vía_de_acceso_origen-'
>--+-+-----+-----+-----+-----<
    '-options-'
```

## Parámetros

### sourcepathspec

Especifica el objeto o contenedor de Active Directory que desea restaurar. Si se especifica un contenedor, su contenido se restaurará también. Puede especificar el nombre distinguido completo de un objeto o un contenedor o sólo el atributo del nombre ('cn' o 'ou'), donde es posible utilizar el comodín. Los siguientes caracteres especiales requieren un carácter de escape, la barra inclinada invertida, (\), si alguno está incluido en el nombre:

- \
- #
- +
- =
- <
- >

Por ejemplo, "cn=test#" se especificará como "cn=test\#".

El cliente no puede mostrar nombres de objetos que contengan un asterisco (\*) como parte del nombre.

No utilice caracteres comodín cuando especifique un nombre distinguido.

Tabla 1. Mandato restore Adobjects: opciones relacionadas

Opción	Dónde se utiliza
adlocation	Sólo línea de mandatos.
dateformat (la opción no se tiene en cuenta si no se ha especificado adlocation)	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
pitdate (la opción no se tiene en cuenta si no se ha especificado adlocation)	Sólo línea de mandatos.

Opción	Dónde se utiliza
pittime (la opción no se tiene en cuenta si no se ha especificado adlocation)	Sólo línea de mandatos.
replace	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
timeformat (la opción no se tiene en cuenta si no se ha especificado adlocation)	Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

## Ejemplos

Tarea

Restaurar un objeto suprimido de Active Directory específico.

**Mandato:** restore adobj "CN=Administrator,CN=Users,DC=bryan,DC=test,DC=ibm,DC=com"

Tarea

Restaurar todos los objetos suprimidos ubicados originalmente en el contenedor Usuarios.

**Mandato:** restore adobj "CN=Users,DC=bryan,DC=test,DC=ibm,DC=com"

Tarea

Restaurar objetos individuales de Active Directory del servidor de IBM Spectrum Protect local. Utilice las opciones pitdate y pittime para realizar una selección en una lista de versiones de copia de seguridad más y menos recientes.

**Mandato:** restore adobj "cn=guest" -adloc=server -pitdate=03/17/2008 -pittime=11:11:11

Tarea

Restaurar todos los usuarios suprimidos cuyo nombre empieza por Fred.

**Mandato:** restore adobjects "cn=Fred\*"






Tarea

Restaurar todas las unidades organizativas cuyo nombre sea testou.

**Mandato:** restore adobjects "ou=testou"

## Restore Backupset

El mandato restore backupset restaura un juego de copias de seguridad del servidor de IBM Spectrum Protect, de un archivo local o de un dispositivo de cinta local. Puede restaurar todo el juego de copias de seguridad o, en algunos casos, archivos específicos del juego de copias de seguridad.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-REStore Backupset--+-----+----->
      '+-----+-----sourcefilespec-'
      '-{filespacename}-'

>--+-----+-----+-----+-----+----->
      '-destinationfilespec-' '-options-'


>--+backupsetname+--+-----+-----<
      +-localfilename+ '- -LOCation= --+server+-'
      '-tapedevice----'           +-file---+
                                   '-tape---'
```

{filespacename}

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación de trabajo de cuyos archivos se realizó copia de seguridad o el nombre de espacio de archivos virtual para el grupo.

Especifique un nombre de espacio de archivos cuando restaure un conjunto de copias de seguridad que contenga un grupo.

Especifique un nombre de espacio de archivos cuando el parámetro *sourcefilespec* no exista en el sistema de destino. Esto puede suceder si el nombre de la etiqueta de unidad ha sido modificado o si está restaurando archivos de los que ha realizado copia de seguridad desde otro nodo con etiquetas de unidad distintas de las suyas.

 **Sistemas operativos Windows**Nota: Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. Sólo son válidas las comillas simple en modalidad de bucle. Por ejemplo, {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.

sourcefilespec

Especifica la vía de acceso de origen de una parte del conjunto de copias de seguridad. El valor predeterminado es restaurar todo el conjunto de copias de seguridad.

destinationfilespec

Especifica la vía de acceso de destino para los archivos restaurados. Si no especifica *sourcefilespec*, no puede especificar *destinationfilespec*. Si no especifica un destino, el cliente de copia de seguridad y archivado restaura los archivos en la vía de acceso de origen inicial. Si está restaurando más de un archivo, debe terminar la especificación de archivo con un delimitador de directorio (/); de lo contrario, el cliente presupone que el último nombre es un nombre de archivo e indica que se ha producido un error. Si está restaurando un único archivo, tiene la opción de terminar la especificación de archivo con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo. Cuando *sourcefilespec* no existe en la estación de trabajo de destino, debe especificar *destinationfilespec*.

-BACKUPSETName=

Especifica el nombre del conjunto de copias de seguridad desde el que se realiza una operación de restauración. No puede utilizar caracteres comodín para especificar el nombre del juego de copias de seguridad. El valor de *backupsetname* depende de la ubicación del conjunto de copias de seguridad y se corresponde con una de las opciones siguientes:

*backupsetname*

Especifica el nombre del conjunto de copias de seguridad del servidor desde el que se realiza la operación de restauración. Si se especifica *location*, debe establecer *-location=server*.

*localfilename*

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer *-location=file*.

*tapedevice*

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer *-location=tape*.

-LOCation=

Especifica la ubicación del conjunto de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect. Si especifica el parámetro de ubicación, el valor debe corresponder a una de las tres opciones siguientes:

server

Especifica que el juego de copias de seguridad se encuentra en el servidor de IBM Spectrum Protect. Server es la ubicación predeterminada.

file

Especifica que el conjunto de copias de seguridad se encuentra en un sistema de archivos disponible.

tape

Especifica que el conjunto de copias de seguridad se encuentra en un dispositivo de cinta disponible.

Tabla 1. mandato Restore Backupset: opciones relacionadas

Opción	Dónde se utiliza
dirsonly	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
ifnewer	Sólo línea de mandatos.
preservepath	Sólo línea de mandatos.

Opción	Dónde se utiliza
Sistemas operativos Windowsquiet	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS Xquiet	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows replace	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X replace	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows skipntpermissions	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows subdir	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X subdir	Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.

## Ejemplos

### Tarea

Restaurar el conjunto de copias de seguridad denominado monthly\_financial\_data.87654321 del servidor.

```
dsmc restore backupset
-backupsetname=monthly_financial_data.87654321
-loc=server
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Restaurar todo el conjunto de copias de seguridad contenido en el archivo:/home/budget/weekly\_budget\_data.ost.

```
dsmc restore backupset
-backupsetname="/home/budget/weekly_budget_data.ost"
-loc=file
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Restaurar todo el conjunto de copias de seguridad del dispositivo /dev/rmt0.

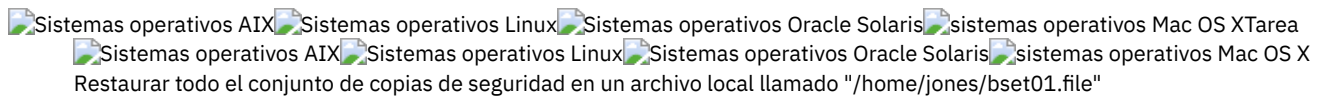
```
dsmc restore backupset
"-backupsetname=/dev/rmt0" -loc=tape
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Restaurar un único archivo denominado /home/jones/budget.dev del dispositivo de cinta /dev/rmt0 en la vía de acceso de origen original.

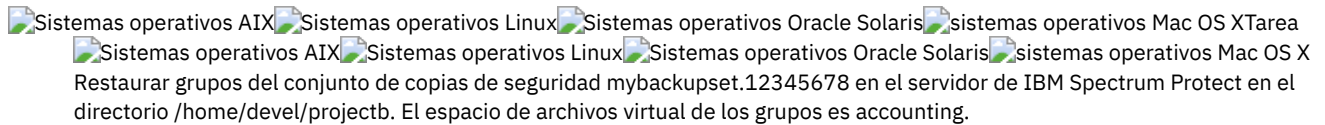
```
dsmc restore backupset
-backupsetname=/dev/rmt0 "/home/jones/budget.dev"
-loc=tape
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS XTarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Restaurar todos los archivos del directorio budget que tienen la extensión .txt desde cintas del dispositivo /dev/rmt0 en la vía de acceso original.

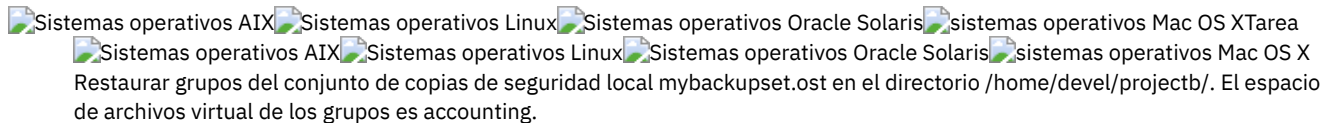
```
dsmc restore backupset "/home/budget/*.txt"
-backupsetname=/dev/rmt0 -loc=tape
```

 Restaurar todo el conjunto de copias de seguridad en un archivo local llamado "/home/jones/bset01.file"

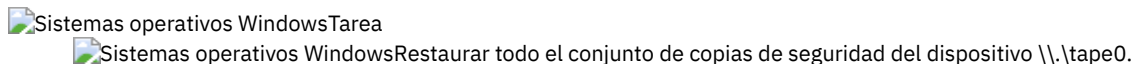
```
dsmc restore backupset  
-backupsetname="/home/jones/bset01.file"  
-loc=file
```

 Restaurar grupos del conjunto de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio /home/devel/projectb. El espacio de archivos virtual de los grupos es accounting.

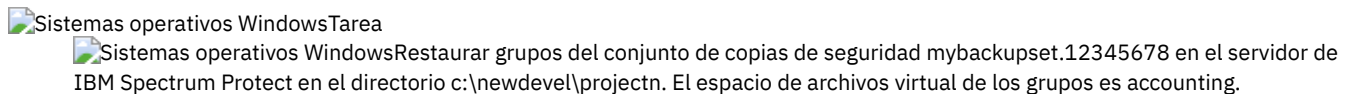
```
dsmc restore backupset {/accounting}/*  
/home/devel/projectb/  
-backupsetname=mybackupset.12345678 -loc=server  
-subdir=yes
```

 Restaurar grupos del conjunto de copias de seguridad local mybackupset.ost en el directorio /home/devel/projectb/. El espacio de archivos virtual de los grupos es accounting.

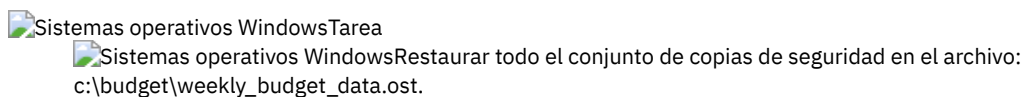
```
dsmc restore backupset {/accounting}/*  
/home/devel/projectb/  
-backupsetname=mybackupset.ost  
-loc=server -subdir=yes
```

 Restaurar todo el conjunto de copias de seguridad del dispositivo \\.\tape0.

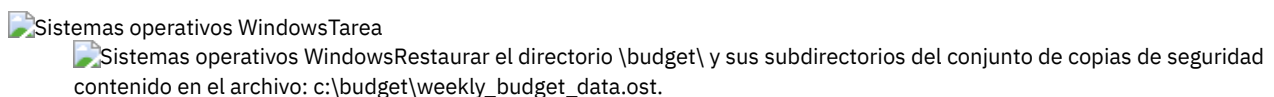
```
dsmc restore backupset  
-backupsetname=\\.\tape0 -loc=tape
```

 Restaurar grupos del conjunto de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio c:\newdevel\projectn. El espacio de archivos virtual de los grupos es accounting.

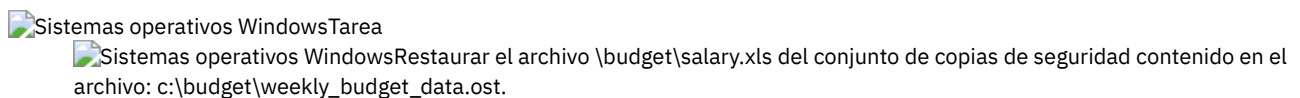
```
dsmc restore backupset {accounting}\*  
c:\newdevel\projectn\  
-backupsetname=mybackupset.12345678  
-loc=server -subdir=yes
```

 Restaurar todo el conjunto de copias de seguridad en el archivo: c:\budget\weekly\_budget\_data.ost.

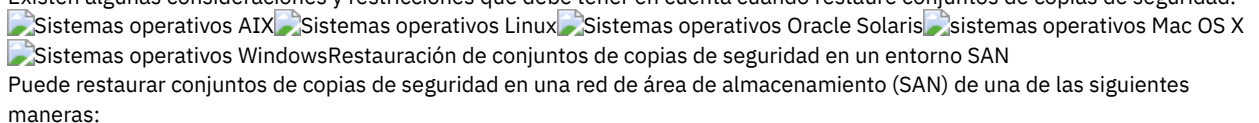
```
dsmc restore backupset  
-backupsetname=c:\budget\weekly_budget_data.ost  
-loc=file
```

 Restaurar el directorio \budget\ y sus subdirectorios del conjunto de copias de seguridad contenido en el archivo: c:\budget\weekly\_budget\_data.ost.

```
dsmc restore backupset m:\budget\  
-backupsetname=c:\budget\weekly_budget_data.ost  
-loc=file -subdir=yes
```

 Restaurar el archivo \budget\salary.xls del conjunto de copias de seguridad contenido en el archivo: c:\budget\weekly\_budget\_data.ost.

```
dsmc restore backupset m:\budget\salary.xls  
-backupsetname=c:\budget\weekly_budget_data.ost  
-loc=file -subdir=yes
```

- Restauración de conjuntos de copias de seguridad: consideraciones y restricciones  
Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.
-  Restauración de conjuntos de copias de seguridad en un entorno SAN  
Puede restaurar conjuntos de copias de seguridad en una red de área de almacenamiento (SAN) de una de las siguientes maneras:










- restore Backupset sin el parámetro backupsetname  
El mandato restore backupset se puede utilizar sin el parámetro backupsetname.

## Restauración de conjuntos de copias de seguridad: consideraciones y restricciones

Existen algunas consideraciones y restricciones que debe tener en cuenta cuando restaure conjuntos de copias de seguridad.









### Consideraciones de restauración del conjunto de copias de seguridad






Al restaurar conjuntos de copias de seguridad, tenga en cuenta lo siguiente:

- Si el objeto que desea restaurar se ha generado desde un nodo cliente cuyo nombre es distinto del nodo actual, especifique el nombre del nodo original con el parámetro filespace en cualquiera de los mandatos restore.
- Si no puede restaurar un conjunto de copias de seguridad desde el medio portable, póngase en contacto con el administrador de IBM Spectrum Protect para asegurarse de que el medio portable se creó en un dispositivo con un formato compatible con el suyo.
- Si utiliza el mandato restore backupset en la línea de mandatos inicial con el parámetro `-location=tape` o `-location=file`, el cliente no intenta ponerse en contacto con el servidor de IBM Spectrum Protect.
- Cuando restaure un grupo a partir de un conjunto de copias de seguridad:
  - Se restaurará todo el grupo, o todos los grupos, del espacio de archivos virtual. Si hay varios grupos en el mismo espacio de archivos virtual, no podrá restaurar un solo grupo especificando el nombre de grupo. No puede restaurar una parte de un grupo especificando una vía de acceso de archivo.
  - Especifique un grupo utilizando los valores siguientes:
    - Especifique el nombre de espacio de archivos individual con el parámetro filespace.
    - Utilice la opción subdir para incluir subdirectorios.
- Se proporciona soporte limitado para la restauración de conjuntos de copias de seguridad desde dispositivos de cinta conectados al sistema cliente. Se debe utilizar siempre un controlador de dispositivo nativo proporcionado por el fabricante del dispositivo. El controlador de dispositivo proporcionado por IBM para que lo utilice el servidor de IBM Spectrum Protect no se puede utilizar en el sistema cliente para restaurar juegos de copias de seguridad locales.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Si un conjunto de copias de seguridad contiene archivos de distintos propietarios, el propio conjunto de copias de seguridad será propiedad del ID de usuario root y los ID de usuarios que no sean root no verán el conjunto de copias de seguridad. En tal caso, los ID de usuario que no son root pueden restaurar sus archivos si el administrador de IBM Spectrum Protect `rd>` les proporciona el nombre del juego de copias de seguridad. Los usuarios que no sean root sólo podrán restaurar sus propios archivos.
-  Sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Para permitir que la GUI del cliente restaure un conjunto de copias de seguridad de un dispositivo local, sin que sea necesaria una conexión al servidor, utilice la opción `localbackupset`.

### Consideraciones de restauración del conjunto de copias de seguridad

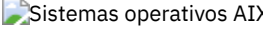
Al restaurar conjuntos de copias de seguridad, tenga en cuenta las siguientes restricciones:

- No es posible restaurar ni utilizar los datos de los conjuntos de copias de seguridad de los que se ha hecho una copia de seguridad mediante la API.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No puede restaurar datos de imagen de un conjunto de copias de seguridad mediante la utilización del mandato `restore backupset`. Sólo puede restaurar datos de imagen de un conjunto de copias de seguridad con el mandato `restore image`.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows No puede restaurar datos de imagen de un conjunto de copias de seguridad local (`location=tape` o `location=file`). Sólo puede restaurar datos de imagen de un juego de copias de seguridad del servidor de IBM Spectrum Protect.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Restauración de conjuntos de copias de seguridad en un entorno SAN

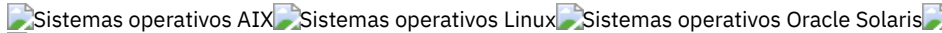

Puede restaurar conjuntos de copias de seguridad en una red de área de almacenamiento (SAN) de una de las siguientes maneras:

- Si el conjunto de copias de seguridad se encuentra en un dispositivo de almacenamiento conectado con la SAN, especifique el dispositivo mediante la utilización del parámetro *filename* y utilice la opción *location=tape* donde se aplique. El cliente de copia de seguridad y archivado restaura el conjunto de copias de seguridad directamente del dispositivo de almacenamiento conectado a SAN, consiguiendo un rendimiento de restauración de alta velocidad.  
 Nota: es preciso asegurarse de que la cinta adecuada está montada en la unidad de cintas conectada a SAN antes de emitir el mandato restore. El cliente de copia de seguridad/archivado no iniciará un autocambiador SCSI para montar la cinta de forma automática.
- Si el conjunto de copias de seguridad no está en medios locales o en un dispositivo de almacenamiento conectado a SAN, puede especificar el conjunto de copias de seguridad utilizando la opción *backupsetname*. Utilice la opción *location=server* para restaurar el conjunto de copias de seguridad directamente desde el servidor mediante la utilización de Lan.

## restore Backupset sin el parámetro backupsetname

El mandato restore backupset se puede utilizar sin el parámetro backupsetname.

La sintaxis preferida para el mandato restore backupset requiere el parámetro backupsetname. Antes de la especificación del parámetro backupsetname, el cliente de copia de seguridad y archivado ha restaurado los conjuntos de copias de seguridad con una sintaxis distinta. Se admite la sintaxis anterior, pero se recomienda, siempre que sea posible, que siga la sintaxis que requiere el parámetro backupsetname. La sintaxis anterior está documentada para aquellos casos en los que no se puede sustituir por la sintaxis preferida.

## Clientes soportados

Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-REStore Backupset--+-+-----+-----+-----+----->
                        '+-----+-----sourcefilespec-'
                        '-{filespaceName}-'

>+-+-----+-----+-----+-----+-----+-----+----->
  '-destinationfilespec-' '-options-' '+-localfilename+'
                                '-tapedevice----'

>+-+-----+-----+-----+-----+-----+-----+-----<<
  '-lOCation---+-server+-'
                    +-file---+
                    '-tape---'
```

## Parámetros

### opciones


Todas las opciones que son válidas con la sintaxis preferida de restore backupset son válidas con la sintaxis anterior de restore backupset.

### {filespaceName}

Nombra el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere restaurar. Éste es el nombre de la unidad de la estación de trabajo de cuyos archivos se realizó copia de seguridad o el nombre de espacio de archivos virtual para el grupo.

Especifique un nombre de espacio de archivos cuando restaure un conjunto de copias de seguridad que contenga un grupo.

Especifique un nombre de espacio de archivos cuando el parámetro *sourcefilespec* no exista en el sistema de destino. Esto puede suceder si el nombre de la etiqueta de unidad ha sido modificado o si está restaurando archivos de los que ha realizado copia de seguridad desde otro nodo con etiquetas de unidad distintas de las suyas.

 Nota: Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. Sólo son válidas las comillas simple en modalidad de bucle. Por ejemplo, {"NTFSDrive"} y {'NTFSDrive'} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.

sourcefilespec



Especifica la vía de acceso de origen de una parte del conjunto de copias de seguridad. El valor predeterminado es restaurar todo el conjunto de copias de seguridad.

#### destinationfilespec

Especifica la vía de acceso de destino para los archivos restaurados. Si no especifica *sourcefilespec*, no puede especificar *destinationfilespec*. Si no especifica un destino, el cliente restaura los archivos en la vía de acceso de origen inicial. Si está restaurando más de un archivo, debe terminar la especificación de archivo con un delimitador de directorio (/); de lo contrario, el cliente presupone que el último nombre es un nombre de archivo e indica que se ha producido un error. Si está restaurando un único archivo, tiene la opción de terminar la especificación de archivo con un nombre de archivo si desea cambiar el nombre del archivo restaurado por uno nuevo. Si *sourcefilespec* no existe en la estación de trabajo de destino, debe especificar *destinationfilespec*.

#### backupsetname

Especifica el nombre del juego de copias de seguridad del servidor de IBM Spectrum Protect. Si se especifica el parámetro *location*, debe establecer `-location=server`.

#### localfilename

Especifica el nombre de archivo del primer volumen del juego de copias de seguridad. Debe establecer `-location=file`.

#### tapedevice

Especifica el nombre del dispositivo de cinta que contiene el volumen del juego de copias de seguridad. Tiene que utilizar un controlador de dispositivo proporcionado por Windows, no el controlador de dispositivo que proporciona IBM. Debe establecer `-location=tape`.

#### LOCation=

Especifica la ubicación del conjunto de copias de seguridad. Si no especifica el parámetro de ubicación, el cliente buscará juegos de copias de seguridad en el servidor de IBM Spectrum Protect. Si especifica el parámetro de ubicación, el valor debe corresponder a una de las tres opciones siguientes:

#### server

Especifica que el juego de copias de seguridad se encuentra en el servidor. Server es la ubicación predeterminada.

#### file

Especifica que el conjunto de copias de seguridad se encuentra en un sistema de archivos disponible.

#### tape

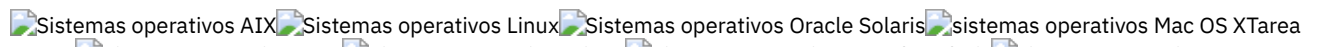
Especifica que el conjunto de copias de seguridad se encuentra en un dispositivo de cinta disponible.

## Ejemplos

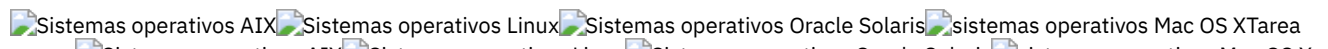
### Tarea

Restaurar el juego de copias de seguridad denominado `monthly_financial_data.87654321` del servidor.

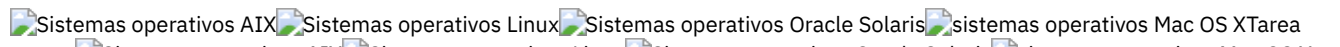
```
dsmc restore backupset monthly_financial_data.87654321 -loc=server
```

 Restaurar todo el conjunto de copias de seguridad contenido en el archivo: `/home/budget/weekly_budget_data.ost`.

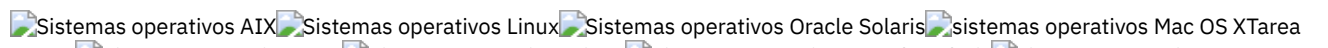
```
dsmc restore backupset "/home/budget/weekly_budget_data.ost" -loc=file
```

 Restaurar todo el juego de copias de seguridad del dispositivo `/dev/rmt0`.

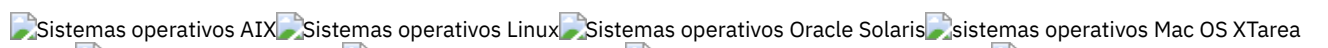
```
dsmc restore backupset "/dev/rmt0" -loc=tape
```

 Restaurar un único archivo denominado `/home/jones/budget.dev` del dispositivo de cinta `/dev/rmt0` en la vía de acceso de origen original.

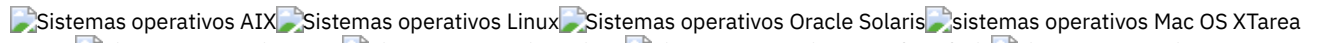
```
dsmc restore backupset /dev/rmt0 "/home/jones/budget.dev" -loc=tape
```

 Restaurar todos los archivos del directorio `budget` que tienen la extensión `.txt` desde una o más cintas del dispositivo `/dev/rmt0` en la vía de acceso original.

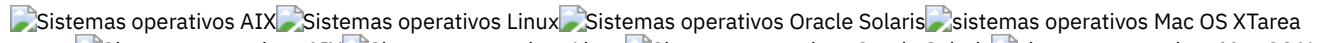
```
dsmc restore backupset /dev/rmt0 "/home/budget/*.txt" -loc=tape
```

 Restaurar todo el juego de copias de seguridad contenido en el archivo local `"/home/jones/bset01.file"`

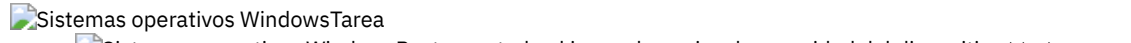
```
dsmc restore backupset "/home/jones/bset01.file" -loc=file
```

 Restaurar grupos del juego de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio /home/devel/projectb. El espacio de archivos virtual de los grupos es accounting.


```
dsmc restore backupset mybackupset.12345678 {/accounting}/* /home/devel/projectb/ -loc=server -subdir=yes
```

 Restaurar grupos del juego de copias de seguridad local mybackupset.ost en el directorio /home/devel/projectb/. El espacio de archivos virtual de los grupos es accounting.


```
dsmc restore backupset mybackupset.ost {/accounting}/* /home/devel/projectb/ -loc=server -subdir=yes
```

 Restaurar todo el juego de copias de seguridad del dispositivo \\.\tape0.


```
dsmc restore backupset \\.\tape0 -loc=tape
```

 Restaurar grupos del juego de copias de seguridad mybackupset.12345678 en el servidor de IBM Spectrum Protect en el directorio c:\newdevel\projectn. El espacio de archivos virtual de los grupos es accounting.

```
dsmc restore backupset mybackupset.12345678 {accounting}* c:\newdevel\projectn\ -loc=server -subdir=yes
```

 Restaurar todo el juego de copias de seguridad en el archivo: c:\budget\weekly\_budget\_data.ost.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost -loc=file
```

 Restaurar el directorio \budget\ y sus subdirectorios del conjunto de copias de seguridad contenido en el archivo: c:\budget\weekly\_budget\_data.ost.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost m:\budget* -loc=file -subdir=yes
```

 Restaurar el archivo \budget\salary.xls del conjunto de copias de seguridad contenido en el archivo: c:\budget\weekly\_budget\_data.ost.

```
dsmc restore backupset c:\budget\weekly_budget_data.ost m:\budget\salary.xls -loc=file -subdir=yes
```

## Restore Group

---

Utilice el mandato restore group para restaurar miembros específicos o todos los miembros de una copia de seguridad de grupo.

Nota:


1. Utilice la opción pick para que se visualice una lista de grupos a partir de los que poder seleccionar el grupo que desea restaurar.
2. Utilice la opción showmembers con la opción pick para visualizar y restaurar uno o más miembros de un grupo. En este caso, primero debe seleccionar el grupo del que desea restaurar miembros específicos y, a continuación, debe seleccionar el miembro o miembros del grupo que desea restaurar.
3. Puede restaurar un grupo de un juego de copias de seguridad.



## Clientes soportados

---

 Este mandato es válido para todos los clientes, excepto Mac OS X.









 Este mandato es válido para todos los clientes.


## Sintaxis


---

```
>>-REStore Group--+-+-----+-+-----+-+-----+-+-----+-+-----><
                    '-options-'          '-destino-'
```

## Parámetros

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Especifica el nombre del espacio de archivos virtual y el nombre del grupo que desea restaurar en el servidor.

































 Sistemas operativos Windows **origen**

 Sistemas operativos Windows Especifica el nombre del espacio de archivos virtual (entre llaves) y el nombre del grupo que desea restaurar en el servidor.

**destino**

Especifica la vía de acceso en la que desea colocar el grupo o uno o más miembros del grupo. Si no especifica un destino, el cliente restaurará los archivos en su ubicación original.

Tabla 1. Mandato restore Group: opciones relacionadas

Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris followsymbolic	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
fromdate	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS XSólo línea de mandatos.
fromtime	Sólo línea de mandatos.
ifnewer	Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
latest	Sólo línea de mandatos.
pick	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
preservepath	Sólo línea de mandatos.
 Sistemas operativos Windows replace	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris replace	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows showmembers	 Sistemas operativos Windows Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris showmembers  (no se aplica a Mac OS X)	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Sólo línea de mandatos.
 Sistemas operativos Windows skipntpermissions	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.

Opción	Dónde se utiliza
Sistemas operativos Windows skipntsecuritycrc	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows subdir	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris subdir	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows tapeprompt	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris tapeprompt	Sistemas operativos AIX  Sistemas operativos Linux Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
todate	Sólo línea de mandatos.
totime	Sólo línea de mandatos.

## Ejemplos

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Tarea Restaurar todos los miembros de la copia de seguridad de grupo /virtfs/group1 en su ubicación original en el sistema cliente.

**Mandato:**

```
restore group /virtfs/group1
```

Sistemas operativos Windows  
 Sistemas operativos Windows  
 Tarea Restaurar todos los miembros de la copia de seguridad de grupo virtfs\group1 en su ubicación original en el sistema cliente.

**Mandato:**

```
restore group {virtfs}\group1
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Tarea Visualizar todos los grupos del espacio de archivos virtual /virtfs. Utilice la opción showmembers para visualizar una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea restaurar.

**Mandato:**

```
restore group /virtfs/  
* -pick -showmembers
```

Sistemas operativos Windows  
 Sistemas operativos Windows  
 Tarea Visualizar todos los grupos del espacio de archivos virtual virtfs. Utilice la opción showmembers para visualizar una lista de miembros de grupo a partir de los que poder seleccionar el miembro o miembros que desea restaurar.

**Mandato:**

```
restore group {virtfs}  
* -pick -showmembers
```

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Tarea Visualizar una lista de los grupos del espacio de archivos virtual /virtfs desde la que podrá seleccionar uno o varios grupos para su restauración.




**Mandato:**

```
restore group /virtfs/* -pick
```

Sistemas operativos Windows  
 Sistemas operativos Windows  
 Tarea Visualizar una lista de los grupos del espacio de archivos virtual virtfs desde la que podrá seleccionar uno o varios grupos para su restauración.

**Mandato:**

```
restore group {virtfs}\* -pick
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  Sistemas operativos Windows





## Restore Image

---

El mandato `restore image` restaura un sistema de archivos o una imagen de volumen RAW cuya copia de seguridad se ha realizado con el mandato `backup image`.

El mandato `restore` obtiene la imagen de copia de seguridad del servidor de IBM Spectrum Protect, o del interior de un conjunto de copias de seguridad del servidor de IBM Spectrum Protect, cuando se especifica la opción `backupsetname`. Este mandato puede restaurar una imagen base activa o una imagen base a un instante específico con sus actualizaciones incrementales asociadas.




Nota:

-  Sistemas operativos Windows La cuenta que ejecuta el cliente de copia de seguridad y archivado debe tener autorización de administrador para realizar correctamente cualquier tipo de restauración de imagen.
-  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris La utilización de la opción incremental con el mandato `restore image` para realizar una copia de seguridad de imágenes dinámica no recibe soporte.
- Si utiliza IBM Spectrum Protect HSM for Windows o IBM Spectrum Protect for Space Management, y restaura una copia de seguridad de imagen del sistema de archivos y planifica ejecutar la reconciliación, deberá restaurar los archivos cuya copia de seguridad se ha efectuado tras la copia de seguridad de imágenes. De lo contrario, los archivos migrados que se crearon tras la copia de seguridad de la imagen caducarán del almacenamiento del archivado de HSM en el servidor de IBM Spectrum Protect.

Puede utilizar la opción `verifyimage` con el mandato `restore image` para especificar que desea activar la detección de sectores defectuosos en el volumen de destino. Si se detectan sectores defectuosos en el volumen de destino, el cliente emite un mensaje de aviso en la consola y en el registro de errores.

Si existen sectores defectuosos en el volumen de destino, puede utilizar la opción `imagetofile` con el mandato `restore image` para especificar que desea restaurar la imagen de origen en un archivo. Más tarde, puede utilizar el programa de utilidad de copia de datos que elija para transferir la imagen del archivo a un volumen de disco.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Consideraciones:

- La API debe estar instalada para utilizar el mandato `restore image`.
-  Sistemas operativos Oracle Solaris La restauración de imagen no está soportada para el sistema de archivos QFS de Sun.
-  Sistemas operativos Linux La restauración de imagen no está admitida en los sistemas de archivos GPFS en Linux x86\_64, Linux on POWER y Linux para System.
-  Sistemas operativos Linux En sistemas Linux, algunos sistemas de archivos como ext2, ext3, ext4, btrfs y xfs utilizan un UUID (universally unique identifier) para que se identifiquen con el sistema operativo. Si crea una copia de seguridad de imagen de tal volumen y la restaura en una ubicación distinta, es posible que tenga dos volúmenes con el mismo UUID. Si utiliza UUID para definir los sistemas de archivos en `/etc/fstab`, tenga en cuenta que es posible que el cliente de copia de seguridad y archivado no pueda montar correctamente el sistema de archivos restaurado debido al conflicto de UUID. Para evitar esta situación, restaure la imagen a su ubicación original. Si debe restaurarla a una ubicación distinta, cambie el UUID de cualquier volumen original o restaurado antes de montar el sistema de archivos restaurado. Consulte la documentación de Linux para obtener instrucciones sobre cómo cambiar un UUID. También es posible que deba editar manualmente el archivo `/etc/fstab` para que se pueda montar el volumen original, el volumen restaurado, o ambos volúmenes.
- Si utiliza la opción `pick`, se visualizará la siguiente información para las imágenes del sistema de archivos de las que el cliente ha realizado copia de seguridad:
  - Tamaño de imagen
  - Tamaño almacenado - Este valor es el tamaño de la imagen real que se almacena en el servidor de IBM Spectrum Protect. La imagen almacenada en el servidor tiene un tamaño que equivale a la capacidad del volumen.
  - Tipo de sistema de archivos
  - Fecha y hora de la copia de seguridad
  - La clase de gestión que está asignada a las copias de seguridad de imágenes
  - Si la copia de seguridad de imágenes es una copia activa o inactiva
  - El nombre de la imagen
- Si por algún motivo se daña una imagen restaurada, puede utilizar la herramienta `fsck` para intentar repararla.

 Sistemas operativos Windows Consideraciones:

- La API de IBM Spectrum Protect debe estar instalada para utilizar el mandato `restore image`.
- Puede restaurar un sistema de archivos NTFS o ReFS en un volumen FAT32 o viceversa.
- El volumen de destino en el que restaure debe existir y tener el mismo tamaño o mayor que el volumen de origen.
- El diseño físico del volumen de destino (en bandas, duplicado) puede ser diferente.
- Los datos incluidos en la copia de seguridad de imágenes se grabarán encima del volumen de destino.

- No tiene que formatear un volumen de destino antes de restaurar una copia de seguridad de imagen que contiene un sistema de archivos.
- El cliente requiere un bloqueo exclusivo en el volumen de destino que se restaura. El cliente bloquea, restaura, desbloquea, desmonta y monta el volumen durante una operación de restauración. Durante el proceso de restauración, el volumen de destino no está disponible para otras aplicaciones.
- Si utiliza la opción pick, se visualizará la siguiente información para las imágenes del sistema de archivos de las que el cliente realiza copia de seguridad:
  - Tamaño de imagen
  - Tamaño almacenado - Este valor es el tamaño de imagen real almacenado en el servidor. La opción imagegapsize se puede establecer de modo que sólo se haga copia de seguridad de los bloques utilizados en un sistema de archivos. Por lo tanto, el tamaño de la imagen almacenada en el servidor puede ser más pequeño que el tamaño del volumen. Para las copias de seguridad de imágenes en línea, la imagen almacenada puede ser más grande que el sistema de archivos, en función del tamaño de los archivos de la caché.
  - Tipo de sistema de archivos
  - Fecha y hora de la copia de seguridad
  - Clase de gestión que se asigna a la copia de seguridad de imágenes
  - Si la copia de seguridad de imágenes es una copia activa o inactiva
  - El nombre de la imagen
- Si se daña una imagen restaurada, utilice el programa de utilidad chkdsk para comprobar y reparar los sectores defectuosos o las incoherencias de datos (a menos que el volumen restaurado sea RAW).

## Clientes soportados

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Esta opción es válida para clientes de AIX, Linux y Oracle Solaris.

Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

```
>>-REStore Image--+-+-----+-----+--sourcefilespec--+-+----->
                    '- --options-' '- --"sourcefilespec"- '
>--+-+-----+-----+-----<<
    '- --destinationfilespec- '
```

## Parámetros

### sourcefilespec

Especifica el nombre de un sistema de archivos imagen de origen para restaurar. Sólo puede especificarse una imagen origen; no pueden utilizarse caracteres comodín.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris **destinationfilespec**  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris Especifica el nombre de un sistema de archivos montado existente o la vía de acceso y el nombre de archivo en el que se restaurará el sistema de archivos de origen. El valor predeterminado es la ubicación original del sistema de archivos.

Sistemas operativos Windows **destinationfilespec**  
 Sistemas operativos Windows Especifica el nombre de un sistema de archivos montado existente o la vía de acceso y el nombre de archivo en el que se restaurará el sistema de archivos de origen. El valor predeterminado es la ubicación original del sistema de archivos. Puede restaurar un sistema de archivos NTFS o ReFS en un volumen FAT32 o viceversa.

Tabla 1. Mandato restore image: opciones relacionadas

Opción	Dónde se utiliza
backupsetname	Sólo línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris dateformat	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows dateformat	Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
deletefiles	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.

Opción	Dónde se utiliza
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris fromowner	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Sólo línea de mandatos.
imagetofile	Sólo línea de mandatos.
inactive	Sólo línea de mandatos.
incremental	Sólo línea de mandatos.
noprompt	Sólo línea de mandatos.
pick	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris timeformat	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
Sistemas operativos Windows timeformat	Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
verifyimage	Sólo línea de mandatos.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 El mandato restore image no define ni monta el espacio de archivos de destino. El volumen de destino debe existir, ser lo suficientemente grande para contener el origen y, si contiene un sistema de archivos, deberá tratarse de un volumen montado. Si una copia de seguridad de imagen contiene un sistema de archivos y los restaura en otra ubicación, tenga en cuenta lo siguiente:

Sistemas operativos Windows  
 El mandato restore image no define ni monta el espacio de archivos de destino. El volumen de destino debe existir, ser lo suficientemente grande para contener el origen y, si contiene un sistema de archivos, deberá tratarse de un volumen montado. El volumen de destino debe correlacionarse con una letra de unidad. Si una copia de seguridad de imágenes contiene un sistema de archivos y los restaura en otra ubicación, tenga en cuenta lo siguiente:

- Si el volumen de destino es más pequeño que el volumen de origen, la operación fallará.
- Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Si el volumen de destino es más grande que el volumen de origen, tras la operación de restauración perderá la diferencia entre los tamaños. El espacio perdido puede recuperarse incrementando el tamaño del volumen, que también aumentará el tamaño del volumen restaurado.
- Sistemas operativos Windows  
 Si el volumen de destino es más grande que el volumen de origen, tras la operación de restauración perderá la diferencia entre los tamaños. Si el volumen de destino se encuentra en un disco dinámico, el espacio perdido se puede recuperar incrementando el tamaño del volumen. Aumentar el tamaño del volumen también aumentará el tamaño del volumen restaurado.

## Ejemplos

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
**Tarea**  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Restaurar el directorio /home/test en el que se ha montado el volumen lógico en su ubicación original.

Mandato: `dsmc rest image /home/test`


Sistemas operativos Windows  
**Tarea**  
 Sistemas operativos Windows  
 Restaurar la unidad e: en su ubicación original.

Mandato: `dsmc rest image e:`




Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
**Tarea**  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris  
 Restaura el directorio /home/proj sobre el que está montado el volumen lógico en su ubicación original y aplique los cambios de la última copia de seguridad incremental de la imagen original que está registrada en el servidor. Entre los cambios se incluye la supresión de archivos.

Mandato: `dsmc restore image /home/proj -incremental -deletefiles`


Sistemas operativos Windows  
**Tarea**

 Sistemas operativos Windows Restaura la unidad `h:` a su ubicación original y aplique los cambios desde la última copia de seguridad incremental de la imagen original registrada en el servidor. Entre los cambios se incluye la supresión de archivos.




Mandato: `dsmc restore image h: -incremental -deletefiles`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tarea Restaurar el sistema de archivos `/usr` en su ubicación original. Utilice la opción `verifyimage` para activar la detección de sectores defectuosos en el volumen de destino.


Mandato: `dsmc restore image /usr -verifyimage`

 Sistemas operativos Windows Tarea Restaurar la unidad `d:` en su ubicación original. Utilice la opción `verifyimage` para activar la detección de sectores defectuosos en el volumen de destino.


Mandato: `dsmc restore image d: -verifyimage`

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris Tarea Si existen sectores defectuosos en el volumen de destino, utilice la opción `imagetofile` para restaurar el sistema de archivos `/usr` en el archivo `/home/usr.img` para evitar que se dañen los datos.




Mandato: `dsmc restore image /usr /home/usr.img -imagetofile`

 Sistemas operativos Windows Tarea Si existen sectores defectuosos en el volumen de destino, utilice la opción `imagetofile` para restaurar la unidad `d:` en el archivo `e:\diskD.img` para evitar que se dañen los datos.

Mandato: `dsmc restore image d: e:\diskD.img -imagetofile`

 Sistemas operativos Windows Tarea Restaurar la unidad `e:` del conjunto de copias de seguridad llamado `weekly_backup_data.12345678` en su ubicación original.

Mandato: `restore image e: -backupsetname=weekly_backup_data.12345678`

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows



## Restore NAS


---

El mandato `restore nas` restaura la imagen de un sistema de archivos perteneciente a un servidor de archivos NAS (almacenamiento conectado a red). Cuando se utilice una sesión de línea de mandatos interactiva con un ID que no es un ID de administración, se le solicitará un ID de administrador.

El servidor de archivos NAS realiza el proceso de traspaso de datos externos. Un proceso del servidor realiza la restauración.

Si ha utilizado la opción `toc` con el mandato `backup nas` o la opción `include.fs.nas` para guardar la información de la Tabla de contenido (TOC) para cada copia de seguridad del sistema de archivos, puede utilizar el mandato de servidor `QUERY TOC` para determinar el contenido de una copia de seguridad del sistema de archivos con el mandato de servidor `RESTORE NODE` para restaurar archivos individuales o árboles de directorios. También puede utilizar el cliente web para examinar todo el árbol del sistema de archivos y seleccionar los archivos y directorios que han de restaurarse. Si no guarda la información de las TOC, podrá restaurar archivos individuales o árboles de directorios con el mandato de servidor `RESTORE NODE`, si conoce el nombre calificado al completo de cada archivo o directorio y sepa en qué imagen se ha realizado la copia de seguridad de ese objeto.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Utilice la opción `nasnodename` para especificar el nombre de nodo del servidor de archivos NAS. El nombre de nodo NAS identifica el servidor de archivos NAS en el servidor de IBM Spectrum Protect. Debe inscribir el nombre de nodo NAS en el servidor. Especifique la opción `nasnodename` en el archivo de opciones del sistema cliente (`dsm.sys`). El valor del archivo de opciones del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos.

 Sistemas operativos Windows Utilice la opción `nasnodename` para especificar el nombre de nodo del servidor de archivos NAS. El nombre de nodo NAS identifica el servidor de archivos NAS en el servidor de IBM Spectrum Protect. Debe inscribir el nombre de nodo NAS en el servidor. Especifique la opción `nasnodename` en el archivo de opciones del cliente (`dsm.opt`). El valor del archivo de opciones del cliente es el valor predeterminado, pero este valor puede modificarse temporalmente en la línea de mandatos.

Puede utilizar la opción `pick` para visualizar una lista de imágenes de NAS que sean propiedad del nodo NAS que especifique. En esta lista puede seleccionar una o varias imágenes para restaurarlas. Si selecciona varias imágenes para restaurarlas con la opción `pick`, no

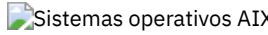
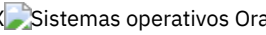


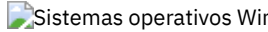
utilice la opción monitor o las restauraciones se realizarán en serie. Para iniciar varios procesos de restauración simultáneamente al realizar la restauración de varias imágenes, no especifique monitor=yes.

Utilice la opción monitor para especificar si desea supervisar una imagen del sistema de archivos NAS y visualizar información sobre el proceso en la pantalla.

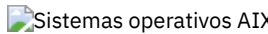
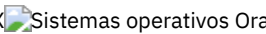

Utilice el mandato monitor process para visualizar una lista de los procesos de restauración actuales de todos los nodos NAS para los que el ID de usuario de administración está autorizado. El ID de usuario de administración debe tener como mínimo autorización de propietario de cliente sobre el nodo NAS y sobre el nodo de la estación de trabajo cliente que están utilizando desde la línea de mandatos o desde la Web.

Utilice el mandato cancel process para detener el proceso de restauración de NAS.

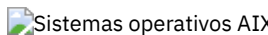
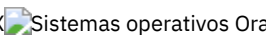
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Con independencia de la plataforma del cliente utilizada, las especificaciones del sistema de archivos NAS utilizan como separador la barra inclinada (/), como en el ejemplo siguiente: /vol/vol0.

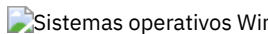
 Sistemas operativos Windows Una especificación del sistema de archivos NAS utiliza los convenios siguientes:

- Independientemente de la plataforma del cliente, en las especificaciones de sistema de archivos NAS se utiliza la barra inclinada (/) como separador, tal como se muestra en el siguiente ejemplo: /vol/vol0.
- En el sistema de archivos NAS es necesario utilizar llaves {} como delimitadores de los nombres de sistemas de archivos cuando se utiliza la línea de mandatos, por ejemplo: {/vol/vol0}.

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  Sistemas operativos Windows

## Clientes soportados

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Este mandato sólo es válido para los clientes AIX y Solaris.

 Sistemas operativos Windows Este mandato es válido para todos los clientes Windows.

## Sintaxis

```
>>-REStore NAS--+-+-----+----- --sourcefilespec----->
                '- --options-'

>+-----+-----<
  '- --destinationfilespec-'
```

## Parámetros

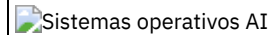

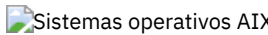
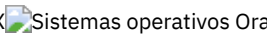
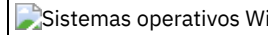
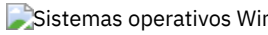
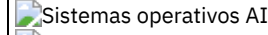

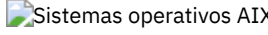
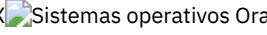
### sourcefilespec















Especifica el nombre de la imagen del sistema de archivos NAS que desea restaurar. Este parámetro es necesario a menos que utilice la opción pick para mostrar una lista de las imágenes de NAS en la que puede realizar una selección. No se pueden utilizar caracteres comodín cuando se especifica sourcefilespec.

### destinationfilespec





Especifica el nombre de un sistema de archivos montado existente en el dispositivo NAS en el que desea restaurar la imagen. Este parámetro es opcional. El valor predeterminado es la ubicación original del sistema de archivos en el dispositivo NAS.

Tabla 1. Mandato restore NAS: opciones relacionadas



Opción	Dónde se utiliza
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris dateformat	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
inactive	Sólo línea de mandatos.
mode	Sólo línea de mandatos.
monitor	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris nasnodename	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.

Opción	Dónde se utiliza
 Sistemas operativos Windows nasnodename	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris numberformat	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows numberformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.
pick	Sólo línea de mandatos.
pitdate	Sólo línea de mandatos.
pittime	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Oracle Solaris timeformat	 Sistemas operativos AIX  Sistemas operativos Oracle Solaris Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows En el archivo de opciones del cliente (dsm.opt) o en la línea de mandatos.

## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Tarea  Sistemas operativos AIX  Sistemas operativos Oracle Solaris  
Restaurar la imagen del sistema de archivos NAS /vol/vol1 en el sistema de archivos /vol/vol2 del servidor de archivos NAS denominado nas1.

**Mandato:** restore nas -nasnodename=nas1 /vol/vol1 /vol/vol2

 Sistemas operativos Windows  
Tarea  Sistemas operativos Windows  
Restaurar la imagen del sistema de archivos NAS /vol/vol1 en el sistema de archivos /vol/vol2 del servidor de archivos NAS denominado nas1.

**Mandato:** restore nas -nasnodename=nas1 {/vol/vol1} {/vol/vol2}

Tarea  
Restaurar imágenes NAS inactivas.

**Mandato:** restore nas -nasnodename=nas2 -pick -inactive

 Sistemas operativos Windows

## Restore Systemstate

El mandato restore systemstate está en desuso para las operaciones de restauración del estado del sistema en línea.

Restricción:

Ya no puede restaurar el estado del sistema en un sistema que sigue en línea. En lugar de ello, utilice el método de recuperación basado en ASR para restaurar el estado del sistema en modo Windows PE fuera de línea. Para obtener más información, consulte los siguientes artículos de la wiki de IBM Spectrum Protect:

- Best Practices for Recovering Windows Server 2012 and Windows 8
- Best Practices for Recovering Windows Server 2012 R2 and Windows 8.1

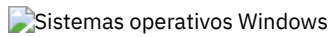
Si intenta restaurar el estado del sistema con el mandato dsmc restore systemstate, desde la GUI del cliente de archivado y copia de seguridad, o desde el cliente web, aparecerá el siguiente mensaje:

```
ANS5189E Online SystemState restore has been deprecated. Please use offline
WinPE method for performing system state restore.
```


 Sistemas operativos Linux  Sistemas operativos Windows

## Restore VM

Utilice el mandato restore vm para restaurar una máquina virtual de la que se había realizado previamente una copia de seguridad.



El mandato restore VM se puede utilizar para restaurar las máquinas virtuales de Microsoft Hyper-V y las máquinas virtuales de VMware. La información para cada tipo de restauración se presenta en su propio encabezado. Si está restaurando una máquina virtual que forma parte de un conjunto de Hyper-V, puede saltarse el texto *Restauración de máquinas virtuales VMware*. Si está restaurando una máquina virtual VMware, no necesita leer el texto *Restauración VM para máquinas virtuales Hyper-V*.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect for Virtual Environments.



## Restauración VM para máquinas virtuales VMware

---

El mandato Restore VM se puede utilizar para restaurar tanto máquinas virtuales VMware como plantillas de máquina virtual VMware.

Si tiene el cliente de archivado de copia de seguridad instalado en un sistema distinto configurado como un servidor de copia de seguridad vStorage, puede restaurar las copias de seguridad de la máquina virtual completas en el servidor ESX o ESXi de las que proceden, o a un servidor distinto. Para restaurar las copias de seguridad de máquina virtual completas en un servidor diferente, utilice la opción -host. El cliente de copia de seguridad histórica copia los datos del servidor de IBM Spectrum Protect a través de la LAN o SAN. A continuación, el cliente graba los datos directamente en el servidor ESX, utilizando el método de transporte que se ha especificado en el archivo de opciones del cliente.


Restaurar una copia de seguridad de máquina virtual completa crea una nueva máquina virtual; la información sobre configuración y contenido de la nueva máquina es idéntico a la que existía al crear la copia de seguridad. Todos los discos de máquinas virtuales se restauran en un punto específico en el tiempo como discos virtuales en la máquina virtual recién creada.

Al restaurar un disco específico, utilizando la sintaxis :vmdk=, se actualiza una máquina virtual existente con los datos del disco virtual especificado. Solo los discos especificados se restauran en la máquina virtual existente; otros discos de la máquina virtual no se modifican. La máquina virtual existente en la que está restaurando el disco debe apagarse antes de iniciar la operación de restauración.

Para crear una nueva máquina virtual, especifique el parámetro -vmname e indique el nombre de la nueva máquina virtual. El parámetro -vmname crea una nueva máquina virtual con una configuración que es idéntica a la que existía cuando la copia de seguridad se produjo. Si también especifica la sintaxis :vmdk=, los datos se restauran en cualquier disco que se incluya en los parámetros :vmdk=; los discos que no se incluyan se restaurarán, pero sólo como discos no formateados que no contengan datos.


Las máquinas virtuales se restauran en su agrupación de recursos, clúster o carpeta originales si existen los contenedores. Durante una operación de restauración, si el destino (un vCenter o un host ESXi) no tiene los contenedores necesarios, la máquina virtual se restaurará en la ubicación predeterminada de nivel superior en el host ESXi de destino. Si utiliza el cliente de línea de mandatos para restaurar una máquina virtual y si la máquina virtual no se puede restaurar en su ubicación de inventario original, se visualiza un mensaje informativo (ANS2091I). Si utiliza la GUI Java™ para restaurar una máquina virtual y si la máquina virtual no puede restaurarse en su ubicación de inventario original, el mensaje informativo no se visualiza, pero la máquina virtual se restaura de todas formas en la ubicación predeterminada de nivel superior.


Los códigos de protección de datos de los cuales se han ejecutado copias de seguridad al ejecutar el mandato backup vm se restauran con la máquina virtual. Los códigos de protección de datos se utilizan para excluir máquinas virtuales de copias de seguridad y especificar la política de retención de copias de seguridad.

 Las copias de seguridad de máquina virtual completas creadas anteriormente con VCB (VMware Consolidated Backup - Copia de seguridad consolidada de VMware) se pueden seguir restaurando utilizando los pasos de restauración de VCB originales. Para restaurar las copias de seguridad de la máquina virtual completas que ha creado VCB, consulte Restauración de copias de seguridad de máquina virtual completa creadas con VMware Consolidated Backup. Si utiliza VCB para restaurar una máquina virtual, utilice el programa conversor de VMware en el cliente para mover los archivos restaurados a un estado de ejecución en un servidor de VMware. Si el cliente de archivado y copia de seguridad se está ejecutando en una máquina virtual, y si se ha realizado una copia de seguridad a nivel de archivo de los archivos de la máquina virtual con un cliente de la versión 7.1 o anterior, puede restaurar las versiones de copia de seguridad en la máquina virtual utilizando la interfaz de línea de mandatos o la GUI de Java.

## Clientes soportados

---

 Este mandato solo es válido en clientes de Linux instalados en un servidor de copias de seguridad vStorage para una máquina virtual VMware.

 Este mandato solo es válido en clientes de Windows instalados en un servidor de copias de seguridad vStorage para una máquina virtual VMware.

## Sintaxis

---

```

      .----- .
      V .-:vmdk=all-vmdk----- . |
>>-REStore VM--sourcevmspec-----+-----+----->
      +-:vmdk=cnfg-----+
      +-:vmdk=disk label-----+
      '-:vmdk=etiqueta de disco-'

>+-----+-----+----->
+- -- -VMName="newVMname" [* <fecha y hora>]-+
+- --DATACENTER="myDatacenter"-----+
+- --HOST="myHost"-----+
'- --DATASTORE="myDatastore"-----'

>+-----+-----+-----<
'- --options-' '-destinationfilespec-'

```

## Parámetros

Cualquier parámetro que contenga espacios debe estar entre comillas (" ").

### sourcevmspec

Especifique el nombre de la máquina virtual (o plantilla de la máquina virtual) que desea restaurar.

### VMName \*timestamp

Especifica el nombre nuevo para la máquina virtual después de que se haya restaurado, si no desea utilizar el nombre especificado por *sourcevmspec*.

Puede utilizar el símbolo \* (asterisco) como comodín para representar el nombre de la máquina virtual que se restaura. La colocación de caracteres válidos antes o después del asterisco puede crear un prefijo o sufijo en el nombre de la máquina virtual restaurada.

Los caracteres siguientes no están soportados en nombres de máquinas virtuales restauradas: <q>;\\"\*?,<>/\\|. Un mandato de restauración que incluya caracteres no soportados fallará con el mensaje de error ANS9117E.

VMWare no admite nombres de máquina virtual de más de 80 caracteres.

Se puede añadir una opción de indicación de fecha y hora, que registra la fecha y la hora de la restauración, al nombre de la máquina virtual que se restaura. La salida de opción utiliza los formatos DATEFORMAT y TIMEFORMAT definidos en el archivo de opciones para determinar cómo especificar la serie de indicación de fecha y hora. Se utiliza un guión como delimitador en las fechas devueltas por los parámetros de indicación de fecha y hora.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB o si el parámetro FROM especifica LOCAL.

### DATACENTER

Especifica el nombre del centro de datos para restaurar la máquina virtual como se define en el vSphere vCenter. Si el centro de datos se encuentra en una carpeta, debe especificar la opción -datacenter al restaurar la máquina virtual e incluir la estructura de la carpeta del centro de datos en el nombre del centro de datos. Por ejemplo, la siguiente sintaxis es válida:

```
-datacenter=nombre_carpeta/nombre_centrodatos
```

Cuando restaure una máquina virtual mediante la GUI, debe restaurar la máquina virtual en una ubicación diferente. Si restaura en la ubicación original, no puede especificar el nombre de la carpeta del centro de datos. Sin un nombre de carpeta para ayudar a localizar el centro de datos originales, la operación de restauración fallará.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

### HOST

Especifica el nombre de dominio del servidor del host ESX donde se realizará la restauración, como se ha definido en vSphere vCenter.

Este parámetro distingue entre mayúsculas y minúsculas y debe ser el mismo valor que el nombre de host mostrado en el cliente web de VMware vSphere. Para confirmar el nombre de host en el cliente web de vSphere, seleccione un host y pulse Gestionar > Redes > Configuración de TCP/IP > DNS.


Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

### DATASTORE

Especifica el almacén de datos VMware en el que se restaura la máquina virtual. El almacén de datos solo puede estar en SAN, NAS, un dispositivo iSCSI o un volumen virtual VMware (VVOL). Solo puede especificar un almacén de datos al restaurar una máquina virtual. Si no especifica un parámetro datastore, el archivo VMDK de la máquina virtual se restaura en el almacén de datos donde estaba cuando se creó la copia de seguridad.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

 Sistemas operativos Windows *destinationfilespec*

 **Sistemas operativos Windows** Este parámetro es solo para restauraciones de VMware VCB. Especifica la ubicación donde se restauran los archivos de imagen de la máquina virtual completa de VCB. Si no se especifica esta opción, se utiliza la opción `vmbackdir`.

`:vmdk=all-vmdk`

Esta opción especifica que todos los discos virtuales (archivos \*.vmdk) se incluyen cuando la máquina virtual se restaura. Éste es el valor predeterminado.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

`:vmdk=cnfg`

Esta opción especifica que se restaure la información de configuración de máquina virtual. La información de configuración siempre se restaura cuando se crea una máquina virtual nueva. Sin embargo, de forma predeterminada la configuración no se restaura cuando se actualiza una máquina virtual existente con discos virtuales seleccionados.

Normalmente, la restauración de información de configuración en una máquina virtual existente falla porque la información de configuración restaurada está en conflicto con la información de configuración de máquina virtual existente. Utilice esta opción si se ha suprimido el archivo de configuración existente para una máquina virtual en el servidor ESX y quiere utilizar la configuración de la copia de seguridad para restaurarlo.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

`:vmdk=etiqueta de disco`

Esta opción se utiliza para especificar la etiqueta de disco de los discos virtuales que desea incluir en la operación de restauración. Especifique esta opción únicamente si desea restaurar datos de forma selectiva de discos específicos.

Nota: En el mandato `Restore VM`, los nombres de etiqueta de los archivos vmdk que desea incluir (`:vmdk=` parámetro) en una operación `Restore VM` debe especificarse con el nombre de etiqueta `English-language`, ya que se muestra en la salida del mandato `Backup VM vmname -preview`. Ejemplos de las etiquetas vmdk `English` son "Hard Disk 1", "Hard Disk 2", etc.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.



`:-vmdk=etiqueta de disco`







Esta opción se utiliza para especificar la etiqueta de disco de uno o más discos virtuales que desea excluir en la operación de restauración.

Nota: En el mandato `Restore VM`, los nombres de etiqueta de los archivos vmdk que desea excluir (`:-vmdk=` parameter) de una operación `Restore VM` deben especificarse con el nombre de etiqueta `English-language`, ya que se muestra en la salida del mandato `Backup VM vmname -preview`. Ejemplos de las etiquetas vmdk `English` son "Hard Disk 1", "Hard Disk 2", etc.

Nota: Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.


Tabla 1. Mandato `Restore VM`: opciones relacionadas cuando se restauran máquinas virtuales VMware

Opción	Dónde se utiliza
<code>datacenter</code>	Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
<code>datastore</code>	Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
<code>host</code>	Línea de mandatos o archivo de opciones. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
<code>inactive</code>	Línea de mandatos.
<code>pick</code>	Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
<code>pitdate</code>	Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
<code>pittime</code>	Línea de mandatos. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.
 <b>Sistemas operativos Windows</b> <code>vmautostartvm</code> Este parámetro sólo es válido cuando se especifica <code>instantaccess</code> como el valor de <code>vmrestoretype</code> .	 <b>Sistemas operativos Windows</b> Línea de mandatos o archivo de opciones del cliente.

Opción	Dónde se utiliza
vmbackdir	Línea de mandatos o archivo de opciones del cliente.
vmbackuplocation	Línea de mandatos.
vmbackuptype	Línea de mandatos o archivo de opciones del cliente.
vmdefaultdvportgroup	Línea de mandatos o archivo de opciones del cliente
vmdefaultdvswitch	Línea de mandatos o archivo de opciones del cliente
vmdefaultnetwork	Línea de mandatos o archivo de opciones del cliente
vmdiskprovision Este parámetro sólo es válido cuando se especifica instantrestore como el valor de vmrestoretype.	Línea de mandatos o archivo de opciones del cliente.
 Sistemas operativos Windows vmiscsiserveraddress Este parámetro sólo es válido cuando se especifica instantaccess o instantrestore como el valor de vmrestoretype.	 Sistemas operativos Windows Línea de mandatos o archivo de opciones del cliente.
vmmaxrestoresessions	Línea de mandatos o archivo de opciones del cliente.
 Sistemas operativos Windows vmrestoretype	 Sistemas operativos Windows Línea de mandatos.
 Sistemas operativos Windows vmtempdatastore Este parámetro sólo es válido cuando se especifica instantrestore como el valor de vmrestoretype.	 Sistemas operativos Windows Línea de mandatos o archivo de opciones del cliente.
vmvstortransport	Línea de mandatos o archivo de opciones del cliente. Este parámetro no es válido para restaurar máquinas virtuales de VMware de las que se hizo copia de seguridad utilizando VCB.

## Ejemplos

### Sistemas operativos Windows Tarea

 Sistemas operativos Windows Para realizar una restauración instantánea o una operación de acceso instantáneo desde la línea de mandatos, consulte Casos de ejemplo para ejecutar el acceso instantáneo de máquina virtual completa y restauración de máquina virtual instantánea completa desde la línea de mandatos del cliente de archivado y copia de seguridad.

#### Tarea

Restaurar la versión más reciente de la copia de seguridad de *myVM* con su nombre original. Utilice la interfaz de gestión VMware para suprimir la máquina virtual inicial, antes de restaurarla con esta sintaxis.

```
dsmc restore vm myvm
```

#### Tarea

Restaurar la versión de copia de seguridad más reciente de *myvm* a una máquina nueva que se crea con el nombre "Test Machine", y con el destino de restauración del centro de datos, host de ESX y almacén de datos todos especificados en el mandato.

```
dsmc restore vm myvm -vmname="Test Machine"
-datacenter="myDatacenter" -host="myHostName"
-datastore="myDatastore"
```

#### Tarea

Restaurar la versión más reciente de la copia de seguridad de *myvm* con el nuevo nombre *myvm\_restored*.

```
dsmc restore vm myvm -vmname="*_restored"
-datacenter="myDatacenter" -host="myHostName"
-datastore="myDatastore"
```

#### Tarea

Restaurar la versión más reciente de la copia de seguridad de *myvm* con un nuevo nombre, mostrando la fecha y hora, similar a *myvm\_03-22-2017\_14-41-24*.

```
dsmc restore vm myvm -vmname="*_<timestamp>"
-datacenter="myDatacenter" -host="myHostName"
-datastore="myDatastore"
```

#### Tarea

Restaurar la versión más reciente de la copia de seguridad de *myvm*. Restaurar el centro de datos denominado *mydatacenter*. El centro de datos está dentro de vCenter; la vía de acceso relativa dentro de vCenter es *dirA/datacenters/*.

```
dsmc restore vm myvm -vmname="Test Machine"  
-datacenter="dirA/datacenters/myDatacenter"  
-host="myHostName" -datastore="myDatastore"
```

#### Tarea

Restaurar una plantilla de máquina virtual en la misma ubicación y con el mismo nombre.

```
dsmc restore vm nombrePlantillaVm
```

#### Tarea

Restaurar una plantilla de máquina virtual en una ubicación nueva.

```
dsmc restore vm nombrePlantillaVm-vmname=nombreNuevo  
-datastore=almacénDatosNuevo -host=hostNuevo  
-datacenter=centroDatosNuevo
```

#### Tarea

Restaurar únicamente Hard Disk 2 y Hard Disk 3 en la máquina virtual existente denominada *vm1*.

```
dsmc restore vm "vm1:vmdk=Hard Disk 2:vmdk=Hard Disk 3"
```

#### Tarea

Restaurar todos los discos de la máquina virtual existente denominada *vm1*, pero no restaurar los datos del Hard Disk 4.

```
dsmc restore vm "vm1:-vmdk=Hard Disk 4"
```

#### Tarea

Restaura solo los datos del Hard Disk 1 a la *vm1* máquina virtual existente; no actualiza ninguna información de configuración.

Nota: Cuando restaura una máquina virtual existente, el comportamiento predeterminado es no actualizar la información de configuración.

```
dsmc restore vm "vm1:vmdk=Hard Disk 1:-vmdk=cnfg"
```

#### Tarea

Restaurar todos los discos de la máquina virtual existente denominada *vm1*.

```
dsmc restore vm "vm1:vmdk=all-vmdk"
```

Este mandato actualiza todos los discos virtuales en una máquina virtual existente, denominada *vm1*. Tenga en cuenta que esta acción es distinta a la acción que se realiza mediante `dsmc restore vm vm1`, que crea una nueva máquina virtual denominada *vm1* (*vm1* no debe existir para que `dsmc restore vm vm1` sea satisfactorio).

#### Tarea

Definir un máximo de tres sesiones para utilizarlas en operaciones de restauración de discos virtuales en la máquina virtual *vm1*:

```
dsmc restore vm vm1 -vmmxrestoresessions=3
```


Importante: Para máquinas virtuales de Windows: Si intenta ejecutar una restauración de máquina virtual completa de una copia de seguridad de protección de aplicaciones creada con 2 o más intentos de instantánea, la instantánea del proveedor de sistema estará presente en la máquina virtual restaurada. A medida que la aplicación escriba en el disco, el espacio de almacenamiento de instantáneas crecerá hasta que se quede sin espacio en disco.

En general, si se ha utilizado la protección de aplicaciones durante una copia de seguridad, utilice solo la restauración de la protección de aplicaciones. Al restaurar la aplicación, el volumen se revierte automáticamente. Sin embargo, si tiene que restaurar la máquina virtual completa, debe revertir o suprimir la instantánea.

Una vez restaurada la máquina virtual completa, asegúrese de que la restauración se haya realizado correctamente y de que los datos no estén dañados. Si los datos no están dañados, suprima la instantánea. Si los datos están dañados, revierta la instantánea para restaurar la integridad de los datos.

Puede determinar qué instantánea suprimir o revertir buscando el archivo `dsmShadowCopyID.txt` en el directorio raíz de cada volumen restaurado. Este archivo contiene los ID de las instantáneas creadas durante los intentos de instantánea. Puede utilizar el mandato `diskshadow delete shadows` para suprimir estos ID, o bien el mandato `revert` para revertir la instantánea. Una vez completadas la supresión o la reversión, también puede suprimir el archivo `dsmShadowCopyID.txt`.

Para obtener más información, consulte el apartado `INCLUDE.VMSNAPSHOTATTEMPTS`.

 Sistemas operativos Windows

## Restore VM para máquinas virtuales Microsoft Hyper-V

Utilice el mandato Restore VM para restaurar huéspedes Hyper-V. Puede restaurar huéspedes de Hyper-V a un disco local, un disco conectado SAN, un volumen compartido de clúster o a un uso compartido de servidor de archivos remotos. Los usos compartidos de servidor de archivos remoto deben estar en un sistema Windows Server 2012 o posterior.

Si la máquina virtual que está restaurando existe, el cliente de archivado y copia de seguridad se cerrará y suprimirá todos los archivos que conforman la máquina virtual. El cliente la restaurará a partir de la imagen que se almacena en el servidor de IBM Spectrum Protect. Si la máquina virtual es un miembro de un clúster de Windows Server 2012, la máquina virtual se sitúa fuera de línea del clúster, lo que detiene la máquina virtual. Los archivos se suprimen y, a continuación, el cliente la restaura a partir de la copia de seguridad de IBM Spectrum Protect.

Consejo: Aunque el cliente concluya la máquina virtual antes de que se suprima, la conclusión manual de la máquina virtual antes de ejecutar el mandato Restore VM es una práctica recomendada a seguir para llevar las actividades de aplicaciones en curso a una detención ordenada. A continuación, utilice el mandato Restore VM para restaurar la máquina virtual de forma que su contenido y su configuración sean idénticos a lo que había cuando se realizó la copia de seguridad.

## Clientes soportados

Este mandato es válido en clientes Windows soportados instalados en un sistema de host Hyper-V.

## Sintaxis

```
>>-REStore VM-- --sourcevmspec----->
>--+-----+----->
  '- -targetpath=--vía_acceso--+-----+'
                                     '- -vmname=--nombre_máquina_virtual_nuevo-'
>--+-----+-----<
  '+-----+'
  '- --options-'
```

## Parámetros

Cualquier parámetro que contenga espacios se debe incluir entre comillas dobles (" ").

El parámetro *sourcevmspec* es obligatorio. Los demás parámetros son opcionales. Considere los escenarios siguientes para determinar los parámetros a utilizar:

- Para restaurar la máquina virtual en la vía de acceso original utilizando el nombre de máquina virtual original, utilice sólo el parámetro *sourcevmspec*. La máquina virtual se restaura con su GUI de VMware original.
- Para restaurar la máquina virtual en una vía de acceso alternativa utilizando el nombre de máquina virtual original, utilice los parámetros *sourcevmspec* y *-targetpath*. La máquina virtual se restaura en la vía de acceso especificada con un nuevo GUID de VMware. La máquina virtual de la vía de acceso original no se elimina.
- Para restaurar la máquina virtual en una vía de acceso alternativa utilizando un nombre de máquina virtual nuevo, utilice los parámetros *sourcevmspec*, *-targetpath* y *-vmname*. La máquina virtual se restaura en la vía de acceso especificada con el nombre nuevo y un nuevo GUID de VMware. La máquina virtual con el nombre original en la vía de acceso original no se suprime.

El parámetro *-vmname* sólo es válido para restaurar máquinas virtuales cuya copia de seguridad se ha realizado mediante las modalidades *iffull* o *ifincremental*. Este parámetro se ignora para las máquinas virtuales cuya copia de seguridad se ha realizado mediante las modalidades *full* o *incremental* suministradas en releases anteriores del producto.

### *sourcevmspec*

Especifica el nombre de la máquina virtual que desea restaurar. El nombre de la máquina virtual distingue entre mayúsculas y minúsculas. No puede utilizar caracteres comodín en el nombre de la máquina virtual.

### *-targetpath=path*

Especifica la vía de acceso en la que desea restaurar la máquina virtual.

Este parámetro es necesario si se ha utilizado el parámetro *-vmname*; de lo contrario, es opcional. Utilice este parámetro para restaurar la máquina virtual en una vía de acceso alternativa.

### *-vmname=new\_vm\_name*

Especifica un nuevo nombre para la máquina virtual. El nombre puede contener 1-100 caracteres. Los caracteres siguientes son válidos: \ / : ; , \* ? " ' < > |

Este parámetro requiere el parámetro *-targetpath*.

Tabla 2. Mandato Restore VM: opciones relacionadas cuando se restauran máquinas virtuales Hyper-V



Opción	Dónde se utiliza
inactive	Línea de mandatos
pick	Línea de mandatos
pitdate	Línea de mandatos
pittime	Línea de mandatos
replace	Línea de mandatos, archivo de opciones del cliente o editor de preferencias de cliente.
vmbackdir	Línea de mandatos, archivo de opciones del cliente.

## Ejemplos

### Tarea

Restaurar la versión de copia de seguridad más reciente denominada VM1 a la unidad y vía de acceso que había cuando se realizó la copia de seguridad.

```
dsmc restore vm VM1
```

### Tarea

Restaurar la versión de copia de seguridad más reciente denominada vm1 a la unidad y vía de acceso que había cuando se realizó la copia de seguridad. Sustituir la máquina virtual existente sin consultar.

```
dsmc restore vm vm1 -replace=yes
```

### Tarea

Restaurar la máquina virtual con copia de seguridad llamada VM1 a otro nombre (vm2):

```
dsmc restore vm VM1 -VmName=vm2
```

### Tarea

Restaurar la máquina virtual con copia de seguridad llamada vm1, y asignarla a un nombre nuevo (vm2). Emita una solicitud antes de sobrescribir vm2, si dicha máquina virtual ya existe.

```
dsmc restore vm vm1 -VmName=vm2 -replace=prompt
```

### Tarea

Restaurar la máquina virtual llamada vm1 a una unidad y vía de acceso específicas, sin cambiar el nombre de la máquina virtual:

```
dsmc restore vm vm1 -targetpath="E:\New Path"
```

### Tarea

Restaurar la máquina virtual denominada vm1, pero cambiarle el nombre a vm2 y restaurarla en una vía de acceso nueva:

```
dsmc restore vm vm1 -VmName=vm2 -targetpath=F:\NewPath
```

### Tarea

Utilizar -pick y -inactive para mostrar copias de seguridad activas e inactivas para una máquina virtual denominada vm1. Puede elegir la copia de seguridad que desea restaurar de una lista:

```
dsmc restore vm vm1 -pick -inactive
```


## Retrieve


El mandato retrieve obtiene copias de archivos archivados del servidor de IBM Spectrum Protect. Puede recuperar archivos específicos o directorios completos.

Utilice la opción description para especificar las descripciones asignadas a los archivos que desea recuperar.

Utilice la opción pick para mostrar una lista de los archivos en la que puede seleccionar el archivo que desea recuperar.

Recupere los archivos en el mismo directorio desde donde se archivaron o en un directorio distinto. El cliente de copia de seguridad y archivado utiliza la opción preservepath con el valor subtree como valor predeterminado para restaurar los archivos.


 sistemas operativos Mac OS XNota: Cuando se recupera un directorio, la fecha y la hora de modificación de éste se establecen en la fecha y la hora de la recuperación, no en la fecha y la hora que tenía el directorio cuando se realizó la copia archivada de éste. Esto se debe a que el cliente de copia de seguridad y archivado recupera primero los directorios y luego añade los archivos a los directorios.

 Sistemas operativos WindowsNota:

1. Cuando se recupera un directorio, la fecha y la hora de modificación de éste se establecen en la fecha y la hora de la recuperación, no en la fecha y la hora que tenía el directorio cuando se realizó la copia archivada de éste. Esto se debe a que el cliente de copia de seguridad y archivado recupera primero los directorios y luego añade los archivos a los directorios.
2. Si se intenta recuperar un archivo cuyo nombre es el mismo que el nombre abreviado de un archivo ya existente se producirá un error. Por ejemplo, si se quiere recuperar un archivo cuyo nombre específico es ABCDEF~1.DOC en el mismo directorio en el que se encuentra un archivo llamado abcdefghijk.doc, la recuperación falla porque el sistema operativo Windows convierte el nombre del archivo llamado abcdefghijk.doc en el nombre abreviado ABCDEF~1.DOC. La función de recuperación trata este caso como una duplicación de archivos.

Si se produce este error, ejecute cualquiera de las acciones siguientes para corregirlo:

- Recuperar el archivo con el nombre abreviado que ha especificado en una ubicación distinta.
- Detener la operación de recuperación y cambiar el nombre del archivo existente.
- Desactivar el soporte de nombres de archivos abreviados en Windows.
- No utilizar nombres de archivos que entren en conflicto con el convenio de denominación abreviada de archivos. Por ejemplo, no utilice ABCDEF~1.DOC.

 Sistemas operativos Windows El nombre de la estación de trabajo forma parte del nombre de archivo. Por lo tanto, si se realizan copias archivadas en una estación de trabajo y se desea recuperarlas en otra estación de trabajo, debe especificarse un destino. Ello sucede incluso en el caso de que se recuperen los archivos en la misma estación de trabajo física, pero ésta tiene un nuevo nombre. Por ejemplo, para recuperar el archivo c:\doc\h2.doc en su directorio original en la estación de trabajo, denominada star, debería especificar lo siguiente:

```
dsmc retrieve c:\doc\h2.doc \\star\c$\
```






Se ha cambiado el nombre de la estación de trabajo denominada star por meteor. Para recuperar el archivo c:\doc\h2.doc en meteor, debe especificar:

```
dsmc retrieve c:\doc\h2.doc \\meteor\c$\
```

También puede entrarse:

```
dsmc retrieve c:\doc\h2.doc \\star\c$\
```

Puede especificar el mandato de las dos formas anteriores, cualquiera de ellas, pues si el nombre de la estación de trabajo no se incluye en la especificación de archivo, se da por supuesto el nombre de la estación de trabajo local (en este caso, meteor).

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows

## Clientes soportados

Este mandato es válido para todos los clientes.

 sistemas operativos Mac OS X  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X





## Sintaxis





```
>>-REtrieve--+-----+---+--sourcefilespec--+----->
      '- --options-' '- --"sourcefilespec"-'
>--+-----+-----><
      '- --destinationfilespec-'
```


 Sistemas operativos Windows


## Sintaxis

```
>>-REtrieve--+-----+----->
      '- --options-'
>--+--sourcefilespec-----+----->
      '- --{--filespace--}--sourcefilespec-'
>--+-----+-----><
      '- --destinationfilespec-'
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
sourcefilespec


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica la vía de acceso y el nombre del archivo que se desea recuperar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.

 Sistemas operativos Windows  
sourcefilespec





 Sistemas operativos Windows  
Especifica la vía de acceso y el nombre del archivo que se desea recuperar. Utilice caracteres comodín para especificar un grupo de archivos o todos los archivos de un directorio.





Nota: Si incluye filespace, no incluya una letra de unidad en la especificación de archivo.

 Sistemas operativos Windows  
filespace{}




 Sistemas operativos Windows  
Especifica el espacio de archivos (incluido entre llaves) del servidor que contiene los archivos que quiere recuperar. Este nombre es la etiqueta de la unidad de la estación de trabajo cuyas copias fueron archivadas. Utilice el nombre de espacio de archivos si el nombre de etiqueta de unidad ha sido modificado o si está recuperando archivos archivados desde otro nodo cuyos nombres de etiqueta de unidad son diferentes de los suyos.

Nota: Debe especificar un nombre de espacio de archivos NTFS o ReFS en minúsculas o en minúsculas y mayúsculas indicado entre comillas con llaves. Por ejemplo, {"NTFSDrive"}. En la modalidad de bucle son válidas las comillas dobles o comillas simples. Por ejemplo: {"NTFSDrive"} y {NTFSDrive} son igualmente válidos. En la modalidad por lotes, sólo se pueden utilizar las comillas simples. El requisito de las comillas simples es una limitación del sistema operativo.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
destinationfilespec

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Especifica la vía de acceso y el nombre de archivo en el que desea grabar los archivos. Si no especifica un destino, el cliente restaura los archivos en la vía de acceso de origen inicial.

Nota: si no especifica un destino, el cliente de copia de seguridad y archivado determina si puede accederse al sistema de archivos original. Si no es posible acceder al sistema de archivos original, el cliente no restaura el archivo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  
Este problema también puede darse si elimina la opción virtualmountpoint del archivo dsm.sys. En este caso, puede especificar otro destino o restaurar la opción virtualmountpoint original en el archivo dsm.sys, reiniciar el cliente y volver a intentar el mandato.

 Sistemas operativos Windows  
destinationfilespec



















 Sistemas operativos Windows  
Especifica la vía de acceso y el nombre de archivo en el que desea grabar los archivos. Si no especifica un destino, el cliente restaura los archivos en la vía de acceso de origen inicial.








Cuando especifique la serie destinationfilespec, tenga en cuenta los puntos siguientes:

- Si sourcefilespec especifica un único archivo, destinationfilespec puede ser un archivo o un directorio.
- Si sourcefilespec contiene algún carácter comodín o si especifica la opción `subdir=yes`, destinationfilespec debe ser un directorio y debe terminar por el delimitador de directorios (\).









Nota: Si la vía de acceso de destino o cualquier parte de ella no existe, el cliente creará una vía de acceso.

Tabla 1. mandato Retrieve: opciones relacionadas


Opción	Dónde se utiliza
 Sistemas operativos Windows dateformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X dateformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
description	Sólo línea de mandatos.
dironly	Sólo línea de mandatos.
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X followsymbolic	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.


Opción	Dónde se utiliza
fromdate	Sólo línea de mandatos.
fromnode	Sólo línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X fromowner	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X Sólo línea de mandatos.
fromtime	Sólo línea de mandatos.
ifnewer	Sólo línea de mandatos.
pick	Sólo línea de mandatos.
preservepath	Sólo línea de mandatos.
 Sistemas operativos Windows replace	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X replace	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows skipntpermissions	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos
 Sistemas operativos Windows skipntsecuritycrc	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos
 Sistemas operativos Windows subdir	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X subdir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows tapeprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X tapeprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows timeformat	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X timeformat	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones de usuario del cliente (dsm.opt) o línea de mandatos.
to date	Sólo línea de mandatos.
totime	Sólo línea de mandatos.

## Ejemplos









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Tarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar un único archivo denominado budget.

```
retrieve /home/devel/projecta/budget
```


 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Recuperar un único archivo denominado budget.fin.

```
ret c:\devel\projecta\budget.fin
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar todos los archivos que tienen la extensión .c del directorio /home/devel/projecta.


```
retrieve "/home/devel/projecta/*.c"
```

 Sistemas operativos Windows Tarea









 Sistemas operativos Windows Recuperar todos los archivos que tienen la extensión .c del directorio c:\devel\projecta.

```
ret c:\devel\projecta\*.c
```

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Recuperar todos los archivos que tienen la extensión de archivo .c del directorio \devel\projecta en el espacio de archivos winnt.

```
ret {winnt}\devel\projecta\*.c
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar todos los archivos en el directorio /home.


```
retrieve /home/
```

 Sistemas operativos Windows Tarea









 Sistemas operativos Windows Recuperar todos los archivos en el directorio c:\devel.

```
ret c:\devel\*
```

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Recuperar todos los archivos del directorio proj del espacio de archivos abc.

```
ret {abc}\proj\*.*
```









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar todos los archivos que tienen la extensión de archivo .c desde el directorio /home/devel/projecta hasta el directorio /home/newdevel/projectn/projecta. Si el directorio /projectn o /projectn/projecta no existe, se creará.

```
retrieve "/home/devel/projecta/*.c" /home/newdevel/projectn/
```

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Recuperar todos los archivos que tienen la extensión de archivo .c desde el directorio c:\devel\projecta hasta el directorio c:\newdevel\projectn\projecta. Si el directorio projectn o \projectn\projecta no existe, se creará.

```
ret c:\devel\projecta\*.c c:\newdevel\projectn\
```









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar archivos en el directorio /user/project. Utilizar la opción pick.

```
ret "/user/project/*" -pick
```









 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Recuperar archivos en el directorio c:\project. Utilizar la opción pick.

```
ret c:\project\* -pick
```


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar todos los archivos que se han archivado del directorio /proj con la descripción "2012 survey results".

```
retrieve "/proj/*" -desc="2012 survey results"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Recuperar la copia archivada /home/devel/budget que tiene la descripción "mi presupuesto" en la unidad de cintas /dev/rmt1.


```
mkfifo fifo
dd if=fifo of=/dev/rmt1&
dsmc retrieve -replace=yes -description="mi presupuesto"
/home/devel/budget fifo
```

#### sistemas operativos Mac OS X





 sistemas operativos Mac OS X Recuperar un archivo del espacio de archivos renombrado Jaguar\_OLD en su ubicación original. Especifique el origen y el destino como se indica a continuación:

```
ret Jaguar_OLD/user5/Documents/myresume.doc /Users/user5/Documents/
```

#### Sistemas operativos Windows

 Sistemas operativos Windows Recuperar un archivo desde el espacio de archivos renombrado \\nodo\h\$\_OLD en su ubicación original. Especifique el origen y el destino como se indica a continuación:

```
ret \\your-node\h$_OLD\docs\myresume.doc h:\docs\
```


-  sistemas operativos Mac OS X  Sistemas operativos Windows Recuperación de archivos desde espacios de archivos que no están activados para Unicode  
Si desea recuperar archivos de espacios de archivos cuyos nombres ha cambiado el cliente activado para Unicode, deberá especificar el origen en el servidor y el destino en el cliente.
-  Sistemas operativos Windows Recuperación de corrientes designadas  
El cliente de copia de seguridad y archivado recupera las corrientes designadas sólo en términos de archivo.
-  Sistemas operativos Windows Recuperación de archivos esparcidos  
Cuando se recuperen archivos esparcidos en un sistema de archivos que no sea NTFS ni ReFS, establezca el valor de tiempo de espera de comunicación del servidor (IDLETIMEOUT) en el valor máximo de 255 para evitar que la sesión del cliente exceda el tiempo de espera.


#### sistemas operativos Mac OS X Sistemas operativos Windows


## Recuperación de archivos desde espacios de archivos que no están activados para Unicode

---


Si desea recuperar archivos de espacios de archivos cuyos nombres ha cambiado el cliente activado para Unicode, deberá especificar el origen en el servidor y el destino en el cliente.

 sistemas operativos Mac OS X Esta sección sólo se aplica a Mac OS X. Por ejemplo, imaginemos que Jaguar es el nombre del disco de arranque y que desea realizar el archivado de todos los archivos .log del directorio /Users/user5/Documents. Antes de que se produzca la operación de archivado, el servidor cambia el nombre del espacio de archivos por Jaguar\_OLD. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado /. El nuevo espacio de archivos activado para Unicode sólo contiene el directorio Users/user5/Documents y los archivos \*.log especificados en la operación.

 sistemas operativos Mac OS X Si desea recuperar un archivo del espacio de archivos *nombre cambiado* (old) en su ubicación original, deberá especificar el origen y el destino de la forma siguiente:

 Sistemas operativos Windows Si desea recuperar archivos de espacios de archivos cuyos nombres ha cambiado el cliente activado para Unicode, deberá especificar el origen en el servidor y el destino en el cliente. Por ejemplo, ha realizado el archivado de los archivos del disco H, denominado \\nodo\h\$, antes de instalar el cliente. Después de la instalación, emita el mandato de archivado siguiente:

```
arc h:\logs\*.log
```

 Sistemas operativos Windows Antes de que tenga lugar el archivado, el servidor cambiará el nombre del espacio de archivos por \\nodo\h\$\_OLD. La operación de archivado coloca los datos especificados en la operación actual en el espacio de archivos activado para Unicode denominado \\nodo\h\$. Ahora, ese espacio de archivos sólo contiene el directorio \logs y los archivos \*.log. Si desea recuperar un archivo del espacio de archivos *renombrado* (old) en su ubicación original, debe entrar el origen y el destino como se indica a continuación:

```
retrieve \\nodo\h$_OLD\docs\informe.doc h:\docs\
```

#### Sistemas operativos Windows


## Recuperación de corrientes designadas

---

El cliente de copia de seguridad y archivado recupera las corrientes designadas sólo en términos de archivo.

Los directorios de sistemas Windows pueden contener corrientes designadas. Durante una operación de restauración, las corrientes designadas asociadas a un directorio siempre se modificarán (independientemente del valor de la opción prompt) durante la

recuperación.

 Sistemas operativos Windows

## Recuperación de archivos esparcidos

---

Cuando se recuperen archivos esparcidos en un sistema de archivos que no sea NTFS ni ReFS, establezca el valor de tiempo de espera de comunicación del servidor (IDLETIMEOUT) en el valor máximo de 255 para evitar que la sesión del cliente exceda el tiempo de espera.





Si se restauran más datos de los que permite la cuota de disco de Microsoft, puede que ocurra lo siguiente:

- Si el usuario que realiza la recuperación dispone de una cuota de disco (por ejemplo, el usuario pertenece al grupo de operadores de copia de seguridad), el cliente de copia de seguridad y archivado no recupera los datos que sobrepasen la cuota de disco del usuario de recuperación y muestra el mensaje "Disco lleno".
- Si el usuario que realiza la recuperación no dispone de una cuota de disco (por ejemplo, pertenece al grupo de administradores), el cliente de copia de seguridad y archivado recupera todos los datos y transfiere la propiedad de los archivos que sobrepasen la cuota de disco del propietario original al usuario que realiza la recuperación (en este caso, el administrador).


## Schedule


---





El mandato schedule inicia el planificador cliente en la estación de trabajo. El planificador cliente debe estar en ejecución para que se pueda iniciar el trabajo planificado.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X **Usuario autorizado:** el mandato schedule inicia el planificador cliente en la estación de trabajo. El planificador cliente debe estar en ejecución para que se pueda iniciar el trabajo planificado.





Nota:


1. El mandato schedule no se puede utilizar si la opción managedservices se ha establecido en `schedule`.
2.  sistemas operativos Mac OS X Sólo para Mac OS X: para utilizar el mandato schedule, especifique `managedservices none` en el archivo `dsm.opt`.
3. Este mandato sólo es válido en la línea de mandatos inicial. No es válido en la modalidad interactiva ni en un archivo de macro.






 Sistemas operativos Windows Si la opción `schedmode` se establece para el sondeo, el planificador cliente establecerá contacto con el servidor para gestionar los sucesos planificados en función del intervalo de hora que ha especificado con la opción `querryschedperiod` en el archivo de opciones del cliente (`dsm.opt`). Si el administrador indica un valor en la opción `querryschedperiod` para todos los nodos, dicho valor modifica el valor indicado en el cliente.





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si la opción `schedmode` se establece para el sondeo, el planificador cliente establecerá contacto con el servidor para gestionar los sucesos planificados en función del intervalo de hora que ha especificado con la opción `querryschedperiod` en el archivo de opciones de usuario cliente (`dsm.opt`). Si el administrador indica un valor en la opción `querryschedperiod` para todos los nodos, dicho valor modifica el valor indicado en el cliente.


 Sistemas operativos Windows Si se están utilizando comunicaciones TCP/IP, el servidor puede solicitar a la estación de trabajo que inicie un suceso planificado cuando sea la hora de ejecutarlo. Para ello, establezca la opción `schedmode` en `prompted` en el archivo de opciones del cliente (`dsm.opt`) o en el mandato `schedule`.











 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Si se están utilizando comunicaciones TCP/IP, el servidor puede solicitar a la estación de trabajo que inicie un suceso planificado cuando sea la hora de ejecutarlo. Para ello, establezca la opción `schedmode` en `prompted` en el archivo de opciones del cliente (`dsm.opt`) o en el mandato `schedule`.

 Sistemas operativos Windows Una vez que se inicia el planificador cliente, éste continúa ejecutando e iniciando los sucesos planificados hasta que se pulse Control+Pausa, se reinicie la estación de trabajo o se apague la misma para finalizarlo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X Puede utilizar la opción `sessioninitiation` con el mandato `schedule` para controlar si el servidor o el cliente ha de iniciar las sesiones por medio de un cortafuegos.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Después de haber iniciado el planificador cliente, éste seguirá ejecutando e iniciando los sucesos planificados hasta que se pulse Ctrl+C, se detenga el proceso del planificador con el mandato de UNIX `kill`, vuelva a iniciarse la estación de trabajo o se apague ésta para finalizarlo.

 sistemas operativos Mac OS Xna vez que se inicia el planificador del cliente, éste sigue ejecutando e iniciando sucesos planificados hasta que se pulsa Ctrl+C, se efectúa una doble pulsación en la tecla Q, se inicia de nuevo la estación de trabajo o se apaga la misma para finalizarlo.

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsNota: *no se puede entrar este mandato en modalidad interactiva.*  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos Windows

## Cientes soportados



















































Este mandato es válido para todos los clientes.

## Sintaxis

```
>>-SCHEDULE--+-+-----+----->>
      '- --options-'
```

## Parámetros

Tabla 1. mandato Schedule: opciones relacionadas

Opción	Dónde se utiliza
 Sistemas operativos Windows maxcmdretries	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X maxcmdretries	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows password	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt)
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X password	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt)
 Sistemas operativos Windows querschedperiod	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X querschedperiod	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows retryperiod	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X retryperiod	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows schedlogname	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X schedlogname	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.



Opción	Dónde se utiliza
Sistemas operativos Windows schedmode	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X schedmode	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
Sistemas operativos Windows sessioninitiation	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X sessioninitiation	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
Sistemas operativos Windows tcpclientport	Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X tcpclientport	Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.

## Ejemplos

sistemas operativos Mac OS X Sistemas operativos Windows  
Tarea  
 sistemas operativos Mac OS X Sistemas operativos Windows  
Arrancar el planificador cliente.

**Mandato:** `dsmc sch -password=notell`

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Tarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Para AIX: iniciar el planificador durante el arranque del sistema especificando este mandato en el archivo `/etc/inittab`. Asegúrese de que la opción **passwordaccess** esté establecida en `generate`.

**mandato:** `tsm::once:/usr/bin/dsmc sched > /dev/null 2>&1 #TSM`

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Tarea  
 Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Iniciar de forma interactiva el planificador y mantenerlo en funcionamiento como proceso de fondo.

**Mandato:** `nohup dsmc sched 2> /dev/null &`

Sistemas operativos Windows  
Cuando ejecute el mandato `schedule`, todos los mensajes relacionados con el trabajo planificado se enviarán al archivo `dsmsched.log` o al archivo que ha especificado con la opción `schedlogname` en el archivo de opciones del cliente (`dsm.opt`). Si no especifica una vía de acceso de directorio con el nombre del archivo en la opción `schedlogname`, `dsmsched.log` residirá en el directorio de trabajo actual.

Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
Cuando ejecute el mandato `schedule`, todos los mensajes relacionados con el trabajo planificado se enviarán al archivo `dsmsched.log` o al archivo que ha especificado con la opción `schedlogname` en el archivo de opciones del sistema del cliente (`dsm.sys`). Si no especifica una vía de acceso de directorio con el nombre del archivo en la opción `schedlogname`, `dsmsched.log` residirá en el directorio de trabajo actual, a excepción de cuando se utilice Mac OS X. Para Mac OS X, `dsmsched.log` residirá en el directorio `/Library/Logs/tivoli/tsm/`.






Sistemas operativos AIX Sistemas operativos Linux Sistemas operativos Oracle Solaris sistemas operativos Mac OS X  
 Sistemas operativos Windows  
Importante: Establezca la variable de entorno `DSM_LOG` para asignar un nombre a un directorio donde los permisos predeterminados permitan el acceso necesario para evitar que se produzcan anomalías en la grabación de las anotaciones y la finalización de procesos en determinados casos.

## Selective

El mandato selective realiza copias de seguridad de los archivos que especifique. Si estos archivos se dañan o se pierden, podrá sustituirlos por las versiones de copia de seguridad del servidor.


Al ejecutar una copia de seguridad selectiva, todos los archivos son aptos para la copia de seguridad, salvo que se excluyan de la misma, o no satisfagan los requisitos de clase de gestión para la serialización.





Durante una copia de seguridad selectiva, se envían copias de los archivos al servidor, incluso si no se han modificado desde la última copia de seguridad, lo que puede generar más de una copia del mismo archivo en el servidor. Si ocurre esto, puede que no se tengan en el servidor tantas versiones distintas de nivel inferior del archivo como se pretendía. El límite de versiones podría consistir únicamente en archivos idénticos. Para evitarlo, utilice el mandato incremental para realizar copias de seguridad sólo cuando los archivos se modifiquen o sean nuevos.


     
 Puede realizar copias de seguridad selectivas de archivos únicos o directorios. También puede utilizar caracteres comodín para realizar copia de seguridad de grupos de archivos relacionados.

Si establece la opción subdir en yes al realizar una copia de seguridad de una vía de acceso y un archivo específicos, el cliente hace una copia de seguridad de forma recursiva todos los subdirectorios bajo esa vía de acceso y las instancias del archivo especificado que existan en los subdirectorios.





Durante una copia de seguridad selectiva, se puede hacer una copia de seguridad de una vía de acceso de directorio, incluso en el caso de que el archivo específico del que se tiene que hacer una copia de seguridad no se encuentra. Por ejemplo, el siguiente mandato sigue realizando la copia de seguridad de dir1 y dir2, aunque el archivo bogus.txt no exista.






  
selective /Users/user1/Documents/dir1/bogus.txt

     
selective "/dir1/dir2/bogus.txt"

  
selective c:\dir1\dir2\bogus.txt

Si vuelve a emitirse el mandato selective por haberse producido una anomalía en las comunicaciones o una pérdida de la sesión, las estadísticas de la transferencia visualizarán el número de bytes que el cliente intenta transferir durante *todos* los intentos de ejecución del mandato. Por ello, es posible que las estadísticas de bytes transferidos no coincidan con las estadísticas de archivos, como las relativas al tamaño de archivo.

    Puede utilizar la opción removeoperandlimit para especificar que se elimina el límite de 20 operandos. Si especifica la opción removeoperandlimit con el mandato selective, no se aplicará el límite de 20 operandos, y las únicas restricciones serán los recursos disponibles u otros límites del sistema operativo.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```

      .----- .
      v         |
>>-Selective----- --filespec--+-----+<<
                          '- --options-'
```

## Parámetros





---


### filespec

Especifique la vía de acceso y el nombre del archivo del que desea realizar la copia de seguridad. Utilice caracteres comodín para incluir un grupo de archivos o todos los archivos de un directorio.





Para incluir varias especificaciones de archivo, separe cada especificación de archivo con un carácter de espacio. Si se incluyen varias especificaciones de archivo, y dos o más de las especificaciones tienen directorios padre comunes, entonces es posible





hacer una copia de seguridad para los objetos de directorio comunes más de una vez. Las condiciones bajo las que este comportamiento ocurre son dependientes del tiempo de ejecución, pero el comportamiento por sí mismo no tiene efectos adversos.





 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Por ejemplo, si la especificación de archivo es /home/amr/ice.doc /home/amr/fire.doc, entonces se pueden hacer copia de seguridad de /home y /home/amr dos veces. La copia de seguridad de los objetos de archivo, ice.doc y fire.doc, se hace solo una vez.

 Sistemas operativos Windows Por ejemplo si la especificación de archivo es C:\proposals\drafts\ice.doc C:\proposals\drafts\fire.doc, entonces se puede hacer copia de seguridad de C:\proposals y C:\proposals\drafts dos veces. La copia de seguridad de los objetos de archivo ice.doc y fire.doc se hace solo una vez.


Si desea evitar incluir el directorio padre compartido más de una vez, utilice separar, no superponer mandatos selective para realizar copias de seguridad de cada especificación de archivo.


 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Si hace una copia de seguridad de un sistema de archivos, incluya una barra inclinada final (/home/).

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Existe un límite de 20 operandos. Este límite previene un número excesivo de sesiones cuando el procesador de mandatos de shell de UNIX expande los caracteres comodín. Puede impedir que la expansión del shell supere el límite de 20 operandos colocando entre comillas las especificaciones de archivo que contienen caracteres comodín ("home/docs/\*").

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris Puede utilizar la opción removeoperandlimit para especificar que se elimina el límite de 20 operandos. Si especifica la opción removeoperandlimit, el límite de 20 operandos no se aplica y queda restringido únicamente a los recursos disponibles u otros límites del sistema operativo. Por ejemplo, elimine el límite de 20 operandos para realizar una copia de seguridad de 21 especificaciones de archivo:































```
selective -removeoperandlimit filespec1 filespec2 ... filespec21
```

 Sistemas operativos Windows Si hace una copia de seguridad de un sistema de archivos, incluya una barra inclinada final (C:\).

 Sistemas operativos Windows Puede especificar tantas especificaciones de archivo como lo permitan los recursos disponibles u otros límites del sistema operativo.



Puede utilizar la opción filelist, en lugar de las especificaciones de archivo, para identificar qué archivos se han de incluir en esta operación. Sin embargo, estos dos métodos se excluyen mutuamente. No puede incluir parámetros de especificación de archivo y utilizar la opción filelist. Si se especifica la opción filelist, cualquiera de las especificaciones de archivo que se incluyen se ignoran.





Tabla 1. Mandato selective: opciones relacionadas

Opción	Dónde se utiliza
 Sistemas operativos Windows changingretries	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X changingretries	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X En el archivo de opciones del sistema cliente (dsm.sys) o en la línea de mandatos.
 Sistemas operativos Windows compressalways	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compressalways	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows compression	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X compression	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
dirsonly	Sólo línea de mandatos.


Opción	Dónde se utiliza
filelist	Sólo línea de mandatos.
filesonly	Sólo línea de mandatos.
 Sistemas operativos Windows postsnapshotcmd	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X preservelastaccessdate	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows preservelastaccessdate	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows presnapshotcmd	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X removeoperandlimit	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  sistemas operativos Mac OS X Sólo línea de mandatos.
 Sistemas operativos Windows skipntpermissions	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows skipntsecuritycrc	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux snapshotcachesize	 Sistemas operativos AIX  Sistemas operativos Linux Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX snapshotproviderfs	 Sistemas operativos AIX Archivo de opciones del sistema (dsm.sys) en una stanza del servidor o con la opción include.fs.
 Sistemas operativos Windows snapshotproviderfs	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o con la opción include.fs.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows snapshotroot	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  Sistemas operativos Windows Sólo línea de mandatos.
 Sistemas operativos Windows subdir	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X subdir	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos Windows tapeprompt	 Sistemas operativos Windows Archivo de opciones del cliente (dsm.opt) o línea de mandatos.
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X tapeprompt	 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Archivo de opciones del usuario cliente (dsm.opt) o línea de mandatos.


## Ejemplos

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar la copia de seguridad del archivo `proja` en el directorio `/home/devel`.

**Mandato:** `selective /home/devel/proja`

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Realizar la copia de seguridad del archivo `proja.dev` en el directorio `c:\devel`.

**Mandato:** `sel c:\devel\proja.dev`









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar la copia de seguridad de todos los archivos del directorio `/home/devel` cuyos nombres de archivo empieza por `proj`.

**Mandato:** `selective "/home/devel/proj*"`


 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Realizar la copia de seguridad de todos los archivos del directorio `c:\devel` cuyos nombres de archivo empiezan por `proj`.

**Mandato:** `sel c:\devel\proj*.*`









 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar la copia de seguridad de todos los archivos del directorio `/home/devel` cuyos nombres de archivo empieza por `proj`.  
Realizar copia de seguridad de un único archivo denominado `budget` en el directorio `/user/home`.

**Mandato:** `selective "/home/devel/proj*" /user/home/budget`









 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Realizar la copia de seguridad de todos los archivos del directorio `c:\devel` cuyos nombres de archivo empiezan por `proj`. Realizar la copia de seguridad de todos los archivos que tienen la extensión de archivo `.fin` en el directorio `c:\planning`.


**Mandato:** `sel c:\devel\proj* c:\planning\*.fin`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Realizar la copia de seguridad del sistema de archivos `/home`.

**Mandato:** `selective /home/ -subdir=yes`


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
Suponiendo que ha iniciado una instantánea del sistema de archivos `/usr` y ha montado la instantánea como `/snapshot/day1`, ejecute una copia de seguridad selectiva del árbol de directorios `/usr/dir1/sub1` desde la instantánea local y gestiónelo en el servidor de IBM Spectrum Protect debajo del nombre de espacio de archivos `/usr`.

**Mandato:** `dsmc sel "/usr/dir1/sub1/*" -subdir=yes -snapshotroot=/snapshot/day1`

 Sistemas operativos Windows Tarea

 Sistemas operativos Windows Suponiendo que ha iniciado una instantánea de la unidad `C:\` y que ha montado la instantánea como `\\florence\c$\snapshots\snapshot.0`, ejecute una copia de seguridad selectiva del árbol de directorios `c:\dir1\sub1` de la instantánea local y gestiónela en el servidor de IBM Spectrum Protect en el nombre de espacios de archivos `C:\`.

**Mandato:** `dsmc sel c:\dir1\sub1\* -subdir=yes -snapshotroot=\\florence\c$\snapshots\snapshot.0`

-  Sistemas operativos Windows Soporte de archivos abiertos  
Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).
- Asociación de una instantánea local a un espacio de archivos del servidor  
Utilice la opción `snapshotroot` con el mandato `selective` junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

 Sistemas operativos Windows

## Soporte de archivos abiertos

---

Si se ha configurado el soporte de archivos abiertos, el cliente de copia de seguridad y archivado realiza una operación de copia de seguridad de instantánea o de archivado de los archivos que otras aplicaciones han bloqueado (o utilizan).

Utilice VSS como el proveedor de instantáneas; configure snapshotproviderimage o snapshotproviderfs en VSS.


Nota:

1. Puede utilizar la opción `include.fs` para establecer opciones de instantánea para cada sistema de archivos.
2. El soporte de archivos abiertos solo se admite en volúmenes fijos locales, (montados en letras de unidad o en puntos de montaje de volúmenes) con formato de sistemas de archivos NTFS o ReFS. Este soporte incluye los volúmenes conectados con la SAN que satisfacen estos requisitos.
3. Si el cliente no puede crear una instantánea, se produce una recuperación de error en una copia de seguridad no OFS; el mismo soporte de copia de seguridad se realiza si la característica OFS no estuviera configurada.
4. Para activar el soporte de archivos abiertos en un entorno de clúster, todos los sistemas del clúster deberán tener configurada la característica OFS.

## Asociación de una instantánea local a un espacio de archivos del servidor

---

Utilice la opción `snapshotroot` con el mandato `selective` junto con una aplicación de otro proveedor de software independiente que proporcione una instantánea de un volumen lógico para asociar los datos de la instantánea local con los datos del espacio de archivos reales que se almacenan en el servidor de IBM Spectrum Protect. La opción `snapshotroot` no proporciona ningún recurso para tomar una instantánea de volumen, sólo para gestionar los datos que ha creado una instantánea de volumen.

 **Sistemas operativos AIX** Sólo AIX: puede realizar una copia de seguridad selectiva basada en instantáneas mediante la especificación de la opción `snapshotproviderfs=JFS2`.



## Set Access

---

El mandato `set access` otorga a usuarios determinados de otros nodos acceso a las versiones de copia de seguridad o copias archivadas.

También puede utilizar el mandato `set access` para otorgar a usuarios de otros nodos acceso a las imágenes de copia de seguridad.



Puede otorgar a un usuario determinado acceso a un archivo o imagen específicos, a varios archivos o imágenes o a todos los archivos de un directorio. Cuando da acceso a otro usuario, éste puede restaurar o recuperar sus objetos. Especifique en el mandato si se otorga acceso a las copias archivadas o las copias de seguridad.

 **Sistemas operativos Linux**  **Sistemas operativos Windows** Para máquinas virtuales de VMware, puede ofrecer a un usuario de otro nodo acceso a las copias de seguridad de una máquina virtual específica.

Cuando se exporta un nodo a otro servidor de IBM Spectrum Protect, se pueden cambiar las reglas de acceso en el servidor de importación. Si se aplica una regla de acceso a todos los espacios de archivos en el servidor de exportación, la regla de acceso del servidor de exportación está restringida únicamente a aquellos espacios de archivos que se importan. Los espacios de archivos están restringidos en la regla de acceso en el servidor de importación por razones de seguridad. Así mismo, las reglas de acceso no reconocen la primera aparición de un carácter comodín en la especificación de archivo cuando restaura o recupera. Esto significa que si restaura o recupera con un carácter comodín en una especificación de archivo, los subdirectorios se ignoran.

Consejo: Si exporta un nodo a otro servidor de IBM Spectrum Protect, no utilice un único carácter comodín como especificación de archivo en la regla de acceso. En lugar de eso, cree una regla de acceso para cada uno de los espacios de archivos.

Nota: no puede otorgar acceso a copias de seguridad y copias archivadas con un único mandato.

 **sistemas operativos Mac OS X**  **Sistemas operativos Windows** Cuando se cambia el nombre de un espacio de archivos existente durante la conversión de Unicode, las reglas de acceso que se han definido para el espacio de archivos siguen aplicándose al espacio de archivos original. Sin embargo, deberán definirse las nuevas reglas de acceso que han de aplicarse al nuevo espacio de archivos Unicode.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-SET Access---+-- --Archive+----->
      '- --Backup--'

>--+-- --filespec-----+-- --nodo--+-----+--<
+-- --{--filespacename--}--filespec+      '- --user-'
+-imagen-sa-----+
'-TYPE=VM-- --vmname-----'
```

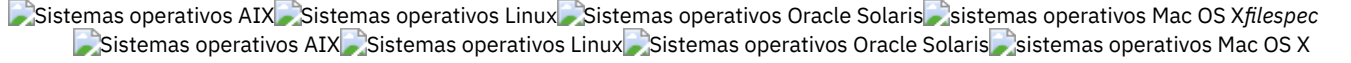
## Parámetros

### Archive

Permite acceder a copias archivadas o imágenes.

### Backup

Permite acceder a las versiones de copia de seguridad de los archivos o imágenes.

 Especifica la vía de acceso, el archivo, la imagen o el directorio para el que otorga acceso al otro nodo o usuario. Utilice caracteres comodín para especificar un grupo de archivos o de imágenes o bien todos los archivos de un directorio, todos los objetos de una rama de directorios o todos los objetos de un sistema de archivos. Utilice un único asterisco "\*" en la especificación de archivo para otorgar acceso a todos los archivos o todas las imágenes de los que el usuario es propietario y de los que se ha realizado copia de seguridad en el servidor. Cuando se especifica el mandato `set access backup "*" node`, no se realiza ninguna comprobación con el servidor; se da por supuesto que, como mínimo, dispone de un objeto cuya copia de seguridad ha realizado.

Si se otorga acceso a una rama del directorio de trabajo actual, especifique solo la rama. Si se otorga acceso a objetos que no se encuentren en una rama del directorio de trabajo actual, deberá especificarse la vía de acceso completa. La especificación de archivo a la que se otorga acceso debe tener al menos un objeto de versión de copia de seguridad o de copia archivada (archivo o directorio) en el servidor.

Para especificar todos los archivos de un directorio determinado, especifique `/home/mine/proj1/*` en la línea de mandatos.

Para otorgar acceso a todos los objetos bajo un determinado nivel, utilice un asterisco, un delimitador de directorio y un asterisco al final de la especificación de archivo. Por ejemplo, para otorgar acceso a todos los objetos de `home/test`, utilice la especificación de archivo `home/test/*/*`.

Importante: La utilización del formato `/*/*` sin ninguna indicación adicional no otorgará acceso a los objetos del directorio especificado; solo podrá accederse a los directorios incluidos en el directorio especificado.

Las reglas son básicamente las mismas si se trata del directorio raíz. Especifique `/*` en un mandato de acceso establecido, y `/*/*` en otro, si desea que otro usuario disponga de acceso a todos los archivos y directorios que se encuentran en el directorio raíz, o debajo de él. La primera indicación `/*` otorga acceso a todos los directorios y a todos los archivos del directorio raíz. La segunda indicación `/*` permite acceder a todos los directorios y archivos que se encuentran debajo del directorio raíz.

Por ejemplo:

- La estructura de directorios consta de varios niveles: `/home/sub1/subsub1`.
- El directorio `/home` contiene los archivos `h1.txt` y `h2.txt`.
- El directorio `/home/sub1` contiene el archivo `s1.htm`.
- El directorio `/home/sub1/sub2` contiene el archivo `ss1.cpp`.

Para que pueda accederse a todos los archivos del directorio `/home/sub1/sub2`, especifique:

```
set access backup /home/sub1/sub2/* * *
```

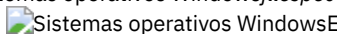
Para que solo pueda accederse a los archivos del directorio `/home`, especifique:

```
set access backup /home/* * *
```

Para que pueda accederse a todos los archivos de todos los directorios que se encuentran en el directorio `/home`, o debajo de él, escriba:

```
set access backup /home/* * *
set access backup /home/*/* * * *
```

 **filespec**

 Especifica la vía de acceso, el archivo, la imagen o el directorio para el que se otorga acceso al otro nodo o usuario. Utilice caracteres comodín para especificar un grupo de archivos o de imágenes o bien todos los archivos de un directorio, todos los objetos de una rama de directorios o todos los objetos de una unidad. Sin embargo, no puede utilizar un

comodín para especificar todas las unidades. Utilice un único asterisco "\*" en la especificación de archivo para otorgar acceso a todos los archivos o todas las imágenes de los que el usuario es propietario y de los que se ha realizado copia de seguridad en el servidor. Cuando se especifica el mandato `set access backup "*" node`, no se realiza ninguna comprobación con el servidor; se da por supuesto que, como mínimo, dispone de un objeto cuya copia de seguridad ha realizado.

Si se otorga acceso a una rama del directorio de trabajo actual, especifique sólo la rama. Si se otorga acceso a objetos que no se encuentren en una rama del directorio de trabajo actual, deberá especificarse la vía de acceso completa. La especificación de archivo a la que se otorga acceso debe tener al menos un objeto de versión de copia de seguridad o de copia archivada (archivo o directorio) en el servidor.

Para especificar todos los archivos de un directorio determinado, especifique `d:\test\mine\proj1\*` en la línea de mandatos.

Para otorgar acceso a todos los objetos bajo un determinado nivel, utilice un asterisco, un delimitador de directorio y un asterisco al final de la especificación de archivo. Por ejemplo, para otorgar acceso a todos los objetos de `d:\test`, utilice la especificación de archivo `d:\test\*\*`.

Importante: La utilización del formato `\*\*` sin ninguna indicación adicional no otorgará acceso a los objetos del directorio especificado; solo podrá accederse a los directorios inferiores al directorio especificado.

Las reglas son básicamente las mismas si se trata del directorio raíz. Escriba `\*` en un mandato de acceso establecido, y `\*\*` en otro, si desea que otro usuario disponga de acceso a todos los archivos y directorios que se encuentran en el directorio raíz, o debajo de él. La primera indicación `\*` otorga acceso a todos los directorios y a todos los archivos del directorio raíz. La segunda indicación `\*` permite acceder a todos los directorios y archivos que se encuentran debajo del directorio raíz.

Nota:

1. Utilice el nombre del espacio de archivos si se ha modificado el nombre de etiqueta de la unidad.
2. si incluye el filespace name, no incluya una letra de unidad en la especificación de archivo.

Por ejemplo:

- La estructura de directorios consta de varios niveles: `d:\test\sub1\subsub1`.
- El directorio `d:\test` contiene los archivos `h1.txt` y `h2.txt`.
- El directorio `d:\test\sub1` contiene el archivo `s1.htm`.
- El directorio `d:\test\sub1\sub2` contiene el archivo `ss1.cpp`.

Para que pueda accederse a todos los archivos del directorio `d:\test\sub1\sub2`, especifique:

```
set access backup d:\test\sub1\sub2\* * *
```

Para que solo pueda accederse a los archivos del directorio `d:\test`, especifique:

```
set access backup d:\test\* * *
```

Para que pueda accederse a todos los archivos de todos los directorios que se encuentran en el directorio `d:\test`, o debajo de él, escriba:

```
set access backup d:\test\* * *
set access backup d:\test\*\* * *
```

 Sistemas operativos Windows{filespace name}






 Sistemas operativos Windows Identifica el nombre de espacio de archivos (incluido entre llaves) del servidor que contiene los archivos a los que se está otorgando acceso. Este nombre es el nombre de etiqueta de la unidad de la estación de trabajo desde donde se realizó la operación de copia de seguridad o copia archivada. Utilice el nombre del espacio de archivos si se ha modificado el nombre de etiqueta de la unidad.

image-fs









Es el nombre del sistema de archivos de imagen a compartir. Puede especificarse con un asterisco (\*) para permitir el acceso a todas las imágenes cuyo propietario es el usuario que otorga el acceso.

 Sistemas operativos Linux  Sistemas operativos Windows-TYPE=VM *vmname*

 Sistemas operativos Linux  Sistemas operativos Windows Este parámetro es necesario si está utilizando este mandato para proporcionar otro usuario con acceso a las copias de seguridad de la máquina virtual VMware. La opción *vmname* solo se especifica si se indica -TYPE=VM; *vmname* es el nombre de la máquina virtual VMware a la que está permitiendo el acceso.

nodo


Especifica el nodo cliente del usuario al que se está otorgando acceso. Utilice caracteres comodín para otorgar acceso a más de un nodo con nombres de nodo similares. Utilice un asterisco (\*) para otorgar acceso a todos los nodos.


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X user  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Se trata de un parámetro opcional que restringe el acceso al usuario indicado del nodo especificado. Para permitir que cualquier usuario autorizado acceda a la copia de seguridad de los datos o a los datos archivados, especifique `root` como usuario.







## Ejemplos





---

 Sistemas operativos Windows Tarea





 Sistemas operativos Windows Otorgar al usuario del nodo\_2 autorización para restaurar todos los archivos que tienen la extensión .c del directorio c:\devel\proja.





```
set access backup c:\devel\proja\*.c node_2
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea


 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Otorgar al usuario del nodo\_2 autorización para restaurar el archivo budget del directorio /home/user.


```
set access backup /home/user/budget node_2
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Otorgar a nodo\_3 autorización para recuperar todos los archivos del directorio /home/devel/proja.





```
set ac archive /home/devel/proja/ node_3
```

 Sistemas operativos Windows Tarea


 Sistemas operativos Windows Otorgar al usuario del nodo\_3 autorización para recuperar todos los archivos del directorio c:\devel, pero no permitir el acceso a los archivos de los subdirectorios de c:\devel, como c:\devel\proj.


```
set access archive c:\devel\* node_3
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea





 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Otorgar a todos los nodos cuyos nombres terminen por bldgb autorización para restaurar todas las versiones de copia de seguridad de los directorios que tienen el nombre de espacio de archivos project.





```
set ac b "{project}/*" "*bldgb"
```

 Sistemas operativos Windows Tarea





 Sistemas operativos Windows Otorgar a todos los nodos cuyos nombres terminen por bldgb autorización para restaurar todas las versiones de copia de seguridad de todos los directorios de la unidad d:. La unidad d: tiene el nombre de espacio de archivos project.





```
set ac b {project}\* *bldgb
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Otorgar a cualquier usuario autorizado en node1 la autorización para recuperar todos los archivos del directorio /home/devel/projb.



```
set access archive /home/devel/projb/ node1 root
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Otorgar al usuario elena del nodo\_5 autorización para restaurar todas las imágenes del espacio de archivos montado en el directorio /home/devel/proja.

```
set acc backup "home/devel/proja/*/*" node_5 elena
```

 Sistemas operativos Linux  Sistemas operativos Windows Tarea

 Sistemas operativos Linux  Sistemas operativos Windows Otorgar al nodo denominado myOtherNode autorización para restaurar archivos de copias de seguridad de la máquina virtual VMware denominada myTestVM.

```
set access backup -TYPE=VM myTestVM myOtherNode
```

## Set Event

---

Con el mandato set event puede especificar las circunstancias que se deben dar cuando se suprimen datos archivados.

Puede utilizar el mandato set event de las siguientes maneras:

- Impedir la supresión de datos al final de su período de retención asignado
- Permitir que caduquen los datos, según define el grupo de copia de archivado (liberar una espera de suspensión)
- Iniciar la ejecución del reloj de caducidad cuando tenga lugar un suceso concreto (notificar al servidor que se ha producido un suceso).

Los objetos afectados pueden especificarse con una especificación de archivo estándar (incluidos los caracteres comodín), una lista de archivos cuyos nombres se encuentren en el archivo que se ha especificado mediante la utilización de la opción `filelist` o un grupo de copias archivadas cuya descripción se ha especificado con la opción `description`.

Nota: Cuando sólo se utiliza una especificación de archivo, `<filespec>`, se verán afectadas todas las copias archivadas de los archivos o carpetas que coincidan con la especificación de archivo. Si desea que se vean afectadas ciertas versiones de un archivo, utilice la opción `-pick` y seleccione uno de los elementos que aparecen en la lista.

## Interacción con servidores de nivel inferior

---

Si el mandato `set event` se emite cuando el cliente está conectado con un servidor que no admite la política basada en sucesos (anterior a IBM Spectrum Protect 5.2.2), el mandato se rechazará y se generará un mensaje de error en el que se indicará que el servidor actual no admite la política basada en sucesos.

## Clientes soportados

---

Este mandato es válido para todos los clientes.

## Sintaxis

---

```
>>-SET Event---- -TYPE=---+-Hold-----+----->
                               +-Release-----+
                               '-Activateretention-'

>-- --<filespec>-- -- -filelist=<filespec>-- -- -description=---->
>-- -pick-----><
```

## Parámetros

---

TYPE=

Especifica el valor del tipo de suceso. Este parámetro debe especificarse.

hold

Impide que se suprima el objeto, independientemente de la política de caducidad.

release

Permite que tenga lugar la caducidad controlada por sucesos habitual.

*activateretention*

Indica al servidor que se ha producido el suceso de control e inicia la ejecución del reloj de caducidad.

-pick

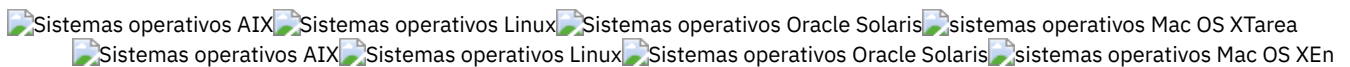
Proporciona una lista de objetos que el usuario puede seleccionar para aplicar el suceso.

Las opciones siguientes también se pueden utilizar y tienen la misma finalidad que habitualmente:

- Dateformat
- Numberformat
- Noprompt
- Subdir
- Timeformat

## Ejemplos


---

 el ejemplo siguiente se muestran la salida detallada y la información de las estadísticas del mandato `set event type=hold /home/accounting/ledgers/*05.books`, con objetos revinculados (frente a la notación de objetos de copia archivada o cualquier otra notación).

```
Rebinding--> 274 /home/accounting/ledgers/
  jan05.books
Rebinding--> 290 /home/accounting/ledgers/
  feb05.books
```









```
Número total de objetos archivados:      0
Número total de objetos con errores:     0
Número total de objetos revinculados:    2
Número total de bytes transferidos:      0 B
Tiempo de transferencia de datos:        0,00 s
Velocidad de transferencia de datos de red: 0,00 KB/s
Velocidad de transferencia de datos compuesta: 0,00 KB/s
Objetos comprimidos al:                  0%
Tiempo transcurrido en el proceso: 00:00:02
```

#### Sistemas operativos Windows Tarea

 Sistemas operativos Windows En el ejemplo siguiente se muestran la salida detallada y la información de las estadísticas del mandato `set event set event type=hold \\user\c$\tsm521\debug\bin\winnt_unicode\dsm.opt`, con objetos revinculados (frente a la notación de objetos de copia archivada o cualquier otra notación).

```
Rebinding--> 274 \\user\c$\tsm521\debug\
  bin\winnt_unicode\dsm.opt
Rebinding--> 290 \\user\c$\tsm521\debug\
  bin\winnt_unicode\dsm.opt
```


```
Número total de objetos inspeccionados:  2
Número total de objetos archivados:      0
Número total de objetos actualizados:    0
Número total de objetos revinculados:    2
Número total de objetos suprimidos:      0
Número total de objetos caducados:       0
Número total de objetos con errores:     0
Número total de bytes transferidos:      0 B
Tiempo de transferencia de datos:        0,00 s
Velocidad de transferencia de datos de red: 0,00 KB/s
Velocidad de transferencia de datos compuesta: 0,00 KB/s
Objetos comprimidos al:                  0%
Tiempo transcurrido en el proceso: 00:00:02
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X Tarea  Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X La opción `-pick` cuando se utiliza con el mandato `set event set event type=activate /user/tsm521/common/unix` muestra el tipo de suceso en lugar del nombre de mandato:

```
Scrollable PICK Window - Retention Event :  ACTIVATE
```

Núm.	Fecha/hora archivado	Tamaño	Archivo
1.	08/05/2003 08:47:46	766 B	/user/tsm521 /common/unix
2.	08/01/2003 10:38:11	766 B	/user/tsm521 /common/unix
3.	08/05/2003 08:47:46	5.79 KB	/user/tsm521 /common/unix
4.	08/01/2003 10:38:11	5.79 KB	/user/tsm521 /common/unix
5.	08/05/2003 08:47:46	10.18 KB	/user/tsm521 /common/unix

#### Sistemas operativos Windows Tarea

 Sistemas operativos Windows La opción `-pick` cuando se utiliza con el mandato `set event set event type=activate \\user\c$\tsm521\common\winnt` muestra el tipo de suceso en lugar del nombre del mandato:

```
Scrollable PICK Window - Retention Event :  ACTIVATE
```

Núm.	Fecha/hora archivado	Tamaño	Archivo
1.	08/05/2003 08:47:46	766 B	\\user\c\$\tsm521 \common\winnt
2.	08/01/2003 10:38:11	766 B	\\user\c\$\tsm521 \common\winnt
3.	08/05/2003 08:47:46	5.79 KB	\\user\c\$\tsm521 \common\winnt
4.	08/01/2003 10:38:11	5.79 KB	\\user\c\$\tsm521 \common\winnt

 Sistemas operativos Linux  Sistemas operativos Windows

## Establecer Netappsvm


---


El mandato set netappsvm asocia las credenciales de inicio de sesión para un servidor de gestión de clústeres, que se especifican en el mandato set password, con una máquina virtual de almacenamiento NetApp y el nombre de máquina virtual de almacenamiento (SVM) de datos (Vserver de datos). Debe especificar este mandato antes de crear una copia de seguridad incremental por diferencia de instantánea de un volumen de NetApp en clúster.

Este mandato normalmente sólo se especifica una vez. Los parámetros se almacenan y se reutilizan la próxima vez que realiza una copia de seguridad de un volumen en clúster que esté gestionado por la máquina virtual de almacenamiento. Si traslada una máquina virtual de almacenamiento a otro servidor de gestión de clústeres, deberá volver a especificar este mandato y especificar el nuevo servidor de gestión de clúster. Si fuera necesario, cambie las credenciales de inicio de sesión utilizando el mandato set password.

## Clientes soportados

---

 Sistemas operativos Linux Este mandato es válido para los clientes de archivado y copia de seguridad de Linux que completan copias de seguridad de diferencia de instantáneas de volúmenes de servidor de archivo ONTAP-c-mode de datos en clúster.

 Sistemas operativos Windows Este mandato es válido para clientes de Windows que realicen copias de seguridad de diferencia de instantáneas de volúmenes de servidor de archivo ONTAP-c-mode de datos en clúster.

## Sintaxis

---

```
>>-SET NETAPPSVM--+-svm_hostname--cms_hostname-- svm_name+----><  
    '- -remove--svm_hostname-----'
```

## Parámetros

---

### *svm\_hostname*

Especifica el nombre de host o la dirección IP de la máquina virtual de almacenamiento que gestiona los volúmenes e interfaces lógicas (LIFs), para los volúmenes que quiera proteger.

### *cms\_hostname*

Especifica el nombre de host o la dirección IP del servidor de gestión de clústeres. Especifique el mismo nombre de host que haya especificado para este servidor de gestión de clústeres cuando utilizó el mandato setpassword para establecer las credenciales de inicio de sesión.

### *svm\_name*

Especifica el nombre de los datos de SVM que gestionan los volúmenes montados. Póngase en contacto con el administrador de SVM de NetApp para obtener el nombre de SVM de datos asignado a la máquina virtual.

### *-remove svm\_hostname*

Desasocia la SVM del servidor de gestión de clústeres con el que previamente estaba asociada. Especifique un nombre de host de SVM.

Puede especificar este parámetro si ha asociado de forma accidental una máquina virtual de almacenamiento con un servidor de archivos 7-mode. Si elimina un servidor de archivos 7-mode y asocia un servidor de gestión de clústeres, establezca las credenciales de inicio de sesión para el servidor de gestión de clústeres utilizando el mandato set password.

## Ejemplos

---

Configurar las credenciales y el acceso a una máquina virtual de almacenamiento:






```
set netappsvm svm_example.com cms_filer1.example.com svm_2  
dsmc set password cms_filer1.example.com user_name password
```

Eliminar las asociaciones que se crearon para la máquina virtual de almacenamiento:

```
set netappsvm -remove svm_example.com
```

### Tareas relacionadas:

Protección de volúmenes de servidor de archivos ONTAP NetApp de datos en clúster

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
 Sistemas operativos Windows

## Establecer contraseña

El mandato `set password` cambiará la contraseña de IBM Spectrum Protect para la estación de trabajo o establece las credenciales que se utilizan para acceder a otro servidor.

Si omite las contraseñas antigua y nueva cuando escribe el mandato `set password`, se le solicitará que escriba una vez la contraseña antigua y dos veces la contraseña nueva.

Las contraseñas pueden tener una longitud máxima de 63 caracteres. Las restricciones de contraseña varían, dependiendo del lugar donde se almacenan y gestionan las contraseñas y en función de la versión del servidor IBM Spectrum Protect al que se conecta el cliente.

Si el servidor de IBM Spectrum Protect tiene la versión 6.3.3 o posterior y si usa un servidor de directorios LDAP para autenticar contraseñas:

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```

Las contraseñas son sensibles a las mayúsculas y minúsculas, y están sujetas a restricciones adicionales que puedan imponer las políticas de LDAP.

Si el servidor IBM Spectrum Protect está en la versión 6.3.3 o posterior, y si no utiliza un servidor LDAP para gestionar contraseñas

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9 . ! @ # $ % ^ & * _ - + = ` ( )
| { } [ ] : ; < > , ? / ~
```






Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

Si el servidor IBM Spectrum Protect es anterior a la versión 6.3.3

Utilice cualquiera de los siguientes caracteres para crear una contraseña:

```
a b c d e f g h i j k l m n o p q r s t u v w x y z
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
0 1 2 3 4 5 6 7 8 9
_ - & + .
```

Las contraseñas se almacenan en la base de datos del servidor IBM Spectrum Protect y no distinguen entre mayúsculas y minúsculas.

 Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  Sistemas operativos Windows Recuerde:

En la línea de mandatos, escriba entre comillas todos los parámetros que contengan uno o varios caracteres especiales. Sin las comillas, los caracteres especiales se pueden interpretar como caracteres de escape, caracteres de redirección de archivos u otros caracteres que tienen importancia para el sistema operativo.

 Sistemas operativos Windows

En sistemas Windows:

Escriba los parámetros de mandato entre comillas (").

Ejemplo de línea de mandatos:

```
dsmc set password "t67@#$$%^&" "pass2<w0rd"
```

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris

En sistemas AIX, Linux y Solaris:

Escriba los parámetros de mandato entre comillas simples (').

Ejemplo de línea de mandatos:

```
dsmc set password -type=vmgquest 'Win 2012 SQL' 'tsml2dag\administrator' '7@#$$%^&7'
```

Las comillas no son necesarias cuando escribe una contraseña con caracteres especiales en el archivo de opciones.

## Clientes soportados

Este mandato es válido para todos los clientes.

Los parámetros siguientes se aplican a operaciones de VMware, que sólo están disponibles si utiliza el cliente como transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

- TYPE=DOMAIN
- TYPE=VM
- TYPE=VMGUEST

## Sintaxis

```
>>-SET Password--+-+-----+----->
                    '-oldpw--newpw-'

>--+-+-----+----->
    '-otherserver--otheruserid--otherpassword-'

    .-TYPE=TSM-----
>--+-+-----+-----<<
+-TYPE=DOMAIN-----+
+-TYPE=FASTBack-----+
+-TYPE=FILER-----+
+-TYPE=VM-----+
'-TYPE=VMGUEST ALLVM-'
```

## Parámetros

**contraseñaantigua**

Especifica la contraseña actual para la estación de trabajo.

**contraseñanueva**

Especifica la contraseña nueva para la estación de trabajo.

**other\_server other\_user\_id other\_password**

Estos tres parámetros especifican los atributos que utiliza el cliente para acceder a otro servidor, como un archivador o un host ESXi.

**other\_server**

Especifica el nombre de host o la dirección IP del servidor al que puede acceder el cliente para proteger los archivos.

**other\_user\_id**

El ID de usuario de una cuenta en el servidor que utiliza el cliente para iniciar una sesión en el otro servidor. La cuenta debe tener los privilegios necesarios para realizar las operaciones que se ejecutan una vez que el usuario inicie la sesión en el otro servidor.


**other\_password**

La contraseña asociada con el ID de usuario en el otro servidor.

**TYPE**

Especifica si la contraseña es para el cliente de copia de seguridad y archivado o para otro tipo de servidor.

Utilice **TYPE=TSM** para especificar la contraseña del cliente de copia de seguridad y archivado. El tipo predeterminado es **TYPE=TSM**.

 **Sistemas operativos Windows** Utilice **TYPE=DOMAIN** para establecer las credenciales de administrador de dominios de Windows para permitir que los usuarios inicien sesión en un nodo de proxy remoto de Windows (la interfaz de restauración de archivos) para realizar operaciones de restauración de archivos. Esta opción requiere una licencia para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Utilice el siguiente formato para el mandato `set password -type=domain`:

```
set password -type=domain -validate nombre_administrador contraseña
```

donde:

**VALIDate**

Valida las credenciales de administrador de dominios de Windows antes de que se almacenen las credenciales. Si la validación falla, las credenciales no se almacenan, y los usuarios no podrán iniciar sesión en la interfaz de restauración de archivos. El parámetro `validate` solo es válido con el parámetro **TYPE=DOMAIN**.

*nombre\_administrador*

Especifica el nombre de cuenta de un administrador de dominios. El nombre de cuenta debe contener el nombre de dominio de Windows y el ID de administrador. El nombre de cuenta debe tener el siguiente formato:

*nombre\_dominio\ID\_administrador*

*password*

Especifica la contraseña asociada con la cuenta del administrador de dominios especificada.

Para obtener más información sobre los requisitos de configuración para nodos proxy de montaje remoto, consulte la documentación de IBM Spectrum Protect para entornos virtuales: Protección de datos para.

 Sistemas operativos Linux  Sistemas operativos Windows

Utilice `TYPE=FastBack`, en clientes Linux y Windows, para almacenar las credenciales de Tivoli Storage Manager FastBack necesarias para montar y desmontar los volúmenes de FastBack en el servidor FastBack Disaster Recovery Hub de Windows.

El archivo de contraseñas en el servidor de copia de seguridad vStorage debe tener el ID de administrador de Windows del sistema de centro virtual de VMware o el ID de usuario de UNIX de un servidor ESX específico. Para una copia de seguridad de proxy FastBack, el archivo de contraseñas tiene que contener el ID de administrador y la contraseña de FastBack. A continuación, se muestran algunos ejemplos:

```
dsmc set password 192.0.2.24 admin admin 123 -type=fastback
```

```
dsmc set password 192.0.2.24 WORKGROUP:admin admin 123 -type=fastback
```

```
dsmc set password windserv administrator windpass4 -type=fastback
```

Importante: Tiene que definir las credenciales de usuario necesarias para montar y desmontar los volúmenes de FastBack desde un repositorio en un cliente de archivado y copia de seguridad antes de especificar el submandato de FastBack de copia de seguridad y archivado. Utilice la opción `fbserver` para definir las credenciales.

Aquí tiene una breve descripción de las distintas configuraciones y credenciales que necesita:

- El cliente de archivado y copia de seguridad se instala en un servidor de copia de seguridad vStorage. El cliente del servidor de copia de seguridad vStorage debe conectarse a varios repositorios de unidades compartidas de red.

Siga estos pasos para cada uno de los repositorios de compartición de red en los que esté conectado el cliente:

1. Configure el repositorio para un acceso de red remoto desde FastBack Manager. Consulte la documentación del producto Tivoli Storage Manager FastBack en el IBM® Knowledge Center, en <http://www.ibm.com/support/knowledgecenter/SS9NU9/welcome>.

Este paso establece un nombre de dominio, un ID de usuario de red compartida, y una contraseña de red compartida para conectarse remotamente al repositorio.

2. En la estación de trabajo del cliente de copia de seguridad y archivado, entre manualmente el siguiente mandato:

```
dsmc set password type=fastback FBServer domain:networkaccessuserid  
networkaccesspassword
```

La opción `fbserver` especifica el nombre de host abreviado de la estación de trabajo del servidor FastBack. Para el FastBack DR Hub, la opción `fbserver` especifica el nombre abreviado de la estación de trabajo donde se ha instalado DR Hub.

*Networkaccessuserid* es el ID de administrador de Windows o la contraseña de administración de FastBack.

*Domain* es el nombre de dominio del ID de usuario.

*Networkaccesspassword* es el ID de administrador de Windows o la contraseña de administración de FastBack.

3. Estas credenciales se recuperan en base al nombre corto de host que especifica con la opción `fbserver`.

 Sistemas operativos Linux  Sistemas operativos Windows

Utilice `TYPE=FILER`, en sistemas Linux y Windows, para especificar que esta contraseña es para operaciones de diferencia de instantánea en un servidor de archivos.

Para `TYPE=FILER`, debe especificar un nombre de servidor de archivos, y el ID de usuario y la contraseña que se utilizan para acceder al servidor de archivos. Por ejemplo: `dsmc set password -type=filer myfiler filerid filerpasswd`.

Al especificar `TYPE=FILER`, la contraseña se almacena en el archivo de contraseña (TSM.sth) sin validar que la contraseña sea válida. Las contraseñas almacenadas con `TYPE=FILER` se pueden compartir entre nodos. Por ejemplo, una contraseña almacenada por `NODE_A` puede utilizarla `NODE_B`. Solo se almacena un conjunto de credenciales por servidor de archivos.

Utilice `TYPE=VM` para establecer la contraseña que se utiliza para iniciar sesión en un servidor vCenter o ESX.

```
dsmc SET PASSWORD -type=VM hostname administrator password
```

donde:

*nombre\_host*

Especifica el servidor de VMware VirtualCenter o ESX que desea restaurar, consultar o del que desea hacer una copia de seguridad. Este nombre de host debe coincidir con la sintaxis del nombre de host que se utiliza en la opción `vmchost`. Es decir, si `vmchost` utiliza una dirección IP en lugar de un nombre de host, este mandato debe proporcionar la dirección IP, y no un nombre de host corto o un nombre de host completo.

*administrator*

Especifica la cuenta necesaria para iniciar sesión en el host de vCenter o ESXi.

*password*

Especifica la contraseña asociada con la cuenta de inicio de sesión que ha especificado para el administrador de vCenter o ESXi.

Utilice el Editor de preferencias para establecer las opciones `vmchost`, `vmcuser` y `vmcpw`.

También puede establecer la opción `vmchost` en el archivo de opciones del cliente y luego utilizar el mandato `set password` para asociar el nombre de host con la cuenta del administrador y la contraseña de la cuenta del administrador utilizada para iniciar la sesión en dicho host. Por ejemplo, `set password TYPE=VM myvmchost.example.com administrator_name administrator_password`.

Utilice `TYPE=VMGUEST`, en clientes Linux y Windows, si utiliza la opción `INCLUDE.VMTSMVSS` para proteger una máquina virtual. Utilice el formato siguiente para el mandato `set password`:

```
set password -type=vmguest guest_VM_name administrator password
```

donde:

*nombre\_máquina\_virtual\_invitado*

Especifica el nombre del invitado de máquina virtual que desea proteger.

*administrator*

Especifica la cuenta necesaria para iniciar sesión en la máquina virtual huésped.

*password*

Especifica la contraseña asociada con la cuenta de inicio de sesión.

Si utiliza las mismas credenciales para iniciar sesión en varias máquinas virtuales protegidos por la opción `INCLUDE.VMTSMVSS`, puede establecer la contraseña para todas las máquinas virtuales especificando el parámetro `ALLVM`. El parámetro `ALLVM` hace que se utilicen las mismas credenciales cuando el cliente inicia sesión en cualquier invitado incluido en una opción `INCLUDE.VMTSMVSS`. El mandato `TYPE=TSM` es un ejemplo de cómo utilizar `ALLVM`. En este ejemplo, el nombre de usuario "Administrator" y la contraseña "Password" se utilizan para iniciar la sesión en cualquier máquina virtual que ha incluido en un `INCLUDE.VMTSMVSS` opción:

```
set password -type=vmguest ALLVM Administrator Password
```

También puede establecer una combinación de credenciales compartidas e individuales. Por ejemplo, si la mayoría de las máquinas virtuales en su entorno utilizan las mismas credenciales, pero hay algunas máquinas virtuales que utilizan credenciales diferentes, puede utilizar varios mandatos `set password` para especificar las credenciales. Por ejemplo, suponga que la mayoría de las máquinas virtuales utilizan "Administrator1" como el nombre de usuario y "Password1" como contraseña. Supongamos también que una máquina virtual, llamada VM2, utiliza "Administrator2" como nombre de usuario y "Password2" como contraseña. Los siguientes mandatos se utilizan para establecer las credenciales para esta situación:

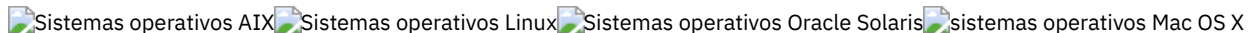
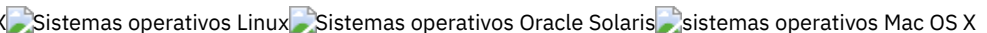
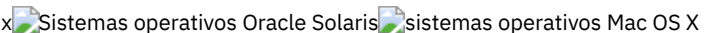


- `set password -type=vmguest ALLVM Administrator1 Password1` (establece las credenciales para la mayoría de las máquinas virtuales).
- `set password -type=vmguest VM2 Administrator2 Password2` (establece credenciales exclusivas para VM2).

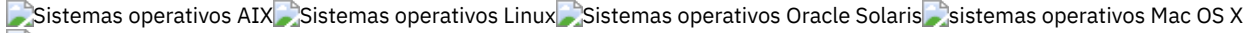
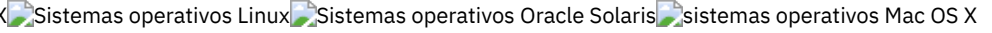

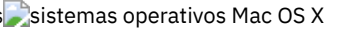
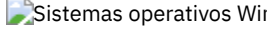
## Ejemplos

A continuación, se muestran ejemplos que utilizan el mandato `set password`.



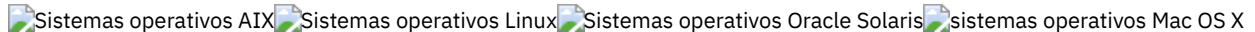
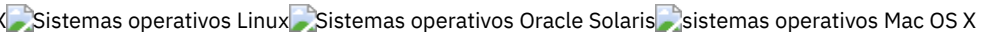

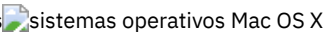
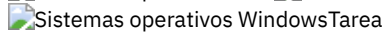
```
set password osecret nsecret
```

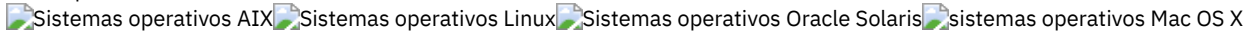


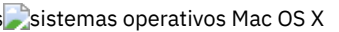
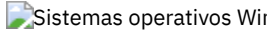
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsConfigurar un ID de usuario y una contraseña para el servidor de archivos myFiler.example.com.

```
dsmc set password -type=filer myFiler.example.com root
```


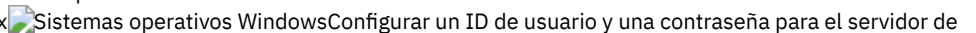
```
Please enter password for user id "root@myFiler.example.com": ***** Re-enter the password for verification:***** ANS0302I Successfully done.
```

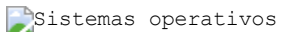
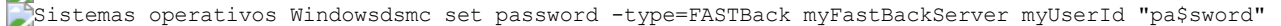
 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsTarea

 Sistemas operativos AIX  Sistemas operativos Linux  Sistemas operativos Oracle Solaris  sistemas operativos Mac OS X  
 Sistemas operativos WindowsConfigurar un ID de usuario y una contraseña para el usuario root en el servidor de archivos myFiler.example.com.

```
dsmc set password -type=filer myFiler.example.com root secret
```

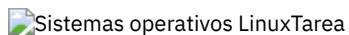
 Sistemas operativos Linux  Sistemas operativos WindowsTarea

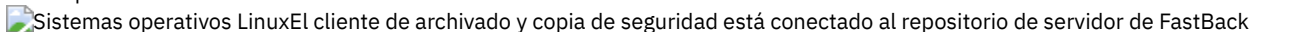
 Sistemas operativos Linux  Sistemas operativos WindowsConfigurar un ID de usuario y una contraseña para el servidor de FastBack myFastBackServer. Utilice la opción -fbserver de los mandatos archive fastback y backup fastback para el nombre del servidor.

 Sistemas operativos Linuxdsmc set password -type=FASTBack myFastBackServer myUserId 'pa\$sword'  
 Sistemas operativos Windowsdsmc set password -type=FASTBack myFastBackServer myUserId "pa\$sword"

#### Importante:


1. El mandato `dsmc set password -type=fastback` tiene que repetirse en una estación de trabajo de proxy de cliente dedicado una vez para cada repositorio de FastBack donde se espera que se conecte el cliente de copia de seguridad y archivado.
2. Para los repositorios de recursos compartidos de red, emita el mandato `dsmc set password -type=fastback` con este formato: `dsmc set password -type=fastback myFBServer domainName:userId password`.  
  
El nombre de servidor especificado, que es `myFBServer` en este ejemplo, debe coincidir con el nombre especificado en la opción `-fbserver` en un mandato `backup fastback` o `archive fastback`.
3. Para el servidor de FastBack o el FastBack Disaster Recovery Hub, el ID de usuario y la contraseña especificados tienen que tener privilegios de administrador de FastBack. Tiene que emitir el mandato `dsmc set password -type=fastback` una vez para cada repositorio de ramificaciones del servidor de FastBack en el FastBack DR Hub al que está previsto que se conecte el cliente de archivado y copia de seguridad.

 Sistemas operativos LinuxTarea

 Sistemas operativos LinuxEl cliente de archivado y copia de seguridad está conectado al repositorio de servidor de FastBack cuyo nombre de host abreviado es `myFBServer`. `user ID` es el ID de usuario de red de FastBack con acceso de lectura/escritura al repositorio compartido. `DOMAIN` es el dominio al que pertenece el ID de usuario. `myNetworkPass` es la contraseña correspondiente para el ID de usuario.

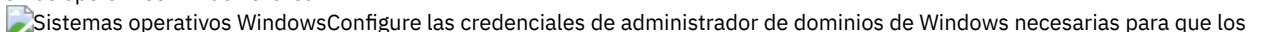
```
dsmc set password -type=fastback myFbServer DOMAIN:USERID myNetworkPass
```

 Sistemas operativos LinuxTarea

 Sistemas operativos LinuxEl cliente de copia de seguridad y archivado está conectado a un repositorio en una máquina DR Hub cuyo nombre de host abreviado es `myFbDrHub`. El ID de usuario es el ID del administrador de Windows. `DOMAIN` es el dominio al que pertenece la máquina DR Hub. `myNetworkPass` es la contraseña correspondiente para el ID de administrador.

```
dsmc set password -type=fastback myFbDrHub DOMAIN:administrator adminPasswd
```

 Sistemas operativos WindowsTarea

 Sistemas operativos WindowsConfigure las credenciales de administrador de dominios de Windows necesarias para que los usuarios inicien sesión en la interfaz de restauración de archivos y guarde las credenciales de dominios de Windows. En este ejemplo, el dominio de Windows en el que están registradas todas las cuentas de usuario se llama `example_domain`. `Kev_the_admin` es el ID del administrador de dominios de Windows y `pas$word!` es la contraseña correspondiente del administrador.


```
dsmc set password -type=domain -val "example_domain\Kev_the_admin" "pas$word!"
```

 Sistemas operativos Linux  Sistemas operativos Windows

## Set Vmtags

---

El mandato set vmtags crea códigos y categorías de protección de datos que se pueden añadir a objetos de inventario VMware. Puede gestionar copias de seguridad de IBM Spectrum Protect de máquinas virtuales en estos objetos de VMware especificando los códigos con herramientas como, por ejemplo, VMware vSphere PowerCLI versión 5.5 R2 o posterior.

 Esta característica sólo está disponible si el cliente opera como un transportador de datos para IBM Spectrum Protect para entornos virtuales: Protección de datos para.

Si se utiliza la Plug-in de cliente de IBM Spectrum Protect vSphere para gestionar las copias de seguridad, no es necesario ejecutar primero el mandato set vmtags. Los códigos y las categorías se crean automáticamente.

Si va a escribir scripts para aplicar estos códigos a objetos de inventario de VMware, solo necesita emitir el mandato set vmtags una vez para que se creen los códigos de protección de datos antes de que se añadan al inventario de VMware.

Puede gestionar las copias de seguridad de máquinas virtuales en los siguientes niveles de objeto de inventario de VMware:

- Centro de datos
- Carpeta (carpetas de clúster y host y carpetas de plantilla y máquina virtual)
- Host
- Clúster de host
- Agrupación de recursos
- Máquina virtual

Para obtener la lista de códigos soportados, consulte "Códigos de protección de datos soportados".

En el caso de los códigos relacionados con las planificaciones, las máquinas virtuales tienen que estar en un conjunto de protección protegido por una planificación. Un conjunto de protección consta de las máquinas virtuales de un contenedor al que se ha asignado el código `Schedule` (IBM Spectrum Protect).

Tras ejecutar el mandato set vmtags, puede asignar los códigos a objetos de VMware para gestionar la protección de las máquinas virtuales. Por ejemplo, puede excluir máquinas virtuales de, o incluirlas en, servicios de copia de seguridad planificada, especificar la política de retención para las copias de seguridad, configurar la coherencia de datos de las instantáneas o seleccionar los discos de la máquina virtual que se van a proteger.

Si los códigos de protección de datos ya existen, la ejecución del mandato set vmtags no vuelve a crear los códigos.


Si está actualizando desde una versión anterior del transportador de datos, al volver a ejecutar el mandato set vmtags se crearán nuevos códigos que están disponibles en la nueva versión del transportador de datos.


Requisitos: Antes de ejecutar el mandato set vmtags, asegúrese de que se cumplan los siguientes requisitos:

- El servidor de VMware vCenter debe tener la Versión 6.0, Actualización 1 o posterior.
- La opción vmchost debe estar configurada en el archivo dsm.opt en los transportadores de datos de Windows o el archivo dsm.sys en los transportadores de datos de Linux. El nombre de usuario y la contraseña asociados al valor vmchost también se deben establecer. Si aún no lo están, puede utilizar el mandato dsmc set password para establecer el nombre de usuario y la contraseña.

## Clientes soportados

---

 Sistemas operativos Linux Este mandato solo es válido en clientes admitidos de Linux x86\_64 instalados en un servidor de seguridad de vStorage que protege los activos de VMware.

 Sistemas operativos Windows Este mandato es válido en clientes admitidos de Windows de 64 bits instalados en el servidor de seguridad de vStorage que protege los activos de VMware.

## Sintaxis

---

```
>>>SET VMTAGS-----<<<
```

## Parámetros

---

No se necesita ningún parámetro para este mandato.



## Ejemplos

---

## Tarea

Cree categorías y códigos de protección de datos que se puedan añadir a los objetos de inventario de VMware:

```
dsmc set vmtags
```

-  Sistemas operativos Linux  Sistemas operativos Windows  
Visión general de los códigos de protección de datos  
Para gestionar la protección de datos de máquinas virtuales, puede asignar códigos de IBM Spectrum Protect a objetos de inventario de VMware. Puede asignar códigos a objetos VMware especificando los valores de protección de datos de Plug-in de cliente de IBM Spectrum Protect vSphere del cliente web de vSphere. Si no utiliza Plug-in de cliente de IBM Spectrum Protect vSphere, puede asignar códigos utilizando herramientas de script como VMware Power CLI.

### Conceptos relacionados:

Clases de gestión y grupos de copia

### Referencia relacionada:

Códigos de protección de datos admitidos

Vmchost

Vmtagdatamover

Establecer contraseña

 Sistemas operativos Windows



## Programa de utilidad de configuración del servicio del cliente IBM Spectrum Protect

---

Se pueden instalar los siguientes servicios del cliente cuando instala el cliente de archivado y copia de seguridad o si utiliza el programa de utilidad de configuración del servicio del cliente de IBM Spectrum Protect:

- Servicio del planificador de copia de seguridad/archivado
- Servicio aceptador de cliente
- Servicio del agente de cliente remoto
- Servicio de motor con registro por diario

Para obtener más información sobre cómo utilizar el programa de utilidad de configuración del servicio del cliente de IBM Spectrum Protect para instalar servicios del cliente, consulte la información relacionada con el mandato dsmcutil:

-  Sistemas operativos Windows Instalar el servicio del planificador de copia de seguridad/archivado  
Utilice la GUI del cliente de copia de seguridad y archivado o el programa de utilidad de configuración de servicios de cliente de IBM Spectrum Protect para instalar el planificador.
-  Sistemas operativos Windows mandato dsmcutil  
El programa de utilidad de configuración del servicio del cliente de IBM Spectrum Protect, dsmcutil, se puede utilizar para instalar los servicios del cliente de copia de seguridad y archivado en estaciones de trabajo locales y remotas de Windows.

### Conceptos relacionados:

mandato dsmcutil

 Sistemas operativos Windows


## Instalar el servicio del planificador de copia de seguridad/archivado

---

Utilice la GUI del cliente de copia de seguridad y archivado o el programa de utilidad de configuración de servicios de cliente de IBM Spectrum Protect para instalar el planificador.

### Acerca de esta tarea

---

- Desde la GUI del cliente de copia de seguridad y archivado, pulse Herramientas y luego Asistente para la instalación. Seleccione la opción Ayuda para configurar el planificador de cliente.
- Si tiene una cuenta que pertenece al grupo Administradores/ Administradores del dominio, puede utilizar el programa de utilidad de configuración de servicios de cliente de IBM Spectrum Protect para configurar los servicios de cliente en estaciones de trabajo de Windows, tanto locales como remotas.
-  Sistemas operativos Windows Utilización de la herramienta de configuración de servicios de cliente (Windows)  
En esta sección se ofrecen los pasos necesarios para utilizar el programa de utilidad de configuración de servicios de cliente para automatizar las copias de seguridad, gestionar los servicios del planificador existentes, crear un planificador nuevo y asociar un aceptador de clientes para gestionar el planificador:

 Sistemas operativos Windows

## mandato dsmcutil

---

El programa de utilidad de configuración del servicio del cliente de IBM Spectrum Protect, dsmcutil, se puede utilizar para instalar los servicios del cliente de copia de seguridad y archivado en estaciones de trabajo locales y remotas de Windows.

Puede utilizar el mandato dsmcutil para instalar los siguientes servicios del cliente:

- Servicio del planificador de copia de seguridad/archivado
- Servicio aceptador de cliente
- Servicio del agente de cliente remoto
- Servicio de motor con registro por diario

La herramienta de configuración de servicios de cliente debe ejecutarse desde una cuenta que pertenezca al grupo Administradores/Administradores del dominio. La sintaxis para el mandato es como se muestra en el siguiente texto:



```
>>-dsmcutil-- --mandato--+-service-----+-----><
                          .-SCHEDuler---.
                          +-CAD-----+
                          +-JOURnal-----+
                          '-REMOTEagent-'
```

Nota: Opciones que especifica con los mandatos dsmcutil que sustituyen a la opción que especificó en su archivo de opciones (dsm.opt).

La cuenta que ejecuta el programa de utilidad debe tener los derechos de usuario apropiados para instalar los servicios y actualizar el Registro de Windows en la estación de trabajo de destino.


Si se especifica una estación de trabajo remota, la cuenta debe tener autorización para conectarse al registro de Windows de la estación de trabajo especificada.

Nota: Para los mandatos y opciones que se documentan aquí, la abreviatura mínima que puede escribir se muestra en mayúsculas.

-  Sistemas operativos Windows Mandatos dsmcutil: opciones necesarias y ejemplos  
Se proporciona información de referencia para los mandatos y ejemplos de dsmcutil.
-  Sistemas operativos Windows Opciones válidas de dsmcutil  
Esta sección enumera las opciones válidas **dsmcutil** que puede especificar para utilizar el servicio del planificador.

### Conceptos relacionados:

Configurar el cliente de IBM Spectrum Protect

 Sistemas operativos Windows

## Mandatos dsmcutil: opciones necesarias y ejemplos

---

Se proporciona información de referencia para los mandatos y ejemplos de dsmcutil.

El mandato INSTall instala y configura los servicios del cliente de copia de seguridad y archivado.

### INSTall Scheduler

---

Instala y configura el servicio del planificador de IBM Spectrum Protect.

Las opciones de mandato obligatorias de INSTall son:

- /name:service\_name
- /password:password
- /clusternode:Yes | No (necesario si está ejecutando Microsoft Cluster Server (MSCS) o Veritas Cluster Server (VCS)).
- /clustername:cluster\_name (necesario si está ejecutando el MSCS o VCS).

Restricción: No especifique un nombre de clúster que tenga más de 64 caracteres. Si especifica más de 64 caracteres y utiliza Veritas Storage Foundation con la función de alta disponibilidad o una configuración de Microsoft Cluster Server, es posible que no pueda instalar o iniciar el servicio del planificador.

La opción /clientdir:client\_dir también se puede utilizar, la opción predeterminada está en el directorio actual.

Los siguientes archivos deben existir en el directorio que especifica client\_dir:

- dsmcsvc.exe
- dscenu.txt
- dsm.opt
- dsmntapi.dll
- tsmutil1.dll

Nota: Si el servicio se está instalando en una estación de trabajo remota, la vía de acceso completa del directorio del cliente debe ser relativa a la estación de trabajo remota de destino. Los nombres UNC no están permitidos para la cuenta del sistema local. Pueden instalarse varios servicios en la misma estación de trabajo.

Consejo: En los mandatos que se proporcionan en los ejemplos siguientes, se utiliza la ubicación predeterminada del programa de instalación del cliente (c:\program files\tivoli\tsm\baclient). Si ha instalado el cliente en una ubicación distinta, sustituya la vía de acceso predeterminada por la vía de instalación personalizada. Si la vía de acceso contiene un espacio, colóquela entre comillas dobles (por ejemplo, "c:\program files\tivoli\tsm\baclient").

#### Tarea

Instale un servicio del planificador denominado `TSM Central Scheduler Service` en la estación de trabajo local. Inicie el servicio automáticamente en el momento de arrancar el sistema. Todos los archivos necesarios deben residir en el directorio actual y el archivo de opciones del cliente debe hacer referencia al servidor de IBM Spectrum Protect donde el nodo ALPHA1 está definido con la contraseña `nodepw`. Se contacta con el servidor para verificar que el nodo y la contraseña especificados son válidos. Cuando se valida la contraseña, se genera (se cifra) en el almacén de contraseñas de:

##### Mandato:

```
dsmcutil install scheduler /name:"TSM Central Scheduler Service"
/node:ALPHA1 /password:nodepw /autostart:yes
```

#### Tarea

Instale un servicio del planificador denominado `TSM Central Scheduler Service` en la estación de trabajo remota PDC. Inicie el servicio automáticamente en el momento de arrancar el sistema. Los archivos obligatorios del servicio del planificador y el archivo de opciones especificado deben residir en el directorio `c:\program files\tivoli\tsm\baclient` de la estación de trabajo remota. La contraseña se cifra en el almacén de contraseñas de . No se contacta con el servidor de IBM Spectrum Protect para validar la contraseña.

##### Mandato:

```
dsmcutil install scheduler /name:"TSM Central Scheduler Service"
/machine:PDC /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:PDC /validate:no /autostart:yes /password:nodepassword
```

#### Tarea

Instale un servicio del planificador denominado `TSM Central Scheduler Service` en la estación de trabajo remota PDC. Inicie el servicio automáticamente en el momento de arrancar el sistema. Los archivos obligatorios del servicio del planificador y el archivo de opciones especificado deben residir en el directorio `c:\program files\tivoli\tsm\baclient` de la estación de trabajo remota. La contraseña se cifra en el almacén de contraseñas de . Se contacta con el servidor de IBM Spectrum Protect que reside en el puerto y host TCP/IP especificados para validar la contraseña.

##### Mandato:

```
dsmcutil install scheduler /name:"TSM Central Scheduler Service"
/machine:PDC /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:PDC /autostart:yes /password:contraseña_nodo
/commmethod:tcip /commserver:alpha1.example.com
/commport:1521
```

#### Tarea

Instale `TSM Central Scheduler Service` en un nodo de un clúster de MSCS (o VCS). Para *group-a* desde una estación de trabajo *node-1*, asegúrese de que *node-1* es el propietario actual de *group-a* y después emita el siguiente mandato.

##### Mandato:

##### Mandato:

```
dsmcutil install scheduler /name:"TSM Central Scheduler Service:
group-a" /clientdir:"c:\program files\tivoli\tsm\baclient"
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
/node:mscs-cluster-group-a /password:n
/validate:no /autostart:yes /startnow:yes
/clusternode:yes /clustername:mscs-cluster
```

Instala y configura el servicio aceptador de cliente. Las opciones obligatorias son:

- /name:service\_name
- /node:node\_name
- /password:password

Otras opciones válidas son:

- /optfile:options\_file
- /httpport:http\_port
- /webports:web\_ports

Tarea

Instale un servicio Client Acceptor denominado `TSM CAD`. El aceptador de clientes utiliza un nodo denominado `test` para conectarse al servidor de IBM Spectrum Protect. Utilice el archivo de opciones `c:\program files\tivoli\tsm\baclient\dsm.opt` para conectar con el servidor.

**Mandato:**

```
dsmcutil install cad /name:"TSM CAD" /node:test /password:test /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

## INSTAll Journal

---

Instala un servicio de motor con registro por diario en todos los clientes Windows. Se crea una base de datos registrada por diario que almacena información que el cliente utiliza para determinar qué archivos son elegibles para un proceso de copia de seguridad antes de que empiece una operación.

En caso necesario, puede utilizar la opción `nojournal` con el mandato incremental para especificar que desea realizar una copia de seguridad incremental completa tradicional.

El servicio de motor con registro por diario se denomina `TSM Journal Service` y utiliza el archivo de configuración `tsmjbbd.ini` del directorio de instalación del cliente de archivado y copia de seguridad.

Nota: El servicio de diario se admite en un entorno Microsoft Cluster Server. Pueden instalarse varios servicios de registro por diario especificando valores de pipe name exclusivos mediante la utilización de los valores de configuración de registro por diario `JournalPipe` y las opciones del cliente.

No hay opciones válidas para este mandato.

Tarea

Instalar el servicio de motor con registro por diario (`TSM Journal Service`).

**Mandato:**

```
dsmcutil install journal
```

## INSTAll REMOTEAgent

---

Instala y configura un servicio del agente de cliente remoto. Las opciones obligatorias son:

- /name:service\_name
- /node:node\_name
- /password:password
- /partnername:partner\_service\_name

Otras opciones válidas son:

- /optfile:options\_file

Tarea

Instale un servicio del agente de cliente remoto denominado `TSM AGENT`. El agente del cliente remoto utiliza un nodo denominado `test` para conectarse al servidor de IBM Spectrum Protect. El archivo de opciones `c:\program files\tivoli\tsm\baclient\dsm.opt` se utiliza para conectarse. El servicio aceptador de cliente asociado es `TSM CAD`.

**Mandato:**

```
dsmcutil install remoteagent /name:"TSM AGENT" /node:test /password:test /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt" /partnername:"TSM CAD"
```

Nota: Tanto el servicio de agente de cliente remoto como el servicio Client Acceptor deben estar instalados para poder ejecutar el cliente web. El servicio Client Acceptor debe instalarse antes que el servicio del agente de cliente remoto. Utilice la opción `/partname:` para especificar el nombre del servicio Client Acceptor asociado.

## REMove

---

Elimina un servicio del cliente instalado. La opción obligatoria es `/name:service_name`.

### Tarea

Elimine el servicio del planificador especificado de la estación de trabajo local.

#### Mandato:

```
dsmcutil remove /name:"TSM Central Scheduler Service"
```

### Tarea

Elimine el servicio de motor con registro por diario TSM Journal Service de la estación de trabajo local.

#### Mandato:

```
dsmcutil remove /name:"TSM Journal Service"
```

## UPDate

---

Actualiza los valores del registro del servicio del planificador. Si la opción obligatoria para este mandato es `/name:service_name`, y se van a actualizar los valores de registro. Otras opciones válidas son:

- `/clientdir:client_dir`
- `/optfile::options_file`
- `/eventlogging:Yes | No`
- `/node:node_name`
- `/autostart:Yes | No`
- `/clusternode:Yes | No` (necesario si se está ejecutando MSCS o VCS).
- `/clustername:cluster_name` (necesario si se está ejecutando MSCS o VCS).

### Tarea

Actualice el directorio del cliente y el archivo de opciones para el servicio del planificador especificado. Todos los archivos obligatorios del servicio del cliente deben residir en el directorio especificado.

Nota: Estas opciones de comunicación especificadas con el mandato `dsmcutil` prevalecen sobre las especificadas en el archivo de opciones del cliente.

#### Mandato:

```
dsmcutil update /name:"TSM Central Scheduler Service"  
/clientdir:"c:\program files\tivoli\tsm\baclient"  
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

### Tarea

Actualice el servicio del planificador especificado para utilizar el protocolo TCP/IP para conectarse al servidor de IBM Spectrum Protect en el nombre de host y en el puerto especificados.

#### Mandato:

```
dsmcutil update /name:"TSM Central Scheduler Service"  
/commserver:ntl.example.com /commport:1521 /commmethod:  
tcpip
```

## UPDate CAD

---

Actualiza los valores del registro del servicio Client Acceptor. Si la opción obligatoria para este mandato es `/name:service_name`, y se van a actualizar los valores de registro. Otras opciones válidas son:

- `/node:node_name`
- `/password:password`
- `/optfile:options_file`
- `/httpport:http_port`
- `/webports:web_ports`
- `/cadschedname:scheduler_name`

### Tarea

Actualice el servicio Client Acceptor de modo que utilice el archivo de opciones y contraseña de cliente especificado. Todos los archivos obligatorios del servicio del cliente deben residir en el directorio especificado.

**Mandato:**

```
dsmcutil update cad /name:"TSM CAD" /password:test  
/optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

## UPDate REMOTEAgent

---

Actualiza los valores del registro del servicio del agente de cliente remoto. Si la opción obligatoria para este mandato es `/name:service_name`, y se van a actualizar los valores de registro. Otras opciones válidas son:

- `/node:node_name`
- `/password:password`
- `/optfile:options_file`
- `/partername:partner_service_name`

**Tarea**

Actualizar un servicio de agente de cliente remoto denominado TSM AGENT. El servicio del agente del cliente remoto utiliza un nodo denominado `test` para conectarse al servidor de IBM Spectrum Protect. El archivo de opciones `c:\program files\tivoli\tsm\baclient\dsm.opt` se utiliza para conectarse al servidor. El servicio aceptador de cliente asociado es TSM CAD.

**Mandato:**

```
dsmcutil update remoteagent /name:"TSM AGENT" /node:test  
/password:test /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"  
/partername:"TSM CAD"
```

## Query Scheduler

---

Consulta los valores del registro del servicio del planificador. Las opciones necesarias son: `/name:service_name`. Otras opciones válidas son:

- `/machine:machine_name`
- `/clientdir`
- `/optfile`
- `/eventlogging`
- `/node`
- `/commmethod`
- `/commport`
- `/commserver`
- `/errorlog`
- `/schedlog`

Nota: No especifique un valor para las opciones no requeridas. El cliente devuelve los valores del registro de la opción para el servicio del planificador que especifique.

**Tarea**

Consulte los valores del registro para el servicio del planificador que especifique.

**Mandato:**

```
dsmcutil query /name:"TSM Central Scheduler Service"
```

**Tarea**

Consulte el valor del registro del directorio del cliente para el servicio del planificador que especifique.

**Mandato:**

```
dsmcutil query /name:"TSM Central Scheduler Service"
```

## Query CAD

---

Consulta los valores del registro del servicio Client Acceptor. La opción necesaria para este mandato es `/name:service_name`. Otras opciones válidas son:

- `/machine:machine_name`
- `/node`
- `/optfile`
- `/httpport`
- `/webports`
- `/clientdir`
- `/partername`



Nota: No especifique un valor para estas opciones.

Tarea

Consulte los valores del registro para el servicio Client Acceptor de cliente que especifique.

**Mandato:**

```
dsmcutil query cad /name:"TSM CAD"
```

## Query Journal

---

Consultar al servicio de motor con registro por diario, TSM Journal Service, en un sistema Windows. No hay opciones válidas para este mandato.

Tarea

Consulte el servicio de motor con registro por diario, TSM Journal Service.

**Mandato:**

```
dsmcutil query journal
```

## Query REMOTEAgent

---

Consulta los valores del registro del servicio del agente de cliente remoto. La opción necesaria para este mandato es `/name:service_name`. Otras opciones válidas son:

- `/machine:machine_name`
- `/node`
- `/optfile`
- `/partnername`
- `/clientdir`

Nota: No especifique un valor para estas opciones.

Tarea

Consulte los valores del registro para el servidor del agente de cliente remoto especificado.

**Mandato:**

```
dsmcutil query remoteagent /name:"TSM AGENT"
```

## List

---

Lista los servicios del cliente instalados. No hay ninguna opción obligatoria.

Tarea

Localice y liste los servicios del cliente de copia de seguridad y archivado instalados en la estación de trabajo local.

**Mandato:**

```
dsmcutil list
```

Tarea

Liste los servicios del cliente de copia de seguridad y archivado instalados en la estación de trabajo remota PDC.

**Mandato:**

```
dsmcutil list /MACHINE:PDC
```

## START

---

Utilice el mandato Start para iniciar un servicio del cliente. El mandato Start requiere la opción `/name:service_name`.

Tarea

Iniciar el servicio de motor con registro por diario, TSM Journal Service.

**Mandato:**

```
dsmcutil start /name:"TSM Journal Service"
```

## STOP

---

Utilice el mandato Stop para detener un servicio del cliente. El mandato Stop requiere la opción `/name:service_name`.

Tarea

Detener el servicio de motor con registro por diario, TSM Journal Service.

**Mandato:**

```
dsmcutil stop /name:"TSM Journal Service"
```

## UPDATEPW

---

Genere una contraseña cifrada de IBM Spectrum Protect. El mandato UPDATEPW requiere las opciones `/node:node_name`, `/password:password` y `/commserver:server_name`. Si la opción `clusternode` está establecida en YES, también se requiere el parámetro `/optfile:`.

Opcionalmente, puede utilizar las opciones siguientes:

- `/validate:Yes | No`
- `/clusternode:Yes | No` (necesario si se está ejecutando MSCS o VCS).
- `/clustername:cluster_name` (necesario si se está ejecutando MSCS o VCS).
- `/force:Yes | No`
- `/optfile:` (para operaciones no de clúster)
- `/commmethod:`
- `/commport:`

La contraseña se valida con el servidor IBM Spectrum Protect si se especifica `/validate:Yes`. La contraseña se actualiza en el servidor si especifica `/updateonserver:Yes`. Si se especifica esta opción, debe especificar la contraseña actual con la opción `/oldpassword:`.

**Tarea**

Actualice la contraseña cifrada para el nodo especificado. Valide y actualice la contraseña en el servidor de IBM Spectrum Protect especificado que reside en el puerto y el nombre de host TCP/IP especificados:

**Mandato:**

```
dsmcutil updatepw /node:alpha1 /commMethod:tcpip  
/commServer:alpha1.example.com /commPort:1500  
/password:newpw /oldpassword:oldpw /updateonserver:yes  
/validate:yes /optfile:"c:\program files\tivoli\tsm\baclient\dsm.opt"
```

## ADDACE

---

Otorga acceso a la contraseña del cliente de archivado y copia de seguridad de IBM Spectrum Protect y a los certificados SSL del cliente para los usuarios no administradores.

A partir de IBM Spectrum Protect Versión 8.1.2, se aplica un control de accesos más estricto para el almacenamiento de contraseñas de IBM Spectrum Protect en los sistemas operativos Windows. De forma predeterminada, sólo la cuenta de administrador, SYSTEM o LocalSystem tiene acceso al almacén de contraseñas y los certificados SSL.

Puede utilizar el mandato `addace` para modificar la lista de control de accesos para permitir usuarios adicionales, por ejemplo, usuarios no administrativos, o procesos como los procesos de cliente de IBM Spectrum Protect Data Protection para acceder al almacén de contraseñas y los certificados SSL.

Se requieren las opciones siguientes:

- `-entity:user | group`
- `-object:ALL | NODENAME | path\TSM.* | path\spclient.*`

Donde:

*user | group*

Usuario o grupo de usuarios de Windows al que se proporciona acceso de lectura y escritura al almacén de contraseñas.

ALL

Otorga acceso a todos los archivos de contraseñas y todos los certificados SSL de los subdirectorios del directorio `C:\ProgramData\Tivoli\TSM\baclient`.

NODENAME

Otorga acceso a todos los archivos de contraseñas y certificados SSL que se encuentran en los subdirectorios del directorio `C:\ProgramData\Tivoli\TSM\baclient\Nodes\nodename`.

*path\TSM.\* | path\spclient.\**

Para las contraseñas de clúster que pueden existir en un directorio de recursos compartidos, otorga acceso a los archivos de contraseñas o archivos de certificado en un directorio específico para un nodo.

Para obtener más información sobre las ubicaciones seguras de contraseñas en Windows, consulte Almacenamiento seguro de contraseñas.

Consejo: El mandato `dsmcutil deleteace` revoca el acceso a los archivos de contraseñas y los certificados SSL.

#### Tarea

Tras instalar y configurar el cliente de archivado y copia de seguridad como administrador, debe proporcionar a Susan, un usuario no administrativo del sistema Windows, acceso a los archivos de contraseñas y los certificados SSL en el nodo de cliente `Alpha1`.

#### Mandato:

```
dsmcutil addace -entity:Susan -object:Alpha1
```

#### Tarea

Un usuario no administrativo de IBM Spectrum Protect for Databases: Data Protection for Microsoft SQL Server ha configurado las contraseñas de IBM Spectrum Protect, pero el administrador también requiere acceso a las contraseñas. El usuario de Data Protection for Microsoft SQL Server otorga acceso a los archivos de contraseñas al administrador emitiendo el mandato siguiente:

#### Mandato:

```
dsmcutil addace -entity:Administrator -object:all
```

#### Tarea

Durante una configuración de clúster, el administrador de Windows requiere proporcionar al nodo de clúster `clusnode_A` acceso a los certificados SSL de cliente.

#### Mandato:

```
dsmcutil addace -entity:Group_A  
-object:C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_A\spclient.*
```

Si los certificados de cliente no están en la ubicación predeterminada (`C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_A\`), se encuentran en el mismo directorio que el archivo `dsm.opt`.

## DELETEACE

---

Revoca el acceso a la contraseña del cliente de archivado y copia de seguridad de IBM Spectrum Protect y los certificados SSL de cliente para los usuarios no administradores.

Puede utilizar el mandato `deleteace` para modificar la lista de control de accesos para eliminar el acceso al almacén de contraseñas y a los certificados de cliente para los usuarios, por ejemplo, usuarios no administrativos o procesos como los procesos de cliente de IBM Spectrum Protect Data Protection.

Se requieren las opciones siguientes:

- `-entity:user | group`
- `-object:ALL | NODENAME | path\TSM.* | path\spclient.*`

Donde:

*user | group*

Usuario o grupo de usuarios de Windows del que se elimina el acceso al almacén de contraseñas o certificados de cliente.

**ALL**

Elimina el acceso de todos los archivos de contraseñas y certificados SSL de los subdirectorios del directorio `C:\ProgramData\Tivoli\TSM\baclient`.

**NODENAME**

Elimina el acceso de todos los archivos de contraseñas y certificados SSL que se encuentran en los subdirectorios del directorio `C:\ProgramData\Tivoli\TSM\baclient\Nodes\nodename`.

*path\TSM.\* | path\spclient.\**

Para las contraseñas de clúster que pueden existir en un directorio de recursos compartidos, elimina el acceso a los archivos de contraseñas o archivos de certificado en un directorio específico para un nodo.

Para obtener más información sobre las ubicaciones seguras de contraseñas en Windows, consulte Almacenamiento seguro de contraseñas.

Consejo: El mandato `dsmcutil addace` otorga acceso a los archivos de contraseñas y certificados SSL.

#### Tarea

Susan, un usuario no administrativo, ha dejado la empresa hace dos días y el administrador debe revocar el acceso a los archivos de contraseñas y los certificados SSL del nodo de cliente `Alpha1`.

#### Mandato:

```
dsmcutil deleteace -entity:Susan -object:Alpha1
```

#### Tarea

El nodo de clúster `clusnode_Z` se traslada fuera de la configuración de clúster y ya no requiere acceder a los certificados SSL de cliente. Emita el mandato siguiente para eliminar el acceso para `clusnode_Z`.

**Mandato:**

```
dsmcutil deleteace -entity:Group_Z  
-object:C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode_Z\spclient.*
```

Si los certificados de cliente no se encuentran en la ubicación predeterminada (C:\ProgramData\Tivoli\TSM\baclient\Nodes\clusnode\_Z\), se encuentran en el mismo directorio que el archivo `dsm.opt`.

**Conceptos relacionados:**


Copia de seguridad con registro por diario

**Tareas relacionadas:**

Opciones válidas de `dsmcutil`

**Referencia relacionada:**

Incremental

 Sistemas operativos Windows

## Opciones válidas de `dsmcutil`

---

Esta sección enumera las opciones válidas **dsmcutil** que puede especificar para utilizar el servicio del planificador.

### Acerca de esta tarea

---

**`/autostart:`**[Yes|No]

Especifica si el servicio del planificador se inicia automáticamente en el momento de arrancar el sistema. El valor predeterminado es *No*.

**`/cadschedname:`***schedulename*

Especifica el nombre del servicio de planificador que se va a gestionar con el aceptador de cliente. Utilice esta opción cuando la opción **`managedservices`** se haya establecido en el *schedule* en el archivo de opciones del *clientdsm.opt*. Puede especificar esta opción solo con el servicio aceptador de cliente.

**`/clientdir:`***clientdir*

La vía de acceso completa del directorio donde residen los archivos del servicio del cliente. Este directorio deber estar relacionado con la estación de trabajo de destino donde está instalado el servicio. Los nombres UNC no están permitidos si la cuenta del sistema local se ha establecido en el inicio de sesión. El valor predeterminado es el directorio actual.

**`/clustername:`***clustername*

Ésta sustituye a la opción **`/group`**.

La opción **`/clustername`** especifica el nombre de clúster al que pertenece el sistema. Puede determinar el nombre del clúster de una de las siguientes maneras:

- En MSCS, ejecute el mandato MSCS, CLUSTER /LIST, desde la línea de mandatos o utilice la herramienta Administrador de clústeres. Cuando se inicia la herramienta Administrador de clústeres, aparecerá una estructura de árbol con el nombre del clúster en la parte superior.
- En VCS, utilice VCS Cluster Manager - Consola Java™ o abra el archivo `main.cf` del directorio `%VCS_HOME%\config`.
- En VCS, utilice el siguiente mandato:

```
haclus -display
```

Restricción: No especifique un nombre de clúster que tenga más de 64 caracteres. Si especifica más de 64 caracteres y utiliza Veritas Storage Foundation con la función de alta disponibilidad o una configuración de Microsoft Cluster Server, es posible que no pueda instalar o iniciar el servicio del planificador de IBM Spectrum Protect.

Esta opción debe utilizarse con la opción **`/clusternode`** :Yes. Esta opción se debe especificar cuando se utiliza el mandato **INSTALL** en un entorno de clúster. También debe especificarse cuando se utiliza el mandato **UPDATE** para modificar la configuración del clúster (**`/clusternode`** y **`/clustername`**).

Esta opción también puede especificarse cuando se utiliza el mandato **UPDATEPW** en un entorno de clúster. Normalmente no es obligatorio. No obstante, si se define más de un servicio del planificador con diferentes configuraciones de clúster para un nodo concreto, la herramienta no puede determinar cuál es la configuración correcta. En este caso, corrija las discrepancias entre los servicios.

Otra alternativa consiste en especificar esta opción con **`/clusternode:`**Yes y **`/force:`**Yes, para obligar a la herramienta a mostrar o actualizar la contraseña con la configuración de clúster especificada.

Esta opción no es obligatoria si se especifica **`/clusternode`** :No.

***/clusternode:***Yes|No

Especifica si hay que activar el soporte para recursos de clúster. El valor predeterminado es *No*. Debe estar ejecutando MSCS o VCS para especificar ***/clusternode:Yes***. Esta opción se debe especificar cuando se utiliza el mandato INSTALL en un entorno de clúster. También debe especificarse cuando se utiliza el mandato UPDATE para modificar la configuración del clúster (***/clusternode, /clustername***).

Esta opción también puede especificarse cuando se utiliza el mandato UPDATEPW en un entorno de clúster. Normalmente no es obligatorio. No obstante, si se define más de un servicio del planificador con diferentes configuraciones de clúster para un nodo concreto, la herramienta no puede determinar cuál es la configuración correcta. En este caso, corrija las discrepancias entre los servicios.

Otra alternativa consiste en especificar esta opción con ***/clustername*** y ***/force:Yes***, para obligar a la herramienta a mostrar o actualizar la contraseña con la configuración de clúster especificada. Si se especifica ***/clusternode :No***, la opción ***/clustername*** no es necesaria.

***/commmethod:***protocol

Especifica el protocolo de comunicaciones del cliente para comunicarse con el servidor de IBM Spectrum Protect. Los protocolos válidos son: TCP/IP y Named Pipes. Si no especifica un valor, el valor se obtiene del archivo de opciones del cliente o se establece en el valor predeterminado del cliente. Esta opción también se puede utilizar con el mandato UPDATEPW para especificar que un protocolo de comunicación se conecte con un servidor al actualizar las contraseñas.

***/commport:***serverport

Especifica el puerto del servidor de IBM Spectrum Protect específico del protocolo. Para TCP/IP, es el puerto de nombre de host especificado. Si no se especifica esta opción, el valor se obtiene del archivo de opciones del cliente o se establece en el valor del cliente predeterminado. Esta opción también se utiliza con el mandato UPDATEPW para especificar un puerto de servidor específico de un protocolo al que conectarse para actualizar contraseñas.

***/commserver:***servername

Especifica el nombre del servidor de IBM Spectrum Protect específico del protocolo. En función del protocolo utilizado, puede ser un nombre de host TCP/IP o un nombre de Named Pipes. Si no se especifica, el valor se obtiene del archivo de opciones del cliente o se establece en el valor del cliente predeterminado.

Esta opción también se puede utilizar con el mandato UPDATEPW para especificar un nombre de servidor específico de un protocolo al que conectarse para actualizar contraseñas.

***/copyfiles***

Especifica que la instalación del servicio se copia a otra ubicación antes de instalar el servicio. Utilice la opción ***/srcdir*** para especificar la vía de acceso de origen completa.

***/errorlog:***errorlog

Especifica el nombre completo de las anotaciones de error del cliente.

***/eventlogging:***[Yes|No]

Activa o desactiva las anotaciones de sucesos para el servicio del planificador especificado. El valor predeterminado es *Yes*.

***/force:***[Yes|No]

Esta opción también puede especificarse cuando se utiliza el mandato UPDATEPW en un entorno de clúster. Normalmente no es obligatorio. No obstante, si se define más de un servicio del planificador con diferentes configuraciones de clúster para un nodo concreto, la herramienta no puede determinar cuál es la configuración correcta. En este caso, corrija las discrepancias entre los servicios.

Otra alternativa consiste en especificar esta opción con ***/clusternode*** y ***/clustername*** (si se especifica ***/clusternode:Yes***), para obligar a la herramienta a mostrar o actualizar la contraseña con la configuración de clúster especificada.

***/httpport:***httpport

Especifica una dirección de puerto TCP/IP para el cliente web.

***/machine:***machinename

Especifica el nombre de una estación de trabajo remota a la que conectarse.

***/name:***nombre\_servicio

Especifica el nombre del servicio del cliente. El nombre debe escribirse entre comillas si contiene espacios en blanco intercalados.

***/node:***nodename

Especifica el nombre de nodo de IBM Spectrum Protect que utiliza el servicio del cliente al conectarse al servidor de IBM Spectrum Protect. También se utiliza cuando se visualiza o se actualiza la contraseña de IBM Spectrum Protect. El valor predeterminado es el nombre de la estación de trabajo.

***/ntaccount:***ntaccount

Especifica la cuenta Windows con la que el servicio inicia la sesión.

***/ntdomain:***ntdomain

Especifica el dominio Windows con el que el servicio inicia la sesión.

***/ntpassword:***ntpassword

Especifica la contraseña Windows de la cuenta con la que el servicio inicia la sesión.

***/oldpassword:***oldpw

Contraseña del servidor Current IBM Spectrum Protect. Se utiliza conjuntamente con la opción */updateonserver* al actualizar una contraseña en el servidor.

***/optfile:***optionsfile

Ruta completa del archivo de opciones de cliente. Se trata del archivo de opciones que el servicio del cliente especificado utiliza para conectarse al servidor de IBM Spectrum Protect. La herramienta también utiliza este archivo para conectarse al servidor de IBM Spectrum Protect para validar y actualizar contraseñas. Tenga en cuenta que, aunque esta opción prevalezca sobre el archivo de opciones predeterminado en el directorio actual (*dsm.opt*), la API de IBM Spectrum Protect requiere que exista un archivo de opciones predeterminado en el directorio actual. Los nombres UNC no están permitidos si la cuenta del sistema local se ha establecido en el inicio de sesión. El archivo predeterminado es *dsm.opt* y está en el directorio ***/clientdir***.

***/partnername:***partner service name

Esta opción se utiliza al instalar un servicio del agente de cliente remoto para especificar el servicio Client Acceptor asociado.

***/password:***password

La contraseña de IBM Spectrum Protect que se genera y cifra.

***/schedlog:***schedlog

Especifica el nombre completo de las anotaciones de planificación cliente.

***/srcdir:***pathname

Utilice esta opción junto con la opción ***/copyfiles*** para especificar la vía de acceso de origen completa para copiar la instalación del servicio en otra ubicación antes de instalarlo.

***/startnow:***[Yes|No]

Especifica si *dsmcutil* inicia el servicio especificado tras ejecutar el mandato; el valor predeterminado es *Yes*. Si especifica **No**, deberá iniciar el servicio manualmente mediante el applet Servicios del panel de control o con el mandato NET START **nombre del servicio**.

***/updateonserver:***[Yes|No]

Especifica si la contraseña especificada se actualiza en el servidor de IBM Spectrum Protect. Requiere el uso de la opción ***/oldpassword***.

***/validate:***[Yes|No]

Especifica si se lleva a cabo validación al visualizar o actualizar la contraseña cifrada. El valor predeterminado es *Yes*.






***/webports:*** webports

Especifica el número de puerto TCP/IP que utiliza el servicio de aceptación de clientes y el servicio del agente de cliente web para comunicaciones con la GUI web.

## Documentación de los clientes de copia de seguridad y archivado en archivos PDF

---

La información acerca de los clientes de copia de seguridad y archivado que hay disponible en el Knowledge Center de IBM también está disponible en formato PDF.

-  Sistemas operativos AIX  Sistemas operativos Linux  sistemas operativos Mac OS X  Sistemas operativos Oracle Solaris  
Guía de instalación y del usuario de los clientes de copia de seguridad y archivado
-  Sistemas operativos Windows  
Guía de instalación y del usuario de los clientes de copia de seguridad y archivado
- Mensajes del cliente y códigos de retorno de la interfaz de programación de aplicaciones

**Conceptos relacionados:**

Instalación de los clientes de archivado y copia de seguridad de IBM Spectrum Protect (UNIX, Linux y Windows)

**Tareas relacionadas:**

Configuración de clientes de copia de seguridad/archivado

IBM Spectrum Protect clientes de archivado y copia de seguridad

**Referencia relacionada:**

Opciones y mandatos del cliente de copia de seguridad/archivado

**Información relacionada:**

Protección para estaciones de trabajo y servidores de archivos

## Desarrollo de soluciones con la interfaz de programación de aplicaciones de

---

La interfaz de programación de aplicaciones (API) de IBM Spectrum Protect está empaquetada con el cliente de copia de seguridad y archivado de IBM Spectrum Protect. Con la API, puede proteger aplicaciones de negocio, como aplicaciones de bases de datos, en el entorno de IBM Spectrum Protect.

- Novedades en la API de IBM Spectrum Protect  
Leer sobre las características nuevas y modificadas. Revise las notas del release antes de instalar el producto.
- Instalación de la API  
La información sobre la instalación de la IBM Spectrum Protect interfaz de programación de aplicaciones (API) viene incluida en

- los procedimientos de instalación para el cliente de archivado y copia de seguridad.
- **Visión general de la API**  
La interfaz de programa de aplicación (API) de IBM Spectrum Protect permite a un cliente de aplicación utilizar las funciones de gestión de almacenamiento.
- **Crear y ejecutar la aplicación de API de ejemplo**  
El paquete de la API incluye las aplicaciones de ejemplo que demuestran el contexto de las llamadas de función de la API. Instale una aplicación de ejemplo y revise el código de origen para entender cómo utilizar las llamadas de función.
- **Consideraciones para el diseño de una aplicación**  
Cuando diseña una aplicación, tiene que tener una gran comprensión de muchos aspectos de la API.
- **Conceptos básicos sobre la interoperatividad**  
API tiene dos tipos de interoperatividad: entre el cliente de copia de seguridad y archivado y las aplicaciones API y entre sistemas operativos diferentes.
- **Utilización de la API con Unicode**  
La API IBM Spectrum Protect soporta Unicode UCS2, una página de códigos de doble byte y de longitud fija cuyo código apunta a todas las páginas conocidas como Japonés, Chino o Alemán. Soporta hasta 65535 códigos únicos.
- **Llamadas a función de la API**
- **Archivo de origen de códigos de retorno de la API: dsrmc.h**  
El archivo de cabecera dsrmc.h contiene todos los códigos de retorno que la API puede devolver a una aplicación.
- **Archivos de origen de definiciones de tipo de API**
- **Archivo de origen de las definiciones de la función de la API**  
Este apéndice contiene el archivo de encabezado dsmapifp.h para poder ver las definiciones de la función de API.
- **Referencia de códigos de retorno de la API**

**Conceptos relacionados:**

Clientes de archivado y copia de seguridad de IBM Tivoli Storage Manager

**Referencia relacionada:**

Archivos PDF para imprimir

## Novedades en la API de IBM Spectrum Protect

---

Leer sobre las características nuevas y modificadas. Revise las notas del release antes de instalar el producto.

- **Actualizaciones de API**  
Obtenga información sobre las nuevas características y actualizaciones para la API (interfaz de programación de aplicaciones) de IBM Spectrum Protect versión 8.1.
- **Notas del release para la Interfaz de programación de aplicaciones de IBM Spectrum Protect Versión 8.1**  
La API (Interfaz de programación de aplicaciones) de IBM Spectrum Protect V8.1 está disponible. Si desea obtener información importante sobre la instalación, lea este documento. También podrá aprender aspectos sobre actualizaciones de productos, problemas de compatibilidad, limitaciones y problemas conocidos.
- **Archivos léame para los fixpacks de la interfaz de programación de la aplicación de IBM Spectrum Protect versión 8.1**  
Archivos léame para los fixpacks de la interfaz de programación de aplicaciones (API) de IBM Spectrum Protect versión 8.1 en la base de conocimiento de soporte cuando hay una actualización de fixpack.
- **Últimas actualizaciones de la documentación**  
Se pueden realizar actualizaciones de la documentación de la interfaz de programación de aplicaciones (API) de IBM Spectrum Protect tras la publicación de la documentación en IBM® Knowledge Center.

## Actualizaciones de API

---

Obtenga información sobre las nuevas características y actualizaciones para la API (interfaz de programación de aplicaciones) de IBM Spectrum Protect versión 8.1.

Release	Nuevas características y actualizaciones
---------	--

Release	Nuevas características y actualizaciones
8.1.2	<p>Configuración avanzada de seguridad</p> <p>A partir de IBM Spectrum Protect Versión 8.1.2, se han introducido algunos cambios en el cliente de archivado y copia de seguridad para funcionar con el servidor de IBM Spectrum Protect V8.1.2, lo que proporciona mejorara la seguridad de las comunicaciones entre el cliente y el servidor. Para obtener más información, consulte Actualizaciones del cliente de archivado y copia de seguridad.</p> <p>Trusted Communication Agent (TCA) está en desuso</p> <p>Debido a la comunicación mejorada que se presenta en IBM Spectrum Protect V8.1.2, Trusted Communication Agent (TCA) ya no está disponible. Para obtener más información, consulte:</p> <ul style="list-style-type: none"> <li>• Almacenamiento seguro de contraseñas</li> <li>• Habilitación de usuarios no root para que gestionen sus propios datos</li> </ul> <p>Actualizaciones de mantenimiento</p> <p>Se ha actualizado la documentación de la API para incluir las actualizaciones de mantenimiento.</p>
8.1.0	<p>IBM® Tivoli Storage Manager es ahora IBM Spectrum Protect</p> <p>IBM Spectrum Protect Versión 8.1 es la próxima generación de Tivoli Storage Manager. Esta nueva versión va más allá de un simple cambio de nombre en la documentación y la interfaz de usuario. Se trata de una evolución hacia un nuevo nivel de protección de datos, diseñado para satisfacer las complejas demandas del mundo actual.</p> <p>Para obtener más información, consulte la publicación Conozca IBM Spectrum Protect.</p> <p>Ya no se crea un ID de usuario de administración de forma predeterminada con el mandato de servidor REGISTER NODE</p> <p>A partir de IBM Spectrum Protect V8.1, el mandato de servidor REGISTER NODE no crea automáticamente un ID de usuario de administración que coincida con el nombre de nodo. Esta actualización de producto está diseñada para optimizar la autenticación de usuario a un servidor LDAP (Lightweight Directory Access Protocol).</p> <p>Esta actualización de producto no afecta a los nodos de cliente existentes, sino que afecta al proceso de registro de nuevos nodos de cliente, incluidos pero sin limitarse a los nodos para los clientes de copia de seguridad y archivado de IBM Spectrum Protect. En algunos casos, es posible que tenga que crear un ID de usuario de administración al registrar un nodo. Puede crear el ID de usuario de administración emitiendo el comando REGISTER NODE y especificando el parámetro USERID. Para obtener información sobre los tipos de clientes afectados, consulte nota técnica 7048963.</p> <p>Para obtener más información sobre la creación de un ID de usuario de administración, consulte Crear un usuario administrativo con autorización de propietario de cliente.</p> <p>Se ha dejado de mantener el soporte de sistemas operativos de cliente</p> <p>Para aprovechar las nuevas características del producto, instale el cliente de archivado y copia de seguridad V8.1 y la API en uno de los sistemas operativos soportados. Para obtener la lista actual de sistemas operativos soportados, consulte nota técnica 1243309.</p> <p>Los siguientes sistemas operativos ya no están soportados por el cliente de archivado y copia de seguridad:</p> <ul style="list-style-type: none"> <li>• Sistemas operativos Windows de 32 bits (cliente y API).</li> <li>• Sistemas operativos Windows Server 2008, Windows Server 2008 R2, Windows 7 y Windows 8.</li> <li>• Sistemas operativos HP-UX. Puede seguir utilizando la API de IBM Spectrum Protect en un sistema operativo HP-UX. Para obtener instrucciones de instalación, consulte Instalación de la API de HP-UX Itanium 2.</li> <li>• Linux on Power Systems (big endian). Puede seguir utilizando la API de IBM Spectrum Protect en Linux on Power Systems (big endian). Para obtener instrucciones de instalación, consulte Instalación de la API en Linux on Power Systems (Big Endian).</li> <li>• Sistemas operativos Solaris SPARC. Puede seguir utilizando la API de IBM Spectrum Protect en los sistemas operativos Solaris SPARC. Las instrucciones para instalar la API están incluidas en el tema, Instalación del cliente de Oracle Solaris.</li> </ul>

## Notas del release para la Interfaz de programación de aplicaciones de IBM Spectrum Protect Versión 8.1



La API (Interfaz de programación de aplicaciones) de IBM Spectrum Protect V8.1 está disponible. Si desea obtener información importante sobre la instalación, lea este documento. También podrá aprender aspectos sobre actualizaciones de productos, problemas de compatibilidad, limitaciones y problemas conocidos.

## Contenido

---

- Descripción
- Anuncio
- Compatibilidad con versiones anteriores
- Requisitos del sistema
- Instalación de la API
- Actualizaciones, limitaciones y problemas conocidos

## Descripción

---

La API de IBM Spectrum Protect permite que un cliente de aplicación utilice las funciones de gestión de almacenamiento. La API incluye llamadas de función que pueden utilizarse en una aplicación para realizar las operaciones siguientes:

- Iniciar o finalizar una sesión
- Asignar clases de gestión a objetos antes de almacenarse en un servidor
- Realizar copias de seguridad o archivado de objetos en un servidor
- Restaurar o recuperar objetos de un servidor
- Consultar al servidor acerca de información sobre objetos almacenados
- Gestionar espacios de archivos
- Enviar eventos de retención

La API la utilizan desarrolladores de software para crear nuevas aplicaciones que funcionen con IBM Spectrum Protect.

La publicación *IBM Spectrum Protect Utilización de la interfaz de programación de aplicaciones* proporciona información acerca de cómo utilizar la API de IBM Spectrum Protect.

La API de IBM Spectrum Protect está disponible en los siguientes sistemas operativos:

- HP-UX
- IBM® AIX
- Linux
- Mac OS X
- Sistemas operativos Microsoft Windows de 64 bits
- Oracle Solaris

Para obtener una lista de APAR que se han arreglado en esta versión, consulte nota técnica 1993247.

## Anuncio

---

El anuncio para la familia de productos de IBM Spectrum Protect V8.1 incluye la siguiente información:

- Descripción detallada del producto, incluida una descripción de las funciones nuevas
- Declaración de posicionamiento del producto
- Detalles sobre pedidos y embalajes
- Información sobre compatibilidad internacional

Para buscar el anuncio del producto, siga estos pasos:

1. Vaya al sitio web de anuncio del producto.
2. En el campo Search for, escriba el identificador del producto (PID) de su producto. El PID de IBM Spectrum Protect es 5725-W98.
3. En el campo Information Type, seleccione Announcement letters y pulse Search.
4. En la lista Search in, seleccione Product Number.
5. Opcional: en el panel Refine Your Search del lado izquierdo de la ventana, seleccione el país en el que reside.
6. En la sección Sort by, seleccione Newest first.

## Compatibilidad con versiones anteriores

---

Para fines de compatibilidad con las versiones anteriores, consulte Consideraciones acerca de la compatibilidad y actualización del cliente/servidor de IBM Spectrum Protect.

## Requisitos del sistema

---

Para obtener información sobre la compatibilidad de hardware y software, consulte el documento de requisitos detallados del sistema en las siguientes páginas web:

Requisitos de clientes Apple Macintosh

Nota técnica 1053584

Requisitos de la API Itanium de HP-UX

Nota técnica 1197146

IBM AIX requisitos de clientes

Nota técnica 1052226

Requisitos de clientes de Linux on Power Systems

Nota técnica 1169963

Requisitos de clientes Linux x86\_64

Nota técnica 1052223

Requisitos de clientes de Linux on z Systems

Nota técnica 1066436

Requisitos de clientes de Microsoft Windows

Nota técnica 1197133

Requisitos de la API de Oracle Solaris SPARC

Nota técnica 1052211

Requisitos de cliente de Oracle Solaris x86\_64

Nota técnica 1232956

## Instalación de la API

---

Para obtener instrucciones de instalación, consulte el apartado Instalación de la API.

## Actualizaciones, limitaciones y problemas conocidos

---

La documentación sobre actualizaciones, limitaciones y problemas conocidos se documenta como notas técnicas en la base de conocimiento de Soporte en IBM Support Portal for IBM Spectrum Protect. IBM Software Support actualiza la bases de datos de conocimientos a medida que se detectan y resuelven problemas. Buscando en esta base de datos podrá encontrar métodos alternativos o soluciones para los problemas.

Limitaciones y problemas conocidos

Para obtener información acerca de las limitaciones y los problemas conocidos que afectan a la API de IBM Spectrum Protect V8.1, consulte nota técnica 1993248.

Actualizaciones de la documentación

Para obtener información que no estaba disponible en la fecha de publicación, consulte las actualizaciones de documentación en nota técnica 7048957.

## Archivos léame para los fixpacks de la interfaz de programación de la aplicación de IBM Spectrum Protect versión 8.1

---

Archivos léame para los fixpacks de la interfaz de programación de aplicaciones (API) de IBM Spectrum Protect versión 8.1 en la base de conocimiento de soporte cuando hay una actualización de fixpack.

Consulte los archivos léame del fixpack de la API de IBM Spectrum Protect Versión 8.1

## Últimas actualizaciones de la documentación

---

Se pueden realizar actualizaciones de la documentación de la interfaz de programación de aplicaciones (API) de IBM Spectrum Protect tras la publicación de la documentación en IBM® Knowledge Center.

Para ver las últimas actualizaciones de la documentación, consulte la Nota técnica 7048957 en el Portal de soporte de IBM.

## Instalación de la API

---

La información sobre la instalación de la IBM Spectrum Protect interfaz de programación de aplicaciones (API) viene incluida en los procedimientos de instalación para el cliente de archivado y copia de seguridad.

- Instalación de clientes de archivado y copia de seguridad Tivoli Storage Manager (UNIX, Linux y Windows)

## Visión general de la API

---

La interfaz de programa de aplicación (API) de IBM Spectrum Protect permite a un cliente de aplicación utilizar las funciones de gestión de almacenamiento.

La API incluye llamadas de función que pueden utilizarse en una aplicación para realizar las operaciones siguientes:

- Iniciar o finalizar una sesión
- Asignar clases de gestión a objetos antes de almacenarse en un servidor
- Realizar copias de seguridad o archivado de objetos en un servidor
- Restaurar o recuperar objetos de un servidor
- Consultar al servidor acerca de información sobre objetos almacenados
- Gestionar espacios de archivos
- Enviar eventos de retención

Cuando un desarrollador de aplicación instala la API, recibe los archivos que necesita un usuario final de una aplicación:

- La biblioteca compartida de la API.
- El archivo de mensajes.
- Los archivos de opciones de cliente de ejemplo.
- El código de origen de los archivos del encabezado de la API que necesita la aplicación.
- El código de origen de una aplicación de ejemplo, y el archivo para construirlo.

Para restaurar el registro de las compilaciones de todas las aplicaciones de 64 bits deben ejecutarse utilizando opciones de compilador compatibles con 64 bits. Por ejemplo, debe utilizarse '-q64' cuando se construyen aplicaciones API en AIX, y '-m64' en Linux. Consulte los archivos de construcción de ejemplo para obtener más información.

Importante: Cuando instala la API, asegúrese de que todos los archivos están en el mismo nivel.

Para obtener información acerca de cómo instalar la API, consulte Instalación de los clientes de copia de seguridad y archivado de IBM Spectrum Protect.

Las referencias a UNIX y Linux incluyen sistemas operativos AIX, HP-UX, Linux, Mac OS X y Oracle Solaris.

- Conceptos básicos de los archivos de opciones y configuración  
Los archivos de opciones y configuración definen las condiciones y límites bajo las cuales se ejecuta la sesión.
- Configuración del entorno de la API  
La API utiliza variables de entorno exclusivas para localizar archivos. Es posible utilizar diferentes archivos para las aplicaciones de la API de los que utiliza el cliente de archivado/copia de seguridad. Las aplicaciones pueden utilizar la llamada de función dsmSetup para modificar los valores que las variables de entorno configura.

## Conceptos básicos de los archivos de opciones y configuración

---

Los archivos de opciones y configuración definen las condiciones y límites bajo las cuales se ejecuta la sesión.

Un administrador o un usuario final pueden configurar los valores de las opciones para:

- Configurar la conexión a un servidor
- Controlar qué objetos se envían al servidor y con qué clase de gestión se asocian

Las opciones se definen en uno o dos archivos cuando instala la API en la estación de trabajo.

En sistemas operativos UNIX y Linux, las opciones residen en dos archivos de opciones:

- dsm.opt - el archivo de opciones del cliente
- dsm.sys - el archivo de opciones de sistema del cliente

En otros sistemas operativos, el archivo de opciones del cliente (dsm.opt) contiene todas las opciones.

Restricción: La API no soporta las siguientes opciones de cliente de archivado y copia de seguridad:

- autofsrename
- changinretries
- domain
- eventlogging

- groups
- subdir
- users
- virtualmountpoint

También puede especificar opciones en la llamada de función `dsmInitEx`. Utilice el parámetro de la cadena de opciones o el parámetro del archivo de configuración de la API.

La misma opción puede derivar de más de un origen de configuración. Cuando esto ocurre, el origen con la prioridad más alta tiene preferencia. Tabla 1 lista la secuencia de prioridad.

Tabla 1. Configurar orígenes en orden de prioridad descendente

Prioridad	UNIX y Linux	Windows	Descripción
1	archivo <code>dsm.sys</code>  (opciones del sistema del cliente)	no aplicable	Este archivo contiene opciones que un administrador del sistema solo establece para UNIX y Linux.  Consejo: Si el archivo <code>dsm.sys</code> contiene stanzas de servidor, asegúrese de que la opción <code>passwordaccess</code> especifica el mismo valor ( <code>prompt</code> o <code>generate</code> ) en cada una de las stanzas.
2	Serie de opciones  (opciones de cliente)	Serie de opciones  (todas las opciones)	Una de estas opciones surte efecto cuando pasa como un parámetro a una llamada <code>dsmInitEx</code> . La lista puede contener opciones como, por ejemplo, <code>compressalways</code> , <code>servername</code> (solo UNIX y Linux), o <code>tcpserveraddr</code> (no UNIX).  Con la cadena de opción de la API, un cliente de la aplicación puede realizar cambios a los valores de la opción en el campo de configuración de la API y en el archivo de opciones del cliente. Por ejemplo, es posible que la aplicación consulte al usuario final si se requiere compresión. Dependiendo de las respuestas del usuario, puede crear una cadena de opciones de la API con esta opción y pasarla a la llamada <code>dsmInitEx</code> .  Para obtener más información sobre el formato de la cadena de opción de la API, consulte <code>dsmInitEx</code> . También puede establecer este parámetro en NULO. Esto indica que no existe una cadena de opciones de la API en esta sesión.
3	Archivo de configuración de la API  (opciones de cliente)	Archivo de configuración de la API  (todas las opciones)	Los valores que establezca en el archivo de configuración de API sustituyen a los valores que haya establecido en el archivo de opciones de cliente. Establezca las opciones en el archivo de configuración de API con valores que sean los adecuados en la sesión de IBM Spectrum Protect para el usuario. Los valores surten efecto cuando el nombre del archivo de configuración de la API pasa como un parámetro en la llamada <code>dsmInitEx</code> .  También puede configurar este parámetro en NULO. Esto indica que no existe un archivo de configuración de la API en esta sesión.
4	<code>dsm.opt</code> , archivo  (opciones de cliente)	<code>dsm.opt</code> , archivo  (todas las opciones)	En sistemas operativos UNIX y Linux el archivo <code>dsm.opt</code> contiene únicamente las opciones del usuario. En otros sistemas operativos, el archivo <code>dsm.opt</code> contiene todas las opciones. Para omitir las opciones en estos campos, siga los métodos que se describen en esta tabla.

**Conceptos relacionados:**

Opciones de proceso

## Configuración del entorno de la API

La API utiliza variables de entorno exclusivas para localizar archivos. Es posible utilizar diferentes archivos para las aplicaciones de la API de los que utiliza el cliente de archivado/copia de seguridad. Las aplicaciones pueden utilizar la llamada de función `dsmSetup` para modificar los valores que las variables de entorno configura.

Consejo: En Windows, el directorio de la instalación predeterminado es `%SystemDrive%\Archivos de programa\Common Files\Tivoli\TSM\api`

Tabla 1 incluye una lista de las variables del entorno de la API por sistema operativo.

Tabla 1. Variables de entorno de la API

Variables	UNIX and Linux	Windows
DSMI_CONFIG	El nombre calificado al completo para el archivo de opciones del cliente (dsm.opt).	El nombre calificado al completo para el archivo de opciones del cliente (dsm.opt).
DSMI_DIR	Apunta a la ruta que contiene el dsm.sys, subdirectorio en_US, y otro idioma nacional compatible (NLS). El subdirectorio en_US debe contener dsmclientV3.cat.	Apunta a la ruta que contiene dscenu.txt y cualquier archivo de mensaje NLS.
DSMI_LOG	Apunta a la ruta del archivo dsierorr.log.	Apunta a la ruta del archivo dsierorr.log.  Si se define la opción del clienteerrorlogname, la ubicación que especifica la opción sustituye al directorio que especifica el DSMI_LOG.

## Crear y ejecutar la aplicación de API de ejemplo

El paquete de la API incluye las aplicaciones de ejemplo que demuestran el contexto de las llamadas de función de la API. Instale una aplicación de ejemplo y revise el código de origen para entender cómo utilizar las llamadas de función.

Seleccione uno de los siguientes paquetes de aplicación API de ejemplo:

- El interactivo, paquete de aplicación de hebra única (dapi\*)
- El paquete de aplicación de varias hebras (callmt\*)
- La aplicación de prueba de agrupación de objetos lógica (dsmgrp\*)
- La aplicación de ejemplo de política de retención basada en evento (callevnt)
- La aplicación de ejemplo de retención de eliminación (callhold)
- La aplicación de ejemplo de protección de retención de datos (callret)
- El programa de ejemplo de almacenamiento intermedio de datos de IBM Spectrum Protect (callbuff)

Como ayuda para la iniciación, revise el procedimiento para crear la aplicación de ejemplo dapismp en su plataforma:

- Para aplicaciones UNIX o Linux, consulte Archivos de origen de aplicación de ejemplo UNIX o Linux.
- Para aplicaciones Windows, consulte Aplicación de ejemplo de 64 bits de Windows.

La aplicación de ejemplo dapismp crea su propia corriente de datos cuando archiva o realiza copias de seguridad de los objetos. No lee o graba objetos al sistema de archivos del disco local. El nombre del objeto no se corresponde con ningún archivo de la estación de trabajo. La "seed string" que emite genera un patrón que puede comprobarse cuando el objeto se restaura o recupera. Una vez se ha compilado la aplicación de ejemplo y se ha ejecutado **dapismp** para iniciarlas, puede seguir las instrucciones que aparecen en la pantalla.

- Archivos de origen de aplicación de ejemplo UNIX o Linux  
Para construir y ejecutar la aplicación de ejemplo de UNIX o Linux, debe asegurarse de que cuenta con ciertos archivos de origen. Una vez que ha construido la aplicación de ejemplo, puede compilarla y ejecutarla.
- Aplicación de ejemplo de 64 bits de Windows  
Para crear y ejecutar la aplicación de ejemplo para sistemas Microsoft Windows de 64 bits, debe instalar la API de IBM Spectrum Protect y asegurarse de tener determinados archivos de origen.

## Archivos de origen de aplicación de ejemplo UNIX o Linux

Para construir y ejecutar la aplicación de ejemplo de UNIX o Linux, debe asegurarse de que cuenta con ciertos archivos de origen. Una vez que ha construido la aplicación de ejemplo, puede compilarla y ejecutarla.

Los archivos que aparecen en una lista en Tabla 1 incluyen los archivos de origen y otros archivos que necesita para construir la aplicación de ejemplo que se incluye en el paquete de la API.

Tabla 1. Archivos que necesita para construir la aplicación de ejemplo de API para UNIX o Linux

Nombres de archivos	Descripción
README_api_enu	archivo README

Nombres de archivos		Descripción
dsmrc.h dsmapi64.h dsmapi64p.h dsmapi64fp.h release.h		Archivo de encabezado de los códigos de retorno Archivo de encabezado de definiciones de tipo corriente Archivo de encabezado de definiciones de tipo específico del sistema operativo Archivo de encabezado de prototipo de función Archivo de encabezado de valores de release
dapibkup.c dapidata.h dapiinit.c dapint64.h dapint64.c dapipref.c dapiproc.c dapiproc.h	dapiw.c dapiqry.c dapirc.c dapismp.c dapitype.h dapiutil.h dapiutil.c	Módulos para la aplicación de ejemplo de línea de mandato
makesmp[64].xxx		Archivo para construir dapismp del sistema operativo. xxx indica el sistema operativo.
callmt1.c callmt2.c		Archivos de ejemplo de varias hebras
callmtu1.c callmtu2.c		Archivos de ejemplo Unicode de varias hebras
libApiDS.xx libApiDS64.xx, o libApiTSM64.xx		Biblioteca compartida (el sufijo depende de la plataforma)
dsmgrp.c callevnt.c callhold.c callret.c callbuff.c dpsthread.c		Agrupar archivos de ejemplo Código de origen de ejemplo de política de retención basada en evento Código de origen de ejemplo de retención de eliminación Código de origen de ejemplo de protección de retención de datos

- Compilación de la aplicación de ejemplo de UNIX o Linux  
Compile la aplicación de la API de ejemplo dapismp utilizando un compilador para el sistema operativo.

## Aplicación de ejemplo de 64 bits de Windows

Para crear y ejecutar la aplicación de ejemplo para sistemas Microsoft Windows de 64 bits, debe instalar la API de IBM Spectrum Protect y asegurarse de tener determinados archivos de origen.

Restricciones:

- Para obtener mejores resultados, utilice la carga dinámica. Por ejemplo, consulte el archivo dynaload.c y la implementación en el código de muestra.
- Los archivos para la aplicación de ejemplo están en los siguientes directorios:
  - api64\obj  
Contiene los archivos de objeto del programa de ejemplo de la API.
  - api64\samprun  
Contiene el programa de ejemplo dapismp. El programa de ejemplo contiene el directorio de ejecución.
- El DLL tsmapi64.dll es un DLL de 64 bits.
- Utilice el Microsoft C/C++ Compiler versión 15 y el archivo make makesmp64.mak para compilar la aplicación de ejemplo de API dapismp. Es posible que tenga que ajustar los archivos make para su entorno, especialmente, la biblioteca o los directorios de inclusión.
- Después de compilar la aplicación, ejecute la aplicación de muestra emitiendo el mandato **dapismp** desde el directorio api64\samprun.
- Seleccione de la lista de opciones que se visualizan. Asegúrese de que ejecuta la acción de inicio de sesión antes de ejecutar cualquier otra acción.

- Siempre prefije el espacio de archivo, los nombres de alto y bajo rango con el delimitador de ruta correcto (\) cuando lo introduzca, por ejemplo:\myfilespace. Debe utilizar este prefijo incluso cuando especifique el carácter comodín asterisco (\*).

En sistemas operativos Windows , los archivos de origen que debe tener para compilar la aplicación de ejemplo están listados en Tabla 1. La aplicación de ejemplo está incluida en el paquete de API. Para su comodidad, un archivo ejecutable precompilado (dapismp.exe) también se incluye.

Tabla 1. Archivos para compilar la aplicación de ejemplo de API de Windows 64 bits

Nombres de archivos	Descripción
api.txt	archivo README
tsmapi64.dll	DLL de la API
dsmrc.h	Archivo de encabezado de códigos de retorno
dsmapi64.h	Archivo de encabezado de definiciones de tipo corriente
dsmapi64p.h	Archivo de encabezado de definiciones de tipo específico del sistema operativo
dsmapi64pif.h	Archivo de encabezado de prototipo de función
dsmapi64idl.h	Archivo de encabezado de prototipo de función cargado de forma dinámica
release.h	Archivo de encabezado de valores de release
dapidata.h dapint64.h dapitype.h dapiutil.h	Archivos de encabezado de Código fuente
tsmapi64.lib	Biblioteca implícita
dapibkup.c dapiinit.c dapint64.c dapipref.c dapiproc.c dapiproc.h dapipw.c dapiqry.c dapirc.c dapismp64.c dapiutil.c dynaload.c	Archivos de código fuente de dapismp.exe
makesmpx64.mak (Windows x64) makesmp64.mak (Windows IA64)	Archivos de construcción para la aplicación de ejemplo
callmt1.c callmt2.c callmtu164.c callmtu264.c	Archivos de ejemplo de varias hebras
dpstthread.c	Código de origen de archivo de ejemplo
callevnt.c callhold.c callret.c callbuff.c	Código de origen de política de retención basada en evento Código de origen de ejemplo de retención de eliminación Código de origen de ejemplo de protección de retención de datos Código de origen de ejemplo de almacenamiento intermedio compartido (no de copia).

## Consideraciones para el diseño de una aplicación

---

Cuando diseña una aplicación, tiene que tener una gran comprensión de muchos aspectos de la API.

Para lograr esa comprensión de la API, revise los siguientes temas:

- Determinar los límites de tamaño
- Mantenimiento del control de la versión de la API
- Utilizar varias hebras
- Señales y manejadores de señal
- Iniciar o finalizar una sesión
- ID y nombres de objeto
- Control del acceso a los archivos de contraseñas
- Acceder a objetos como propietario de sesión
- Acceder a objetos de nodos y propietarios
- Gestionar espacios de archivos
- Asociar objetos con clases de gestión
- Retener y liberar la caducidad/eliminación
- Consultas para el sistema IBM Spectrum Protect
- Enviar datos a un servidor
- Diagramas de ejemplo de copia de seguridad/archivado
- Agrupación de archivos
- Resumen del diagrama de estado para la API de IBM Spectrum Protect

Cuando diseñe la aplicación, revise las consideraciones en Tabla 1. Las estructuras de inicio con los campos memset pueden cambiar en los releases posteriores. El valor stVersion aumenta con cada mejora del producto.

Tabla 1. Consideraciones de la API para el diseño de una aplicación

Elementos de diseño	Consideraciones
<b>Configurar entorno local</b>	<p>La aplicación debe establecer el entorno local antes de llamar a la API. Para establecer el entorno local al valor predeterminado, añada el siguiente código a la aplicación:</p> <pre>setlocale(LC_ALL, "");</pre> <p>Para configurar el entorno local en otro valor, utilice la misma llamada con el entorno local apropiado en el segundo parámetro. Busque información específica en la documentación relativa al sistema operativo que utilice.</p>



Elementos de diseño	Consideraciones
Control de sesión	<p>Aplique las siguientes directrices al control de sesión:</p> <ul style="list-style-type: none"> <li>• Asigne un nombre de nodo exclusivo para cada cliente de archivado y copia de seguridad de IBM Spectrum Protect y producto del cliente de la API de IBM Spectrum Protect que utilice. Los siguientes productos son ejemplos de estos clientes: <ul style="list-style-type: none"> <li>◦ IBM Spectrum Protect for Mail</li> <li>◦ IBM Spectrum Protect HSM for Windows</li> </ul> </li> <li>• Utilice un nombre de propietario coherente en un procedimiento de restauración y copia de seguridad.</li> <li>• Utilice la opción passwordaccess para gestionar el acceso al archivo de contraseña protegida.</li> <li>• Asegúrese de que las sesiones de los movimientos de datos terminan cuando se completa la tarea para que los dispositivos del servidor se liberen y se puedan utilizar en otras sesiones.</li> <li>• Para permitir una transferencia de datos sin LAN, utilice la llamada a función dsmSetup con el indicador multithread establecido en activado.</li> <li>• En AIX, cuando utiliza aplicaciones de varias hebras o sin LAN, especialmente cuando se ejecutan máquinas con varios procesadores, configure la variable de entorno AIXTHREAD_SCOPE en S en el entorno antes de iniciar la aplicación, para que el rendimiento y la planificación sean mejores. Por ejemplo: <pre>EXPORT AIXTHREAD_SCOPE=S</pre> <p>Estableciendo AIXTHREAD_SCOPE en S, las hebras de usuario creadas con los atributos predeterminados se colocan en el alcance de contención del sistema. Si una hebra de usuario se crea con un alcance de contención de sistema, se vincula a una hebra de kernel y es planificada por dicho kernel. La hebra del kernel subyacente no se comparte con otra hebra de usuario. Para obtener más información acerca de esta variable de entorno, consulte el tema siguiente:</p> <p>Utilizar varias hebras</p> </li> </ul> <ul style="list-style-type: none"> <li>• Asegúrese de que sólo una hebra de la sesión llama a una función API en cualquier momento. Las aplicaciones que utilizan varias hebras con el mismo manejador de sesión deben sincronizar las llamadas de la API. Por ejemplo, utilice mutex con el fin de sincronizar las llamadas de la API: <ul style="list-style-type: none"> <li>◦ getTSMMutex()</li> <li>◦ emita la llamada de la API TSM</li> <li>◦ releaseTSMMutex()</li> </ul> <p>Utilice este método sólo cuando las hebras comparten un manejador. Puede utilizar llamadas paralelas para las funciones de la API si las llamadas tienen diferentes manejadores de sesión.</p> </li> <li>• Implemente un modelo de productor/consumidor con hebras para el movimiento de datos. Las llamadas de la API son síncronas y las llamadas para la función dsmGetData y función dsmSendData se bloquean hasta que terminan. Al utilizar un modelo de productor/consumidor, la aplicación puede leer el siguiente almacenamiento intermedio mientras espera a la red. También, esta disociación de lectura/escritura de datos y red, aumenta el rendimiento cuando hay un atasco en la red o retrasos. En general, se espera lo siguiente: <pre>Hebra de datos &lt;---&gt; cola de almacenamientos intermedios compartida &lt;---&gt; hebra de comunicación (emiten llamadas a la API de IBM Spectrum Protect)</pre> </li> <li>• Utilice la misma sesión para varias operaciones para evitar producir una sobrecarga. Para aplicaciones que tratan con muchos objetos pequeños, implemente la agrupación de sesión para la misma sesión se pueda utilizar en múltiples operaciones pequeñas. La sobrecarga se asocia con la apertura y cierre de una sesión para el servidor IBM Spectrum Protect. La llamada dsmInit/dsmInitEX está serializada así que incluso en una aplicación de múltiples hebras sólo se puede iniciar una hebra cada vez. Igualmente, durante el inicio de sesión, la API envía un número de consultas únicas al servidor.</li> </ul>

Elementos de diseño	Consideraciones
<b>Secuencia de operación</b>	<p>El servidor IBM Spectrum Protect bloquea las entradas de la base de datos del espacio de archivo durante algunas operaciones. Las siguientes reglas se aplican cuando se están diseñando aplicaciones API de IBM Spectrum Protect :</p> <ul style="list-style-type: none"> <li>Las consultas bloquean el espacio de archivo durante toda la transacción.</li> <li>El bloqueo de consulta se puede compartir con otras operaciones de consulta, con el fin de que varias operaciones de consulta en el mismo espacio de archivo se ejecuten de forma simultánea.</li> <li>Las siguientes operaciones se utilizan para modificar la base de datos del servidor de IBM Spectrum Protect (DB Chg): enviar, obtener, cambiar el nombre, actualizar y suprimir.</li> <li>La finalización de una operación DB Chg requiere un bloqueo de espacio de archivo durante el cambio de la base de datos al final de la transacción.</li> <li>Se pueden ejecutar a la vez varias operaciones DB Chg en el mismo espacio de archivo. Es posible que haya un retraso mientras la secuencia espera al bloqueo al final de la transacción.</li> <li>El bloqueo de la consulta no se puede compartir con las operaciones DB Chg. Una operación DB Chg retrasa el principio de una consulta en el mismo espacio de archivo, con lo que las aplicaciones deben separar y serializar consultas desde las operaciones DB Chg en el mismo espacio de archivo.</li> </ul>
<b>Denominación de objeto</b>	<p>Cuando pone nombre a los objetos, tenga en cuenta los siguientes factores:</p> <ul style="list-style-type: none"> <li>Los nombres de objeto específicos son nombres de objeto de alto rango y de bajo rango. Si en el nombre se incluye un identificador único, como el indicador de fecha, entonces las copias de seguridad de los objetos están siempre activas. Los objetos caducan sólo cuando están marcados como inactivo por parte de la llamada a función <code>dsmDeleteObj</code>.</li> <li>El método de restauración para objetos determina cómo dar formato al nombre para consultas fáciles. Si pretende utilizar una restauración de objeto parcial (POR), no es posible utilizar la compresión. Para suprimir la compresión, utilice la función <code>dsmSendObj objAttr objCompressed=bTrue</code>.</li> </ul>
<b>Agrupación de objetos</b>	<p>Agrupe objetos de manera lógica utilizando espacios de archivos. Un espacio de archivos es un contenedor en el servidor que proporciona una categoría de agrupación para los objetos. La API consulta todos los espacios de archivos durante el inicio de sesión y también durante las consultas, así que el número de espacios de archivos debe estar restringido. Una suposición razonable es que una aplicación establezca 20 - 100 espacios de archivo por nodo. La API puede ofrecer servicios para más espacios de archivo, pero cada espacio de archivo conlleva una sobrecarga para la sesión. Para crear una separación más granular, utilice el objeto <code>directory</code> en la aplicación.</p>
<b>Manejo de objeto</b>	<p>No almacene valores <code>objectID</code> para utilizarlos para restauraciones futuras. No se garantiza que estos valores sean persistentes durante la vida del objeto.</p> <p>Durante la restauración, preste especial atención al orden de restauración. Después de la consulta, ordene este valor antes de la restauración. Si está utilizando varios tipos de medios de serie, entonces acceda a ellos en sesiones separadas. Para obtener información, consulte el tema siguiente:</p> <p>Seleccionar y ordenar objetos por orden de restauración</p>
<b>Clase de gestión</b>	<p>Tenga en cuenta cuánto control necesita tener la aplicación sobre la clase de gestión que está asociada con los objetos de aplicación. Es posible definir estancias de inclusión, o bien especificar un nombre en la llamada de función <code>dsmSendObj</code>.</p>
<b>Tamaño de objeto</b>	<p>IBM Spectrum Protect necesita saber una estimación de tamaño por cada objeto. Tenga en cuenta cómo calcula la aplicación el tamaño de un objeto. Es mejor la sobrevaloración del tamaño de objeto que la infravaloración.</p>

- Determinar los límites de tamaño  
Algunas estructuras de datos o campos en la API tienen una limitación de tamaño. Estas estructuras son a menudo nombres u otros campos de texto que no pueden exceder una longitud predeterminada.
- Mantenimiento del control de la versión de la API  
Todas las API tiene algún tipo de control de la versión. La versión de API que utiliza en su aplicación debe ser compatible con la versión de la biblioteca de API instalada en la estación de trabajo del usuario.
- Utilizar varias hebras  
La API de varias hebras permite a las aplicaciones crear varias sesiones con el servidor IBM Spectrum Protect dentro del mismo proceso. La API se puede introducir de nuevo. Las llamadas pueden ejecutarse en paralelo desde dentro de distintas hebras.
- Señales y manejadores de señal  
La aplicación maneja señales del usuario o del sistema operativo. Si el usuario entra una secuencia de pulsación CTRL+C , la

aplicación debe alcanzar la señal y enviar llamadas `dsmTerminate` para cada una de las hebras activas. A continuación, llame a `dsmCleanUp` para salir. Si las sesiones no están cerradas adecuadamente, pueden producirse resultados inesperados en el servidor.

- Iniciar o finalizar una sesión  
IBM Spectrum Protect es un producto basado en sesión, y todas las actividades deben realizarse dentro de una sesión IBM Spectrum Protect. Para iniciar una sesión, la aplicación inicia la llamada `dsmInitEx`. Esta llamada debe realizarse antes de cualquier otra llamada API que no sea `dsmQueryApiVersionEx`, `dsmQueryCliOptions`, o `dsmSetUp`.
- ID y nombres de objeto  
El servidor IBM Spectrum Protect es un servidor de almacenamiento de objeto cuya función principal es almacenar y recuperar de forma eficaz los objetos nombrados. El ID del objeto es único en cada objeto y permanece con el objeto durante toda la vida del objeto *excepto* cuando realiza exportaciones o importaciones.
- Acceder a objetos como propietario de sesión  
Cada objeto tiene un nombre de propietario asociado. Las normas que determinan a qué objetos se accede dependen de qué nombre de propietario se utilice cuando se inicia una sesión. Utilice este valor de propietario de sesión para controlar el acceso al objeto.
- Acceder a objetos de nodos y propietarios  
Hay tres llamadas de función compatibles con distintos nodos y propietarios en la misma plataforma: **`dsmSetAccess`**, **`dsmDeleteAccess`**, y **`dsmQueryAccess`**. Estas funciones, junto con las opciones de cadena `-fromnode` y `-fromowner` que se pasan en `dsmInitEx`, permiten una consulta a través de distintos nodos, así como restaurar y recuperar procesos a través de la API.
- Gestionar espacios de archivos  
Debido a que el espacio de archivos es tan importante para la operación del sistema, se utiliza un grupo de llamadas por separado para registrar, actualizar y eliminar los identificadores de espacio de archivos. Antes de almacenar cualquier objeto asociado con un espacio de archivo en el sistema, debe primero registrar el espacio de archivo con IBM Spectrum Protect.
- Asociar objetos con clases de gestión  
Una función principal de IBM Spectrum Protect es el uso de políticas (clases de gestión) para definir cómo se almacenan y gestionan los objetos en el almacenamiento IBM Spectrum Protect. Un objeto se asocia con una clase de gestión cuando se archiva o se realiza una copia de seguridad.
- Retener y liberar la caducidad/eliminación  
Puede retener la eliminación y la caducidad de objetos de archivado en respuesta a una acción pendiente o en curso que requiere que se retengan los datos particulares. En caso de que se inicie una acción que requiera el acceso a los datos, dichos datos deben estar disponibles hasta que la acción haya concluido y ya no sea necesario el acceso a los datos como parte del proceso. Después de determinar que la suspensión ya no se requiere, se reinicia la eliminación y caducidad normal de acuerdo al periodo de retención original.
- Consultas para el sistema IBM Spectrum Protect  
La API cuenta con varias consultas, como la consulta de clase de gestión, que las aplicaciones pueden utilizar.
- Eficiencia del servidor  
Utilice estas directrices cuando recupere o envíe objetos al servidor de IBM Spectrum Protect.
- Enviar datos a un servidor  
La API permite que los clientes de aplicación envíen datos, objetos nombrados y sus datos asociados al almacén del servidor IBM Spectrum Protect.
- Configuración de la API para enviar datos de rendimiento al supervisor de rendimiento de cliente  
El supervisor de rendimiento de cliente es un componente del Centro de administración de Tivoli Storage Manager que se utiliza para mostrar datos de rendimiento recopilados por la API. El supervisor de rendimiento de cliente registra y muestra los datos de rendimiento para las operaciones de restauración, archivado y copia de seguridad de cliente.
- Enviar objetos al servidor  
Los clientes de aplicaciones pueden enviar datos o objetos nombrados y sus datos asociados a un almacenamiento IBM Spectrum Protect utilizando funciones de archivado y de copia de seguridad de API. Los componentes de copia de seguridad y archivado del sistema permiten el uso de procedimientos de gestión diferentes para los datos que se envían a almacenamiento.
- Desduplicación de datos  
La desduplicación de datos es un método para reducir las necesidades de almacenamiento eliminando datos redundantes.
- Migración tras error de la aplicación  
Cuando el servidor de IBM Spectrum Protect no está disponible debido a una interrupción, las aplicaciones que utilizan la API pueden utilizar la migración tras error automáticamente a un servidor secundario para la recuperación de datos.
- Diagramas de ejemplo de copia de seguridad/archivado  
La API está diseñada para flujos lógicos sencillos y transiciones claras entre los distintos estados de la aplicación del cliente. Esta transición de estado capta fallos lógicos y errores de programa muy temprano en el ciclo de desarrollo, mejorando en gran medida la calidad y fiabilidad del sistema.
- Agrupación de archivos  
La API de IBM Spectrum Protect tiene un protocolo de agrupación de archivos que relaciona a varios objetos separados. Es posible mencionar y gestionar estos archivos como un grupo lógico en el servidor. Un grupo lógico requiere que todos los miembros del grupo y el líder pertenezcan al mismo nodo y espacio de archivo en el servidor.
- Recibir datos de un servidor  
Los clientes de aplicaciones pueden recibir datos u objetos con nombre y sus datos asociados del almacenamiento de IBM

Spectrum Protect utilizando las funciones de restauración y recuperación. La función de restauración accede a los objetos de los que se hizo una copia de seguridad previamente, y la función de recuperación accede a los objetos que han sido archivados.

- Actualizar y eliminar objetos en el servidor

Las aplicaciones API pueden utilizar la llamada de función **dsmUpdateObj** o **dsmUpdateObjEx** para actualizar objetos que fueron archivados o a los que se le realizó una copia de seguridad. Utilice cualquiera de las llamadas en el estado de sesión únicamente, y actualice los objetos de uno en uno. Utilice **dsmUpdateObjEx** para actualizar cualquiera de los objetos que contienen el mismo nombre.

- Registro de eventos

Una aplicación de la API puede registrar mensajes de eventos en ubicaciones centrales. La aplicación puede dirigir el registro al servidor IBM Spectrum Protect, la máquina local o ambos. La llamada a función **dsmLogEventEx** se lleva a cabo dentro de una sesión. Para ver los mensajes registrados en el servidor, utilice el mandato de consulta **actlog** a través del cliente administrativo.

- Resumen del diagrama de estado para la API de IBM Spectrum Protect

Una vez que haya leído todas las consideraciones para crear su propia aplicación con la API de IBM Spectrum Protect, revise este resumen de diagrama de estado en toda la aplicación.

## Determinar los límites de tamaño

Algunas estructuras de datos o campos en la API tienen una limitación de tamaño. Estas estructuras son a menudo nombres u otros campos de texto que no pueden exceder una longitud predeterminada.

Los siguientes campos son ejemplos de estructuras de datos que tienen límites de tamaño:

- Tipo de aplicación
- Descripción de la copia archivada
- Destino de grupo de copia
- Nombre de grupo de copia
- Información de espacio de archivo
- Nombre de clase de gestión
- Nombre de propietario de objeto
- Contraseña

Estos límites están definidos como constantes dentro del archivo de cabecera **dsmapi.h**. Las asignaciones de almacenamiento deben basarse en estas constantes en lugar de en los números que introduce. Para obtener más información, consulte el apartado Archivos de origen de definiciones de tipo de API.

## Mantenimiento del control de la versión de la API

Todas las API tiene algún tipo de control de la versión. La versión de API que utiliza en su aplicación debe ser compatible con la versión de la biblioteca de API instalada en la estación de trabajo del usuario.

**dsmQueryApiVersionEx** debe ser la primera llamada de la API que introduce en el sistema cuando utiliza la API. Esta llamada realiza una de las tareas siguientes:

- Confirma que la biblioteca de la API está instalada y está disponible en el sistema del usuario final
- Devuelve el nivel de la versión de la biblioteca API a la que accede la aplicación

La API es compatible con versiones superiores. Las aplicaciones escritas con releases o versiones antiguas de la biblioteca de la API funcionan correctamente cuando se ejecuta una versión posterior.

Determinar el release de la biblioteca API es muy importante porque es posible que algunos releases tengan requisitos de memoria y definiciones de estructura de datos distintos. La compatibilidad con versiones inferiores es poco probable. Consulte Tabla 1 para obtener más información sobre la plataforma.

Tabla 1. Información sobre la compatibilidad de la plataforma

Plataforma	Descripción
Windows	Los archivos de mensajes deben estar al mismo nivel que los de la biblioteca (DLL).
UNIX o Linux	La biblioteca de API y los archivos de mensajes deben estar en el mismo nivel.

La llamada **dsmQueryApiVersionEx** devuelve la versión de la biblioteca de la API que está instalada en la estación de trabajo del usuario final. Puede entonces comparar el valor devuelto con la versión de la API que está utilizando el cliente de la aplicación.

El número de la versión de la API del cliente de la aplicación se introduce en el código de objeto compilado como un conjunto de cuatro constantes definidas en **dsmapi.h**:

```

DSM_API_VERSION
DSM_API_RELEASE
DSM_API_LEVEL
DSM_API_SUB_LEVEL

```

Consulte el apartado Archivos de origen de definiciones de tipo de API.

La versión de la API del cliente de la aplicación es normalmente inferior o igual que la biblioteca de la API instalada en el sistema del usuario. Tenga cuidado con cualquier otra condición. Puede introducir la llamada **dsmQueryApiVersionEx** en cualquier momento, independientemente de que se haya iniciado la sesión API.

Las estructuras de datos que la API utiliza también tienen información de control de la versión. Las estructuras tienen información de la versión en el primer campo. A medida que las estructuras mejoran, el número de versión aumenta. Cuando inicia el campo de la versión, utilice el valor de la Versión de la estructura definida en dsmapitd.h.

Figura 1 demuestra el tipo de definición de la estructura, **dsmApiVersionEx** del archivo de encabezado, **dsmapitd.h**. El ejemplo a continuación define una variable global que se denomina **apiLibVer**. También demuestra cómo utilizarlo en una llamada a **dsmQueryApiVersionEx** con el fin de devolver la versión de la biblioteca de la API del usuario final. Por último, el valor que se devuelve se compara con el número de la versión de la interfaz de programación de aplicaciones (API) de la aplicación.

Figura 1. Un ejemplo de cómo obtener el nivel de la versión de la API

```

typedef struct
{
    dsUInt16_t      stVersion;          /* Structure version          */
    dsUInt16_t version;                /* API version                */
    dsUInt16_t release;                /* API release                */
    dsUInt16_t level;                 /* API level                  */
    dsUInt16_t subLevel;              /* API sub level              */
} dsmApiVersionEx;

dsmApiVersionEx apiLibVer;

memset(&apiLibVer, 0x00, sizeof(dsmApiVersionEx));
dsmQueryApiVersionEx(&apiLibVer);

/* check for compatibility problems */
dsInt16_t appVersion= 0, libVersion = 0;
appVersion=(DSM_API_VERSION * 10000)+(DSM_API_RELEASE * 1000) +
            (DSM_API_LEVEL * 100) + (DSM_API_SUBLEVEL);
libVersion = (apiLibVer.version * 10000) + (apiLibVer.release * 1000) +
            (apiLibVer.level * 100) + (apiLibVer.subLevel);
if (libVersion < appVersion)
{
    printf("\n*****\n");
    printf("The IBM Spectrum Protect API library is lower than the application version\n");
    printf("Install the current library version.\n");
    printf("*****\n");
    return 0;
}

printf("* API Library Version = %d.%d.%d.%d *\n",
       apiLibVer.version,
       apiLibVer.release,
       apiLibVer.level,
       apiLibVer.subLevel);

```

## Utilizar varias hebras

La API de varias hebras permite a las aplicaciones crear varias sesiones con el servidor IBM Spectrum Protect dentro del mismo proceso. La API se puede introducir de nuevo. Las llamadas pueden ejecutarse en paralelo desde dentro de distintas hebras.

Consejo: Cuando ejecuta una aplicación con una API de varias hebras, utilice la llamada **dsmQueryAPIVersionEx**.

Para ejecutar la API en modo de varias hebras, configure el valor de *mtflag* en **DSM\_MULTITHREAD** de la llamada **dsmSetUp**. La llamada **dsmSetUp** debe ser la primera llamada después de la llamada **dsmQueryAPIVersionEx**. Esta llamada debe volver antes de que ninguna hebra llame a **dsmInitEx**. Cuando todas las hebras han finalizado el proceso, introduzca una llamada a **dsmCleanUp**. El proceso principal no debe finalizar antes de que todas las llamadas finalicen el proceso. Consulte **callmt1.c** en la aplicación de ejemplo.

Restricción: De forma predeterminada la API es un modo de hebra única. Si una aplicación no llama a **dsmSetUp** con el valor *mtflag* configurado en **DSM\_MULTITHREAD**, la API sólo permite una sesión por proceso.

Una vez que **dsmSetUp** finaliza correctamente, la aplicación puede iniciar varias hebras e introducir varias llamadas **dsmInitEx**. Cada una de las llamadas **dsmInitEx** devuelve un manejador para dicha sesión. Cualquier llamada subsiguiente en dicha hebra para esa sesión debe utilizar ese valor de manejador. Algunos valores son variables de entorno de proceso ancho (valores configurados en **dsmSetUp**). Cada una de las llamadas **dsmInitEx** analiza las opciones de nuevo. Las hebras se pueden ejecutar con opciones diferentes especificando un archivo de sobrescritura o una cadena de opciones en la llamada **dsmInitEx**. Esto capacita a distintas hebras ir a diferentes servidores o bien utilizar nombres de nodo distintos.

Recomendación: En HP, configure la pila de hebra en 64K o en un valor superior. Es posible que el valor predeterminado de la pila de hebras (32K) no sea suficiente

Para permitir que los usuarios de una aplicación tengan una sesión sin LAN, utilice **dsmSetUp mtFlag DSM\_MULTITHREAD** en la aplicación. Esto es necesario incluso si la aplicación es de una única hebra. Este indicador activa las hebras necesarias para la interfaz IBM Spectrum Protect sin LAN.

## Señales y manejadores de señal

---

La aplicación maneja señales del usuario o del sistema operativo. Si el usuario entra una secuencia de pulsación CTRL+C, la aplicación debe alcanzar la señal y enviar llamadas **dsmTerminate** para cada una de las hebras activas. A continuación, llame a **dsmCleanUp** para salir. Si las sesiones no están cerradas adecuadamente, pueden producirse resultados inesperados en el servidor.

La aplicación requiere manejadores de señal, tales como SIGPIPE y SIGUSR1, para obtener señales que hacen que la aplicación finalice. A continuación la aplicación recibe el código de retorno de la API. Por ejemplo, para ignorar SIGPIPE añada la siguiente instrucción en la aplicación: `signal(SIGPIPE, SIG_IGN)`. Una vez añadida esta información, en lugar de la aplicación existente en un conducto roto, se devuelve el código de retorno adecuado.

## Iniciar o finalizar una sesión

---

IBM Spectrum Protect es un producto basado en sesión, y todas las actividades deben realizarse dentro de una sesión IBM Spectrum Protect. Para iniciar una sesión, la aplicación inicia la llamada **dsmInitEx**. Esta llamada debe realizarse antes de cualquier otra llamada API que no sea **dsmQueryApiVersionEx**, **dsmQueryCliOptions**, o **dsmSetUp**.

Se puede llamar a la función **dsmQueryCliOptions** únicamente antes de la llamada **dsmInitEx**. La función devuelve los valores de opciones importantes, como de archivos de opciones, configuraciones de compresión y parámetros de comunicación. La función **dsmInitEx** configura una sesión con el servidor tal y como se indica en el pase de la llamada o se define en los archivos de opciones.

El nombre del nodo del cliente, el nombre del propietario y los parámetros de la contraseña pasan a la llamada **dsmInitEx**. El nombre del propietario distingue entre mayúsculas y minúsculas, pero no lo hacen el nombre del nodo y la contraseña. Los nodos del cliente de aplicación deben estar registrados en el servidor antes de que se inicie la sesión.

Cada vez que un cliente de aplicación de API inicia una sesión con el servidor, el tipo de aplicación de cliente se registra con el servidor. Especifique siempre una abreviatura del sistema operativo para el valor de tipo de aplicación porque este valor se entra en el campo de plataforma en el servidor. La longitud máxima de la cadena es **DSM\_MAX\_PLATFORM\_LENGTH**.

La llamada de función **dsmInitEx** establece la sesión IBM Spectrum Protect con el archivo de configuración de la API y la lista de opciones del cliente de la aplicación. El cliente de la aplicación puede utilizar el archivo de configuración de la API y la lista de opciones para definir un número de opciones IBM Spectrum Protect. Estos valores modifican los valores definidos en los archivos de configuración del usuario durante la instalación. Los usuarios no pueden cambiar las opciones que defina el administrador. Si el cliente de la aplicación no cuenta con su propio archivo de configuración y lista de opciones, es posible configurar ambos parámetros en NULO. Para obtener más información acerca de los archivos de configuración, consulte el tema siguiente:

Conceptos básicos de los archivos de opciones y configuración

La llamada a función **dsmInitEx** establece la sesión de IBM Spectrum Protect, utilizando parámetros que permiten la verificación ampliada.

Compruebe la llamada de función **dsmInitEx** y el código de retorno de la información **dsmInitExOut**. El administrador ha cancelado la última sesión si el código de retorno es **ok (RC=ok)** y el código de retorno de la información (**infoRC**) es **DSM\_RC\_REJECT\_LASTSESS\_CANCELED**. Para finalizar la sesión actual de inmediato, llame a **dsmTerminate**.

La llamada **dsmQuerySessOptions** devuelve los mismos campos que la llamada **dsmQueryCliOptions**. La llamada se puede establecer únicamente dentro de una sesión. Los valores reflejan las opciones de cliente que son válidas durante esa sesión, desde los archivos de opciones así como cualquier modificación de la llamada **dsmInitEx**.

Una vez que inicia una sesión, la aplicación puede enviar una llamada a **dsmQuerySessInfo** con el fin de determinar los parámetros del servidor que están configurados en dicha sesión. Con esta llamada se devuelven a la aplicación elementos como el dominio de política y

los límites de transacción.

Finalizar una sesión con una llamada **dsmTerminate**. Cualquier conexión con el servidor está cerrada y todos los recursos asociados con esta sesión están liberados.

Para obtener un ejemplo del inicio y final de una sesión, consulte el tema siguiente:

Figura 1

El ejemplo define un número de variables globales y locales que se utilizan en llamadas a `dsmInitEx` y `dsmTerminate`. La llamada `dsmInitEx` toma un puntero a `dsmHandle` como parámetro, mientras la llamada `dsmTerminate` toma el `dsmHandle` como parámetro. El ejemplo en Figura 2 muestra los detalles de `rcApiOut`. La función `rcApiOut` llama a la función API `dsmRCMsg`, que traduce un código de retorno en un mensaje. La llamada `rcApiOut` imprime después el mensaje para el usuario. En la aplicación de ejemplo de la API se incluye una versión de `rcApiOut`. La función `dsmApiVersion` es una definición de tipo que se encuentra en el archivo de cabecera `dsmapihd.h`.

- Seguridad de sesión  
El sistema basado en la sesión de IBM Spectrum Protect tiene componentes de seguridad que permiten a las aplicaciones iniciar sesiones de forma segura. Estas medidas de seguridad prohíben el acceso no autorizado al servidor y ayudan a garantizar la integridad del sistema.
- Control del acceso a los archivos de contraseñas  
Para controlar el acceso a los archivos de contraseñas protegidos en sistemas UNIX y Linux, puede iniciar sesión como usuario autorizado y establecer la opción `passwordaccess` en `generate`.
- Crear un usuario administrativo con autorización de propietario de cliente  
Un usuario administrativo con autorización de propietario de cliente puede definir los parámetros en la llamada de función `dsmInitEx` para empezar las sesiones. Este usuario funciona como un "usuario administrativo" con autorización para restaurar y realizar copias de seguridad en los nodos definidos.

## Seguridad de sesión

---

El sistema basado en la sesión de IBM Spectrum Protect tiene componentes de seguridad que permiten a las aplicaciones iniciar sesiones de forma segura. Estas medidas de seguridad prohíben el acceso no autorizado al servidor y ayudan a garantizar la integridad del sistema.

Todas las sesiones que se inician en el servidor deben completar un proceso de inicio de sesión que requiere una contraseña. Cuando la contraseña se une al nombre del nodo del cliente, se garantiza la autorización adecuada al conectarse al servidor. El cliente de la aplicación proporciona esta contraseña al API para iniciar la sesión.

Existen dos métodos de proceso de contraseña disponibles: `passwordaccess=prompt` o `passwordaccess=generate`. Si utiliza la opción `passwordaccess=prompt`, debe incluir el valor de la contraseña en cada llamada **dsmInitEx**. O bien, es posible proporcionar el nombre de propietario y nodo en la llamada **dsmInitEx**.

Las contraseñas tienen periodos de caducidad asociados. Si una llamada **dsmInitEx** falla con un código de retorno de contraseña caducada (`DSM_RC_REJECT_VERIFIER_EXPIRED`), el cliente de la aplicación deben introducir la llamada `dsmChangePW` utilizando el manejador que devuelve **dsmInitEx**. Esto actualiza la contraseña antes de que la sesión se establezca correctamente. El ejemplo en Figura 3 demuestra el procedimiento para cambiar una contraseña utilizando **dsmChangePW**. El propietario de inicio de sesión debe utilizar un ID de usuario `root` o un ID de usuario autorizado para cambiar la contraseña.

El segundo método, `passwordaccess=generate`, cifra y almacena el valor de la contraseña en un archivo. El nombre de nodo y el nombre de propietario no se puede proporcionar en la llamada **dsmInitEx**, y se utilizan los valores predeterminados del sistema. Esto protege la seguridad del archivo de la contraseña. Cuando la contraseña caduca, el parámetro `generate` crea una nueva y actualiza el archivo de contraseña automáticamente.

Sugerencias:

1. Si dos máquinas físicas distintas tienen el mismo nombre de nodo IBM Spectrum Protect o se definen varias rutas en un nodo utilizando varias secciones del servidor, es posible que `passwordaccess=generate` sólo funcione en la sección que se utiliza primero después de la caducidad de la contraseña. Durante el primer contacto entre el cliente y el servidor, se solicita al usuario la misma contraseña para cada sección de servidor por separado y se almacena una copia de la contraseña para cada sección. Cuando caduca la contraseña, se genera una nueva para la sección que establece el primer contacto entre el cliente y el servidor. Todos los intentos posteriores de conectar mediante otras secciones de servidor fallarán, puesto que no existe enlace lógico entre sus copias de la contraseña anterior y la copia actualizada generada por la primera sección utilizada después de que caducara la contraseña. En este caso, debe actualizar las contraseñas antes de que caduquen o después de que caduquen con el fin de subsanar la situación del siguiente modo:
  - a. Ejecute **dsmadmc** y actualice la contraseña en el servidor.
  - b. Ejecute **dsmc -servername=stanza1** y utilice la nueva contraseña para generar una entrada adecuada.

- c. Ejecute **dsmc -servername=stanza2** y utilice la nueva contraseña para generar la entrada adecuada.
2. Para UNIX o Linux: solo el usuario root o el usuario autorizado pueden cambiar la contraseña cuando utilizan *passwordaccess=prompt*. Solo el usuario root o un usuario autorizado pueden iniciar el archivo de contraseña utilizando *passwordaccess=generate*.
- Restricción: Las opciones usuarios y grupos no se reconocen.

Una aplicación puede restringir el acceso de usuario por otros métodos, como por ejemplo configurar los filtros de acceso.

Las aplicaciones que utilizan varias conexiones IP a un único servidor IBM Spectrum Protect deben usar el mismo nombre de nodo y la contraseña de cliente de IBM Spectrum Protect para cada sesión. Siga estos pasos para habilitar esta compatibilidad:

1. Defina una sección del servidor IBM Spectrum Protect en el archivo dsm.sys.
2. En las conexiones que no utilizan la dirección IP predeterminada, especifique los valores de las opciones de la dirección *TCPserver* y *TCPport* en la llamada **dsmInitEx**.

Estos valores modifican la información de conexión del IP, pero la sesión utiliza el mismo nodo de la sección dsm.sys y la información de la contraseña.

Nota: Los nodos de un clúster comparten una única contraseña.

Figura 1. Un ejemplo de iniciar y finalizar una sesión

```
dsmApiVersionEx * apiApplVer;
char *node;
char *owner;
char *pw;
char *confFile = NULL;
char *options = NULL;
dsInt16_t rc = 0;
dsUInt32_t dsmHandle;
dsmInitExIn_t initIn;
dsmInitExOut_t initOut;
char *userName;
char *userNamePswd;

memset(&initIn, 0x00, sizeof(dsmInitExIn_t));
memset(&initOut, 0x00, sizeof(dsmInitExOut_t));
memset(&apiApplVer, 0x00, sizeof(dsmApiVersionEx));
apiApplVer.version = DSM_API_VERSION; /* Set the applications compile */
apiApplVer.release = DSM_API_RELEASE; /* time version. */
apiApplVer.level = DSM_API_LEVEL;
apiApplVer.subLevel = DSM_API_SUBLEVEL;

printf("Doing signon for node %s, owner %s, with password %s\n", node, owner, pw);

initIn.stVersion = dsmInitExInVersion;
initIn.dsmApiVersionP = &apiApplVer
initIn.clientNodeNameP = node;
initIn.clientOwnerNameP = owner ;
initIn.clientPasswordP = pw;
initIn.applicationTypeP = "Sample-API AIX";
initIn.configfile = confFile;
initIn.options = options;
initIn.userNameP = userName;
initIn.userPasswordP = userNamePswd;
rc = dsmInitEx(&dsmHandle, &initIn, &initOut);

if (rc == DSM_RC_REJECT_VERIFIER_EXPIRED)
{
    printf("*** Password expired. Select Change Password.\n");
    return(rc);
}
else if (rc)
{
    printf("*** Init failed: ");
    rcApiOut(dsmHandle, rc); /* Call function to print error message */
    dsmTerminate(dsmHandle); /* clean up memory blocks */
    return(rc);
}
}
```

Figura 2. Details of rcApiOut

```
void rcApiOut (dsUInt32_t handle, dsInt16_t rc)
{
    char *msgBuf ;
```



```

if ((msgBuf = (char *)malloc(DSM_MAX_RC_MSG_LENGTH+1)) == NULL)
{
    printf("Abort: Not enough memory.\n") ;
    exit(1) ;
}

dsmRCMsg(handle, rc, msgBuf);
printf("
free(msgBuf) ;
return;
}

```

Figura 3. An example of changing a password

```

printf("Enter your current password:");
gets(current_pw);
printf("Enter your new password:");
gets(new_pw1);
printf("Enter your new password again:");
gets(new_pw2);
/* If new password entries don't match, try again or exit. */
/* If they do match, call dsmChangePW. */

rc = dsmChangePW(dsmHandle,current_pw,new_pw1);
if (rc)
{
    printf("*** Password change failed. Rc =
}
else
{
    printf("*** Your new password has been accepted and updated.\n");
}
return 0;

```

## Control del acceso a los archivos de contraseñas

---

Para controlar el acceso a los archivos de contraseñas protegidos en sistemas UNIX y Linux, puede iniciar sesión como usuario autorizado y establecer la opción `passwordaccess` en `generate`.

### Procedimiento

---

Complete estos pasos cuando establezca `passwordaccess` en `generate`::

1. Grabe la aplicación con una llamada a `dsmSetUp` la cual pasa `argv[0]`. `argv[0]` contiene el nombre de la aplicación que llama al API. La aplicación puede ejecutar un usuario autorizado; no obstante, el administrador debe decidir el nombre de inicio de sesión del usuario autorizado.
2. Configure el bit de ID de usuario efectivo (bit S) para el ejecutable de aplicación en On. El propietario del archivo ejecutable de la aplicación podrá entonces convertirse en usuario autorizado y crear un archivo de contraseña, actualizar contraseñas y ejecutar aplicaciones. El propietario del archivo ejecutable debe ser el mismo que el ID de usuario que ejecuta el programa. En el siguiente ejemplo, `User` es `user1`, el nombre del archivo ejecutable de la aplicación `applA`, y `user1` tiene permisos de lectura y grabación en el directorio `/home/user1`. El archivo ejecutable `applA` tiene los siguientes permisos:

```
-rwsr-xr-x user1 group1 applA
```

3. Indique a los usuarios de la aplicación que utilicen el nombre de usuario autorizado para iniciar sesión. IBM Spectrum Protect verifica que el ID de inicio de sesión coincide con el propietario ejecutable de la aplicación antes de que permita acceder al archivo de contraseña protegido.
4. Configure la opción `passworddir` en el archivo `dsm.sys` para apuntar a un directorio en el que el usuario tenga permisos de lectura y grabación. Por ejemplo, escriba la siguiente línea en la stanza del servidor del archivo `dsm.sys`:

```
passworddir /home/user1
```

5. Cree el archivo de contraseña y asegúrese de que el usuario autorizado sea su propietario.
6. Inicie sesión como `user1` y ejecute `applA`.
7. Llame a `dsmSetUp` y pase a `argv`.

## Crear un usuario administrativo con autorización de propietario de cliente

---

Un usuario administrativo con autorización de propietario de cliente puede definir los parámetros en la llamada de función `dsmInitEx` para empezar las sesiones. Este usuario funciona como un "usuario administrativo" con autorización para restaurar y realizar copias de

seguridad en los nodos definidos.

## Procedimiento

---

Para recibir autorización de propietario de cliente, realice los pasos siguientes en el servidor:

1. Definir el usuario administrativo:

```
REGister Admin admin_name password
```

Donde:

- *admin\_name* es el nombre del usuario administrativo.
- *password* es la contraseña del administrador.

2. Definir el nivel de autorización. Los usuarios con autorización de política o sistema también tienen autorización de propietario de cliente.

```
Otorgar autorización admin_name classes authority node
```

Donde:

- *admin\_name* es el usuario administrativo.
- *classes* es el nodo.
- *authority* tiene uno de estos niveles de autorización:
  - *owner*: autorización de copia de seguridad y restauración para el nodo
  - *node*: nodo único
  - *domain*: grupo de nodos

3. Definir el acceso a un nodo único.

```
Register Node node_name password userid=ID de usuario
```

Donde:

- *node\_name* es el nodo del usuario del cliente
- *password* es la contraseña del nodo de usuario del cliente
- *ID de usuario* es el nombre de usuario administrativo

## Resultados

---

Cuando la aplicación utiliza el usuario administrativo, la función `dsmInitEx` se llama con los parámetros `userName` y `yuserNamePswd`.

```
dsmInitEx
    clientNodeName = NULL
    clientOwnerName = NULL
    clientPassword = NULL
    userName = 'administrative user' name
    userNamePswd = 'administrative user' password
```

Puede configurar la opción `passwordaccess` a `generate` o `prompt`. Con ambos parámetros, el valor `userNamePswd` inicia la sesión. Cuando se inicia la sesión, puede ocurrir cualquier proceso de restauración o copia de seguridad para ese nodo.

## ID y nombres de objeto

---

El servidor IBM Spectrum Protect es un servidor de almacenamiento de objeto cuya función principal es almacenar y recuperar de forma eficaz los objetos nombrados. El ID del objeto es único en cada objeto y permanece con el objeto durante toda la vida del objeto *excepto* cuando realiza exportaciones o importaciones.

Para cumplir estos requisitos IBM Spectrum Protect cuenta con dos áreas de almacenamiento principales, la base de datos y el almacén de datos.

- La base de datos contiene todos los metadatos, como el nombre o los atributos asociados con el objeto.
- El almacén de datos contiene los datos del objeto. El almacén de datos es una jerarquía de almacenamiento que define el administrador del sistema. Los datos se almacenan de forma eficaz y se administran en línea o en un medio externo, dependiendo de los costes y de las necesidades de acceso.

Cada uno de los objetos almacenado en el servidor tiene un nombre asociado. El cliente controla los siguientes componentes clave del nombre:

- Nombre de espacio de archivo
- Nombre de alto rango
- Nombre de bajo rango

- Tipo de objeto

Al tomar decisiones sobre cómo nombrar los objetos de una aplicación, es posible que necesite utilizar un nombre externo en los nombres de objeto completos para el usuario final. Concretamente, es posible que el usuario final necesite especificar el objeto en una sentencia de exclusión o inclusión cuando se ejecuta la aplicación. La sintaxis exacta del nombre del objeto en estas sentencias depende de la plataforma. En el sistema operativo de Windows, se utiliza en las sentencias de inclusión o exclusión la letra de la unidad asociada con el espacio de archivo en lugar del propio nombre del espacio del archivo.

Es posible que el valor del ID del objeto que se asignó cuando creó el objeto no sea el mismo que cuando realizó un proceso de restauración. Las aplicaciones deben guardar el nombre del objeto y a continuación realizar la consulta para obtener el ID del objeto actual antes de llevar a cabo una restauración.

- Nombre de espacio de archivo  
El nombre de espacio de archivo es uno de los componentes de almacenamiento más importantes. Puede ser el nombre de un sistema de archivos, unidad de disco o cualquier otro calificador de alto rango que agrupa datos relacionados.
- Nombres de alto y bajo rango  
Otros dos componentes del nombre del objeto son el calificador de nombre de alto rango y el calificador de nombre de bajo rango. El calificador de nombre de alto rango es la ruta del directorio al que pertenece el objeto, y el nombre del calificador de bajo rango es el nombre real del objeto en dicha ruta de directorio.
- Tipo de objeto  
El tipo de objeto define el objeto como un archivo o un directorio. Un archivo es un objeto que contiene tanto atributos como datos binarios, y un directorio es un objeto que contiene sólo atributos.

## Nombre de espacio de archivo

---

El nombre de espacio de archivo es uno de los componentes de almacenamiento más importantes. Puede ser el nombre de un sistema de archivos, unidad de disco o cualquier otro calificador de alto rango que agrupa datos relacionados.

IBM Spectrum Protect utiliza el espacio de archivo para identificar el sistema de archivo o la unidad del disco en el que se encuentran los datos. De este modo, es posible llevar a cabo acciones en todas las entidades de un espacio de objeto como consultar todos los objetos dentro de un espacio de archivo específico. Como el espacio de archivos es un componente tan importante del convenio de denominación de IBM Spectrum Protect, utilice llamadas especiales para registrar, actualizar, consultar o suprimir espacios de archivos.

El servidor también tiene mandatos administrativos para consultar los espacios de archivo en un nodo determinado en el almacenamiento IBM Spectrum Protect, y eliminarlos si es necesario. Todos los datos que almacena el cliente de la aplicación deben tener un nombre de espacio asociado. Seleccione el nombre cuidadosamente para agrupar datos similares en el sistema.

Un cliente de aplicación debe seleccionar nombres de espacio de archivos distintos de los nombres que utiliza un cliente de archivado/copia de seguridad, con el fin de evitar interferencias. El cliente de la aplicación debe publicar los nombres de espacio de archivo para que los usuarios puedan identificar los objetos en sentencias de inclusión y exclusión si fuera necesario.

Nota: En plataformas Windows, una letra de unidad está asociada con un espacio de archivo. Cuando registra o actualiza un espacio de archivo, debe proporcionar una letra de unidad. Debido a que la lista de inclusión/exclusión hace referencia a la letra de unidad, debe anotar cada letra y su espacio de archivo asociado. En el programa de ejemplo dapismp, la letra de unidad se configura en "G" de forma predeterminada.

Consulte Crear y ejecutar la aplicación de API de ejemplo para obtener más información acerca de los programas de ejemplo.

## Nombres de alto y bajo rango

---

Otros dos componentes del nombre del objeto son el calificador de nombre de alto rango y el calificador de nombre de bajo rango. El calificador de nombre de alto rango es la ruta del directorio al que pertenece el objeto, y el nombre del calificador de bajo rango es el nombre real del objeto en dicha ruta de directorio.

Cuando el nombre de espacio de archivo, nombre de alto rango y nombre de bajo rango están concatenados, deben formar un nombre correcto sintácticamente en el sistema operativo en el que se ejecuta el cliente. No es necesario que el nombre exista como un objeto en el sistema o que se parezca a los datos del sistema de archivos local. No obstante, el nombre debe cumplir con las normas de nomenclatura estándar para que se procese correctamente en las llamadas **dsmBindMC**. Consulte Conceptos básicos sobre archivar y realizar copias de seguridad de los objetos para consultar las normas de nomenclatura relacionadas con la gestión de políticas.

## Tipo de objeto

---

El tipo de objeto define el objeto como un archivo o un directorio. Un archivo es un objeto que contiene tanto atributos como datos binarios, y un directorio es un objeto que contiene sólo atributos.

Tabla 1 muestra lo que el cliente de aplicación codifica para los nombres de objeto por plataforma.

Tabla 1. Ejemplos de nombre de objeto de aplicación por plataforma

Plataforma	Código de cliente por nombre de objeto
UNIX o Linux	/myfs/highlev/lowlev
Windows	"myvol\\highlev\\lowlev" Nota: En una plataforma Windows, una barra invertida doble se convierte en una barra invertida única porque una barra invertida es el carácter del espacio. Los nombres de espacio de archivo empiezan con una barra invertida en la plataforma UNIX o Linux, pero no empiezan con una barra invertida en la plataforma Windows.

## Acceder a objetos como propietario de sesión

Cada objeto tiene un nombre de propietario asociado. Las normas que determinan a qué objetos se accede dependen de qué nombre de propietario se utilice cuando se inicia una sesión. Utilice este valor de propietario de sesión para controlar el acceso al objeto.

El propietario de la sesión se configura durante la llamada a **dsmInitEx** en el parámetro *clientOwnerNameP*. Si inicia una sesión con el nombre de propietario **dsmInitEx** de *NULL* y utiliza *passwordaccess=prompt*, dicho propietario de sesión se maneja con la autoridad de la sesión (usuario root o autorizado). Esto también es verdadero si inicia sesión con un ID de usuario root o un ID de usuario autorizado y utiliza *passwordaccess=generate*. Durante una sesión iniciada de esta manera, puede realizar cualquier acción en un objeto propiedad de este nodo independientemente del propietario real de dicho objeto.

Si una sesión se inicia con un nombre de propietario específico, la sesión sólo puede realizar acciones en objetos que tienen un nombre de propietario de objeto asociado. Los archivados o copias de seguridad en el sistema deben tener este nombre de propietario asociado con ellos. Todas las consultas realizadas devuelven sólo los valores que tienen este nombre de propietario asociado. El valor del propietario del objeto se configura durante la llamada **dsmSendObj** en el campo **Owner** de la estructura **ObjAttr**. El nombre de propietario es sensible a mayúsculas y minúsculas. Tabla 1 resume las condiciones bajo las cuales un usuario tiene acceso a un objeto.

Tabla 1. Resumen de acceso de usuario a objetos

Propiedad de sesión	Propiedad de objeto	Acceso de usuario
NULO (raíz, propietario de sistema)	" " (cadena vacía)	Sí
NULO	Nombre específico	Sí
Nombre específico	" " (cadena vacía)	No
Nombre específico	Mismo nombre	Sí
Nombre específico	Nombre diferente	No

## Acceder a objetos de nodos y propietarios

Hay tres llamadas de función compatibles con distintos nodos y propietarios en la misma plataforma: **dsmSetAccess**, **dsmDeleteAccess**, y **dsmQueryAccess**. Estas funciones, junto con las opciones de cadena *-fromnode* y *-fromowner* que se pasan en **dsmInitEx**, permiten una consulta a través de distintos nodos, así como restaurar y recuperar procesos a través de la API.

Por ejemplo, Usuario A en nodo A utiliza la llamada de función **dsmSetAccess** para dar acceso a su copia de seguridad bajo el espacio de archivo /db al Usuario B del Nodo B. La regla de acceso aparece como:

ID	Tipo	Nodo	Usuario	Vía de acceso
1	Copia de seguridad	Nodo B	Usuario B	/db/*/*

Cuando el usuario B inicia sesión en Nodo B, la cadena de opción a **dsmInitEx** es:

```
-fromnode=nodeA -fromowner=userA
```

Estas opciones están configuradas para esta sesión. Todas las consultas acceden a los espacios del archivo, y a los archivos del nodo A. No están permitidas las copias de seguridad y los archivados. Sólo los procesos de consulta, restauración y recuperación están permitidos en los espacios de archivo para los que el Usuario B tiene acceso. Si la aplicación intenta ejecutar cualquier operación utilizando **dsmBeginTxn** (para ejemplos, copias de seguridad o actualizaciones) mientras la sesión está iniciada con una opción *-fromnode* o *-fromowner*, entonces **dsmBeginTxn** falla con el código de retorno **DSM\_RC\_ABORT\_NODE\_NOT\_AUTHORIZED**. Consulte las llamadas de función individuales y **dsmInitEx** para obtener más información.

Consejo: En UNIX y Linux es posible especificar *-fromowner=root* en la cadena de opción que pasa a la llamada de función **dsmInitEx**. Esto permite a los usuarios que no sean de raíz acceder a archivos propiedad de la raíz si se lleva a cabo un acceso.

Utilice la opción *asnodename* en la cadena de opción **dsmInitEx** con la función adecuada para realizar copias de seguridad, archivados, restauraciones, recuperaciones, consultas o eliminaciones de datos bajo el nombre del nodo de destino en el servidor IBM Spectrum Protect. Consulte Soporte de copia de seguridad de varios nodos con el proxy de nodo de cliente para obtener más información sobre cómo habilitar esta opción.

## Gestionar espacios de archivos

Debido a que el espacio de archivos es tan importante para la operación del sistema, se utiliza un grupo de llamadas por separado para registrar, actualizar y eliminar los identificadores de espacio de archivos. Antes de almacenar cualquier objeto asociado con un espacio de archivo en el sistema, debe primero registrar el espacio de archivo con IBM Spectrum Protect.

Utilice la llamada *dsmRegisterFS* para realizar esta tarea. Para obtener más información acerca de los nombres de objeto e ID, consulte ID y nombres de objeto.

El identificador del espacio de archivo es el calificador en el nivel superior de la jerarquía del nombre de tres partes. Agrupar los datos relacionados dentro de un espacio de archivo facilita la gestión de dichos datos. Por ejemplo, el cliente de la aplicación o el administrador del servidor IBM Spectrum Protect pueden eliminar un espacio de archivo y todos los objetos dentro de dicho espacio de archivo.

Los espacios de archivos también permiten que el cliente de aplicaciones proporcione información sobre el espacio de archivos al servidor que el servidor pueda luego consultar. Esta información se devuelve en la consulta en la estructura *qryRespFSData* e incluye la siguiente información de sistema de archivos:

Tipo	Definición
<i>fstype</i>	El tipo de espacio de archivo. Este campo es una cadena de caracteres que configura el cliente de la aplicación.
<i>fsAttr[platform].fsInfo</i>	Un campo de información de cliente que se utiliza para los datos específicos del cliente.
<i>capacity</i>	La cantidad de espacio total en el espacio del archivo.
<i>ocupación</i>	La cantidad de espacio que se ocupa en el espacio de archivos.
<i>backStartDate</i>	El indicador de hora de cuándo se inició la última copia de seguridad (configurado al enviar una llamada <i>dsmUpdateFS</i> ).
<i>backCompleteDate</i>	El indicador de hora de cuándo se finalizó la última copia de seguridad (configurado al enviar una llamada <i>dsmUpdateFS</i> ).

El uso de la capacidad y de la ocupación depende del cliente de la aplicación. Es posible que algunas aplicaciones no necesiten información acerca del tamaño del espacio de archivos, en cuyo caso estos campos pueden de forma predeterminada ser 0. Para obtener más información sobre la consulta de espacios de archivos, consulte Consultas para el sistema IBM Spectrum Protect.

Después de registrar un espacio de archivo en el sistema, es posible archivar o realizar copias de seguridad de los objetos en cualquier momento. Para actualizar los campos de capacidad y de ocupación del espacio de archivos después de una operación de archivado y copia de seguridad, llame a *dsmUpdateFS*. Esta llamada asegura que los valores para la ocupación y capacidad del sistema de archivos son actuales. También es posible actualizar los campos *fsinfo*, *backupstart*, y *backupcomplete*.

Si desea supervisar las últimas fechas de copia de seguridad, entre una llamada *dsmUpdateFS* antes de iniciar la copia de seguridad. Establezca la acción de actualización en *DSM\_FSUPD\_BACKSTARTDATE*. Esto fuerza al servidor la configuración del campo *backStartDate* del espacio de archivo con la hora actual. Tras finalizar la copia de seguridad para ese espacio de archivo, introduzca una llamada *dsmUpdateFS* con la acción de actualización configurada en *DSM\_FSUPD\_BACKCOMPLETEDATE*. Esta llamada crea una indicación de fecha y hora al final de la copia de seguridad.

Si un espacio de archivo ya no es necesario, puede borrarlos con el mandato *dsmDeleteFS*. En un sistema operativo UNIX o Linux, solo el usuario *root* o los usuarios autorizados pueden suprimir los espacios de archivos.

Los ejemplos en Figura 1 demuestran cómo utilizar las tres llamadas de espacio de archivo de UNIX o Linux. Para obtener un ejemplo de cómo utilizar las tres llamadas de espacio de archivos de Windows, consulte el código de programa de ejemplo instalado en el sistema.

Figura 1. Un ejemplo de cómo trabajar con espacios de archivo, Parte 1

```
/* Register the file space if it has not already been done. */

dsInt16      rc;
regFSData    fsData;
char         fsName[DSM_MAX_FSNAME_LENGTH];
char         smpAPI[] = "Sample-API";

strcpy(fsName, "/home/tallan/text");
```

```

memset(&fsData,0x00,sizeof(fsData));
fsData.stVersion = regFSDDataVersion;
fsData.fsName = fsName;
fsData.fsType = smpAPI;
strcpy(fsData.fsAttr.unixFSAttr.fsInfo,"Sample API FS Info");
fsData.fsAttr.unixFSAttr.fsInfoLength =
    strlen(fsData.fsAttr.unixFSAttr.fsInfo) + 1;
fsData.occupancy.hi=0;
fsData.occupancy.lo=100;
fsData.capacity.hi=0;
fsData.capacity.lo=300;

rc = dsmRegisterFS (dsmHandle,fsData);
if (rc == DSM_RC_FS_ALREADY_REGED) rc = DSM_RC_OK; /* already done */
if (rc)
{
    printf("Filespace registration failed: ");
    rcApiOut(dsmHandle, rc);
    free(bkup_buff);
    return (RC_SESSION_FAILED);
}

```

Figura 2. Un ejemplo de cómo trabajar con espacios de archivo, Parte 2

```

/* Update the file space. */

dsmFSUpd    updFilespace;          /* for update FS */

updFilespace.stVersion = dsmFSUpdVersion;
updFilespace.fsType = 0;           /* no change */
updFilespace.occupancy.hi = 0;
updFilespace.occupancy.lo = 50;
updFilespace.capacity.hi = 0;
updFilespace.capacity.lo = 200;
strcpy(updFilespace.fsAttr.unixFSAttr.fsInfo,
    "My update for filespace");
updFilespace.fsAttr.unixFSAttr.fsInfoLength =
    strlen(updFilespace.fsAttr.unixFSAttr.fsInfo);

updAction = DSM_FSUPD_FSINFO |
    DSM_FSUPD_OCCUPANCY |
    DSM_FSUPD_CAPACITY;

rc = dsmUpdateFS (handle,fsName,&updFilespace,updAction);
printf("dsmUpdateFS rc=%d\n", rc);

```

Figura 3. Un ejemplo de cómo trabajar con espacios de archivo, Parte 3

```

/* Delete the file space. */

printf("\nDeleting file space
rc = dsmDeleteFS (dsmHandle,fsName,DSM_REPOS_ALL);
if (rc)
{
    printf(" FAILED!!! ");
    rcApiOut(dsmHandle, rc);
}
else printf(" OK!\n");

```

## Asociar objetos con clases de gestión

---

Una función principal de IBM Spectrum Protect es el uso de políticas (clases de gestión) para definir cómo se almacenan y gestionan los objetos en el almacenamiento IBM Spectrum Protect. Un objeto se asocia con una clase de gestión cuando se archiva o se realiza una copia de seguridad.

Esta clase de gestión determina:

- Cuántas versiones del objeto se guardan si se hacen copias de seguridad de éste
- Cuánto tiempo se guardan las copias archivadas
- Dónde se introducen los objetos en la jerarquía de almacenamiento del servidor

Las clases de gestión consisten tanto en grupos de copias de seguridad como en grupos de copias de archivados. Un grupo de copia es un conjunto de atributos que definen las políticas de gestión de un objeto que se va a archivar o al que se le va a realizar una copia de

seguridad. Si se está realizando una operación de copia de seguridad, se aplican los atributos en el grupo de la copia de seguridad. Si se está realizando un archivado, se aplican los atributos del grupo de la copia de archivado.

El grupo de la copia de archivado o copia de seguridad en una clase de gestión particular puede estar vacío o ser NULO. Si un objeto está vinculado a un grupo de copia de seguridad NULO, no es posible realizar una copia de seguridad a dicho objeto. Si un objeto está vinculado al grupo de copia de archivado NULO, no es posible archivar dicho objeto.

Como el uso de una política es un componente muy importante de IBM Spectrum Protect, la API requiere que a todos los objetos enviados al servidor se les asigne primero una clase de gestión mediante la llamada de **dsmBindMC**. Con el software de IBM Spectrum Protect, puede usar una lista de inclusión-exclusión que afecte al enlace de clase de gestión. La llamada **dsmBindMC** utiliza la lista de inclusión/exclusión para realizar vinculaciones de clase de gestión.

Las sentencias de inclusión pueden asociar una clase de gestión específica con una copia de seguridad o archivado. Las sentencias de exclusión impiden que se realicen copias de seguridad de los objetos pero no archivados.

La API requiere que se llame a **dsmBindMC** antes de realizar una copia de seguridad o archivar un objeto. La llamada **dsmBindMC** devuelve una estructura mcBindKey que contiene información sobre la clase de gestión y los grupos de copia asociados con el objeto. Compruebe el destino del grupo de copia antes de proceder con un envío. Cuando envía varios objetos en una única transacción, deben tener el mismo destino de grupo de copia. La llamada de función **dsmBindMC** devuelve la siguiente información:

Tabla 1. Información devuelta en la llamada dsmBindMC

Información	Descripción
Clase de gestión	El nombre de la clase de gestión que se vinculó al objeto. El cliente de la aplicación puede enviar la llamada <b>dsmBeginQuery</b> con el fin de determinar todos los atributos de esta clase de gestión.
Grupo de copia de seguridad	Informa si existe un grupo de copia de seguridad para esta clase de gestión. Si se realiza una operación de copia de seguridad y no existe un grupo de copias de seguridad, este objeto no se podrá enviar a almacenamiento. Recibe un código de error si intenta enviarlo con la llamada <b>dsmSendObj</b> .
Destino de copia de seguridad	Este campo identifica la agrupación de almacenamiento a la que se envían los datos. Si está realizando varias transacciones de copia de seguridad de un objeto, todos los destinos de la copia dentro de dicha transacción deben ser los mismos. Si un objeto tiene un destino de copia distinto que los objetos anteriores en la transacción, finalice la transacción actual y empiece una transacción nueva antes de enviar el objeto. Recibe un código de error si intenta enviar objetos a distintos destinos de copia dentro de la misma transacción.
Grupo de copias archivadas	Le informa si un grupo de copias archivadas existe para esta clase de gestión. Si se está realizando una operación de archivado y no existe un grupo de copias de archivadas, este objeto no podrá enviarse a almacenamiento. Recibe un código de error si intenta enviarlo utilizando la llamada <b>dsmSendObj</b> .
Destino de copias archivadas	Este campo identifica la agrupación de almacenamiento a la que se envían los datos. Si está realizando varias transacciones de objetos archivados, todos los destinos de la copia dentro de dicha transacción deben ser los mismos. Si un objeto tiene un destino de copia distinto que los objetos anteriores en la transacción, finalice la transacción actual y empiece una transacción nueva antes de enviar el objeto. Recibe un código de error si intenta enviar objetos a distintos destinos de copia dentro de la misma transacción.

Las copias de seguridad de un objeto se pueden revincular a distintas clases de gestión si se realiza una copia de seguridad subsiguiente con el mismo el mismo nombre de objeto que utiliza una clase de gestión distinta a la del original. Por ejemplo, si realiza una copia de seguridad del Objeto A y lo vincula a Mgmtclass1, y más tarde hace una copia de seguridad del Objeto A y lo vincula a Mgmtclass2, la copia de seguridad más actual revincula las copias inactivas a Mgmtclass2. Los parámetros definidos en Mgmtclass2 controlan ahora todas las copias. No obstante, los datos no se mueven si el destino es distinto.

También puede revincular las copias de seguridad a distintas clases de gestión utilizando la llamada **dsmUpdateObj** o **dsmUpdateObjEx** con la acción DSM\_BACKUPD\_MC.

- Clases de gestión de consulta  
Las aplicaciones pueden consultar las clases de gestión con el fin de determinar qué clases de gestión son posibles en un nodo determinado y qué atributos se encuentran en la clase de gestión.

**Referencia relacionada:**

Opción Deduplication

## Retener y liberar la caducidad/eliminación

Puede retener la eliminación y la caducidad de objetos de archivado en respuesta a una acción pendiente o en curso que requiere que se retengan los datos particulares. En caso de que se inicie una acción que requiera el acceso a los datos, dichos datos deben estar

disponibles hasta que la acción haya concluido y ya no sea necesario el acceso a los datos como parte del proceso. Después de determinar que la suspensión ya no se requiere, se reinicia la eliminación y caducidad normal de acuerdo al periodo de retención original.

## Antes de empezar

---

Verifique el servidor tiene licencia emitiendo una llamada `dsmRetentionEvent` de prueba:

1. Consulte un objeto que desee retener y obtenga el ID.
2. Emita el `dsmBeginTxn`, `dsmRetentionEvent` con `Hold`, y `dsmEndTxn`.
3. Si el servidor no tiene licencia, recibe un voto de cancelación con el código de razón de `DSM_RC_ABORT_LICENSE_VIOLATION`.

Restricciones:

1. No es posible emitir más de una llamada `dsmRetentionEvent` en una única transacción.
2. No es posible emitir una retención en un objeto que ya está retenido.

## Procedimiento

---

1. Para retener los objetos, siga estos pasos:
    - a. Consulte al servidor todos los objetos que desea retener. Obtenga el ID de objeto de cada uno de ellos.
    - b. Emita una llamada `dsmBeginTxn`, a continuación emita una llamada `dsmRetentionEvent` con la lista de objetos, seguido de una llamada `dsmEventType: eventHoldObj`. Si el número de objetos excede el valor de `maxObjPerTxn`, utilice varias transacciones.
    - c. Utilice `qryRespArchiveData` en la llamada de función `dsmGetNextQObj` para confirmar que los objetos están retenidos. Compruebe el valor de `objHeld` en `qryRespArchiveData`.
  2. Para liberar los objetos de la retención, siga estos pasos:
    - a. Consulte al servidor todos los objetos que desea liberar. Obtenga el ID de objeto de cada uno de ellos.
    - b. Emita una llamada `dsmBeginTxn`, a continuación emita una llamada `dsmRetentionEvent` con la lista de objetos, seguido de una llamada `dsmEventType: eventReleaseObj`. Si el número de objetos excede el valor de `maxObjPerTxn`, utilice varias transacciones.
    - c. Utilice la respuesta `qryRespArchiveData` en la llamada de función `dsmGetNextQObj` para confirmar si los objetos se han liberado de la retención. Compruebe el valor de `objHeld` en `qryRespArchiveData`.
- Protección de retención de datos archivados  
Los datos que están bajo el control de IBM Spectrum Protect no se pueden modificar mediante agentes no autorizados como, por ejemplo, una persona o un programa. Esta protección se amplía para evitar la supresión de datos, como objetos de archivo, por cualquier agente antes de la caducidad del período de retención.

## Consultas para el sistema IBM Spectrum Protect

---

La API cuenta con varias consultas, como la consulta de clase de gestión, que las aplicaciones pueden utilizar.

## Procedimiento

---

Todas las consultas que se utilizan la llamada `dsmBeginQuery` siguen estos pasos:

1. Envíe la llamada `dsmBeginQuery` con el tipo de consulta apropiado:
  - Copia de seguridad
  - Archivado
  - Objetos de copia de seguridad activos
  - Espacio de archivos
  - Clase de gestión

La llamada `dsmBeginQuery` informa a la API del formato de los datos que se devuelve desde el servidor. Los campos apropiados se pueden colocar en la estructura de datos que pasan por las llamadas `dsmGetNextQObj`. La llamada de inicio de consulta también permite al cliente de la aplicación configurar el alcance de la consulta al especificar adecuadamente los parámetros en la llamada de inicio de consulta.

Restricción: En sistemas de UNIX o Linux, solo el usuario raíz puede consultar los objetos de archivado y copia de seguridad. Este tipo de consulta se conoce como "fast path".

2. Introduzca la llamada `dsmGetNextQObj` para obtener cada uno de los registros de la consulta. Esta llamada pasa un almacenamiento intermedio lo suficientemente grande para retener los datos que devuelve la consulta. Cada tipo de consulta tiene una estructura de datos correspondiente para los datos que se devuelven. Por ejemplo, el tipo de consulta de copia de seguridad tiene una estructura `qryRespBackupData` asociada que se completa cuando se envía la llamada `dsmGetNextQObj`.
3. La llamada `dsmGetNextQObj` normalmente devuelve uno de los siguientes códigos:
  - `DSM_RC_MORE_DATA`: vuelva a enviar la llamada `dsmGetNextQObj` de nuevo.



- DSM\_RC\_FINISHED: no hay más datos. Envíe la llamada dsmEndQuery.
4. Envíe la llamada dsmEndQuery. Cuando se recuperan todos los datos o más datos que no son necesarios, escriba la llamada de dsmEndQuery para finalizar el proceso de consulta. La API vacía los datos que quedan de la cadena de consulta y libera los recursos que se utilizaron para la consulta.

## Resultados

Figura 1 muestra el diagrama de estado para las operaciones de consulta.

Figura 1. Diagrama de estado para consultas generales

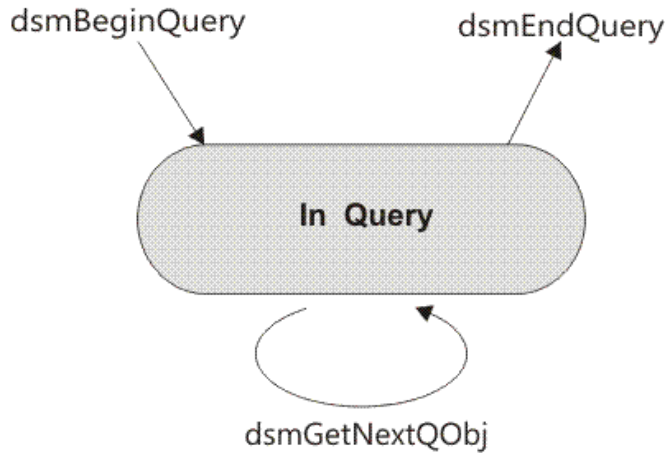
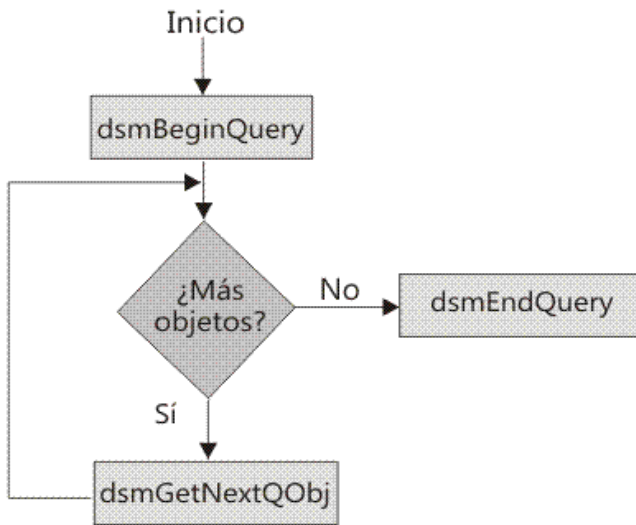


Figura 2 muestra el diagrama de flujo de las operaciones de consulta.

Figura 2. Diagrama de flujo de las consultas generales



- Ejemplo de consultas del sistema  
En este ejemplo una consulta de clase de gestión copia los valores de todos los campos en los grupos de copia de seguridad y copia archivada para una clase de gestión específica.

## Eficiencia del servidor

Utilice estas directrices cuando recupere o envíe objetos al servidor de IBM Spectrum Protect.

- Cuando recupere objetos del servidor de IBM Spectrum Protect, siga estas directrices:
  - Recupere los dos datos en el orden de restauración que proporciona el servidor de IBM Spectrum Protect. El orden de restauración es especialmente importante para los dispositivos de cinta, porque la recuperación de datos sin ordenar puede provocar rebobinados y montados en la cinta.
  - Incluso cuando los datos se almacenan en un dispositivo de disco, puede ahorrar tiempo cuando las recuperaciones están ordenadas.
  - Realice todo el trabajo que sea posible en una sola sesión del servidor de IBM Spectrum Protect.
  - No inicie y detenga sesiones múltiples.

- Cuando envíe objetos al servidor de IBM Spectrum Protect, siga estas directrices:
  - Envíe múltiples objetos en una sola transacción.
  - Evite enviar un objeto por transacción, especialmente cuando los datos se envíen directamente a un dispositivo de cinta. Parte de la transacción del dispositivo de cinta consiste en asegurar que los datos de los almacenamientos intermedios de la memoria de acceso aleatorio (RAM) se graben en el soporte.

**Conceptos relacionados:**

Seleccionar y ordenar objetos por orden de restauración

**Información relacionada:**

Iniciar o finalizar una sesión

## Enviar datos a un servidor

---

La API permite que los clientes de aplicación envíen datos, objetos nombrados y sus datos asociados al almacén del servidor IBM Spectrum Protect.

Consejo: Es posible hacer una copia de seguridad o archivar los datos. Realice todas las operaciones de envía dentro de una misma transacción.

- El modelo de transacción  
Todos los datos enviados al almacenamiento de IBM Spectrum Protect durante una operación de archivado o copia de seguridad se realiza en una transacción. Un modelo de transacción proporciona un nivel alto de integridad de los datos, pero impone algunas restricciones que un cliente de aplicación debe tener en cuenta.
- Agregación de archivo  
los servidores IBM Spectrum Protect utilizan una función llamada agregación de archivo. Con la agregación de archivo, todos los objetos que se envían en una misma transacción se almacenan juntos, lo cual ahorra espacio y mejora el rendimiento. Aún así es posible consultar y restaurar los objetos de forma separada.
- Transferencia de datos sin LAN  
La API puede sacar provecho de la transferencia de datos sin LAN si la opción **dsmSetUp** para las lecturas múltiples es ON. La API devuelve la existencia de un destino sin LAN en la estructura de respuesta **Query Mgmt Class archDetailCG** o en el campo **backupDetailCG bLanFreeDest**.
- Operaciones de grabación simultánea  
Puede configurar las agrupaciones del almacenamiento de servidor IBM Spectrum Protect para grabar simultáneamente en una agrupación de almacenamiento primario y copiar la agrupación o agrupaciones de almacenamiento de copias durante una copia de seguridad o archivado. Utilice esta configuración para crear múltiples copias del objeto.
- Mejora del rendimiento de la API  
Es posible utilizar las opciones de cliente `tcpbufsize` y `tcpnodelay` y el parámetro API `DataBlk` con el fin de mejorar el rendimiento API.

## El modelo de transacción

---

Todos los datos enviados al almacenamiento de IBM Spectrum Protect durante una operación de archivado o copia de seguridad se realiza en una transacción. Un modelo de transacción proporciona un nivel alto de integridad de los datos, pero impone algunas restricciones que un cliente de aplicación debe tener en cuenta.

Iniciar una transacción con una llamada a **dsmBeginTxn** o finalizar una transacción con una llamada a **dsmEndTxn**. Una transacción única es una acción atómica. Los datos que se envían dentro de los límites de una transacción están comprometidos al sistema al final de la transacción o se devuelven si la transacción finaliza de forma prematura.

Las transacciones pueden consistir de envíos únicos de objetos o de múltiples envíos de objetos. Para mejorar el rendimiento del sistema al disminuir la actividad del sistema, envíe objetos pequeños en una transacción múltiple de objetos. El cliente de la aplicación determina si las transacciones únicas o múltiples son adecuadas.

Envíe todos los objetos dentro de una transacción múltiple de objetos al mismo destino de la copia. Si necesita enviar un objeto a distintas ubicaciones que el objeto anterior, finalice la transacción actual e inicie una nueva. Dentro de la transacción nueva, puede enviar el objeto al destino de copia nuevo.

Nota: No se comprueba la coherencia del destino de la copia a los objetos que no contienen ningún bit de datos (*sizeEstimate=0*).

IBM Spectrum Protect limita el número de objetos que se pueden enviar a una transacción de objeto múltiple. Para encontrar este límite, llame a **dsmQuerySessInfo** y examine el campo **maxObjPerTxn**. Este campo muestra el valor de la opción *TXNGroupmax* que está configurada en el servidor.

El cliente de la aplicación debe hacer un seguimiento de los objetos enviados dentro de una transacción para llevar a cabo reintentos de proceso o procesos de error si la transacción finaliza de forma prematura. Tanto el servidor como el cliente pueden detener una

transacción en cualquier momento. El cliente de la aplicación debe estar preparado para gestionar finalizaciones de transacción inesperadas que no se iniciaron.

## Agregación de archivo

los servidores IBM Spectrum Protect utilizan una función llamada agregación de archivo. Con la agregación de archivo, todos los objetos que se envían en una misma transacción se almacenan juntos, lo cual ahorra espacio y mejora el rendimiento. Aún así es posible consultar y restaurar los objetos de forma separada.

Para utilizar esta función todos los objetos de una transacción deben tener el mismo nombre de espacio de archivo. Si el nombre de espacio de archivo cambia dentro de una transacción, el servidor cierra el objeto agregado existente y empieza uno nuevo.

## Transferencia de datos sin LAN

La API puede sacar provecho de la transferencia de datos sin LAN si la opción **dsmSetUp** para las lecturas múltiples es ON. La API devuelve la existencia de un destino sin LAN en la estructura de respuesta **Query Mgmt Class archDetailCG** o en el campo **backupDetailCG bLanFreeDest**.

Puede utilizar operaciones sin LAN en plataformas que están soportadas por el agente de almacenamiento. Se excluye la plataforma Macintosh.

En las siguientes estructuras de salida se proporciona información sin LAN. La estructura (**dsmEndGetDataExOut\_t**) de **dsmEndGetData** incluye el campo **totalLFBytesRecv**. Este es el número total de bytes sin LAN que se reciben. La estructura de salida (**dsmEndSendObjExOut\_t**) de **dsmEndSendObjEx** incluye el campo **totalLFBytesSent**. Este es el número total de bytes sin LAN que se enviaron.

### Información relacionada:

[Movimiento de datos sin LAN: descripción general del agente de almacenamiento](#)

## Operaciones de grabación simultánea

Puede configurar las agrupaciones del almacenamiento de servidor IBM Spectrum Protect para grabar simultáneamente en una agrupación de almacenamiento primario y copiar la agrupación o agrupaciones de almacenamiento de copias durante una copia de seguridad o archivado. Utilice esta configuración para crear múltiples copias del objeto.

Si una operación de grabación simultánea falla, el código de retorno en la función **dsmEndTxn** puede ser **DSM\_RC\_ABORT\_STGPOOL\_COPY\_CONT\_NO**, lo cual indica que la grabación a una de las agrupaciones de almacenamiento ha fallado, y la opción de agrupación de almacenamiento **COPYCONTINUE** de IBM Spectrum Protect se ha establecido en **NO**. La aplicación termina y el administrador del servidor de IBM Spectrum Protect debe resolver el problema.

Para obtener más información sobre cómo configurar las operaciones de grabación simultánea, consulte la documentación del servidor de IBM Spectrum Protect.

## Mejora del rendimiento de la API

Es posible utilizar las opciones de cliente **tcpbuffsize** y **tcpnodelay** y el parámetro API **DataBlk** con el fin de mejorar el rendimiento API.

Tabla 1 describe las acciones que puede realizar para mejorar el rendimiento de la API.

Tabla 1. Opciones de archivado/copia de seguridad y el parámetro API que mejora el rendimiento

Opciones de cliente de archivado/copia de seguridad	Descripción
tcpbuffsize	Especifica el tamaño de almacenamiento intermedio de TCP. El valor predeterminado es 31 KB. Para mejorar el rendimiento, establezca el valor en 32 KB.
tcpnodelay	Especifica si se deben enviar buffers pequeños al servidor en lugar de retenerlos. Para mejorar el rendimiento, establezca esta opción en <b>yes</b> para todas las plataformas. Esta opción es válida sólo para Windows y AIX.
parámetro API	Descripción

Opciones de cliente de archivado/copia de seguridad	Descripción
DataBlk	Este parámetro se utiliza con la llamada de función <b>dsmSendData</b> con el fin de determinar el tamaño de almacenamiento intermedio de la aplicación. Para obtener mejores resultados, establezca el parámetro como un valor múltiplo del valor <i>tcpbuffsize</i> que se especifica con <i>tcpbuffsize</i> menos 4 bytes. Por ejemplo, establezca un valor de 28 para este parámetro cuando el valor de <i>tcpbuffsize</i> se establece en 32 KB.

Cada llamada `dsmSendData` es síncrona y no regresa hasta que los datos transferidos a la API en `dataBlkPtr` se vacían a la red. La API añade una actividad de 4 bytes a cada almacenamiento intermedio de transacción que se coloca en la red.

Por ejemplo, cuando el tamaño del almacenamiento intermedio de la transacción es de 32 KB y el tamaño del almacenamiento intermedio `DataBlk` de la aplicación es de 31 KB, cada almacenamiento intermedio `DataBlk` de la aplicación cabe en un almacenamiento intermedio de comunicaciones y se vacía de inmediato. No obstante, si el almacenamiento intermedio `DataBlk` de la aplicación es exactamente 32 KB, y dado que la API añade una actividad de 4 bytes por almacenamiento intermedio de transacción, hay dos vaciados: uno de 32 KB y otro de 4 bytes. Además, si establece la opción `tcpnodelay` en no, el vaciado de 4 puede llevar hasta 200 milisegundos.

## Configuración de la API para enviar datos de rendimiento al supervisor de rendimiento de cliente

El supervisor de rendimiento de cliente es un componente del Centro de administración de Tivoli Storage Manager que se utiliza para mostrar datos de rendimiento recopilados por la API. El supervisor de rendimiento de cliente registra y muestra los datos de rendimiento para las operaciones de restauración, archivado y copia de seguridad de cliente.

Con la supervisión del rendimiento habilitada, puede mostrar los datos de rendimiento que recopila la API utilizando la supervisión del rendimiento; la supervisión del rendimiento está disponible en el Centro de administración de Tivoli Storage Manager. A partir de la versión 7.1, el componente del Centro de administración ya no se distribuye con Tivoli Storage Manager o IBM Spectrum Protect. Si tiene un Centro de administración que se ha instalado con una versión anterior del servidor, puede seguir utilizándola para mostrar los datos de rendimiento. Si no tiene instalado un Centro de administración, puede descargar la versión que ha publicado anteriormente desde <http://public.dhe.ibm.com/storage/tivoli-storage-management/maintenance/admincenter/v6r3/>. Para obtener información sobre cómo utilizar la supervisión de rendimiento, consulte la documentación del servidor de Tivoli Storage Manager versión 6.3.

- Configuración de las opciones del supervisor de rendimiento de cliente  
Habilite los clientes de IBM Spectrum Protect para utilizar la supervisión del rendimiento especificando los parámetros en el archivo de opciones del cliente. Especifique estas opciones para cada cliente que desee supervisar.

## Enviar objetos al servidor

Los clientes de aplicaciones pueden enviar datos o objetos nombrados y sus datos asociados a un almacenamiento IBM Spectrum Protect utilizando funciones de archivado y de copia de seguridad de API. Los componentes de copia de seguridad y archivado del sistema permiten el uso de procedimientos de gestión diferentes para los datos que se envían a almacenamiento.

El atributo de estimación de tamaño es una estimación del tamaño total del objeto de datos que se envían al servidor. Si la aplicación no conoce el tamaño del objeto exacto, configure `sizeEstimate` en una estimación más alta. Si la estimación es más pequeña que el tamaño real, el servidor IBM Spectrum Protect utiliza recursos extra para gestionar las asignaciones de espacio extra.

Sugerencias:

- Sea tan preciso como sea posible cuando realice esta estimación de tamaño. El usuario utiliza este atributo para la asignación eficaz de espacio y la colocación de objetos dentro de sus recursos de almacenamiento.
- Si el cálculo es menor al tamaño actual, un servidor con almacenamiento en memoria caché no asigna espacio adicional y detiene el envío.

Es posible que tenga problemas si `sizeEstimate` es excesivo. Es posible que el servidor no disponga de suficiente espacio para el tamaño estimado pero tenga espacio para el tamaño real; o es posible que el servidor utilice dispositivos más lentos.

Puede realizar copias de seguridad o archivar objetos que son más grandes que dos gigabytes de tamaño. Los objetos pueden estar comprimidos o descomprimidos.

Para iniciar una operación de envío, llame a **dsmSendObj**. Si tiene más datos de los que pueda enviar en una única operación, puede repetir las llamadas a **dsmSendData** con el fin de transferir el resto de la información. Llame a **dsmEndSendObj** para finalizar la operación de envío.

- Conceptos básicos sobre archivar y realizar copias de seguridad de los objetos  
El componente de respaldo del sistema IBM Spectrum Protect es compatible con varias versiones de objetos nombrados que se almacenan en el servidor.
- Compresión  
Las opciones de configuración en un nodo determinado y la opción `dsmSendObj objCompressed`, determinan si IBM Spectrum Protect comprime el objeto durante un envío. También, los objetos con un `sizeEstimate` inferior a `DSM_MIN_COMPRESS_SIZE` nunca se comprimen.
- Eliminación de copia de almacenamiento intermedio  
La función de eliminación de copia de almacenamiento intermedio elimina la copia de los almacenamientos intermedios entre una aplicación y el servidor IBM Spectrum Protect, lo que da como resultado una mejor utilización del procesador. Para un efecto máximo, utilice este método en un entorno sin LAN.
- Cifrado de la API  
Existen dos métodos de cifrado disponibles para el cifrado de datos: el cifrado gestionado por la aplicación y el cifrado del cliente de IBM Spectrum Protect.

## Conceptos básicos sobre archivar y realizar copias de seguridad de los objetos

El componente de respaldo del sistema IBM Spectrum Protect es compatible con varias versiones de objetos nombrados que se almacenan en el servidor.

Cualquier objeto respaldado en el servidor que tiene el mismo nombre que un objeto que ya está almacenado en el servidor del mismo cliente está sujeto a un control de versión. Los objetos pueden tener un estado activo o inactivo en el servidor. La última copia de un objeto en el servidor que no ha sido desactivada se encuentra en estado activo. Cualquier otro objeto con el mismo nombre, ya sea una versión anterior o una copia desactivada, se considera inactiva. Las construcciones de clase de gestión definen los distintos criterios de gestión. Se asignan a objetos activos e inactivos en el servidor.

Tabla 1 muestra una lista de los campos del grupo de copia que se aplican a estados activos e inactivos:

Tabla 1. Campos de grupo de copia de seguridad

Campo	Descripción
VEREXISTS	El número de versiones inactivas si existen versiones activas.
VERDELETED	El número de versiones inactivas si no existen versiones activas.
RETEXTRA	El número de días que se conservan las versiones inactivas.
RETONLY	El número de días que se conservan las últimas versiones inactivas si no existen versiones activas.

Si cada una de las versiones de copia de seguridad tienen un nombre único, como por ejemplo un sello de hora en el nombre, entonces la asignación de versión no ocurre de forma automática: todos los objetos están activos. Los objetos activos nunca caducan, con lo que una aplicación es responsable de desactivarlos con la llamada `dsmDeleteObj`. En este caso, la aplicación necesita que los objetos desactivados caduquen lo antes posible. El usuario define un grupo de copia de seguridad con `VERDELETED=0` y `RETONLY=0`.

El componente de archivado del sistema IBM Spectrum Protect permite que los objetos estén almacenados en el servidor con controles de caducidad o retención en lugar de con controles de versión. Cada uno de los objetos almacenados son únicos, aunque el nombre de cualquiera de ellos sea el mismo que el de un objeto que ya está archivado. Los objetos archivados tienen un campo de descripción asociado con los metadatos que se pueden utilizar durante una consulta con el fin de identificar un objeto específico.

A cada objeto del servidor IBM Spectrum Protect se le asigna un ID de objeto exclusivo. La persistencia del valor original no está garantizado durante el ciclo de vida de un objeto (especialmente, después de una exportación o importación). Por lo tanto, una aplicación no debe consultar y guardar el ID del objeto original para utilizarlo en restauraciones posteriores. En su lugar, una aplicación debe guardar el nombre del objeto e introducir la fecha. Puede utilizar esta información durante una restauración para consultar objetos y verificar la fecha de introducción. A continuación, el ID de objeto actual se puede utilizar para restaurar el objeto.

## Compresión

Las opciones de configuración en un nodo determinado y la opción `dsmSendObj objCompressed`, determinan si IBM Spectrum Protect comprime el objeto durante un envío. También, los objetos con un `sizeEstimate` inferior a `DSM_MIN_COMPRESS_SIZE` nunca se comprimen.

Si el objeto ya está comprimido (`objCompressed=bTrue`), no se comprime de nuevo. Si no está comprimido, IBM Spectrum Protect decide si comprimir el objeto, en función de los valores de la opción de compresión establecida por el administrador y que esté establecida en los orígenes de configuración de la API.

El administrador puede cambiar los umbrales de compresión en el servidor utilizando el mandato register node (compression=yes, no o client-determined). Si esto está determinado por el cliente, entonces el comportamiento de la compresión está determinado por el valor de opción de compresión en las fuentes de configuración.

Algunos tipos de datos, como los datos que ya están comprimidos, pueden crecer cuando se procesan con el algoritmo de compresión. Cuando esto ocurre, se genera el código de retorno DSM\_RC\_COMPRESS\_GREW. Si se da cuenta de que esto ocurre, pero desea que la operación de envío continúe de todas formas, comuníquese a los usuarios finales con el fin de especificar la siguiente opción en los archivos de opciones:

```
COMPRESSAlways Yes
```

S, durante una función dsmSendData, con la compresión habilitada, obtiene el código de retorno DSM\_RC\_COMPRESS\_GREW, es posible que desee iniciar y enviar el objeto de nuevo sin compresión. Para implementarlo, configure dsmSendObj ObjAttr.objCompressed en bTrue.

La información sobre el comportamiento de compresión durante dsmSendObj se devuelve por la llamada dsmEndSendObjEx. objCompressed especifica si se realizó la compresión. totalBytesSent es el número de bytes enviados por la aplicación. totalCompressedSize es el número de bytes después de la compresión. La llamada dsmEndSendObjEx también tiene un campo totalLFBytesSent que contiene el total de bytes enviados sin LAN.

Atención: Si la aplicación va a utilizar restauraciones o recuperaciones parciales de objetos, no es posible comprimir los datos mientras los envía. Para implementarlo, configure dsmSendObj ObjAttr.objCompressed en bTrue.

- Tipo de compresión  
El tipo de compresión que el cliente utiliza se determina mediante la combinación de compresión y la deduplicación de datos del lado del cliente que se utiliza durante el proceso de copia de seguridad y archivado.

## Eliminación de copia de almacenamiento intermedio

---

La función de eliminación de copia de almacenamiento intermedio elimina la copia de los almacenamientos intermedios entre una aplicación y el servidor IBM Spectrum Protect, lo que da como resultado una mejor utilización del procesador. Para un efecto máximo, utilice este método en un entorno sin LAN.

Los almacenamientos intermedio para el movimiento de datos los asigna IBM Spectrum Protect y se pasa un puntero de vuelta a la aplicación. La aplicación coloca los datos en el almacenamiento intermedio proporcionado, y dicho almacenamiento intermedio pasa a través de las capas de comunicación al agente de almacenamiento (utilizando la memoria compartida). A continuación los datos pasan al dispositivo de cinta, el cual elimina las copias de los datos. Esta función se puede utilizar con operaciones de copia de seguridad o de archivado.

Atención: Cuando utilice este método, preste especial atención a la gestión adecuada del almacenamiento intermedio y a los tamaños de estos. Los buffers se comparten entre los componentes y cualquier sobrescritura de memoria que es el resultado de un error de programación se convierte en un error importante.

La secuencia general de llamadas para archivados/copias de seguridad es la siguiente:

```
dsmInitEx (UseTsmBuffers = True, numTsmBuffers = [how many IBM Spectrum Protect
        -allocated buffers the application needs to allocate])
dsmBeginTxn
for each object in the txn
    dsmBindMC
        dsmSendObject
            dsmRequestBuffer
            dsmSendBufferData (sends and release the buffer used)
        dsmEndSendObjEx
    dsmEndTxn
for each buffer still held
    dsmReleaseBuffer
dsmTerminate
```

La función dsmRequestBuffer se puede llamar varias veces, hasta el valor que especifica la opción numTsmBuffers. Una aplicación puede tener dos hebras: una hebra de producción que rellena los buffers con datos y una hebra de consumo que envía dichos almacenamientos intermedios a IBM Spectrum Protect con la llamada dsmSendBufferData. Cuando se emite una llamada dsmRequestBuffer y se ha alcanzado numTsmBuffers, la llamada dsmRequestBuffer se bloquea hasta que se libera un almacenamiento intermedio. La liberación del almacenamiento intermedio se puede producir llamando a dsmSendBufferData, que envía y libera un almacenamiento intermedio o llamando a dsmReleaseBuffer. Para obtener más información, consulte callbuff.c en el directorio de muestra de la API.

Si en algún momento hay un fallo en el envío, la aplicación debe liberar todos los buffers retenidos y terminar la sesión. Por ejemplo:

```
If failure
  for each data buffer held by application
    call dsmReleaseBuffer
dsmTerminate
```

Si una aplicación llama a `dsmTerminate` y aún está retenido el almacenamiento intermedio, la API no existe. Se devuelve el siguiente código: `DSM_RC_CANNOT_EXIT_MUST_RELEASE_BUFFER`. Si la aplicación no puede liberar el almacenamiento intermedio, debe salir del proceso para forzar una limpieza.

- Eliminación de la copia de almacenamiento intermedio y restauración y recuperación  
El servidor IBM Spectrum Protect controla la cantidad de datos que se colocan en almacenamiento intermedio basándose en la optimización del acceso de cintas con restauración y recuperación. Este método no es beneficioso para la aplicación como método normal de obtención de datos. Durante la creación de un prototipo, compruebe el rendimiento del método de eliminación de copia de almacenamiento intermedio y utilice este método sólo si ve una mejora que merece la pena.

## Cifrado de la API

---

Existen dos métodos de cifrado disponibles para el cifrado de datos: el cifrado gestionado por la aplicación y el cifrado del cliente de IBM Spectrum Protect.

Seleccione y utilice solo uno de estos métodos para cifrar los datos. Los métodos se excluyen mutuamente y si cifra los datos mediante ambos métodos no podrá restaurar o recuperar algunos de los datos. Por ejemplo, presuponga que una aplicación utiliza el cifrado gestionado por aplicación para cifrar el objeto A y, a continuación, utiliza el cifrado del cliente de IBM Spectrum Protect para cifrar el objeto B. Durante la operación de restauración, si la aplicación establece la opción para utilizar el cifrado del cliente de IBM Spectrum Protect e intenta restaurar ambos objetos, solo se puede restaurar el objeto B; el objeto A no se puede restaurar porque lo ha cifrado la aplicación y no el cliente.

Independientemente del método de cifrado que se utilice, el IBM Spectrum Protect debe habilitar el cifrado de la contraseña. De forma predeterminada, el servidor utiliza `SET AUTHENTICATION ON`.

La API utiliza el cifrado AES de 128 bits o AES de 256 bits. El cifrado AES de 256 bits proporciona un cifrado de datos más robusto que el cifrado de datos AES de 128 bits. Los archivos de los que se realiza una copia de seguridad utilizando el cifrado AES de 256 bits no se pueden restaurar con un cliente más antiguo. El cifrado se puede activar con o sin compresión. Si utiliza el cifrado, no se pueden utilizar las funciones de restauración y recuperación de objeto parcial y eliminación de copia de almacenamiento intermedio.

- Cifrado gestionado por la aplicación  
Con el cifrado gestionado por la aplicación, la aplicación proporciona la contraseña clave al API (utilizando la clave `DSM_ENCRYPT_USER`) y es responsabilidad de la aplicación gestionar la contraseña clave.
- Cifrado del cliente de IBM Spectrum Protect  
IBM Spectrum Protect el cifrado de cliente utiliza la clave gestionada por el valor `DSM_ENCRYPT_CLIENTENCRKEY` para proteger los datos. El cifrado de cliente es transparente para la aplicación que utiliza la API, con excepción de que las operaciones de restauración y recuperación de objetos parciales no son viables para objetos cifrados o comprimidos.

## Cifrado gestionado por la aplicación

---

Con el cifrado gestionado por la aplicación, la aplicación proporciona la contraseña clave al API (utilizando la clave `DSM_ENCRYPT_USER`) y es responsabilidad de la aplicación gestionar la contraseña clave.

Atención: Si no se ha guardado la clave de cifrado, y ha olvidado la clave, no se podrán recuperar los datos.

La aplicación proporciona la contraseña clave en la llamada `dsmInitEx` y debe proporcionar la contraseña adecuada cuando llegue el momento de la restauración.

Atención: Si la contraseña clave se pierde, no hay forma de restaurar los datos.

Debe usarse la misma contraseña de clave para las operaciones de copia de seguridad y restauración (o archivado y recuperación) del mismo objeto. Este método no depende del nivel del servidor IBM Spectrum Protect. Para configurar este método, la aplicación necesita realizar lo siguiente:

1. Configure la variable `bEncryptKeyEnabled` en `bTrue` en la llamada a `dsmInitEx`, y configure la variable `encryptionPasswordP` para que apunte a una cadena con la contraseña clave de cifrado.
2. Configure `include.encrypt` para que los objetos `encrypt`. Por ejemplo, para cifrar todos los datos, configure:

```
include.encrypt /.../* (UNIX)
```

e

```
include.encrypt *\...\* (Windows)
```

Para cifrar el objeto /FS1/DB2/FULL, defina:

```
include.encrypt /FS1/DB2/FULL
```

- Configure ENCRYPTKEY=PROMPT|SAVE en la cadena de opción que pasa al API en la llamada dsmInitEx en Windows. Esta opción también se puede establecer en dsm.opt (Windows) o dsm.sys (UNIX o Linux).

De forma predeterminada, la opción encryptkey se configura en prompt. Este valor garantiza que la clave no se almacena automáticamente. Si se especifica guardar con encryptkey, IBM Spectrum Protect almacena la clave en la máquina local, pero en dicho caso sólo una clave es válida para todas las operaciones IBM Spectrum Protect con el mismo nombre de nodo.

Después del envío de un objeto, dsmEndSendObjEx especifica si un objeto ha sido cifrado y qué método se ha utilizado. Los valores posibles en el campo son *encryptionType*:

- DSM\_ENCRYPT\_NO
- DSM\_ENCRYPT\_USER
- DSM\_ENCRYPT\_CLIENTENCRKEY

En la siguiente tabla se incluyen los tipos de cifrado de la API, requisitos previos y las funciones disponibles.

Tabla 1. Tipos de cifrado de API, requisitos previos y funciones disponibles

Tipo	Requisito previo	Función disponible
ENCRYPTIONTYPE	Ninguno	Configure ENCRYPTIONTYPE en la cadena de opción que pasa al API en la llamada dsmInitEx en Windows. ENCRYPTIONTYPE es AES128 de forma predeterminada.
EncryptKey=save	Ninguno	API y copias de seguridad/archivados
EncryptKey=prompt	Ninguno	API y copias de seguridad/archivados
EncryptKey=generate	Ninguno	API y copias de seguridad/archivados
EnableClientEncryptKey	Ninguno	Sólo API

Nota: Se recomienda que la autenticación del servidor esté en ENCENDIDO. Si la autenticación no está activada OFF, la clave no se cifra, pero los datos siguen cifrados. No obstante, esto no se recomienda.

Tabla 2 muestra cómo tanto los usuarios autorizados como los no autorizados pueden cifrar y descifrar datos durante una operación de restauración o copia de seguridad, dependiendo del valor especificado en la opción passwordaccess. El archivo TSM.PWD debe existir para realizar las siguientes operaciones de usuarios autorizados y no autorizados. El usuario autorizado crea el archivo TSM.PWD y configura la opción encryptkey en guardar y la opción passwordaccess en generar.

Tabla 2. Cifrar o descifrar datos con la clave gestionada por la aplicación en UNIX o Linux

Operación	opción passwordaccess	opción encryptkey	Resultado
Copia de seguridad de usuario autorizado	generate	save	Datos cifrados.
	generate	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	save	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
Restauración de usuario autorizado	generate	save	Datos cifrados.
	generate	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	save	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
Copia de seguridad de usuario no autorizado	generate	save	Datos cifrados.
	generate	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.



Operación	opción passwordaccess	opción encryptkey	Resultado
	prompt	save	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
Restauración de usuario no autorizado	generate	save	Datos cifrados.
	generate	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.
	prompt	save	datos cifrados si encryptionPasswordP contiene una contraseña cifrada
	prompt	prompt	Datos cifrados si encryptionPasswordP contiene una contraseña cifrada.

## Cifrado del cliente de IBM Spectrum Protect

IBM Spectrum Protect el cifrado de cliente utiliza la clave gestionada por el valor DSM\_ENCRYPT\_CLIENTENCRKEY para proteger los datos. El cifrado de cliente es transparente para la aplicación que utiliza la API, con excepción de que las operaciones de restauración y recuperación de objetos parciales no son viables para objetos cifrados o comprimidos.

Tanto para el cifrado de cliente de IBM Spectrum Protect como para el cifrado gestionado mediante la aplicación, la contraseña de cifrado hace referencia a un valor de serie que se utiliza para generar la clave de cifrado actual. El valor para la opción de contraseña de cifrado es de 1 a 63 caracteres de longitud, pero la clave generada siempre es de 8 bytes para 56 DES, de 16 bytes para 128 AES y de 32 bytes para 256 AES.

Atención: Si la clave de cifrado no está disponible, los datos no se pueden restaurar o recuperar. Cuando utiliza ENABLECLIENTENCRYPTKEY para el cifrado, la clave de cifrado se guarda en la base de datos del servidor. Para los objetos que utilizan este método, la base de datos del servidor debe existir y contar con los valores adecuados para los objetos para una restauración adecuada. Asegúrese de que realiza copias de seguridad de la base de datos del servidor con frecuencia para evitar que se pierdan los datos.

Este es el método más simple de implementar, cuando una clave de cifrado aleatoria se genera por sesión y se almacena en el servidor de IBM Spectrum Protect con el objeto en la base de datos del servidor. Durante la restauración, la clave almacenada se utiliza para el descifrado. Con este método IBM Spectrum Protect es responsable de la gestión de la clave, y la aplicación no tiene que ocuparse de la clave. Como la clave se almacena en la base de datos del servidor, debe tener una base de datos de IBM Spectrum Protect válida para una operación de restauración de un objeto cifrado. Cuando la clave se transmite entre la API y el servidor, también está cifrada. La transmisión de la clave es segura, y cuando la clave se almacena en la base de datos del servidor de IBM Spectrum Protect está cifrada. La única vez que la clave se destapa con la corriente de datos de exportación es cuando los datos del nodo se exportan entre servidores.

Para habilitar el cifrado de cliente de IBM Spectrum Protect, lleve a cabo los siguientes pasos:

1. Especifique -ENABLECLIENTENCRYPTKEY=YES en la cadena de la opción que se pasa a la API en la llamada dsmInitEx o que define el archivo de opciones del sistema dsm.opt (Windows) o dsm.sys (UNIX o Linux).
2. Configure include.encrypt en los objetos que va a cifrar. Por ejemplo, para cifrar todos los datos, configure:

```
include.encrypt /.../* (UNIX)
```

e

```
include.encrypt *\\...\\* (Windows)
```

Para cifrar el objeto /FS1/DB2/FULL, defina:

```
include.encrypt /FS1/DB2/FULL
```

## Desduplicación de datos

La desduplicación de datos es un método para reducir las necesidades de almacenamiento eliminando datos redundantes.

### Visión general

En IBM Spectrum Protect hay disponibles dos tipos de eliminación de datos duplicados: *eliminación de datos duplicados del lado del cliente* y *eliminación de datos duplicados del lado del servidor*.

*Optimización de almacenamiento de datos del lado de cliente* es una técnica de optimización de almacenamiento de datos que se utiliza en el cliente de archivado y copia de seguridad para eliminar datos redundantes durante el proceso de copia de seguridad y archivado antes de que los datos se transfieran al servidor de IBM Spectrum Protect. El uso de la eliminación de datos duplicados del lado del cliente puede reducir la cantidad de datos que va a enviarse a través de una red de área local.

*La eliminación de datos duplicados del lado del servidor* es una técnica de eliminación de datos duplicados realizada por el servidor. El administrador de IBM Spectrum Protect puede especificar la ubicación de la eliminación de datos duplicados (cliente o servidor) a utilizar con el parámetro DEDUP en el mandato del servidor REGISTER NODE o UPDATE NODE.

## Mejoras

---

Con la optimización de almacenamiento de datos del lado del cliente, puede:

- Excluir archivos específicos en un cliente de una eliminación de duplicados de datos.
- Habilitar una memoria caché de eliminación de duplicados de datos que reduzca el tráfico de la red entre el cliente y el servidor. La memoria caché contiene las extensiones que se enviaron al servidor en operaciones anteriores de copia de seguridad incremental. En lugar de consultar al servidor la existencia de una extensión, el cliente consulta su memoria caché.

Especificar un tamaño y ubicación para una memoria caché de cliente. Si se detecta una incoherencia entre el servidor y la memoria caché local, la memoria caché local se elimina y se vuelve a rellenar.

Nota: Para las aplicaciones que utilizan la API de IBM Spectrum Protect, la memoria caché de eliminación de datos duplicados no se debe utilizar debido a la posibilidad de que se produzcan errores en las copias de seguridad causados por la falta de sincronización de la memoria caché con el servidor de IBM Spectrum Protect. Si hay configuradas varias sesiones de cliente de archivado y copia de seguridad simultáneas, debe haber una caché independiente configurada para cada sesión.

- Habilitar la eliminación de duplicados de datos y la compresión del lado del cliente para reducir la cantidad de datos almacenados por el servidor. Todas las extensiones se comprimen antes de ser enviadas al servidor. Se establece un compromiso entre el ahorro de almacenamiento y la potencia de procesamiento necesaria para comprimir los datos de cliente. En general, si se comprime y optimiza el almacenamiento de datos en el sistema cliente, se utiliza aproximadamente el doble de potencia de procesamiento que la optimización de almacenamiento de datos por sí sola.

El servidor también puede funcionar con datos comprimidos o a los que se ha aplicado la optimización de almacenamiento. Además, los clientes de copia de seguridad y archivado anteriores a V6.2 pueden restaurar los datos comprimidos y con optimización de almacenamiento.

La eliminación de datos duplicados del lado del cliente utiliza el siguiente proceso:

- El cliente crea extensiones. Las *extensiones* son partes de archivos que se comparan con otras extensiones de archivos para identificar duplicados.
- El cliente y el servidor colaboran para identificar las extensiones duplicadas. El cliente envía extensiones no duplicadas al servidor.
- Las operaciones subsiguientes de eliminación de duplicados de datos del cliente crean nuevas extensiones. Es posible que algunas o todas las extensiones coincidan con las extensiones que se crearon en operaciones anteriores de optimización de almacenamiento de datos y que se enviaron al servidor. Las extensiones coincidentes no vuelven a enviarse al servidor.

## Beneficios

---

La optimización de almacenamiento de datos del lado del cliente ofrece varias ventajas:

- Puede reducir la cantidad de datos enviados a la red de área local (LAN).
- La potencia de procesamiento necesaria para identificar datos duplicados se descarga desde el servidor a los nodos cliente. La optimización de almacenamiento de datos del lado del servidor siempre está habilitada para las agrupaciones de almacenamiento preparadas para optimización de almacenamiento. Sin embargo, los archivos que están en agrupaciones de almacenamiento preparadas para optimización de almacenamiento y en las que el cliente haya realizado la optimización de almacenamiento no necesitan procesamiento adicional.
- Se elimina la potencia de procesamiento necesaria para suprimir los datos duplicados en el servidor, lo que produce un ahorro de espacio en el servidor inmediato.

La eliminación de duplicados de datos del lado del cliente tiene una desventaja posible. El servidor no tiene copias completas de los archivos del cliente *hasta* que se realiza una copia de seguridad de las agrupaciones de almacenamiento primarias que contienen extensiones de cliente en una agrupación de almacenamiento de copia sin optimización de almacenamiento. (Las *extensiones* son partes de un archivo que se crean durante el proceso de optimización de almacenamiento de datos). Durante la copia de seguridad de la agrupación de almacenamiento en una agrupación de almacenamiento sin eliminación de datos duplicados, las extensiones del cliente se vuelven a ensamblar en archivos contiguos.

De forma predeterminada, debe realizarse una copia de seguridad de las agrupaciones de almacenamiento primarias de acceso secuencial que están configuradas para optimización de almacenamiento de datos en agrupaciones de almacenamiento de copia sin optimización de almacenamiento antes de poder recuperarlas y antes de poder eliminar datos duplicados. La opción predeterminada garantiza que el servidor tenga copias de archivos completos en todo momento, en una agrupación de almacenamiento primaria o en una agrupación de almacenamiento de copia.

Importante: Para conseguir una mayor reducción de datos, puedes habilitar la eliminación de datos duplicados del lado del cliente y la compresión a la vez. Todas las extensiones se comprimen antes de ser enviadas al servidor. La compresión ahorra espacio, pero aumenta el tiempo de procesamiento en la estación de trabajo del cliente.

Las siguientes opciones están relacionadas con la eliminación de duplicados de datos:

- Eliminación de duplicados
- Dedupcachepath
- Dedupcachesize
- Enablededupcache
- Exclude.dedup
- Include.dedup
  
- Eliminación de datos duplicados del lado del cliente de la API  
La API utiliza *la eliminación de datos duplicados del lado del cliente* en el cliente de archivado y copia de seguridad para eliminar datos redundantes durante el proceso de copia de seguridad y archivado antes de que los datos se transfieran al servidor IBM Spectrum Protect.
- Eliminación de datos duplicados del lado del servidor  
La optimización de almacenamiento de datos del lado del servidor es la optimización de almacenamiento de datos realizada por el servidor.

## Eliminación de datos duplicados del lado del cliente de la API

---

La API utiliza *la eliminación de datos duplicados del lado del cliente* en el cliente de archivado y copia de seguridad para eliminar datos redundantes durante el proceso de copia de seguridad y archivado antes de que los datos se transfieran al servidor IBM Spectrum Protect.

La API utiliza la eliminación de datos duplicados del lado del cliente para eliminar los datos redundantes durante el proceso de copia de seguridad y archivado antes de que se transfieran los datos al servidor de IBM Spectrum Protect. El uso de la eliminación de datos duplicados del lado del cliente puede reducir la cantidad de datos que va a enviarse a través de una red de área local. El uso de la eliminación de datos duplicados del lado del cliente también puede reducir el espacio del almacenamiento del servidor IBM Spectrum Protect.

Cuando el cliente está habilitado para la eliminación de datos duplicados del lado del cliente, y se realiza una operación de copia de seguridad o archivado, los datos se envían al servidor en forma de extensiones. La siguiente vez que se realiza una operación de copia de seguridad o archivado, el cliente y el servidor identifican qué extensiones de datos ya se han archivado o de cuáles ya se ha hecho una copia de seguridad y solo se envían al servidor las extensiones de datos únicas.

Para la deduplicación de datos del lado del cliente, el servidor y la API tienen que estar en la versión 6.2 o posterior.

Antes de utilizar la eliminación de duplicado de datos para realizar copias de seguridad o archivar archivos, el sistema tienen que cumplir los siguientes requisitos:

- El cliente tiene que tener la opción deduplication habilitada.
- El servidor tiene que habilitar el cliente para la eliminación de datos duplicados del lado del cliente con el parámetro DEDUP=CLIENTORSERVER en el mandato REGISTER NODE o UPDATE NODE.
- El destino de la agrupación de almacenamiento de los datos tiene que ser una agrupación de almacenamiento con eliminación de duplicados de datos habilitada. La agrupación de almacenamiento con eliminación de duplicados de datos habilitada es solo de tipo de dispositivo de archivo.
- Asegúrese de que los archivos están vinculados a la clase de gestión correcta.
- Un archivo puede excluirse del proceso de eliminación de datos duplicados del lado del cliente. De manera predeterminada, se incluyen todos los archivos.
- Los archivos tienen que superar los 2 KB.
- El servidor puede limitar el tamaño de transacción máximo para la eliminación de datos duplicados definiendo la opción CLIENTDEDUPTXNLIMIT en el servidor. Consulte la información disponible en la documentación del servidor sobre esta opción.

Si no se cumple alguno de estos requisitos, los datos se procesan de forma normal, sin que se lleve a cabo la eliminación de datos duplicados del lado del cliente.

A continuación se detallan algunas restricciones de la eliminación de datos duplicados:

- El movimiento de datos sin LAN y la eliminación de datos duplicados del lado del cliente se excluyen mutuamente. Si ha habilitado el movimiento de datos sin LAN y la eliminación de datos duplicados del lado del cliente, se completarán las operaciones de movimiento de datos sin LAN y se ignorará la eliminación de datos duplicados del lado del cliente.
- El cifrado y la eliminación de datos duplicados del lado del cliente se excluyen mutuamente. Si ha habilitado el cifrado y la eliminación de datos duplicados del lado del cliente, se completarán las operaciones de cifrado y se ignorará la eliminación de datos duplicados del lado del cliente. Los archivos cifrados y los archivos aptos para la eliminación de datos duplicados del lado del cliente pueden procesarse en la misma operación, pero se llevan a cabo en transacciones distintas.

Requisitos:

1. En cualquier transacción, todos los archivos tienen que incluirse o excluirse en la eliminación de datos duplicados. Si la transacción incluye archivos mixtos, no se realizará correctamente y la interfaz de programación de aplicaciones (API) devolverá un código de `DSM_RC_NEEDTO_ENDTXN`.
  2. Utilice el cifrado del dispositivo de almacenamiento junto con la eliminación de duplicados de datos del lado del cliente. Como la capa de sockets seguros (SSL) se utiliza junto a la optimización de almacenamiento del lado del cliente, no es necesario el cifrado del cliente.
- Las siguientes funciones no están disponibles para la eliminación de datos duplicados del lado del cliente:
    - Cliente de IBM Spectrum Protect for Space Management (HSM)
    - Almacenamiento intermedio compartido con la interfaz de programación de aplicaciones (API)
    - NAS
    - Copia de seguridad de subarchivos
  - La eliminación de copias del almacenamiento intermedio no puede utilizarse con transformaciones de datos tales como compresión, cifrado y eliminación de duplicados de datos.
  - Si utiliza una optimización de almacenamiento del lado de cliente, la API detecta y no puede realizar (con `RC=254`) las copias de seguridad de las extensiones de archivo marcadas como caducadas en el servidor durante el envío de datos al servidor. Si desea volver a entrar la operación, debe incluir esa programación en la aplicación de llamada.
  - Las operaciones de grabación simultánea que tienen lugar en el servidor tienen preferencia sobre la eliminación de datos duplicados del lado del cliente. Si las operaciones de grabación simultánea están habilitadas, no se produce la eliminación de datos duplicados del lado del cliente.

Restricción: Cuando se habilita la eliminación de datos del lado del cliente, la interfaz de programación de aplicaciones (API) no puede recuperarse de un estado en el que el servidor se ha quedado sin almacenamiento en la agrupación de destino, ni siquiera si se ha definido la siguiente agrupación. Se detiene un código de razón de detención

`DSM_RS_ABORT_DESTINATION_POOL_CHANGED` y la operación falla. Existen dos formas de recuperarse de esta situación:

1. Solicite al administrador que añada más volúmenes reutilizables a la agrupación de archivos original.
2. Volver a intentar realizar la operación con la eliminación de datos duplicados deshabilitada.

Para conseguir mayores ahorros en el ancho de banda, puede habilitar una caché local para la eliminación de datos duplicados. La caché local impide que las consultas vayan al servidor de IBM Spectrum Protect. El valor predeterminado de `ENABLEDEDUPCACHE` es `NO`, lo que significa que la memoria caché no está fuera de sincronía con el servidor. Si la memoria caché está fuera de sincronía con el servidor, la aplicación vuelve a enviar todos los datos. Si la aplicación puede reintentar una transacción fallida, y desea utilizar la memoria caché local, establezca la opción `ENABLEDEDUPCACHE` en `YES` en el archivo `dsm.opt` (Windows) o `dsm.sys` (UNIX).

Al final de una restauración, si *todos* los datos se restauraron a través de la interfaz de programación de aplicaciones (API) y el cliente eliminó los datos duplicados del cliente, se calcula un resumen de punto a punto y se compara con el valor calculado en el momento de realizar la copia de seguridad. Si los valores no coinciden, se devuelve el error `DSM_RC_DIGEST_VALIDATION_ERROR`. Si una aplicación recibe este error, los datos están corrompidos. Este error también puede ser resultado de un error pasajero en la red, así que vuelva a intentar llevar a cabo la restauración o recuperación.

Aquí tiene un ejemplo del mandato de sesión de consulta que muestra la información sobre la eliminación de datos duplicados:

```
dsmQuerySessInfo Values:
Server Information:
Server name: SERVER1
Server Host: AVI
Server port: 1500
Server date: 2009/10/6 20:48:51
Server type: Windows
Server version: 6.2.0.0
Server Archive Retention Protection : NO
Client Information:
Client node type: API Test1
Client filespace delimiter: :
Client hl & ll delimiter: \
Client compression: Client determined (3u)
Client archive delete: Client can delete archived objects
Client backup delete: Client CANNOT delete backup objects
Maximum objects in multiple object transactions: 4096
Ian free Enabled: NO
Deduplication : Client Or Server
General session info:
Node: AVI
```

Owner:  
API Config file:

Aquí tiene un ejemplo del mandato de clase de gestión de consulta que muestra la información sobre la eliminación de datos duplicados:

```
Policy Information:  
Domain name: DEDUP  
Policyset name: DEDUP  
Policy activation date: 0/0/0 0:0:0  
Default management class: DEDUP  
Backup retention grace period: 30 days  
Archive retention grace period: 365 days  
Mgmt. Class 1:  
Name: DEDUP  
Description: dedup - values like standard  
Backup CG Name: STANDARD  
Frequency: 0  
Ver. Data Exists: 2  
Ver. Data Deleted: 1  
Retain Extra Ver: 30  
Retain Only Ver: 60  
Copy Destination: AVIFILEPOOL  
Lan free Destination: NO  
Deduplicate Data: YES
```

```
Archive CG Name: STANDARD  
Frequency: 10000  
Retain versions: 365  
Copy Destination: AVIFILEPOOL  
Lan free Destination: NO  
Retain Init : CREATE  
Retain Minimum : 65534  
Deduplicate Data: YES
```

- Excluir archivos de la eliminación de datos duplicados  
Puede excluir archivos de copia de seguridad o archivado de la eliminación de datos duplicados.
- Incluir archivos para la desduplicación de datos  
Puede incluir archivos de copia de seguridad o archivado en la eliminación de datos duplicados.

#### Referencia relacionada:

Opción Deduplication  
Opción Exclude  
Opción Dedupcachepath  
Opción Dedupcachesize  
Opción Enablededupcache  
Opción Ieobjtype

## Excluir archivos de la eliminación de datos duplicados

---

Puede excluir archivos de copia de seguridad o archivado de la eliminación de datos duplicados.

Para excluir archivos del proceso de eliminación de datos duplicados, siga estos pasos:

1. Configure la opción `exclude.dedup` para los objetos que quiere excluir.

Por ejemplo, para excluir todos los datos de eliminación de duplicados para sistemas UNIX, establezca:

```
exclude.dedup /.../*
```

2. Para excluir todos los datos de la eliminación de datos duplicados de los sistemas Windows, defina:

```
exclude.dedup *\\...\\*
```

Importante: Si se envía un objeto a la agrupación de eliminación de datos duplicados, la eliminación de duplicados se produce en el servidor, incluso si el objeto se excluye de la eliminación de datos duplicados del lado del cliente.

## Incluir archivos para la desduplicación de datos

---

Puede incluir archivos de copia de seguridad o archivado en la eliminación de datos duplicados.

Para refinar la lista de archivos que van a incluirse, puede utilizarse la opción `include.dedup` en combinación con la opción `exclude.dedup`.

De forma predeterminada, todos los objetos aptos, se incluyen en la eliminación de datos duplicados.

Aquí tiene algunos ejemplos de UNIX y Linux:

```
exclude.dedup /FS1/.../*  
include.dedup /FS1/archive/*
```

Aquí tiene algunos ejemplos de Windows:

```
exclude.dedup E:\myfiles\...\  
include.dedup E:\myfiles\archive\*
```

## Eliminación de datos duplicados del lado del servidor

---

La optimización de almacenamiento de datos del lado del servidor es la optimización de almacenamiento de datos realizada por el servidor.

El administrador de IBM Spectrum Protect puede especificar la ubicación de la eliminación de datos duplicados (cliente o servidor) a utilizar con el parámetro DEDUP en el mandato del servidor REGISTER NODE o UPDATE NODE.

En una agrupación de almacenamiento con eliminación de datos duplicados habilitada (agrupación de archivos), solo se retiene una instancia de la extensión de datos. Otras instancias de la misma extensión de datos se sustituyen por un puntero que señala hacia la instancia retenida.

Para obtener más información sobre la eliminación de datos duplicados del lado del servidor, consulte la documentación del servidor de IBM Spectrum Protect.

## Migración tras error de la aplicación

---

Cuando el servidor de IBM Spectrum Protect no está disponible debido a una interrupción, las aplicaciones que utilizan la API pueden utilizar la migración tras error automáticamente a un servidor secundario para la recuperación de datos.

El servidor de IBM Spectrum Protect al que se conectan el cliente y la API durante los procesos de producción normales se denomina *servidor primario*. Cuando el servidor primario está configurado para la réplica del nodo, el servidor también se conoce como *servidor de réplica de origen*. Los datos del nodo del cliente en el servidor de réplica se pueden replicar en el *servidor de réplica de destino*. Este servidor también se conoce como *servidor secundario* y es el servidor al que pasa el cliente de forma automática cuando el servidor primario falla.

El cliente y la API deben estar configurados para la migración tras error automática del cliente, y deben conectarse al servidor de la versión 7.1 (o posterior) que replica los datos de nodo del cliente. La configuración para la API es la misma que la configuración para el cliente de archivado y copia de seguridad.

Durante las operaciones normales, la información de conexión para el servidor secundario se envía automáticamente desde el servidor primario durante el proceso de inicio de sesión. La información del servidor secundario se guardará automáticamente en el archivo de opciones del cliente.

Cada vez que la aplicación del cliente inicia sesión en el servidor de IBM Spectrum Protect, intenta contactar con el servidor primario. Si el servidor primario no está disponible, la aplicación se migra automáticamente al servidor secundario utilizando la información del servidor secundario del archivo de opciones del cliente. En la modalidad de migración tras error, la aplicación puede consultar al servidor secundario y restaurar o recuperar los datos replicados.

Debe realizar la copia de seguridad de la aplicación al menos una vez en el servidor primario. La API puede migrarse al servidor secundario para recuperar los datos solo si los datos del nodo del cliente se replicaron desde el servidor primario al servidor secundario.

- Información de estado de migración tras error

La interfaz de programación de aplicaciones proporciona información de estado que puede utilizarse para determinar el estado de la migración tras error y el estado de los datos de réplica del cliente en el servidor secundario.

### Conceptos relacionados:

Configuración y uso de la migración tras error automática del cliente

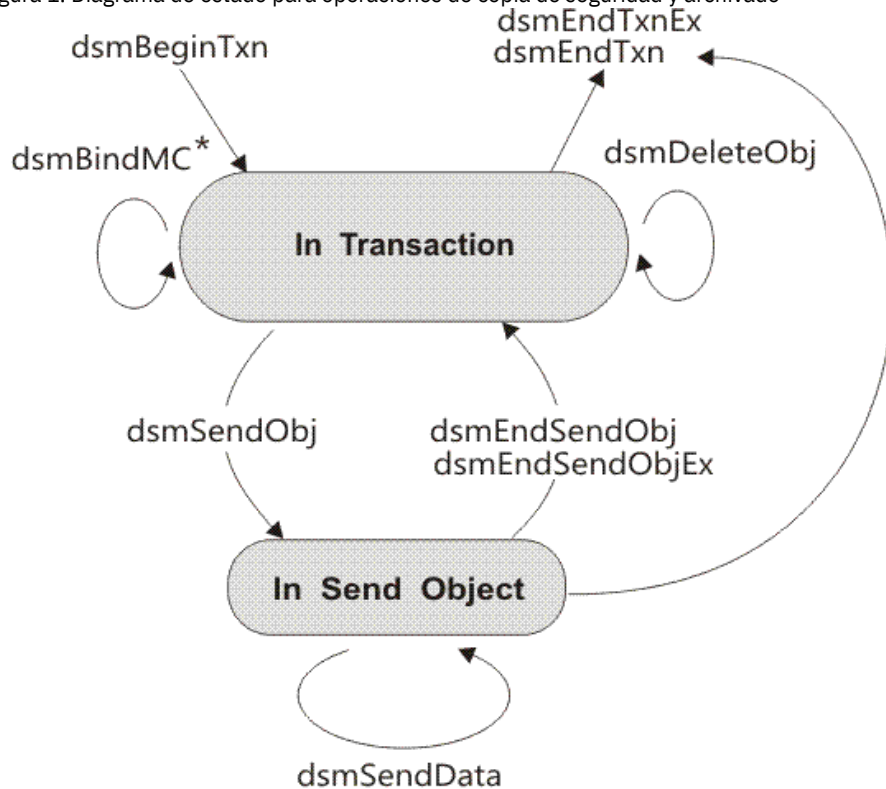
## Diagramas de ejemplo de copia de seguridad/archivado

La API está diseñada para flujos lógicos sencillos y transiciones claras entre los distintos estados de la aplicación del cliente. Esta transición de estado capta fallos lógicos y errores de programa muy temprano en el ciclo de desarrollo, mejorando en gran medida la calidad y fiabilidad del sistema.

Por ejemplo, no es posible realizar una llamada **dsmSendObj** a no ser que se inicie una transacción y se haya realizado anteriormente una llamada **dsmBindMC** para el objeto al que se le está realizando una copia de seguridad.

Figura 1 muestra el diagrama de estado para realizar operaciones de copia de seguridad o archivado dentro de una transacción. La flecha que va de "In Send Object" a **dsmEndTxn** indica que una llamada **dsmEndTxn** se puede iniciar después de una llamada a **dsmSendObj** o **dsmSendData**. Es posible que desee realizar esta operación si ocurre una condición de error durante el envío de un objeto y desea detener toda la operación. En este caso, debe utilizar un voto de DSM\_VOTE\_ABORT. En circunstancias normales, no obstante, llame a **dsmEndSendObj** antes de finalizar la transacción.

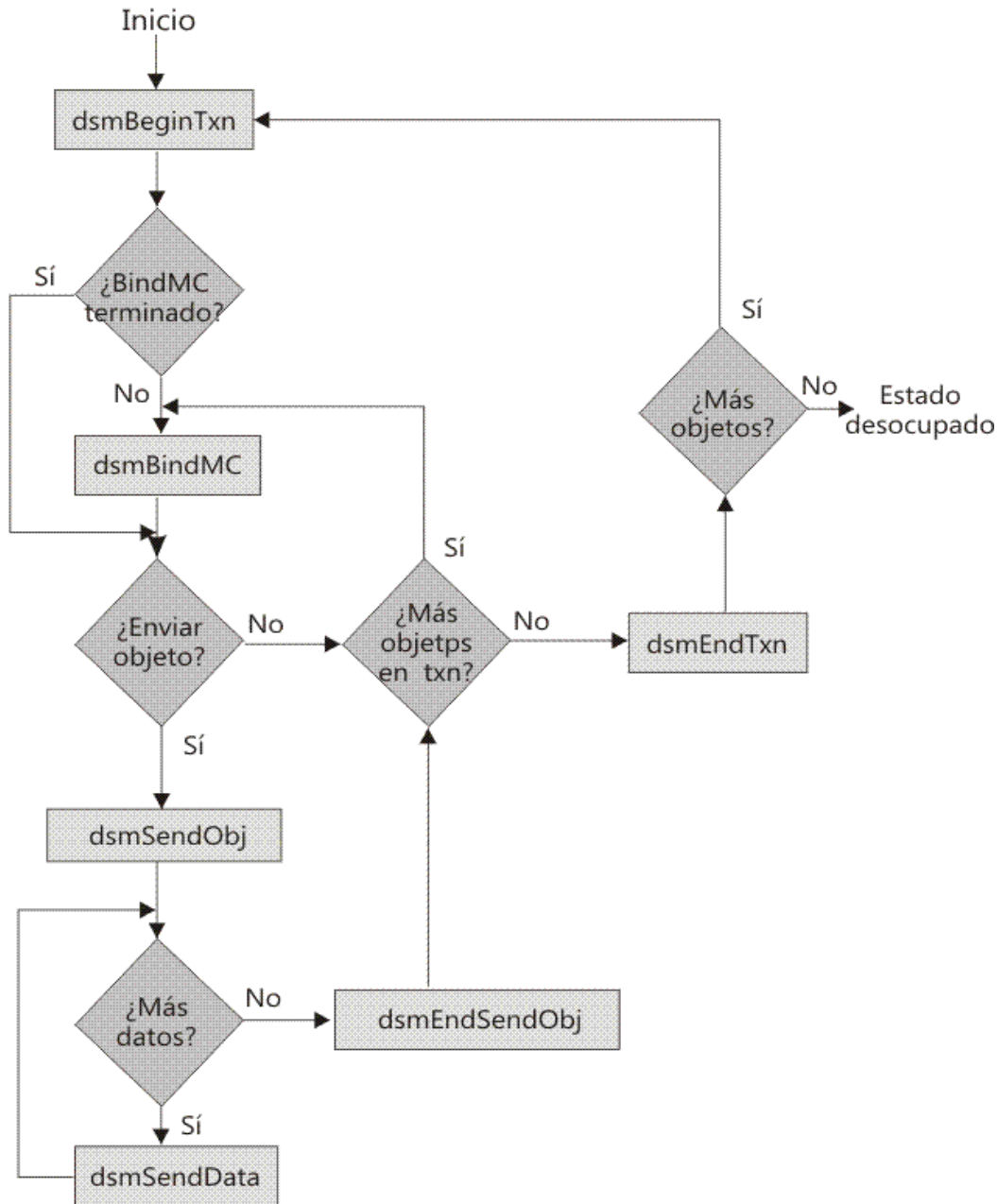
Figura 1. Diagrama de estado para operaciones de copia de seguridad y archivado



\* Puede estar dentro o fuera de una transacción

Figura 2 muestra el organigrama para realizar operaciones de copia de seguridad y archivado dentro de una transacción.

Figura 2. Organigrama de las operaciones de archivado y copia de seguridad



La función principal en estos dos diagramas es el bucle entre las siguientes llamadas de la API desde una transacción:

- **dsmBindMC**
- **dsmSendObj**
- **dsmSendData**
- **dsmEndSendObj**

La llamada **dsmBindMC** es única porque se puede iniciar desde dentro o fuera de los límites de una transacción. También puede iniciarla desde una transacción distinta si fuera necesario. El único requisito de la llamada **dsmBindMC** es que se realice antes de realizar una copia o archivar un objeto. Si el objeto que se está archivando o al que se le está realizando una copia de seguridad no está asociado con una clase de gestión, **dsmSendObj** devuelve un código de error. En este caso, la transacción finaliza con una llamada a **dsmEndTxn** (esta condición de error no aparece en el diagrama).

El diagrama ilustra cómo una aplicación utiliza varias transacciones de objeto. Muestra dónde se pueden colocar los puntos de decisión para determinar si el objeto que se envía encaja dentro de la transacción o si se debe iniciar una transacción nueva.

- Ejemplo de código de funciones de la API que envían datos al almacenamiento de IBM Spectrum Protect storage  
Este ejemplo demuestra el uso de las funciones API que envían datos al almacenamiento de IBM Spectrum Protect. La llamada **dsmSendObj** aparece dentro de una sentencia de cambio, con lo que es posible llamar parámetros distintos dependiendo de si se está realizando una operación de copia de seguridad o de archivado.



## Agrupación de archivos

La API de IBM Spectrum Protect tiene un protocolo de agrupación de archivos que relaciona a varios objetos separados. Es posible mencionar y gestionar estos archivos como un grupo lógico en el servidor. Un grupo lógico requiere que todos los miembros del grupo y el líder pertenezcan al mismo nodo y espacio de archivo en el servidor.

Cada grupo lógico cuenta con un líder de grupo. Si el líder de grupo se elimina, se elimina el grupo. No puede suprimir un miembro que es parte de un grupo. La caducidad de todos los miembros en un grupo depende del líder del grupo. Por ejemplo, si un miembro está marcado para su caducidad, el miembro no caduca a menos que caduque el líder del grupo. No obstante, si un miembro no está marcado para su caducidad y el líder del grupo está caducado, entonces todos los miembros caducan.

Los grupos de archivos contienen únicamente datos de seguridad y no pueden contener datos de archivado. Los objetos archivados pueden utilizar el campo **Archive Description** para facilitar un tipo de grupo si la aplicación lo requiere.

La llamada **dsmGroupHandler** agrupa las operaciones. La función **dsmGroupHandler** debe llamarse desde dentro de una transacción. La mayoría de las condiciones de error se detectan en las llamadas **dsmEndTxnl** o **dsmEndTxnEx**.

La estructura `out` en **dsmEndTxnEx** incluye un campo nuevo, **groupLeaderObjId**. Este campo contiene el ID de objeto del líder del grupo si un grupo fue abierto en esa transacción. Es posible crear un grupo en más de una transacción. Un grupo no se compromete o guarda en el servidor hasta que se realiza un cierre. El **dsmGroupHandler** es una interfaz que acepta cinco operaciones distintas. Incluyen:

- DSM\_GROUP\_ACTION\_OPEN
- DSM\_GROUP\_ACTION\_CLOSE
- DSM\_GROUP\_ACTION\_ADD
- DSM\_GROUP\_ACTION\_ASSIGNTO
- DSM\_GROUP\_ACTION\_REMOVE

Tabla 1 incluye en una lista las acciones de la llamada de función **dsmGroupHandler**:

Tabla 1. funciones dsmGroupHandler

Acción	Descripción
OPEN	La acción OPEN crea un grupo. El siguiente objeto que se envía se convierte en líder de grupo. El líder de grupo no puede tener contenido. Todos los objetos después del primer objeto se convierten en miembros que se añaden al grupo. Para crear un grupo, abra un grupo y pase una cadena única para identificarlo. Este identificador único permite que se abran varios grupos con el mismo nombre. Después de que el grupo se haya abierto, el siguiente objeto que se envía es el líder del grupo. Todos los demás objetos que se envían son miembros del grupo.
CLOSE	La acción CLOSE compromete y guarda un grupo abierto. Para cerrar el grupo, pase el nombre del objeto y la cadena única que se utiliza en la operación de apertura. La aplicación debe comprobar que existen grupos abiertos, y si fuera necesario, cerrarlos o eliminarlos. Un grupo no se compromete o guarda hasta que se realice un cierre del grupo. Una acción CLOSE falla en las siguientes condiciones: <ul style="list-style-type: none"><li>• El grupo que está intentando cerrar tiene el mismo nombre que un grupo abierto existente.</li><li>• Existe incompatibilidad de clase de gestión entre el grupo cerrado actual y el grupo nuevo del mismo nombre que se va a cerrar. En este caso, complete los pasos siguientes:<ol style="list-style-type: none"><li>1. Consulte el grupo cerrado anterior.</li><li>2. Si la clase de gestión del grupo cerrado existente es diferente de la clase de gestión asociada con el grupo abierto actual, emita un <b>dsmUpdateObject</b> con tipo DSM_BACKUPD_MC. Este mandato actualiza el grupo existente a la nueva clase de gestión.</li><li>3. Emita la acción CLOSE.</li></ol></li></ul>
ADD	La acción ADD adjunta un objeto a un grupo. Todos los objetos que se envían después de la acción ADD se asignan al grupo.
ASSIGNTO	La acción ASSIGNTO permite al cliente asignar objetos que existen en el servidor al grupo igual declarado. Esta transacción configura la relación del grupo igual. La acción ASSIGNTO es parecida a la acción ADD, con las siguientes excepciones: <ul style="list-style-type: none"><li>• La acción ADD se aplica a objetos dentro de una transacción en proceso.</li><li>• La acción ASSIGNTO se aplica a un objeto que está en el servidor.</li></ul>
REMOVE	La acción REMOVE elimina un miembro, o una lista de miembros, de un grupo. No es posible eliminar del grupo al líder del grupo. Un miembro de grupo debe eliminarse antes de que puede borrarse.

Utilice los siguientes tipos de consulta para el soporte de grupo:

- **qtBackupGroups**
- **qtOpenGroups**

**qtBackupGroups** consulta a grupos que están cerrados mientras que **qtOpenGroups** consulta a grupos que están abiertos. El almacenamiento intermedio de consulta para los nuevos tipos tiene campos para **groupLeaderObjId** y **objType**. La consulta se realiza de forma distinta dependiendo de los valores de estos dos campos. La siguiente tabla incluye algunas posibilidades de consulta:

Tabla 2. Ejemplo de consultas

groupLeaderObjId.hi	groupLeaderObjId.lo	objType	Resultado
0	0	NULO	Devuelve una lista de todos los líderes de grupo
grpLdrObjId.hi	grpLdrObjId.lo	0	Devuelve una lista de todos los miembros de grupo asignados al líder de grupo específico ( <b>grpLdrObjId</b> ).
grpLdrObjId.hi	grpLdrObjId.lo	objType	Devuelve una lista utilizando <b>BackQryRespEnhanced3</b> , para cada miembro de grupo que se asigna al líder de grupo específico ( <b>grpLdrObjId</b> ), y coincide con el tipo de objeto ( <b>objType</b> ).

La estructura de la respuesta (**qryRespBackupData**) de **dsmGetNextQObj** incluye dos campos para el soporte de grupo:

- **isGroupLeader**
- **isOpenGroup**

Estos campos son distintivos booleanos. El siguiente ejemplo muestra la creación del grupo, la adición de miembros al grupo y el cierre del grupo para confirmar el grupo en el servidor de IBM Spectrum Protect.

Figura 1. Ejemplo del pseudo-código que se utiliza para crear un grupo

```
dsmBeginTxn
    dsmGroupHandler (PEER, OPEN, leader, uniqueId)
    dsmBeginSendObj
        dsmEndSendObj
    dsmEndTxnEx (With objId of leader)
Loop for multiple txns
{
    dsmBeginTxn
        dsmGroupHandler (PEER, ADD, member, groupLeaderObjID)
        Loop for multiple objects
        {
            dsmBeginSendObj
            Loop for data
            {
                dsmSendData
            }
            dsmEndSendObj
        }
    dsmEndTxn
}
dmBeginTxn
    dsmGroupHandler (CLOSE)
dsmEndTxn
```

Para un ejemplo de código, consulte el programa de grupo de muestra `dsmgrp.c` que está incluido en el directorio de la API `sampsr.c`.

## Recibir datos de un servidor

Los clientes de aplicaciones pueden recibir datos u objetos con nombre y sus datos asociados del almacenamiento de IBM Spectrum Protect utilizando las funciones de restauración y recuperación. La función de restauración accede a los objetos de los que se hizo una copia de seguridad previamente, y la función de recuperación accede a los objetos que han sido archivados.

Restricción: El API sólo puede restaurar o recuperar objetos a los que se les ha hecho una copia de seguridad o que han sido archivados con llamadas API.

Ambas funciones de recuperación y restauración inician una operación de consulta. La consulta devuelve información distinta dependiendo de si los datos fueron archivados o se les realizó una copia de seguridad anteriormente. Por ejemplo, una consulta de objetos a los que se les ha realizado una copia de seguridad devuelve información sobre si los objetos están activos o inactivos, mientras que una consulta sobre objetos archivados devuelve información como descripciones de objeto. Ambas consultas devuelven ID de objeto que se utilizan para identificar de forma exclusiva el objeto en el servidor.

- Restauración o recuperación de objeto parcial  
El cliente de la aplicación puede recibir únicamente una parte del objeto. Esto se denomina una restauración de objeto parcial o una recuperación de objeto parcial.
- Restaurar o recuperar datos  
Después de realizar una consulta y de establecer una sesión con el servidor IBM Spectrum Protect, es posible ejecutar un procedimiento para restaurar o recuperar los datos.
- Diagramas de ejemplo de restauración y recuperación  
Se pueden utilizar un diagrama de estado y un diagrama de flujo para ilustrar cómo realizar las operaciones de recuperación o restauración.
- Ejemplo de código de recepción de datos de un servidor  
Este ejemplo ilustra el uso de las funciones de API para recuperar datos del almacenamiento IBM Spectrum Protect.

## Restauración o recuperación de objeto parcial

---

El cliente de la aplicación puede recibir únicamente una parte del objeto. Esto se denomina una restauración de objeto parcial o una recuperación de objeto parcial.

Atención: La recuperación o restauración parcial de objetos cifrados o comprimidos produce resultados imprevisibles.

Nota: Si codifica la aplicación para que utilice una recuperación o restauración parcial de un objeto no es posible comprimir los datos mientras los envía. Para implementar esto, configure *ObjAttr.objCompressed* en *bTrue*.

Para realizar una restauración o recuperación de objeto parcial, asocie los siguientes campos de datos con cada entrada **GetList** de objeto:

desplazamiento

El desplazamiento de byte dentro del objeto en donde empezar a devolver datos.

longitud

El número de bytes de objeto para devolver.

Utilice `DSM_MAX_PARTIAL_GET_OBJ` con el fin de determinar el número máximo de objetos que pueden realizar una recuperación o restauración parcial de una lista **dsmBeginGetData** específica.

Los siguientes campos de datos, utilizados en la llamada **dsmBeginGetData**, determinan qué parte del objeto se restaura o recupera:

- Si tanto el desplazamiento como la longitud son cero, se restaura o recupera todo el objeto del almacenamiento IBM Spectrum Protect.
- Si el desplazamiento es mayor que cero, pero la longitud es cero, el objeto se restaura o recupera del desplazamiento hasta el final.
- Si la longitud es mayor que cero, sólo se recupera o restaura la parte del objeto desde el desplazamiento con la longitud especificada.

## Restaurar o recuperar datos

---

Después de realizar una consulta y de establecer una sesión con el servidor IBM Spectrum Protect, es posible ejecutar un procedimiento para restaurar o recuperar los datos.

### Procedimiento

---

Para restaurar o recuperar datos, complete los pasos siguientes:

1. Consulte al servidor IBM Spectrum Protect para archivar o realizar una copia de seguridad de los datos.
  2. Determine los objetos que se van a restaurar o recuperar del servidor.
  3. Ordene los objetos en el campo Restore Order.
  4. Envíe la llamada `dsmBeginGetData` con la lista de objetos a los que desea acceder.
  5. Envíe la llamada `dsmGetObj` para obtener cada objeto para el sistema. Es posible que se necesiten varias llamadas `dsmGetData` para cada objeto con el fin de obtener todos los datos del objeto asociado. Envíe la llamada `dsmEndGetObj` después de obtener todos los datos de un objeto.
  6. Envíe la llamada `dsmEndGetData` después de que todos los datos para todos los objetos se reciban o para e enviar la operación de recepción.
- Realizar consultas al servidor  
Antes de empezar ninguna operación de restauración o recuperación, consulte primero el servidor IBM Spectrum Protect para determinar qué objetos puede recibir del almacenamiento.
  - Seleccionar y ordenar objetos por orden de restauración  
Una vez que se ha realizado la consulta de copia de seguridad o archivado, el cliente de la aplicación debe determinar qué objetos, si es que hay alguno, se van a restaurar o recuperar.

- Iniciar la llamada `dsmBeginGetData`  
Después de seleccionar y ordenar los objetos que recibir, envíelos a IBM Spectrum Protect para una operación de restauración o de recuperación. La llamada **`dsmBeginGetData`** inicia una operación de restauración o recuperación. Los objetos se devuelven al cliente de la aplicación en el orden solicitado.
- Recibir todos los objetos para restaurar o recuperar  
Una vez que la llamada `dsmBeginGetData` se envía, es posible realizar un procedimiento para recibir cada uno de los objetos que se envían al servidor.

## Realizar consultas al servidor

Antes de empezar ninguna operación de restauración o recuperación, consulte primero el servidor IBM Spectrum Protect para determinar qué objetos puede recibir del almacenamiento.

Para enviar la consulta la aplicación debe introducir las estructuras y listas de parámetros adecuadas para la llamada `dsmBeginQuery`. La estructura debe incluir el espacio de archivos que la consulta examina y entradas que se ajustan a un patrón en los campos de nombre de alto y bajo rango. Si la sesión se inició con un nombre de propietario NULO, no es necesario especificar el campo del propietario. No obstante, si la sesión se inició con un nombre de propietario explícito, sólo se devuelven los objetos asociados con ese nombre de propietario.

La consulta `BackupQuery` de punto en el tiempo proporciona una instantánea del sistema en una hora determinada. Al especificar una fecha válida, es posible consultar todos los archivos a los que se les realizó una copia de seguridad a esa hora. Incluso si un objeto tiene una copia de seguridad activa de una fecha posterior, el punto en el tiempo modifica el estado de un objeto con el fin de que se devuelva la copia inactiva anterior. Para obtener más información, consulte el siguiente ejemplo: `pitDate`.

Una consulta devuelve toda la información que se almacenó con el objeto, además de la información en la tabla siguiente.

Tabla 1. Consultar la información devuelta por el servidor

Campo	Descripción
<code>copyId</code>	Los valores <code>copyIdHi</code> y <code>copyIdLo</code> proporcionan un número de 8 bytes que identifica de manera exclusiva este objeto para el nodo del almacenamiento de IBM Spectrum Protect. Utilice este ID para solicitar un objeto específico del almacenamiento de los procesos de restauración o recuperación.
<code>restoreOrderExt</code>	El valor <code>restoreOrderExt</code> proporciona un mecanismo para recibir objetos del almacenamiento de IBM Spectrum Protect de la manera más eficaz posible. Ordene los objetos para restaurar este valor y asegurarse de que las cintas sólo se montan una vez y se lee de adelante a atrás.

Debe guardar toda o parte de la información de la consulta para los procesos posteriores. No modifique los campos `copyId` y `restoreOrderExt` ya que se necesitan en la operación de restauración real. También es necesario conservarla información necesaria para abrir un archivo de datos o identificar un destino.

Llame a `dsmEndQuery` para finalizar la operación de consulta.

## Seleccionar y ordenar objetos por orden de restauración

Una vez que se ha realizado la consulta de copia de seguridad o archivado, el cliente de la aplicación debe determinar qué objetos, si es que hay alguno, se van a restaurar o recuperar.

Después se ordenan los objetos en orden ascendente (de bajo a alto). Este orden es muy importante para el rendimiento de la operación de restauración. Al ordenar los objetos en los campo **`restoreOrderExt`** se garantiza que los datos se leen desde el servidor en el orden más eficaz.

Primero se restauran todos los datos del disco, seguido de los datos en clases de medios que requieren montajes de volumen (como una cinta). El campo **`restoreOrderExt`** también garantiza que los datos de la cinta se lean en orden con el proceso empezando al principio de la cinta y progresando hacia el final.

Un orden adecuado en el campo **`restoreOrderExt`** significa que no se realizan montajes de cintas duplicados ni rebobinados de cintas innecesarios.

Un valor que no es cero en el campo **`restoreOrderExt.top`** se correlaciona con un dispositivo de acceso de serie único en el servidor IBM Spectrum Protect. Debido a que un dispositivo de acceso de serie sólo se puede utilizar en un punto de sesión/montaje a la vez, la aplicación debe asegurarse de que si utiliza varias sesiones no existen restauraciones simultaneas con el mismo valor **`restoreOrderExt.top`**. De lo contrario la primera sesión es capaz de acceder a los objetos, pero las otras sesiones esperan hasta que la primera sesión termina y el dispositivo esté disponible.

El siguiente ejemplo ilustra cómo ordenar objetos utilizando los campos **Restaurar orden**.

Figura 1. Ordenación de objetos con los campos Restaurar orden

```
typedef struct {
dsStruct64_t      objId;
dsUInt160_t      restoreOrderExt;

} SortOrder;          /* struct used for sorting */

=====
/* the code for sorting starts from here */
dsmQueryType      queryType;
qryBackupData     queryBuffer;
DataBlk           qDataBlkArea;
qryRespBackupData qbDataArea;
dsInt16_t         rc;
dsBool_t          done = bFalse;
int i = 0;
int qry_item;
SortOrder  sortorder[100]; /* sorting can be done up to 100 items
                           only right now. Set appropriate
                           array size to fit your needs */

/*-----+
| NOTE: Make sure that proper initializations have been done to
|   queryType,
|   queryBuffer, qDataBlkArea, and qbDataArea.
|
|-----*/

qDataBlkArea.bufferPtf = (char*) &qbDataArea;

rc = dsmBeginQuery(dsmHandle, queryType, (void *) &queryBuffer);

/*-----+
| Make sure to check rc from dsmBeginQuery
+-----*/
while (!done)
{
    rc = dsmGetNextQObj(dsmHandle, &qDataBlkArea);
    if ((rc == DSM_RC_MORE_DATA) ||
        (rc == DSM_RC_FINISHED))
        &&( qDataBlkArea.numBytes)
    {
        /*-----+
        /* transferring restoreOrderExt and objId */
        /*-----+
        sortorder[i].restoreOrderExt = qbDataArea.restoreOrderExt;
        sortorder[i].objId = qbDataArea.objId;

    } /* if ((rc == DSM_RC_MORE_DATA) || (rc == DSM_RC_FINISHED)) */
    else
    {
        done = bTrue;
        /*-----+
        /* take appropriate action. */
        /*-----+
    }

    i++;
    qry_item++;

} /* while (!done) */
rc = dsmEndQuery(dsmHandle);
/*check rc */
/*-----+
/* sorting the array using qsort. After the call, */
/* sortorder will be sorted by restoreOrderExt field */
/*-----+

qsort(sortorder, qry_item, sizeof(SortOrder), SortRestoreOrder);

/*-----+
| NOTE: Make sure to extract sorted object ids and store them in
|   any data structure you want.
|-----*/
```

```

/*-----+
| int SortRestoreOrder(SortOrder *a, SortOrder *b)
|
| This function compares restoreOrder fields from two structures.
| if (a > b)
|     return(GREATERTHAN);
|| if (a < b)
|     return(LESSTHAN);
|| if (a == b)
|     return(EQUAL);
|-----*/
int SortRestoreOrder(SortOrder *a, SortOrder *b)
{
    if (a->restoreOrderExt.top > b->restoreOrderExt.top)
        return(GREATERTHAN);
    else if (a->restoreOrderExt.top < b->restoreOrderExt.top)
        return(LESSTHAN);
    else if (a->restoreOrderExt.hi_hi > b->restoreOrderExt.hi_hi)
        return(GREATERTHAN);
    else if (a->restoreOrderExt.hi_hi < b->restoreOrderExt.hi_hi)
        return(LESSTHAN);
    else if (a->restoreOrderExt.hi_lo > b->restoreOrderExt.hi_lo)
        return(GREATERTHAN);
    else if (a->restoreOrderExt.hi_lo < b->restoreOrderExt.hi_lo)
        return(LESSTHAN);
    else if (a->restoreOrderExt.lo_hi > b->restoreOrderExt.lo_hi)
        return(GREATERTHAN);
    else if (a->restoreOrderExt.lo_hi < b->restoreOrderExt.lo_hi)
        return(LESSTHAN);
    else if (a->restoreOrderExt.lo_lo > b->restoreOrderExt.lo_lo)
        return(GREATERTHAN);
    else if (a->restoreOrderExt.lo_lo < b->restoreOrderExt.lo_lo)
        return(LESSTHAN);
    else
        return(EQUAL);
}

```

## Iniciar la llamada dsmBeginGetData

---

Después de seleccionar y ordenar los objetos que recibir, envíelos a IBM Spectrum Protect para una operación de restauración o de recuperación. La llamada **dsmBeginGetData** inicia una operación de restauración o recuperación. Los objetos se devuelven al cliente de la aplicación en el orden solicitado.

Rellene la información de estos dos parámetros en estas llamadas:

mountWait

Este parámetro indica al servidor si el cliente de la aplicación espera a que se monte un medio fuera de línea para obtener los datos de un objeto o si dicho objeto debe ignorarse durante el proceso de restauración o recuperación.

dsmGetObjListP

Este parámetro es una estructura de datos que contiene el campo **objId** el cual es una lista de todos los ID de objeto que se restauran o recuperan. Cada **objId** está asociado con una estructura **partialObjData** que describe si todo el **objId** o únicamente una sección particular del objeto va a recuperarse.

Cada **objId** tiene ocho bytes de longitud, con lo que una única solicitud de recuperación o restauración puede contener miles de objetos. El número de objetos que se solicitan en una única llamada está limitada a DSM\_MAX\_GET\_OBJ o DSM\_MAX\_PARTIAL\_GET\_OBJ.

## Recibir todos los objetos para restaurar o recuperar

---

Una vez que la llamada dsmBeginGetData se envía, es posible realizar un procedimiento para recibir cada uno de los objetos que se envían al servidor.

### Acerca de esta tarea

---

El código de retorno DSM\_RC\_MORE\_DATA significa que se ha devuelto un almacenamiento intermedio y debe llamar a dsmGetData de nuevo. Compruebe el DataBlk.numBytes para saber el número real de bytes retornados.

Cuando obtiene todos los datos de un objeto, debe enviar una llamada dsmEndGetObj. Si se reciben más objetos, envíe dsmGetObj de nuevo.

Si desea detener el proceso, por ejemplo, descartar cualquier dato que quede en la cadena de restauración para todos los objetos que no se han recibido todavía envíe la llamada `dsmEndGetData`. Esta llamada deshecha los datos del servidor al cliente. No obstante, es posible que este método tarde en finalizarse. Si desea finalizar una operación de restauración, utilice `dsmTerminate` para cerrar la sesión.

## Procedimiento

1. Envíe la llamada `dsmGetObj` para identificar el objeto que solicitó de la cadena de datos y para obtener el primer bloque de datos que está asociado con el objeto.
2. Envíe más llamadas `dsmGetData`, tantas como sean necesarias, para obtener los datos de objeto restantes.

## Diagramas de ejemplo de restauración y recuperación

Se pueden utilizar un diagrama de estado y un diagrama de flujo para ilustrar cómo realizar las operaciones de recuperación o restauración.

La flecha que va desde "In Get Object" a `dsmEndGetData` indica que puede enviar una llamada `dsmEndGetData` después de una llamada a `dsmGetObj` o `dsmGetData`. Es posible que tenga que hacer esto si ocurre una condición de error mientras obtiene un objeto del almacenamiento IBM Spectrum Protect y desea detener la operación. En circunstancias normales, no obstante, llame primero a `dsmEndGetObj`.

Figura 1. Diagrama de estado para operaciones de restauración y recuperación

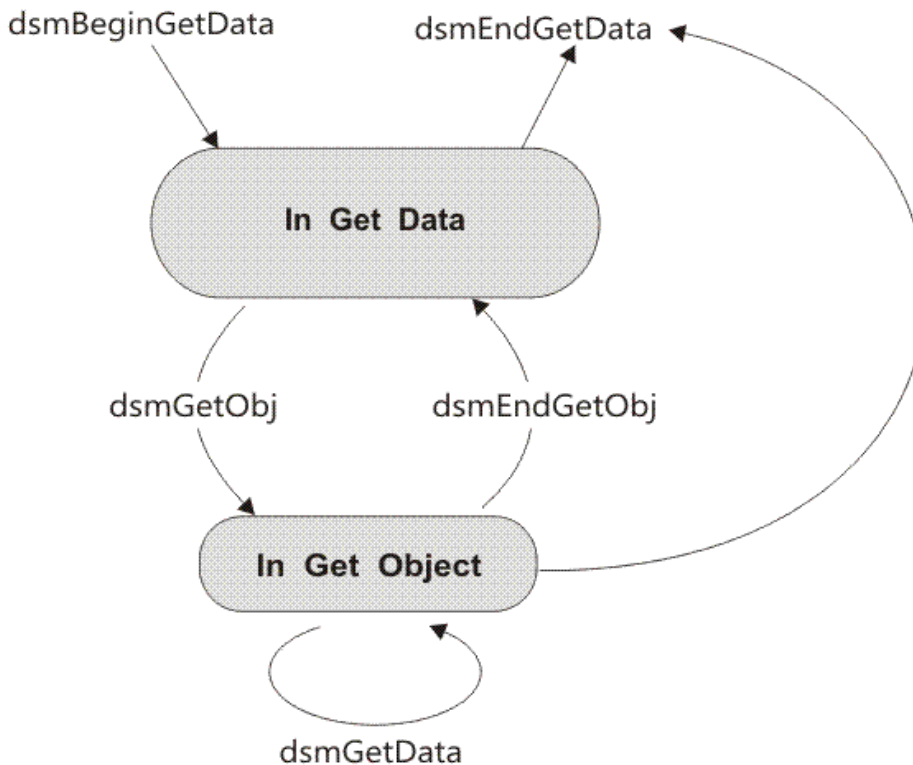
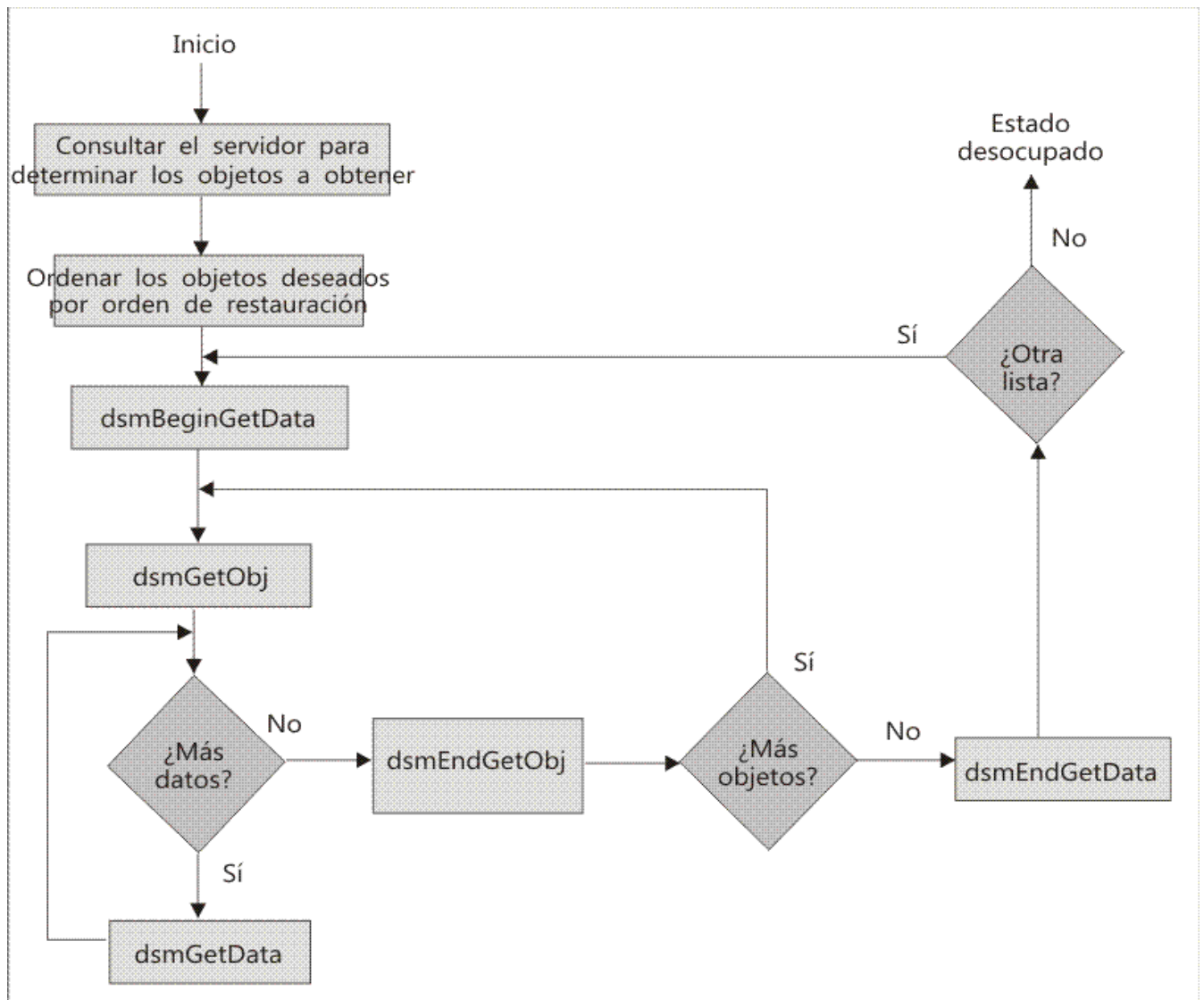


Figura 2 muestra el organigrama para llevar a cabo operaciones de recuperación o restauración.

Figura 2. Organigrama para operaciones de restauración y recuperación



## Ejemplo de código de recepción de datos de un servidor

Este ejemplo ilustra el uso de las funciones de API para recuperar datos del almacenamiento IBM Spectrum Protect.

La llamada de función **dsmBeginGetData** aparece dentro de una sentencia de cambio, con lo que es posible llamar a distintos parámetros dependiendo de si se trata de una operación de restauración o recuperación. La llamada de función **dsmGetData** se llama de dentro de un bucle que de forma repetida obtiene datos de un servidor hasta que se configura un indicador que permite la ejecución del programa para salir del bucle.

Figura 1. Un ejemplo de recibir datos de un servidor

```

/* Call dsmBeginQuery and create a linked list of objects to restore. */
/* Process this list to create the proper list for the GetData calls. */
/* Set up the getList structure to point to this list. */
/* This example is set up to perform a partial object retrieve. To */
/* retrieve only complete objects, set up: */
/*     getList.stVersion = dsmGetListVersion; */
/*     getList.partialObjData = NULL; */
dsmGetList getList;
getList.stVersion = dsmGetListPORVersion; /* structure version */
getList.numObjId = items; /* number of items in list */
getList.objId = (ObjID *)rest_ibuff; /* list of object IDs to restore */
getList.partialObjData = (PartialObjData *) part_ibuff; /* list of partial object data */

switch(get_type)
{
case (Restore_Get) :
    rc = dsmBeginGetData(dsmHandle, bFalse, gtBackup, &getList);

```



```

        break;
    case (Retrieve_Get) :
        rc = dsmBeginGetData (dsmHandle,bFalse,gtArchive,&getList);
        break;
    default : ;
}
if (rc)
{
    printf("*** dsmBeginGetData failed: ");
    rcApiOut(dsmHandle, rc);
    return rc;
}
/* Get each object from the list and verify whether it is on the */
/* server. If so, initialize structures with object attributes for */
/* data validation checks. When done, call dsmGetObj. */
rc = dsmGetObj (dsmHandle,objId,&dataBlk);
done = bFalse;
while(!done)
{
    if ( (rc == DSM_RC_MORE_DATA)
        || (rc == DSM_RC_FINISHED))
    {
        if (rc == DSM_RC_MORE_DATA)
        {
            dataBlk.numBytes = 0;
            rc = dsmGetData (dsmHandle,&dataBlk);
        }
        else
            done = bTrue;
    }
    else
    {
        printf("*** dsmGetObj or dsmGetData failed: ");
        rcApiOut(dsmHandle, rc);
        done = bTrue;
    }
} /* while */
rc = dsmEndGetObj (dsmHandle);
/* check rc from dsmEndGetObj */
/* check rc from dsmEndGetData */
rc = dsmEndGetData (dsmHandle);
return 0;

```

## Actualizar y eliminar objetos en el servidor

---

Las aplicaciones API pueden utilizar la llamada de función **dsmUpdateObj** o **dsmUpdateObjEx** para actualizar objetos que fueron archivados o a los que se le realizó una copia de seguridad. Utilice cualquiera de las llamadas en el estado de sesión únicamente, y actualice los objetos de uno en uno. Utilice **dsmUpdateObjEx** para actualizar cualquiera de los objetos que contienen el mismo nombre.

Para seleccionar un objeto archivado, configure la llamada de función **dsmSendType** en **stArchive**.

- Con **dsmUpdateObj**, sólo se actualiza el último objeto archivado con el nombre asignado.
- Con **dsmUpdateObjEx**, es posible actualizar cualquier objeto al especificar el ID del objeto correcto.

En un objeto archivado, la aplicación puede actualizar los siguientes campos:

- Descripción
- Información de objeto
- Propietario

Para seleccionar un objeto al que se le ha realizado una copia de seguridad, configure **dsmSendType** en **stBackup**. En objetos en los que se les ha realizado una copia de seguridad, sólo se actualiza la copia activa.

En un objeto al que se ha realizado una copia de seguridad, la aplicación puede actualizar los siguientes campos:

- Clase de gestión
- Información de objeto
- Propietario
- Eliminar objetos del servidor

Las aplicaciones API pueden realizar llamadas para eliminar objetos que fueron archivados o desactivar objetos a los que se les ha realizado una copia de seguridad. La supresión de objetos archivados depende de la autorización de nodo que se haya

asignado al registrar el administrador el nodo. Los administradores pueden especificar que los nodos puedan eliminar objetos archivados.

## Registro de eventos

---

Una aplicación de la API puede registrar mensajes de eventos en ubicaciones centrales. La aplicación puede dirigir el registro al servidor IBM Spectrum Protect , la máquina local o ambos. La llamada a función `dsmLogEventEx` se lleva a cabo dentro de una sesión. Para ver los mensajes registrados en el servidor, utilice el mandato de consulta `actlog` a través del cliente administrativo.

Utilice la opción de cliente de IBM Spectrum Protect , `errorlogretention`, para podar el archivo de registro de errores de cliente si la aplicación graba varios mensajes de cliente al registro de cliente `dsmLogType`, `logLocal` o `logBoth`.

Para obtener más información sobre registros de IBM Spectrum Protect, consulte la documentación del servidor de IBM Spectrum Protect.

## Resumen del diagrama de estado para la API de IBM Spectrum Protect

---

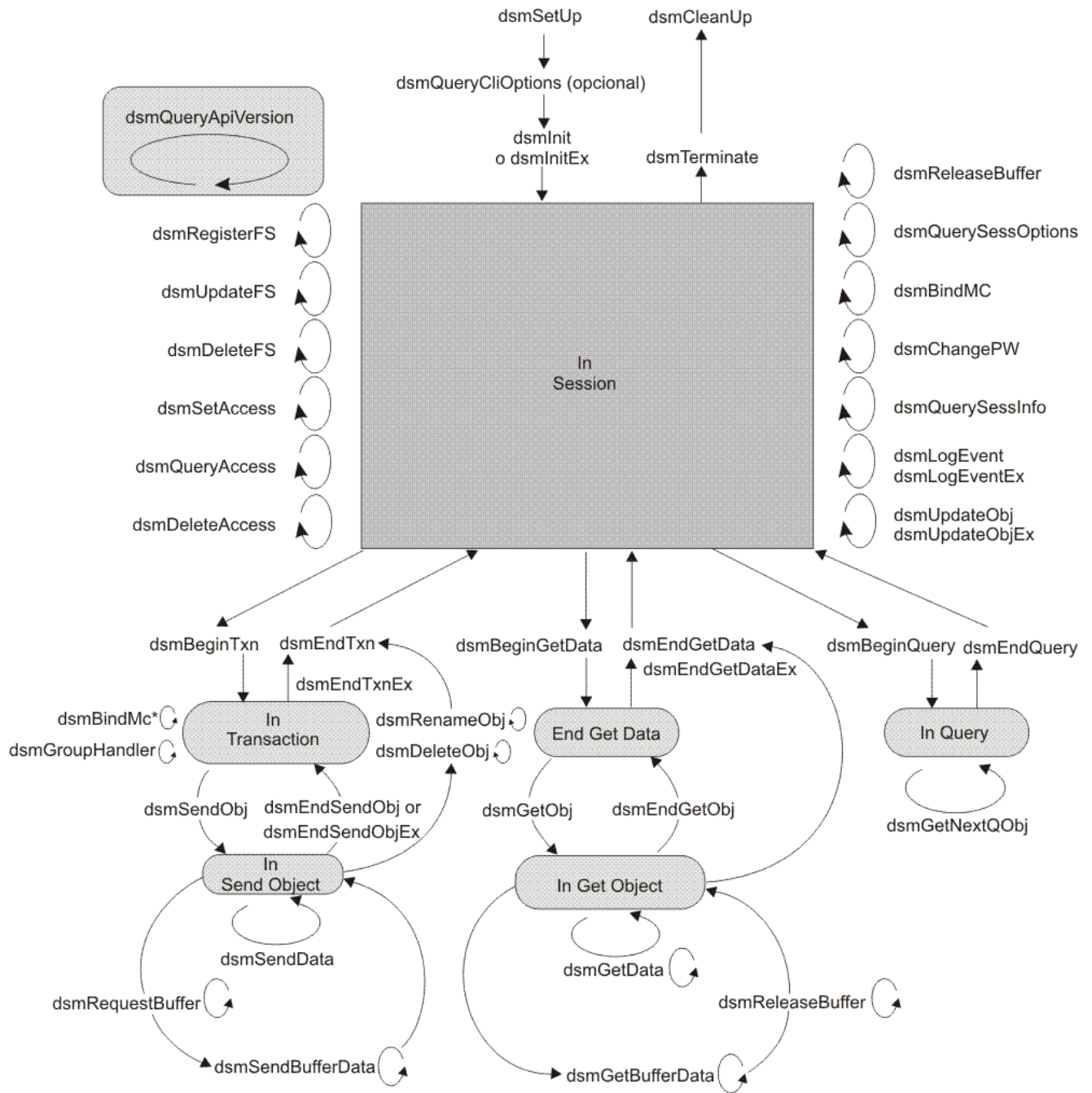
Una vez que haya leído todas las consideraciones para crear su propia aplicación con la API de IBM Spectrum Protect, revise este resumen de diagrama de estado en toda la aplicación.

Figura 1 contiene el diagrama de estado de la API. Contiene todos los diagramas de estado mostrados anteriormente además de varias llamadas que no se han mostrado.

Los puntos en este diagrama incluyen:

- Llamar a **`dsmQueryApiVersionEx`** en cualquier momento. No tiene un estado asociado. Consulte Figura 1 para obtener un ejemplo.
- Llamar a **`dsmQueryCliOptions`** antes de una llamada **`dsmInitEx`** únicamente.
- Utilizar **`dsmRegisterFS`**, **`dsmUpdateFS`**, y **`dsmDeleteFS`** para gestionar espacios de archivo. Estas llamadas se realizan desde dentro de un estado de sesión inactivo. Utilice la llamada **`dsmBeginQuery`** con el fin de consultar espacios de archivo. Para obtener más información acerca de las llamadas de espacios de archivo, consulte Gestionar espacios de archivos.
- Envíe la llamada **`dsmBindMC`** desde una sesión inactiva o desde un estado de transacción de objeto de envío. Consulte el ejemplo en Figura 1.
- Envíe la llamada **`dsmChangePW`** desde un estado de sesión inactivo.  
Nota: Si la llamada **`dsmInitEx`** devuelve un código de retorno de contraseña caducada, la llamada **`dsmChangePW`** debe realizarse antes de iniciar una sesión válida. Consulte Figura 3 para obtener un ejemplo que utiliza **`dsmChangePW`**.
- Si una llamada devuelve un error, el estado se queda como estaba. Por ejemplo, si **`dsmGetObj`** se devuelve con un error, el estado permanece In Get Data y una llamada a **`dsmEndGetObj`** es un error de secuencia de llamada.

Figura 1. Resumen del diagrama de estado de la API



\* Puede estar dentro o fuera de una transacción

## Conceptos básicos sobre la interoperatividad

API tiene dos tipos de interoperatividad: entre el cliente de copia de seguridad y archivado y las aplicaciones API y entre sistemas operativos diferentes.

- Interoperatividad del cliente de archivado/copia de seguridad  
La línea de mandato de archivado/copia de seguridad puede acceder a los objetos API para proporcionar una interoperatividad

limitada. Los objetos de la API sólo pueden visualizarse y accederse desde un cliente de línea de mandato de archivado/copia de seguridad y no pueden verse o accederse desde ninguna de las interfaces gráficas. El cliente de línea de mandato de archivado/copia de seguridad sólo puede restaurar contenido del archivo y nada más, con lo que sólo debe utilizarse para un tipo de operación de salvamento.

- Interoperatividad del sistema operativo

La API de IBM Spectrum Protect es compatible con la interoperatividad entre plataformas. Las aplicaciones en un sistema UNIX o Linux pueden funcionar en espacios de archivo de los que se realizan copias de seguridad desde un sistema de Windows. Del mismo modo, un sistema Windows puede operar en los espacios de archivos de copia de seguridad de un sistema UNIX o Linux.

- Soporte de copia de seguridad de varios nodos con el proxy de nodo de cliente

Las copias de seguridad de varios nodos que comparten almacenamiento se pueden consolidar en un nombre del nodo de destino común del servidor IBM Spectrum Protect. Este método es útil cuando el sistema que ejecuta la copia de seguridad puede cambiar en el tiempo, como con un clúster. Puede utilizar la opción `asnodename` para restaurar datos desde un sistema distinto al otro que ejecutó la copia de seguridad.

## Interoperatividad del cliente de archivado/copia de seguridad

---

La línea de mandato de archivado/copia de seguridad puede acceder a los objetos API para proporcionar una interoperatividad limitada. Los objetos de la API sólo pueden visualizarse y accederse desde un cliente de línea de mandato de archivado/copia de seguridad y no pueden verse o accederse desde ninguna de las interfaces gráficas. El cliente de línea de mandato de archivado/copia de seguridad sólo puede restaurar contenido del archivo y nada más, con lo que sólo debe utilizarse para un tipo de operación de salvamento.

Se proporcionan las siguientes acciones de línea de mandato:

- Eliminar archivado
- Eliminar espacio de archivo
- Consulta
- Restaurar
- Recuperar
- Configurar acceso

La información de ruta contiene los directorios de los objetos de cliente de archivado/copia de seguridad. Por el contrario, es posible que la información de ruta de objeto API no tenga ninguna relación con los directorios existentes: es posible que la ruta esté totalmente inventada. La interoperatividad no cambia este aspecto de los tipos de objeto. Para utilizar esta función correctamente, siga las reglas y restricciones.

Notas:

1. No existe interoperatividad entre el cliente de archivado/copia de seguridad y los objetos API almacenados en un servidor de protección de retención.
  2. No es posible utilizar los GUI de cliente de archivado/copia de seguridad para acceder a archivos que se han almacenado utilizando el cliente API. Sólo es posible utilizar la línea de mandato para acceder a estos archivos.
- Asignar nombres a los objetos de la API  
Establece una convención de nomenclatura para los nombres de objeto de API. La convención de nomenclatura debe ofrecer servicios para el nombre de espacio de archivos, el calificador de alto nivel y el calificador de bajo nivel. El nombre de espacio de archivos y los calificadores de alto nivel pueden hacer referencia a nombres de directorio reales. Cada nombre de objeto puede consistir en más de un nombre de directorio que se aplica al calificador de bajo rango.
  - Mandatos del cliente de copia de seguridad/archivado que se pueden utilizar con la API  
Es posible utilizar un subconjunto de mandatos de cliente de copia de seguridad/archivado dentro de una aplicación. Por ejemplo, puede ver y gestionar objetos que son propiedad de otros usuarios ya sea en el mismo nodo o en nodos distintos.

## Asignar nombres a los objetos de la API

---

Establece una convención de nomenclatura para los nombres de objeto de API. La convención de nomenclatura debe ofrecer servicios para el nombre de espacio de archivos, el calificador de alto nivel y el calificador de bajo nivel. El nombre de espacio de archivos y los calificadores de alto nivel pueden hacer referencia a nombres de directorio reales. Cada nombre de objeto puede consistir en más de un nombre de directorio que se aplica al calificador de bajo rango.

Por comodidad, utilice el nombre del objeto que no tiene el prefijo con la información de directorio como calificador de nivel bajo. Para obtener más información, consulte el apartado ID y nombres de objeto.

Los nombres del espacio de archivos debe estar totalmente calificados cuando se hace referencia a ellos desde la API o la línea de mandatos de la copia de seguridad/archivado. Por ejemplo, en un sistema operativo UNIX o Linux, registra los siguientes espacios de archivo:

- /a
- /a/b

Cuando hace referencia a /a, se muestran los objetos que están relacionados sólo al espacio de archivo /a. Para ver objetos que están relacionados con /a/b, debe especificar /a/b como nombre del espacio de archivos.

Después de registrar ambos espacios de archivo, si hace una copia de seguridad del objeto b en el espacio de archivos /a, la consulta para /a/b continúa mostrando objetos que están relacionados únicamente a espacio de archivos /a/b.

La excepción a esta restricción ocurre en las referencias de espacio de archivo cuando se intenta consultar o eliminar espacios de archivo con la API. En ambos casos, los nombres de espacio de archivos no tiene que estar completos si utiliza un carácter comodín. Por ejemplo, /a\* hace referencia a /a y /a/b.

Consejo: Si le importa la interoperatividad, evite los nombres de espacio de archivos que se solapen.

En los sistemas Windows, introduzca los nombres de espacio de archivos entre corchetes { } para los objetos de la API cuando acceda a los objetos desde la interfaz de línea de mandatos de archivado y copia de seguridad. Los sistemas operativos Windows colocan automáticamente nombres de espacio de archivos en letras en mayúsculas cuando registra o hace referencia a los nombres. Sin embargo, esta función automática no ocurre para el resto de la especificación de nombre de objeto. Si desea una interoperatividad total, introduzca el calificador de alto rango y el de bajo rango en mayúsculas en la aplicación cuando se realizan copias de seguridad de los objetos API. Si la aplicación no tiene calificadores de alto nivel en mayúsculas (nombres de directorio) ni calificadores de bajo nivel (nombres de archivo) antes de enviar los objetos al servidor, no podrá acceder a los objetos directamente por nombre a través del cliente de archivado y copia de seguridad.

Por ejemplo, si hay un objeto almacenado en el servidor como{"FileSpaceName"}\TEST\MYDIRNAME\file.txt, no puede restaurarlo directamente o consultar al objeto file.txt porque la aplicación no puso en mayúsculas el nombre del archivo antes de que se copiase al servidor. La única forma de manipular estos objetos es utilizar los caracteres comodines. Por ejemplo, para consultar \TEST\MYDIRNAME\file.txt, un cliente de archivado y copia de seguridad debe utilizar los caracteres comodín para todas las partes del nombre del objeto que no se pusieron en mayúscula antes de enviarse al servidor. El siguiente mandato debe utilizarse para consultar este archivo file.txt:

```
dsmc query backup {"FileSpaceName"}\TEST\MYDIRNAME\*
```

Si cualquiera de los otros calificadores también se han guardado en minúsculas, esos calificadores también deben consultarse utilizando comodines. Por ejemplo, para consultar un objeto que se guarda como{"FileSpaceName"}\TEST\mydirname\file.txt, utilice el siguiente mandato:

```
dsmc query backup {"FileSpaceName"}\TEST\*\*
```

El siguiente ejemplo demuestra estos conceptos. En Windows y UNIX o en entornos de Linux, no tiene que especificar los calificadores de alto nivel o bajo nivel completos. Sin embargo, si no especifica el calificador completo, debe utilizar el carácter comodín.

Plataforma	Ejemplo
Windows	<p>Para consultar todos los archivos a los que se ha realizado copia de seguridad en el espacio de archivos MYFS, entre la siguiente serie:</p> <pre>dsmc q ba "{MYFS}\*\*"</pre> <p>Debe utilizar al menos un asterisco (*) para cada uno de los calificadores de alto y bajo rango.</p>
UNIX o Linux	<p>Para consultar todos los archivos a los que se ha realizado copia de seguridad en el espacio de archivos /A, entre la siguiente serie:</p> <pre>dsmc q ba "/A/*/*"</pre> <p>Debe utilizar al menos un asterisco (*) para cada uno de los calificadores de alto y bajo rango.</p>

## Mandatos del cliente de copia de seguridad/archivado que se pueden utilizar con la API

Es posible utilizar un subconjunto de mandatos de cliente de copia de seguridad/archivado dentro de una aplicación. Por ejemplo, puede ver y gestionar objetos que son propiedad de otros usuarios ya sea en el mismo nodo o en nodos distintos.

Para ver y gestionar objetos propiedad de otros usuarios ya sea en el mismo nodo o en nodos distintos, lleve a cabo estos pasos:

1. De acceso con el mandato set access.
2. Especifique el propietario y el nodo. Utilice las opciones *fromowner* y *fromnode* de la línea de mandato de archivado/copia de seguridad con el fin de especificar el propietario y el nodo. Por ejemplo:

```
dsmc q ba "/A/*/*" -fromowner=other_owner -fromnode=other_node
```

Tabla 1 describe los mandatos que se pueden utilizar con los objetos API.

Tabla 1. Mandatos de cliente de archivado/copia de seguridad que puede utilizar con los objetos API

Mandato	Descripción
Delete Archive	Los archivos archivados propiedad del usuario actual se pueden eliminar. La configuración del mandato set access no afecta a este mandato.
Delete Filespace	El mandato delete filespace afecta a los objetos de la API.
Consulta	En la línea de mandato de archivado y copia de seguridad es posible consultar los objetos API archivados o que se les ha realizado una copia de seguridad y objetos propiedad de otros usuarios, o que residen en otros nodos. Consulte Asignar nombres a los objetos de la API para obtener más información sobre consultar objetos API.  Utilizar la opción existente <i>-fromowner</i> con el fin de consultar objetos propiedad de un usuario distinto para los que se han dado los permisos de acceso. Utilizar la opción existente <i>-fromnode</i> con el fin de consultar objetos que existen en otro nodo par a el que se definen los permisos de acceso que se han concedido. Para obtener más información, consulte dsmInitEx.
Restaurar Recuperar	Nota: Utilice estos mandatos solo para las situaciones de excepción. Los objetos API cifrados con la clave gestionada por la aplicación se pueden recuperar o restaurar si la clave de cifrado se conoce o guarda en el archivo de la contraseña o en el registro. Los objetos de API se cifran mediante el cifrado transparente que no se puede restaurar o recuperar mediante el cliente de archivado y copia de seguridad.  Estos mandatos devuelven los datos como archivos de bit que se crean utilizando los atributos de archivo predeterminados. Es posible restaurar o recuperar objetos API propiedad de otros usuarios o que son de un nodo diferente. El mandato de acceso determina qué objetos son aptos.
Set Access	El mandato set access permite a los usuarios gestionar objetos API propiedad de otro usuario, o que residen en otro nodo.

## Interoperatividad del sistema operativo

La API de IBM Spectrum Protect es compatible con la interoperatividad entre plataformas. Las aplicaciones en un sistema UNIX o Linux pueden funcionar en espacios de archivo de los que se realizan copias de seguridad desde un sistema de Windows. Del mismo modo, un sistema Windows puede operar en los espacios de archivos de copia de seguridad de un sistema UNIX o Linux.

### Acerca de esta tarea

De forma predeterminada, los objetos de un sistema UNIX son compatibles con los nombres de los objetos de otros sistemas UNIX. De forma predeterminada, los objetos de los sistemas Windows son compatibles con los nombres de los objetos de los sistemas UNIX. Varios parámetros controlan la asignación de nombres de los objetos en los espacios de archivo de IBM Spectrum Protect. Si configura una aplicación de forma adecuada, las aplicaciones que se ejecutan en sistemas tanto Windows como UNIX pueden utilizar los nombres de objetos. Utilice los mismos parámetros para la copia de seguridad y la restauración de objetos.

Restricción: Una aplicación Windows que utiliza Unicode crea un espacio de archivo que no es compatible con las aplicaciones que se ejecutan en sistemas UNIX.

### Procedimiento

Para conseguir la interoperatividad, siga estas tareas de configuración:

1. Establezca una nomenclatura coherente. Seleccione un carácter para el delimitador `dir`, tal como una barra inclinada (/) o una barra invertida (\). Coloque este carácter delimitador de directorios delante del nombre del espacio de archivos, el calificador de alto nivel y el calificador de bajo nivel.
2. Cuando llame a `dsmInitEx`, defina el valor del campo `dirDelimiter` en el carácter delimitador de directorio que ha seleccionado y establezca `bCrossPlatform` en `bTrue`.
3. Configure el indicador `useUnicode` en `bFalse` cuando utiliza la interfaz IBM Spectrum Protect. Los nombres de archivos Unicode no son compatibles con los nombres de archivo que no son de Unicode.

## Soporte de copia de seguridad de varios nodos con el proxy de nodo de cliente

Las copias de seguridad de varios nodos que comparten almacenamiento se pueden consolidar en un nombre del nodo de destino común del servidor IBM Spectrum Protect. Este método es útil cuando el sistema que ejecuta la copia de seguridad puede cambiar en

el tiempo, como con un clúster. Puede utilizar la opción `asnodename` para restaurar datos desde un sistema distinto al otro que ejecutó la copia de seguridad.

## Acerca de esta tarea

---

Utilice la opción `asnodename` en la serie de opciones `dsmInitEx` para hacer copia de seguridad, archivar, restaurar y restablecer o consultar o suprimir datos bajo el nombre de nodo de destino en el servidor IBM Spectrum Protect. También puede especificar la opción `asnodename` en el archivo `dsm.opt` o `dsm.sys`.

Restricción: No utilice nodos de destino como nodos tradicionales, especialmente si cifra los archivos antes de realizar una copia de seguridad de ellos en el servidor.

## Procedimiento

---

Para habilitar esta opción, complete los pasos siguientes:

1. Instale el cliente de la API en todos los nodos de un entorno de datos compartido.
2. Si no está ya registrado, registre cada uno de los nodos con el servidor de IBM Spectrum Protect. Registre los nombres de nodo de "destino" comunes que van a compartir cada uno de los nodos agente utilizados en el entorno de datos compartido.
3. Registre cada uno de los nodos de agente del entorno de datos compartidos con el servidor. El nombre de nodo de agente se utiliza para la autenticación. Los datos no se almacenan utilizando el nombre de nodo del agente cuando se utiliza la opción `asnodename`.
4. Solicite al administrador que otorgue autoridad de proxy a todos los nodos del entorno compartido para acceder al nombre de nodo de destino en el servidor IBM Spectrum Protect, utilizando `grant proxynode`.
5. Utilice el mandato de cliente administrativo `query proxynode` para mostrar los nodos de cliente que tienen autoridad para realizar operaciones de cliente en nombre de otro nodo. Esta autorización la otorga el mandato `grant proxynode`. O bien utilice el mandato `dsmQuery` con el tipo de consulta `qtProxyNodeAuth` con el fin de ver los nodos para los que este nodo puede actuar como proxy.
6. Si la aplicación está utilizando el cifrado de usuario de datos, no `TSMENCRKEY`, asegúrese de que todos los nodos están utilizando la misma clave de cifrado. Debe utilizar la misma clave de cifrado en todos los archivos a los que se les ha realizado una copia de seguridad en el entorno del nodo compartido.

### Tareas relacionadas:

Soporte de copia de seguridad de datos con el proxy del nodo de cliente (sistemas UNIX y Linux)

Soporte de copia de seguridad de datos con el proxy del nodo de cliente (sistemas Windows)

## Utilización de la API con Unicode

---

La API IBM Spectrum Protect soporta Unicode UCS2, una página de códigos de doble byte y de longitud fija cuyo código apunta a todas las páginas conocidas como Japonés, Chino o Alemán. Soporta hasta 65535 códigos únicos.

Restricción: Esta función sólo está disponible en Windows.

Con Unicode, la aplicación puede realizar copias de seguridad y recuperar nombres de archivos en cualquier conjunto de caracteres de la misma máquina. Por ejemplo, en una máquina inglesa, es posible realizar una copia de seguridad y restaurar los nombres de archivo en una página de códigos de cualquier otro idioma.

- **Cuándo se utiliza Unicode**  
Es posible simplificar una aplicación que soporta varios idiomas al grabar una aplicación Unicode y sacar partido de la interfaz Unicode de IBM Spectrum Protect.
- **Configuración de Unicode**  
Para configurar y utilizar Unicode debe realizar un procedimiento particular para que la API registre un espacio de archivo Unicode en el servidor y que todos los nombres de archivo en dicho espacio se conviertan en cadenas Unicode.

## Cuándo se utiliza Unicode

---

Es posible simplificar una aplicación que soporta varios idiomas al grabar una aplicación Unicode y sacar partido de la interfaz Unicode de IBM Spectrum Protect.

Utilice la interfaz Unicode de IBM Spectrum Protect si alguna de las siguientes condiciones es verdadera:

- Si la aplicación ya está compilada para Unicode y estaba convirtiendo a un conjunto de caracteres multibyte (mbcs) antes de llamar al API IBM Spectrum Protect.
- Si está grabando una aplicación nueva y desea capacitarlas para soportar Unicode.
- Si la aplicación utiliza una cadena que le llega de un sistema operativa o de otra aplicación que utiliza Unicode.

Si no necesita Unicode, no es necesario compilar la aplicación de nuevo.

La API continúa soportando la interfaz dsm. El SDK de la API contiene los programas de ejemplo callmtu1.c y callmtu2.c que muestran cómo utilizar la API de Unicode. Utilice **makemtu** para compilar estos programas.

## Configuración de Unicode

---

Para configurar y utilizar Unicode debe realizar un procedimiento particular para que la API registre un espacio de archivo Unicode en el servidor y que todos los nombres de archivo en dicho espacio se conviertan en cadenas Unicode.

Restricción: No es posible almacenar nombres de archivo Unicode y no Unicode en el mismo espacio de archivo.

1. Compilar el código con el indicador `-DUNICODE`.
2. Todas las cadenas de la aplicación deben ser cadenas de caracteres comodín.
3. Siga las estructuras del archivo `tmapitd.h`, y las definiciones de función del archivo `tmapifp.h` en las llamadas al API.
4. Configure el indicador `useUnicode` en `bTrue` en la llamada de función **tsmInitEx**. Cualquier espacio de archivo nuevo se registra como un espacio de archivo Unicode.

Cuando envía datos a espacios de archivo no Unicode registrados previamente, la API continúa enviando nombres de archivo como no Unicode. Renombre los espacios de archivo antiguos en el servidor como `fsname_old` e inicie un espacio de archivo nuevo con datos nuevos. La API restaura los datos que no son Unicode de los espacios de archivo antiguos. Utilice el campo **bIsUnicode** en la estructura **tsmQryRespFSDData** que se devuelve en un espacio de archivo de una consulta para determinar si un espacio de archivo es o no Unicode.

Cada llamada de función **dsmXXX** tiene una llamada de función **tsmXXX** correspondiente. La diferencia entre las dos son las estructuras que utilizan. Todas las estructuras de llamada a función **tsmXXX** tienen tipos `dsChar_t` types para los valores de cadena cuando se compilan con el distintivo `UNICODE`. `dsChar_r` se correlaciona con un carácter comodín. No hay otras diferencias entre estas interfaces.

Restricción: Utilice una interfaz o la otra. No mezcle las interfaces de llamada a función **dsmXXX** y de llamada a función **tsmXXX**. Asegúrese de que utiliza las estructuras de IBM Spectrum Protect y las definiciones de la versión IBM Spectrum Protect.

Algunas constantes continúan definiéndose en el archivo `dsmapiitd.h`, con lo que necesita tanto el archivo `dsmapiitd.h` como el archivo `tsmapiitd.h` en la compilación.

Puede utilizar la interfaz de IBM Spectrum Protect en otros sistemas operativos, como por ejemplo UNIX o Linux, pero en estos sistemas operativos, el tipo `dsChar_t` se correlaciona con `char` porque Unicode solo recibe soporte con sistemas operativos Windows. Sólo puede grabar una variación de la aplicación y compilar en más de un sistema operativo utilizando la interfaz de IBM Spectrum Protect. Si está escribiendo una aplicación nueva, utilice la interfaz de IBM Spectrum Protect.

Si está actualizando una aplicación existente:

1. Convierta las estructuras de llamada a función **dsmXXX** y las llamadas a la interfaz de IBM Spectrum Protect.
2. Migre los espacios de archivos existentes.
3. Realice copias de seguridad de los espacios de archivo nuevo con el indicador `useUnicode` configurado en `true`.

Nota: Después de utilizar un cliente capacitado para Unicode para acceder a un nodo, no es posible conectarse al mismo nodo con una versión antigua de la API o con una API de otro sistema operativo. Si su aplicación utiliza funciones de plataforma cruzada, no utilice el indicador Unicode. No hay compatibilidad de plataforma cruzada entre sistemas operativos Unicode y no Unicode.

Cuando habilita el indicador `useUnicode`, todas las estructuras de cadena se consideran cadenas Unicode. En el servidor, sólo los siguientes campos son verdaderamente Unicode:

- Nombre de espacio de archivo
- Alto rango
- Bajo rango
- Descripción de la copia archivada

Todos los campos restantes convierten a `mbsc` en la página de código local antes de que se envíen al servidor. Los campos, como el nombre de nodo, son cadenas de caracteres comodín. Deben ser válidos en el entorno regional actual. Por ejemplo, en una máquina japonesa, es posible hacer copias de seguridad de archivos con nombres chinos, pero el nombre del nodo debe ser una cadena válida en japonés. El archivo de opción permanece en la página de código actual. Si necesita crear una lista de inclusión/exclusión Unicode, utilice la opción `inclxcl` con un nombre de archivo y cree un archivo Unicode con patrones Unicode.

### Referencia relacionada:

Opción `Inclxcl`

## Llamadas a función de la API

---



Tabla 1 proporciona una lista por orden alfabético de las llamadas de función de la API, una descripción breve y la ubicación de la información más detallada acerca de la llamada de función, la cual incluye:

Elemento	Descripción
<b>Objetivo</b>	Describe la llamada de función.
<b>Sintaxis</b>	<p>Contiene el código C real de la llamada de función. Este código se copia de la versión del archivo de encabezado dsmapifp.h UNIX o Linux. Consulte Archivo de origen de las definiciones de la función de la API.</p> <p>Este archivo cambia ligeramente en otros sistemas operativos. Los programadores de aplicación de otros sistemas operativos deben comprobar su versión del archivo de encabezado, dsmapifp.h, para obtener la sintaxis exacta de las definiciones de la API.</p>
<b>Parámetros</b>	Describe cada uno de los parámetros en la llamada de función, identificándola como una entrada (I) o salida (O), dependiendo de cómo se utilice. Algunos parámetros están diseñados para funcionar tanto de entrada como de salida (I/O). Los tipos de datos que se mencionan en esta sección se definen en el archivo de encabezado dsmapihd.h. Consulte el apartado Archivos de origen de definiciones de tipo de API.
<b>Códigos de retorno</b>	Contiene una lista de los códigos de retorno que son específicos a la llamada de función. Los errores del sistema generales, como los errores de comunicación, problemas del servidor o errores del usuario que puedan aparecer en una llamada no se incluyen en la lista. Los códigos de retorno se definen en el archivo de encabezado dsrmrc.h. Consulte Archivo de origen de códigos de retorno de la API: dsrmrc.h.

Tabla 1. Llamadas a función de la API

Llamada a función y vínculo	Descripción
dsmBeginGetData	Inicia una operación de restauración o recuperación en una lista de objetos del almacenamiento.
dsmBeginQuery	Inicia una solicitud de consulta para IBM Spectrum Protect para obtener información.
dsmBeginTxn	Inicia una o más transacciones que empiezan una acción completa. O bien todas las acciones tienen éxito o ninguna.
dsmBindMC	Asocia o vincula una clase de gestión al objeto que pasa.
dsmChangePW	Cambia una contraseña de IBM Spectrum Protect.
dsmCleanUp	Esta llamada se utiliza si se ha llamado a <b>dsmSetUp</b> .
dsmDeleteAccess	Elimina las reglas de autorización de las copias de seguridad o archivadas de los objetos.
dsmDeleteFS	Elimina un espacio de archivo del almacenamiento.
dsmDeleteObj	Desactiva copias de seguridad, o elimina copias archivadas del almacenamiento.
dsmEndGetData	Finaliza una sesión <b>dsmBeginGetData</b> que obtiene objetos del almacenamiento.
dsmEndGetDataEx	Proporciona el total de bytes sin LAN que fueron enviados.
dsmEndGetObj	Finaliza una sesión <b>dsmGetObj</b> que obtiene datos de un objeto especificado.
dsmEndQuery	Significa el final de una acción <b>dsmBeginQuery</b> .
dsmEndSendObj	Indica el final de los datos que se envían al almacenamiento.
dsmEndSendObjEx	Proporciona información de compresión y el número de bytes que se enviaron.
dsmEndTxn	Finaliza una transacción de IBM Spectrum Protect.
dsmEndTxnEx	Proporciona información acerca del ID del objeto líder que se utiliza en la llamada <b>dsmGroupHandlerfunction</b> .
dsmGetData	Obtiene una cadena de byte de datos de IBM Spectrum Protect y la coloca en el almacenamiento intermedio del llamador.
dsmGetBufferData	Obtiene un almacenamiento intermedio asignado por IBM Spectrum Protect de datos del servidor IBM Spectrum Protect.
dsmGetNextQObj	Obtiene la siguiente respuesta de una llamada previa <b>dsmBeginQuery</b> y la coloca en el almacenamiento intermedio del llamador.
dsmGetObj	Obtiene los datos del objeto solicitados de la corriente de datos y los coloca en el almacenamiento intermedio del llamador.

Llamada a función y vínculo	Descripción
dsmGroupHandler	Realiza una acción en un grupo de archivos lógico dependiendo de la entrada dada.
dsmInit	Inicia una sesión de la API y conecta al cliente con el almacenamiento.
dsmInitEx	Inicia una sesión de la API utilizando parámetros adicionales que permiten la verificación extendida.
dsmLogEvent	Registra un mensaje de usuario al archivo de registros del servidor, al registro de error local o a ambos.
dsmLogEventEx	Registra un mensaje de usuario al archivo de registros del servidor, al registro de error local o a ambos.
dsmQueryAccess	Realiza una consulta al servidor acerca de todas las reglas de autorización de acceso en versiones de copias archivadas o de copias de seguridad de objetos.
dsmQueryApiVersion	Realiza una solicitud de consulta acerca de la versión de la biblioteca de la API a la que accede el cliente de la aplicación.
dsmQueryApiVersionEx	Realiza una solicitud de consulta acerca de la versión de la biblioteca de la API a la que accede el cliente de la aplicación.
dsmQueryCliOptions	Consulta valores de opción importantes en los archivos de opción del usuario.
dsmQuerySessInfo	Inicia una solicitud de consulta a IBM Spectrum Protect sobre información relacionada con la operación de la sesión especificada en <b>dsmHandle</b> .
dsmQuerySessOptions	Consulta valores de opción importantes que son válidos en la sesión especificada en <b>dsmHandle</b> .
dsmRCMsg	Obtiene el texto del mensaje que está asociado con el código de retorno de la API.
dsmRegisterFS	Registra un espacio de archivo nuevo con el servidor.
dsmReleaseBuffer	Devuelve un almacenamiento intermedio asignado por IBM Spectrum Protect.
dsmRenameObj	Renombra el alto y bajo rango del objeto.
dsmRequestBuffer	Obtiene un almacenamiento intermedio asignado por IBM Spectrum Protect para la eliminación de una copia de almacenamiento intermedio.
dsmRetentionEvent	Envía una lista de ID de objetos al servidor, con una operación de evento de retención para que se realice en estos objetos.
dsmSendBufferData	Envía datos de un almacenamiento intermedio asignado por IBM Spectrum Protect.
dsmSendData	Envía una corriente de bytes de datos a IBM Spectrum Protect a través de un almacenamiento intermedio.
dsmSendObj	Inicia una solicitud para enviar un objeto único al almacenamiento.
dsmSetAccess	Da a otros usuarios o nodos acceso a versiones de copia de seguridad o copias archivadas de los objetos, acceso a todos los objetos o acceso a un grupo determinado.
dsmSetUp	Sobrescribe los valores de variable de entorno.
dsmTerminate	Finaliza una sesión con el servidor y limpia el entorno de IBM Spectrum Protect.
dsmUpdateFS	Actualiza un espacio de archivo en el almacenamiento.
dsmUpdateObj	Actualiza la información objInfo que está asociada con una copia de seguridad activa de un objeto que ya está en el servidor, o actualiza objetos archivados.
dsmUpdateObjEx	Actualiza la información objInfo que está asociada con un objeto archivado específico incluso cuando existen varios objetos con el mismo nombre, o actualiza copias de seguridad activas.

- dsmBeginGetData  
La llamada de función **dsmBeginGetData** inicia una operación de restauración o recuperación en la lista de objetos del almacenamiento. La lista de objetos se encuentra dentro de la estructura **dsmGetList** . La aplicación crea esta lista con los valores de la consulta que precede a una llamada a **dsmBeginGetData**.
- dsmBeginQuery  
La llamada a la función dsmBeginQuery inicia una solicitud de consulta al servidor sobre datos, archivos y clases de gestión.
- dsmBeginTxn  
La llamada de función **dsmBeginTxn** inicia una o más transacciones IBM Spectrum Protect que a su vez comienzan una acción

completa; todas las acciones se procesan correctamente o ninguna de ellas. Una acción puede ser una llamada única o una serie de llamadas. Por ejemplo, una llamada **dsmSendObj** seguida por un número de llamadas **dsmSendData** se puede considerar una acción única. Del mismo modo, una llamada **dsmSendObj** con **dataBlkPtr** que indica el área de datos que contiene el objeto del que se realizará una copia de seguridad también se considera una acción única.

- **dsmBindMC**  
La llamada de función **dsmBindMC** asocia, o vincula, una clase de gestión al objeto que pasa. El objeto pasa a través de una lista de inclusión/exclusión a la que se apunta en el archivo de opciones. Si no se encuentra una coincidencia de una clase de gestión específica en la lista de inclusión, se asigna la clase de gestión predeterminada. La lista de inclusión puede impedir objetos de una copia de seguridad pero no de una copia de archivado.
- **dsmChangePW**  
La llamada a función **dsmChangePW** cambia una contraseña de IBM Spectrum Protect. En un sistema operativo de varios usuarios como UNIX o Linux, solo el usuario raíz o el usuario autorizado pueden utilizar esta llamada.
- **dsmCleanUp**  
La llamada de función **dsmCleanUp** se utiliza si se ha llamado a **dsmSetUp**. La llamada de función **dsmCleanUp** debe llamarse después de **dsmTerminate**. No es posible realizar ninguna otra llamada después de llamar a **dsmCleanUp**.
- **dsmDeleteAccess**  
La llamada de función **dsmDeleteAccess** elimina las reglas de autorización actuales para las versiones de las copias de seguridad o las copias de archivado de los objetos. Cuando se suprime una regla de autorización, se revoca el acceso de un usuario a los archivos que especifica la regla.
- **dsmDeleteFS**  
La llamada de función **dsmDeleteFS** elimina un espacio de archivo del almacenamiento. Para eliminar un espacio de archivo, debe tener permisos apropiados que el administrador IBM Spectrum Protect le habrá otorgado. Para determinar si cuenta con los permisos necesarios, llame a **dsmQuerySessInfo**. Esta llamada de función devuelve una estructura de datos de tipo *ApiSessInfo*, que incluye dos campos, *archDel* y *backDel*.
- **dsmDeleteObj**  
La llamada de función **dsmDeleteObj** inactiva copias de seguridad de objetos, elimina copias de seguridad de objetos o eliminar objetos archivados en el almacenamiento. El tipo **dtBackup** inactiva únicamente la copia de seguridad activa actual. El tipo **dtBackupID** elimina del servidor el ID de objeto especificado. Invoque esta función desde una transacción.
- **dsmEndGetData**  
La llamada de función **dsmEndGetData** finaliza una sesión **dsmBeginGetData** que obtiene objetos de un almacenamiento.
- **dsmEndGetDataEx**  
La llamada a función **dsmEndGetDataEx** proporciona el total de bytes fuera de LAN enviados. Es una extensión de la llamada a función **dsmEndGetData**.
- **dsmEndGetObj**  
La llamada a función **dsmEndGetObj** finaliza una sesión **dsmGetObj** que obtiene datos para un objeto específico.
- **dsmEndQuery**  
La llamada de función **dsmEndQuery** significa el final de una acción **dsmBeginQuery**. El cliente de la aplicación envía **dsmEndQuery** con objeto de finalizar una consulta. Esta llamada se envía después de obtener todas las respuestas de la consulta a través de **dsmGetNextQObj**, o se envía para finalizar una consulta antes de que se devuelvan todos los datos.
- **dsmEndSendObj**  
La llamada de función **dsmEndSendObj** indica el final de los datos enviados a almacenamiento.
- **dsmEndSendObjEx**  
La llamada de función **dsmEndSendObjEx** proporciona información adicional y el número de bytes que se procesaron. La información incluye: el total de bytes enviados, información de compresión, bytes fuera de la LAN e información sobre la optimización de almacenamiento.
- **dsmEndTxn**  
La llamada a función **dsmEndTxn** finaliza una transacción de IBM Spectrum Protect. Empareje la llamada de función **dsmEndTxn** con **dsmBeginTxn** para identificar a la llamada o conjunto de llamadas que se consideran una transacción. El cliente de aplicación puede especificar en la llamada **dsmEndTxn** si se debe confirmar o finalizar la transacción.
- **dsmEndTxnEx**  
La llamada de función **dsmEndTxnEx** proporciona la información de ID de objeto de líder de grupo para que se utilice con la llamada de función **dsmGroupHandler**. Es una extensión de llamada a función **dsmEndTxn**.
- **dsmGetData**  
La llamada de función **dsmGetData** obtiene una corriente de byte de datos de IBM Spectrum Protect y la coloca en el almacenamiento intermedio del llamador. El cliente de la aplicación llama a **dsmGetData** cuando hay más datos para recibir de una llamada previa **dsmGetObj** o **dsmGetData**.
- **dsmGetBufferData**  
La llamada a función **dsmGetBufferData** recibe una secuencia de bytes de datos de IBM Spectrum Protect a través de un almacenamiento intermedio. Después de cada llamada la aplicación necesita copiar los datos y liberar el almacenamiento intermedio a través de una llamada a **dsmReleaseBuffer**. Si el número de almacenamientos intermedios que retiene la aplicación es igual al **numTsmBuffers** especificado en la llamada **dsmInitEx**, se bloquea la función **dsmGetBufferData** hasta que se invoque **dsmReleaseBuffer**.
- **dsmGetNextQObj**  
La llamada a función **dsmGetNextQObj** obtiene la siguiente respuesta de consulta de una llamada **dsmBeginQuery** y coloca la

- respuesta en el almacenamiento intermedio del interlocutor.
- **dsmGetObj**  
La llamada de función **dsmGetObj** obtiene los datos de objeto solicitados de la corriente de datos IBM Spectrum Protect y los coloca en el almacenamiento intermedio del llamador. La llamada **dsmGetObj** utiliza el ID de objeto para obtener el siguiente objeto u objeto parcial de la corriente de datos.
  - **dsmGroupHandler**  
La llamada de función **dsmGroupHandler** realiza una acción en un grupo de archivo lógico dependiendo de los datos introducidos. El cliente relaciona un número de objetos con el fin de hacer referencia y administrar el servidor IBM Spectrum Protect como grupo lógico.
  - **dsmInit**  
La llamada de función **dsmInit** inicia una sesión de la API y conecta al cliente con el almacenamiento IBM Spectrum Protect. El cliente de la aplicación sólo puede tener una sesión activa abierta a la vez. Para abrir otra sesión con parámetros distintos, utilice la llamada **dsmTerminate** primero con objeto de finalizar la sesión actual.
  - **dsmInitEx**  
La llamada de función **dsmInitEx** inicia una sesión de la API utilizando los parámetros adicionales para una verificación extendida.
  - **dsmLogEvent**  
La llamada de función **dsmLogEvent** registra un mensaje de usuario (ANE4991 I) en el archivo de registro del servidor, en el registro de error local o en ambos. Una estructura de tipo **logInfo** se pasa en la llamada. Esta llamada debe realizarse con el estado **InSession** dentro de una sesión. No debe ejecutarse durante una operación de envío, obtención o consulta. Para recuperar los mensajes registrados en el servidor, utilice el mandato **query actlog** mediante el cliente administrativo.
  - **dsmLogEventEx**  
La llamada a función **dsmLogEventEx** registra un mensaje en el archivo de registro del servidor, en el registro de errores local o en ambos. Esta llamada debe realizarse con el estado **InSession** dentro de una sesión. La llamada no se puede realizar dentro de una llamada de consulta, envío u obtención.
  - **dsmQueryAccess**  
La llamada de función **dsmQueryAccess** consulta las reglas de autorización de acceso del servidor en las copias de seguridad de los objetos o en las copias archivadas. Un puntero a una agrupación de reglas de acceso pasa a la llamada, y se devuelve la agrupación rellena. Un puntero al número de reglas pasa para indicar cuántas reglas hay en la agrupación.
  - **dsmQueryApiVersion**  
La llamada de función **dsmQueryApiVersion** realiza una solicitud de consulta de la versión de la biblioteca de la API a la que accede el cliente de aplicación.
  - **dsmQueryApiVersionEx**  
La llamada de función **dsmQueryApiVersionEx** realiza una solicitud de consulta de la versión de la biblioteca API a la que accede el cliente de la aplicación.
  - **dsmQueryCliOptions**  
La llamada de función **dsmQueryCliOptions** consulta valores de opción importantes en los archivos de opción del usuario. Una estructura de tipo **optStruct** se pasa en la llamada y contiene la información. Esta llamada se realiza antes de invocar **dsmInitEx**, y determina la configuración antes de la sesión.
  - **dsmQuerySessInfo**  
La llamada de función **dsmQuerySessInfo** inicia una solicitud de consulta a IBM Spectrum Protect sobre información relacionada con la operación de la sesión especificada en **dsmHandle**. Una estructura de tipo **ApiSessInfo** se pasa en la llamada, con toda la información relacionada con la sesión disponible. Esta llamada se inicia después de una llamada **dsmInitEx** correcta.
  - **dsmQuerySessOptions**  
La llamada de función **dsmQuerySessOptions** consulta valores de opción importantes que son válidos en la sesión especificada en **dsmHandle**. Una estructura de tipo **optStruct** se pasa en la llamada y contiene la información.
  - **dsmRCMsg**  
La llamada de función **dsmRCMsg** obtiene el texto del mensaje asociado con el código de retorno de la API.
  - **dsmRegisterFS**  
La llamada de función **dsmRegisterFS** registra un espacio de archivo nuevo con el servidor IBM Spectrum Protect. Registre un espacio de archivo primero antes de realizar ninguna copia de seguridad de éste.
  - **dsmReleaseBuffer**  
La función **dsmReleaseBuffer** devuelve un almacenamiento intermedio a IBM Spectrum Protect. La aplicación llama a **dsmReleaseBuffer** después de que se haya llamado un **dsmGetDataEx** y que la aplicación haya movido todos los datos fuera del almacenamiento intermedio y esté listo para liberarlo. **dsmReleaseBuffer** requiere que **dsmInitEx** se llame con **UseTsmBuffers** configurada en **true** y que se haya proporcionado un valor que no sea cero en **numTsmBuffers**. También se debe invocar **dsmReleaseBuffer** si la aplicación está a punto de invocar **dsmTerminate** y todavía retiene almacenamientos intermedios de datos.
  - **dsmRenameObj**  
La llamada de función **dsmRenameObj** renombra el alto y bajo rango del objeto. En copias de seguridad de objetos, pasa el nombre de objeto actual y cambia el nombre de alto rango o el de bajo rango. En objetos archivados, pasa el nombre del espacio de archivo y el ID del objeto y cambia el nombre de alto rango o el de bajo rango. Utilice esta llamada de función dentro de las llamadas **dsmBeginTxn** y **dsmEndTxn**.

- **dsmRequestBuffer**  
La función **dsmRequestBuffer** devuelve un almacenamiento intermedio a IBM Spectrum Protect. La aplicación invoca **dsmRequestBuffer** después de que se haya invocado **dsmGetDataEx** y de que la aplicación haya movido todos los datos fuera del almacenamiento intermedio y esté lista para liberarlo.
- **dsmRetentionEvent**  
La llamada de función **dsmRetentionEvent** envía una lista de ID de objetos al servidor de IBM Spectrum Protect con una operación de evento de retención para que se realice en estos objetos. Utilice esta llamada de función dentro de las llamadas **dsmBeginTxn** y **dsmEndTxn**.
- **dsmSendBufferData**  
La llamada de función **dsmSendBufferData** envía una corriente de bytes de datos a IBM Spectrum Protect a través de un almacenamiento intermedio proporcionado en una llamada **dsmReleaseBuffer** anterior. El cliente aplicación puede pasar cualquier tipo de datos para que se almacenen en el servidor. Normalmente estos datos son datos de archivos, pero no necesariamente. Puede llamar a **dsmSendBufferData** varias veces, si la corriente de bytes de datos que está enviando es demasiado larga. Independientemente de si la llamada falla o se procesa correctamente, se libera el almacenamiento intermedio.
- **dsmSendData**  
La llamada de función **dsmSendData** envía una corriente de bytes de datos a IBM Spectrum Protect a través de un almacenamiento intermedio. El cliente aplicación puede pasar cualquier tipo de datos para que se almacenen en el servidor. Normalmente estos datos son datos de archivos, pero no necesariamente. Puede llamar a **dsmSendData** varias veces, si la corriente de bytes de datos que desea enviar es demasiado larga.
- **dsmSendObj**  
La llamada de función **dsmSendObj** inicia una solicitud para enviar un único objeto al almacenamiento. Se pueden realizar varias llamadas **dsmSendObj** y llamadas asociadas **dsmSendData** dentro de los límites de una transacción por motivos de rendimiento.
- **dsmSetAccess**  
La llamada de función **dsmSetAccess** da a otros usuarios o nodos acceso a versiones de copia de seguridad o copias archivadas de los objetos, acceso a todos los objetos o acceso a un grupo determinado. Cuando se otorga acceso a otro usuario, dicho usuario puede consultar, restaurar o recuperar los archivos. Este mandato soporta comodines en los siguientes campos: *fs, hl, ll, nodo, propietario*.
- **dsmSetUp**  
La llamada de función **dsmSetUp** sobrescribe los valores de la variable del entorno. Llame a **dsmSetUp** antes de a **dsmInitEx**. Los valores que se pasan en la estructura **envSetUp** sobrescriben las variables de entorno existentes o predeterminadas. Si especifica NULL en un campo, los valores se toman del entorno. Si no configura un valor, se toman los valores predeterminados.
- **dsmTerminate**  
La llamada de función **dsmTerminate** finaliza una sesión con el servidor IBM Spectrum Protect y limpia el entorno IBM Spectrum Protect.
- **dsmUpdateFS**  
La llamada a función **dsmUpdateFS** actualiza un espacio de archivos en el almacenamiento IBM Spectrum Protect. Esta actualización garantiza que el administrador tenga un registro actualizado de su espacio de archivos.
- **dsmUpdateObj**  
La llamada de función **dsmUpdateObj** actualiza la metainformación asociada con un objeto archivado o copia de seguridad activos que ya está en el servidor. Los datos de bit de la aplicación no se ven afectados. Para actualizar un objeto, debe asignar un nombre específico sin comodines. Para actualizar un objeto archivado, configure **dsmSendType** en **stArchive**. Solo se actualiza el último objeto archivado nombrado.
- **dsmUpdateObjEx**  
La llamada de función **dsmUpdateObjEx** actualiza la meta información que está asociada con los objetos de archivado o las copias de seguridad en el servidor. Los datos de bit de la aplicación no se ven afectados. Para actualizar un objeto, debe asignar un nombre sin comodines o bien especificar el ID del objeto con el fin de actualizar un objeto archivado específico. No se pueden utilizar caracteres comodín cuando se especifica el nombre. Para actualizar un objeto al que se le ha realizado una copia de seguridad, configure el parámetro **dsmSendType** en **stBackup**. Para actualizar un objeto archivado, configure el parámetro **dsmSendType** en **stArchive**.

**Referencia relacionada:**

Códigos de retorno de la API

## dsmBeginGetData

---

La llamada de función **dsmBeginGetData** inicia una operación de restauración o recuperación en la lista de objetos del almacenamiento. La lista de objetos se encuentra dentro de la estructura **dsmGetList**. La aplicación crea esta lista con los valores de la consulta que precede a una llamada a **dsmBeginGetData**.

El llamador debe en primer lugar utilizar los campos del orden de restauración que se obtienen de la consulta del objeto con el fin de ordenar la lista que se incluye en esta llamada. Esto garantiza que los objetos se restauran del almacenamiento de la forma más eficaz posible sin tener que rebobinar o remontar las cintas de datos.

Al obtener objetos enteros, el *dsmGetList.numObjID* máximo es *DSM\_MAX\_GET\_OBJ*. Al obtener objetos parciales, el máximo es *DSM\_MAX\_PARTIAL\_GET\_OBJ*.

Siga la llamada a **dsmBeginGetData** con una o más llamadas a **dsmGetObj** con el fin de obtener todos los objetos de la lista. Después de obtener todos los objetos, o que no se necesiten datos adicionales, se envía la llamada **dsmEndGetObj**.

Cuando se obtienen todos los objetos, o se cancela **dsmEndGetObj** se envía la llamada **dsmEndGetData**. A continuación puede iniciar el ciclo de nuevo.

## Sintaxis

```
dsInt16_t dsmBeginGetData (dsUInt32_t          dsmHandle,  
                          dsBool_t          mountWait,  
                          dsmGetType        getType,  
                          dsmGetList        *dsmGetObjListP);
```

## Parámetros

*dsUInt32\_t* *dsmHandle* (I)

El manejador que asocia esta llamada con una llamada *dsmInitEx*.

*dsBool\_t* *mountWait* (I)

Un valor booleano verdadero o falso indica si el cliente de la aplicación espera que se monten medios desconectados si los datos que se necesitan están actualmente desconectados. Si *mountWait* es verdadero, la aplicación espera a que el servidor monte los medios necesarios. La aplicación espera hasta que el soporte esté montado o la solicitud cancelada.

*dsmGetType* *getType* (I)

Un tipo enumerado que consiste en *gtBackup* y *gtArchive* indica qué tipo de objeto se va a obtener.

*dsmGetList* *\*dsmGetObjListP* (I)

Esta estructura contiene información acerca de los objetos o bien de los objetos parciales que se van a restaurar o recuperar. La estructura apunta a una lista de ID de objetos y, en el caso de una recuperación o restauración parcial, a una lista de desplazamientos y longitudes asociadas. Si la aplicación utiliza la función de recuperación o restauración parcial de objetos, configure el campo **dsmGetList.stVersion** en **dsmGetListPORVersion**. En una restauración o recuperación de objeto parcial, no es posible comprimir datos mientras los envía. Para implementar esto, configure **ObjAttr.objCompressed** en *bTrue*.

Consulte Figura 1 y Archivos de origen de definiciones de tipo de API para obtener más información acerca de esta estructura.

Consulte Restauración o recuperación de objeto parcial para obtener más información acerca de restauraciones o recuperaciones de objeto parciales.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno de *dsmBeginGetData*

Código de retorno	Explicación
<i>DSM_RC_ABORT_INVALID_OFFSET</i> (33)	El desplazamiento que se especificó durante la recuperación de un objeto parcial es mayor que la longitud del objeto.
<i>DSM_RC_ABORT_INVALID_LENGTH</i> (34)	La longitud que se especificó durante la recuperación de un objeto parcial es mayor que la longitud del objeto, o el desplazamiento y la longitud se extienden más allá del final del objeto.
<i>DSM_RC_NO_MEMORY</i> (102)	No queda RAM para finalizar la solicitud.
<i>DSM_RC_NUMOBJ_EXCEED</i> (2029)	<b>dsmGetList.numObjId</b> es mayor que <i>DSM_MAX_GET_OBJ</i> .
<i>DSM_RC_OBJID_NOTFOUND</i> (2063)	No se ha encontrado el ID del objeto. No se restauró el objeto.
<i>DSM_RC_WRONG_VERSION_PARM</i> (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.

## dsmBeginQuery

La llamada a la función *dsmBeginQuery* inicia una solicitud de consulta al servidor sobre datos, archivos y clases de gestión.

En especial, *dsmBeginQuery* consulta:

- Datos archivados

- Datos de copia de seguridad
- Datos de copia de seguridad activos
- Espacios de archivo
- Clases de gestión

Los datos de la consulta que se extraen de la llamada se obtienen por una o más llamadas a `dsmGetNextQObj`. Cuando se ha completado la consulta, se envía la llamada `dsmEndQuery`.

## Sintaxis

---

```
dsInt16_t dsmBeginQuery (dsUInt32_t dsmHandle,
                        dsmQueryType queryType,
                        dsmQueryBuff *queryBuffer);
```

## Parámetros

---

`dsUInt32_t dsmHandle` (I)

El manejador que asocia esta llamada con una llamada `dsmInitEx` anterior.

`dsmQueryType queryType` (I)

Identifica el tipo de consulta a ejecutar. Asigne una de las siguientes opciones:

`qtArchive`

Consultas de objetos archivados.

`qtBackup`

Consultas de objetos de copias de seguridad.

`qtBackupActive`

Consultas de objetos de copias de seguridad activas sólo para el nombre del espacio del archivo completo que pase. Esta consulta se denomina "ruta de acceso rápida" y es una forma eficaz de consultar objetos activos del almacenamiento.  
Requisito previo: Debe iniciar sesión como usuario root en un sistema operativo UNIX o Linux.

`qtFilespace`

Consultas de espacios de archivo registrados.

`qtMC`

Consultas de clases de gestión definidas.

`qtBackupGroups`

Consultas de grupos que están cerrados.

`qtOpenGroups`

Consultas de grupos que están abiertos.

`qtProxyNodeAuth`

Consultas de los nodos de los que puede actuar éste como proxy.

`qtProxyNodePeer`

Consultas de nodos peer con el mismo objetivo.

`dsmQueryBuff *queryBuffer` (I)

Identifica un puntero de un almacenamiento intermedio que está correlacionado con una estructura de datos concreta. Esta estructura está asociada con el tipo de consulta transmitida. Estas estructuras pueden contener el criterio de selección de cada tipo de consulta. Rellene los campos de cada estructura con el fin de especificar el ámbito de la consulta que desea ejecutar. El campo `stVersion` de cada estructura contiene el número de versión de estructura.

Las estructuras de datos y sus campos relacionados incluyen los siguientes elementos:

`qryArchiveData`

#### objName

El nombre del objeto completo. Puede utilizar un comodín, como por ejemplo un asterisco (\*) o un signo de interrogación (?), en la parte de rango alto o de rango bajo del nombre. Un asterisco corresponde a cero o más caracteres, y un interrogante corresponde exactamente a un carácter. El campo objType de objName puede tener más de uno de los siguientes valores:

- DSM\_OBJ\_FILE
- DSM\_OBJ\_DIRECTORY
- DSM\_OBJ\_ANY\_TYPE

Para obtener más información acerca de los nombres de rango alto y de rango bajo, consulte el tema siguiente: Nombres de alto y bajo rango.

#### propietario

El nombre del propietario del objeto.

#### insDateLowerBound

El límite inferior para la fecha de inserción en la que se archivó el objeto. Para obtener el límite superior predeterminado, configure el componente del año en DATE\_MINUS\_INFINITE.

#### insDateUpperBound

El límite superior para la fecha de inserción en la que se archivó el objeto. Para obtener el límite superior predeterminado, configure el componente del año en DATE\_PLUS\_INFINITE.

#### expDateLowerBound

El límite inferior de la fecha de caducidad. Los valores predeterminados de ambos campos de fecha de caducidad son los mismos que los campos de fecha de inserción.

#### expDateUpperBound

El límite superior de la fecha de caducidad.

#### descr

La descripción del archivado. Entre un asterisco (\*) para buscar todas las descripciones.

#### qryBackupData

##### objName

El nombre del objeto completo. Puede utilizar un comodín, como por ejemplo un asterisco (\*) o un signo de interrogación (?), en la parte de rango alto o de rango bajo del nombre. Un asterisco corresponde a cero o más caracteres, y un interrogante corresponde exactamente a un carácter. El campo objType de objName puede tener más de uno de los siguientes valores:

- DSM\_OBJ\_FILE
- DSM\_OBJ\_DIRECTORY
- DSM\_OBJ\_ANY\_TYPE

Para obtener más información acerca de los nombres de rango alto y de rango bajo, consulte el tema siguiente: Nombres de alto y bajo rango.

##### propietario

El nombre del propietario del objeto.

##### objState

Puede consultar por uno de los siguientes estados de objeto:

- DSM\_ACTIVE
- DSM\_INACTIVE
- DSM\_ANY\_MATCH

##### pitDate

El valor punto en el tiempo. Una consulta que utiliza este campo devuelve el último objeto al que se le realizó una copia de seguridad antes de dicha fecha y hora. objState puede estar activo o inactivo. Los objetos que se eliminaron antes de pitDate no se devuelven. Por ejemplo:



Mon - backup ABC(1), DEF, GHI  
Tue - backup ABC(2), delete DEF  
Thr - backup ABC(3)

El viernes, llame a la consulta con el punto en el tiempo en miércoles a las 12:00:00, y devuelve la siguiente información:

ABC(2) - an Inactive copy  
GHI - an Active copy

La llamada no devuelve DEF porque ese objeto se eliminó antes del valor de punto en el tiempo.

#### qryABackupData

##### objName

El nombre del objeto completo. Puede utilizar un comodín, como por ejemplo un asterisco (\*) o un signo de interrogación (?), en la parte de rango alto o de rango bajo del nombre. Un asterisco corresponde a cero o más caracteres, y un interrogante corresponde exactamente a un carácter. El campo objType de objName puede tener más de uno de los siguientes valores:

- DSM\_OBJ\_FILE
- DSM\_OBJ\_DIRECTORY
- DSM\_OBJ\_ANY\_TYPE

Para obtener más información acerca de los nombres de rango alto y de rango bajo, consulte el tema siguiente: Nombres de alto y bajo rango.

#### qryFSData

##### fsName

Introduzca el nombre de un espacio de archivo específico en este campo o introduzca un asterisco (\*) con el fin de extraer información sobre todos los espacios de archivo registrados.

#### qryMCData

##### mcName

Introduzca el nombre de una clase de gestión específica en este campo o introduzca una cadena vacía (" ") con el fin de extraer información sobre todas las clases de gestión.

Nota: No puede utilizar un asterisco (\*).

##### mcDetail

Determina si se devuelve o no la información sobre la clase de gestión en la copia de seguridad y en los grupos de copia de archivado. Son válidos los valores siguientes:

- bTrue
- bFalse

#### qryBackupGroup:

##### groupType

El tipo de grupo es DSM\_GROUPTYPE\_PEER.

##### fsName

El nombre de espacio de archivos.

##### propietario

ID del propietario.

##### groupLeaderObjId

ID del objeto líder del grupo.

##### objType

El tipo de objeto.

#### qryProxyNodeAuth:

##### targetNodeName

El nombre de nodo de destino.

peerNodeName

El nombre de nodo del igual.

hlAddress

La dirección del igual del nombre de alto rango.

llAddress

La dirección del igual del nombre de rango bajo.

qryProxyNodePeer:

targetNodeName

El nombre de nodo de destino.

peerNodeName

El nombre de nodo del igual.

hlAddress

La dirección del igual del nombre de alto rango.

llAddress

La dirección del igual del nombre de rango bajo.

## Códigos de retorno

La tabla siguiente describe los códigos de retorno de la llamada a función dsmBeginQuery.

Tabla 1. Códigos de retorno para dsmBeginQuery

Código de retorno	Número de código de retorno	Explicación
DSM_RC_NO_MEMORY	102	No hay suficiente memoria para completar la solicitud.
DSM_RC_FILE_SPACE_NOT_FOUND	124	No se ha encontrado el espacio del archivo especificado.
DSM_RC_NO_POLICY_BLK	2007	La información de la política de servidor no está disponible.
DSM_RC_INVALID_OBJTYPE	2010	Tipo de objeto no válido.
DSM_RC_INVALID_OBJOWNER	2019	Nombre de propietario de objeto no válido.
DSM_RC_INVALID_OBJSTATE	2024	Condición de objeto no válida.
DSM_RC_WRONG_VERSION_PARM	2065	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.

## dsmBeginTxn

La llamada de función **dsmBeginTxn** inicia una o más transacciones IBM Spectrum Protect que a su vez comienzan una acción completa; todas las acciones se procesan correctamente o ninguna de ellas. Una acción puede ser una llamada única o una serie de llamadas. Por ejemplo, una llamada **dsmSendObj** seguida por un número de llamadas **dsmSendData** se puede considerar una acción única. Del mismo modo, una llamada **dsmSendObj** con **dataBlkPtr** que indica el área de datos que contiene el objeto del que se realizará una copia de seguridad también se considera una acción única.

Intente agrupar más de un objeto en una transacción única en las operaciones de transferencia de datos. La agrupación de objetos resulta en mejoras de rendimiento significativas en el sistema IBM Spectrum Protect. Desde una perspectiva de cliente y servidor, esto supone una cierta carga de productividad adicional al iniciar y finalizar cada transacción.

Existen limitaciones con respecto a lo que se puede realizar dentro de una transacción única. Estas transacciones incluyen:

- Un número máximo de objetos que se pueden enviar o eliminar en una transacción única. Este límite se encuentra en los datos que **dsmQuerySessInfo** devuelve en el campo *ApiSessInfo.maxObjPerTxn*. Esto se corresponde con la opción del servidor

*TxnGroupMax.*

- Todos los objetos que se envían al servidor (ya sean copias de seguridad o archivados) dentro de una transacción única deben tener el mismo destino de copia que está definido en la vinculación de la clase de gestión del objeto. Este valor se encuentra en los datos que devuelve **dsmBindMC** en los campos **mcBindKey.backup\_copy\_dest** o **mcBindKey.archive\_copy\_dest**.

Con la API, o el cliente de la aplicación puede supervisar y controlar estas restricciones, o bien la API. Si es la API la que está supervisando las restricciones, los códigos de retorno adecuados de las llamadas de la API notifican al cliente de la aplicación si se está alcanzando una o más restricciones.

Siempre coincida una llamada **dsmBeginTxn** con una llamada **dsmEndTxn** con el fin de optimizar el conjunto de acciones dentro de un par de llamadas **dsmBeginTxn** y **dsmEndTxn**.

## Sintaxis

```
dsInt16_t dsmBeginTxn (dsUInt32_t dsmHandle);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno de dsmBeginTxn

Código de retorno	Explicación
DSM_RC_ABORT_NODE_NOT_AUTHORIZED (36)	FROMNODE o FROMOWNER no está permitido en las operaciones TXN.

## dsmBindMC

La llamada de función **dsmBindMC** asocia, o vincula, una clase de gestión al objeto que pasa. El objeto pasa a través de una lista de inclusión/exclusión a la que se apunta en el archivo de opciones. Si no se encuentra una coincidencia de una clase de gestión específica en la lista de inclusión, se asigna la clase de gestión predeterminada. La lista de inclusión puede impedir objetos de una copia de seguridad pero no de una copia de archivado.

El cliente de la aplicación puede utilizar los parámetros que se devuelven en la estructura **mcBindKey** con el fin de determinar si los objetos deben archivar o se les debe realizar una copia de seguridad, o si debe iniciarse una transacción nueva debido a distintos destinos de copia. Para obtener más información, consulte el apartado **dsmBeginTxn**.

Llame a **dsmBindMC** antes de llamar a **dsmSendObj** porque todos los objetos deben tener una clase de gestión asociada. Esta llamada puede realizarse dentro o fuera de una transacción. Por ejemplo, dentro de una transacción de varios objetos, si **dsmBindMC** indica que el objeto tiene destinos de copia distintos al objeto anterior, la transacción debe finalizarse y debe iniciarse una nueva. En este caso, no se requiere otra **dsmBindMC** porque ya se ha realizado una en este objeto.

## Sintaxis

```
dsInt16_t dsmBindMC (dsUInt32_t dsmHandle,  
    dsmObjName *objNameP,  
    dsmSendType sendType,  
    mcBindKey *mcBindKeyP);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmObjName \*objNameP (I)

Un puntero a la estructura que contiene el nombre del espacio del archivo, el nombre de alto y bajo rango y el tipo de objeto.

dsmSendType sendType (I)

Identifica si se realiza esta vinculación de clase de gestión en envíos de copias archivadas o de seguridad. Los valores posibles para esta llamada incluyen:

Nombre	Descripción
<b>stBackup</b>	Una copia de seguridad de objeto

Nombre	Descripción
<b>stArchive</b>	Una copia archivada de objeto
<b>stBackupMountWait</b>	Una copia de seguridad de objeto
<b>stArchiveMountWait</b>	Una copia archivada de objeto

En la llamada **dsmBindMC**, **stBackup** y **stBackupMountWait** son equivalentes, y **stArchive** y **stArchiveMountWait** son equivalentes.

**mcBindKey \*mcBindKeyP** (O)

Esta es la dirección de una estructura **mcBindKey** donde se devuelve la información de clase de gestión. El cliente de la aplicación puede utilizar la información que se devuelve aquí para determinar si este objeto encaja dentro de una transacción de varios objetos, o para realizar una consulta de clase de gestión en la clase de gestión que está vinculada al objeto.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para **dsmBindMC**

Código de retorno	Explicación
DSM_RC_NO_MEMORY (102)	No queda RAM para finalizar la solicitud.
DSM_RC_INVALID_PARM (109)	Uno de los parámetros que se pasó tiene un valor no válido.
DSM_RC_TL_EXCLUDED (185)	La copia de seguridad del objeto está excluida y no se puede enviar.
DSM_RC_INVALID_OBJTYPE (2010)	Tipo de objeto no válido.
DSM_RC_INVALID_SENDDTYPE (2022)	Tipo de envío no válido.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.

## dsmChangePW

La llamada a función **dsmChangePW** cambia una contraseña de IBM Spectrum Protect. En un sistema operativo de varios usuarios como UNIX o Linux, solo el usuario raíz o el usuario autorizado pueden utilizar esta llamada.

En sistemas operativos Windows, puede especificar la contraseña en el archivo **dsm.opt**. En este caso, **dsmChangePW** no actualiza el archivo **dsm.opt**. Después de que se haya realizado la llamada a **dsmChangePW**, debe actualizar el archivo **dsm.opt** por separado.

Esta llamada debe procesarse correctamente si **dsmInitEx** devuelve **DSM\_RC\_VERIFIER\_EXPIRED**. La sesión finaliza si la llamada **dsmChangePW** falla en este caso.

Si se llama a **dsmChangePW** por algún otro motivo, la sesión permanece abierta independientemente del código de retorno.

## Sintaxis

```
dsInt16_t dsmChangePW (dsUInt32_t dsmHandle,
char *oldPW,
char *newPW);
```

## Parámetros

**dsUInt32\_t dsmHandle** (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

**char \*oldPW** (I)

La contraseña antigua del llamador. La longitud máxima es **DSM\_MAX\_VERIFIER\_LENGTH**.

**char \*newPW** (I)

La contraseña nueva del llamador. La longitud máxima es **DSM\_MAX\_VERIFIER\_LENGTH**.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmChangePW

Código de retorno	Explicación
DSM_RC_ABORT_BAD_VERIFIER (6)	Se ha especificado una contraseña incorrecta.
DSM_RC_AUTH_FAILURE (137)	Error de autenticación. Contraseña antigua incorrecta.
DSM_RC_NEWPW_REQD (2030)	Se debe introducir un valor para la contraseña nueva.
DSM_RC_OLDPW_REQD (2031)	Se debe especificar un valor para la contraseña antigua.
DSM_RC_PASSWD_TOOLONG (2103)	La contraseña especificada es demasiado larga.
DSM_RC_NEED_ROOT (2300)	El llamador de API debe ser un usuario root o un usuario autorizado.

## dsmCleanUp

La llamada de función **dsmCleanUp** se utiliza si se ha llamado a **dsmSetUp**. La llamada de función **dsmCleanUp** debe llamarse después de **dsmTerminate**. No es posible realizar ninguna otra llamada después de llamar a **dsmCleanUp**.

No existen códigos de retorno específicos de esta llamada.

### Sintaxis

```
dsInt16_t DSMLINKAGE dsmCleanUp
(dsBool_t mtFlag);
```

### Parámetros

dsBool\_t mtFlag (I)

Este parámetro especifica que la API fue utilizado en una única hebra o en un modo de varias hebras. Dentro de los valores posibles se incluyen los siguientes:

- DSM\_SINGLETHREAD
- DSM\_MULTITHREAD

## dsmDeleteAccess

La llamada de función **dsmDeleteAccess** elimina las reglas de autorización actuales para las versiones de las copias de seguridad o las copias de archivado de los objetos. Cuando se suprime una regla de autorización, se revoca el acceso de un usuario a los archivos que especifica la regla.

Cuando se utiliza **dsmDeleteAccess**, sólo es posible eliminar las reglas de una en una. Obtenga el ID de la regla mediante el mandato **dsmQueryAccess**.

No existen códigos de retorno específicos de esta llamada.

### Sintaxis

```
dsInt16_t DSMLINKAGE dsmDeleteAccess
(dsUInt32_t dsmHandle,
dsUInt32_t ruleNum);
```

### Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

dsUInt32\_t ruleNum (I)

El ID de la regla de acceso de la regla que está eliminada. Este valor se obtiene de una función de llamada **dsmQueryAccess**.

## dsmDeleteFS

La llamada de función **dsmDeleteFS** elimina un espacio de archivo del almacenamiento. Para eliminar un espacio de archivo, debe tener permisos apropiados que el administrador IBM Spectrum Protect le habrá otorgado. Para determinar si cuenta con los permisos necesarios, llame a **dsmQuerySessInfo**. Esta llamada de función devuelve una estructura de datos de tipo *ApiSessInfo*, que incluye dos campos, *archDel* y *backDel*.

Nota:

- En un sistema operativo UNIX o Linux, solo un usuario root o un usuario autorizado pueden suprimir un espacio de archivos.
- Si el espacio de archivo que necesita eliminar contiene versiones de copia de seguridad, debe tener autorización para eliminar copias de seguridad (**backDel** = BACKDEL\_YES). Si el espacio de archivo contiene copias archivadas, debe tener autorización para eliminar archivados (**archDel** = ARCHDEL\_YES). Si el espacio de archivo contiene tanto copias archivadas como versiones de copia de seguridad, debe tener ambos tipos de autorización para supresión.
- Cuando se utiliza un servidor de gestión de archivado, un espacio de archivo no se puede realmente eliminar. Esta llamada de función devuelve *rc=0* a pesar de que el espacio de archivo no se eliminó. La única forma de comprobar si el espacio de archivo se ha eliminado es emitiendo una consulta de espacio de archivos al servidor.
- La función de supresión del espacio de archivos del servidor IBM Spectrum Protect es un proceso en segundo plano. Si se producen errores distintos a los detectados antes de pasar un código de retorno, se grabarán en el registro del servidor IBM Spectrum Protect.

## Sintaxis

```
dsInt16_t dsmDeleteFS (dsUInt32_t          dsmHandle,  
                      char                *fsName,  
                      unsigned char       repository);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

char \*fsName (I)

Un puntero al nombre del espacio de archivo que se va a eliminar. El carácter comodín no está permitido.

unsigned char repository (I)

Indica si el espacio de archivo que se va a eliminar es un repositorio de copia de seguridad, de archivado o ambos. Los valores posibles para este campo son:

```
DSM_ARCHIVE_REP    /* archive repository */  
DSM_BACKUP_REP     /* backup repository */  
DSM_REPOS_ALL      /* all repository types */
```

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmDeleteFS

Código de retorno	Explicación
DSM_RC_ABORT_NOT_AUTHORIZED (27)	No tiene la autorización necesaria para eliminar el espacio de archivo.
DSM_RC_INVALID_REPOS (2015)	Valor de repositorio no válido.
DSM_RC_FSNAME_NOTFOUND (2060)	No se ha encontrado el nombre del espacio de archivo.
DSM_RC_NEED_ROOT (2300)	El llamador de la API no debe ser un usuario root.

## dsmDeleteObj

La llamada de función **dsmDeleteObj** inactiva copias de seguridad de objetos, elimina copias de seguridad de objetos o eliminar objetos archivados en el almacenamiento. El tipo **dtBackup** inactiva únicamente la copia de seguridad activa actual. El tipo **dtBackupID** elimina del servidor el ID de objeto especificado. Invoque esta función desde una transacción.

Para obtener más información, consulte el apartado **dsmBeginTxn**.

Antes de enviar **dsmDeleteObj**, envíe la secuencia de consulta que se describen en Consultas para el sistema IBM Spectrum Protect para que obtenga la información de **delInfo**. La llamada a **dsmGetNextQObj** devuelve una estructura de datos llamada **qryRespBackupData** a consultas de copias de seguridad o **qryRespArchiveData** a consultas de copias archivadas. Estas estructuras de datos contienen información que necesita en **delInfo**.

El valor de **maxObjPerTxn** determina el número máximo de objetos que se pueden eliminar en una única transacción. Para obtener este valor, llame a **dsmQuerySessInfo**.

Consejo: Su nodo debe tener el permiso adecuado que haya establecido su administrador. Para eliminar objetos archivados, debe tener autorización para eliminar copias archivadas. Para inactivar un objeto de copia de seguridad, no necesita autorización para suprimir

copias de seguridad.

## Sintaxis

```
dsInt16_t dsmDeleteObj (dsUInt32_t dsmHandle,  
                        dsmDelType delType,  
                        dsmDelInfo delInfo)
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmDelType delType (I)

Indica qué tipo de objeto (copia de seguridad o archivada) se va a eliminar. Dentro de los valores posibles se incluyen los siguientes:

Nombre	Descripción
<b>dtArchive</b>	El objeto que se va a eliminar se archivó anteriormente.
<b>dtBackup</b>	Al objeto que se va a desactivar se le ha realizado una copia de seguridad anteriormente.
<b>dtBackupID</b>	Al objeto que se va a desactivar se le ha realizado una copia de seguridad anteriormente. Restricción: Al utilizar este <b>delType</b> con <i>objID</i> se elimina la copia de seguridad del objeto del servidor. Sólo un propietario del objeto puede eliminarlo.  Es posible eliminar cualquier versión (activa o inactiva) de un objeto. El servidor reconcilia las versiones. Si elimina una versión activa de un objeto, la primera versión inactiva se transforma en activa. Si elimina una versión inactiva de un objeto, todas las versiones antiguas avanzan. El nodo debe estar registrado con el permiso <b>backDel</b> .

dsmDelInfo delInfo (I)

Una estructura cuyos campos identifican al objeto. Los campos son distintos, dependiendo de si el objeto es una copia de seguridad o una copia archivada. La estructura para desactivar una copia de seguridad de un objeto *delBack*, contiene el nombre del objeto y el grupo de la copia del objeto. La estructura de un objeto archivado, *delArch*, contiene el ID del objeto.

La estructura para eliminar una copia de seguridad de un objeto *delBackID*, contiene el ID del objeto.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para *dsmDeleteObj*

Código de retorno	Explicación
DSM_RC_FS_NOT_REGISTERED (2061)	El nombre del espacio de archivos no está registrado.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.

## dsmEndGetData

La llamada de función **dsmEndGetData** finaliza una sesión **dsmBeginGetData** que obtiene objetos de un almacenamiento.

La llamada de función **dsmEndGetData** se inicia después de que todos los objetos que desea restaurar se hayan procesado, o bien finalizar el proceso de obtención de forma prematura. Llame a **dsmEndGetData** para finalizar una sesión **dsmBeginGetData** antes de poder continuar otro proceso.

Dependiendo de cuándo se llame a **dsmEndGetData**, es posible que la API necesite finalizar el proceso parcial de la corriente de datos antes de que se pueda detener el proceso. El llamador, por lo tanto, no puede esperar un retorno inmediato de esta llamada. Utilice **dsmTerminate** si la aplicación necesita cerrar la sesión y finalizar la restauración de forma inmediata.

No existen códigos de retorno específicos de esta llamada.

## Sintaxis

```
dsInt16_t dsmEndGetData (dsUInt32_t dsmHandle);
```

## Parámetros

---

dsUInt32\_t dsmHandle (I)  
El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## dsmEndGetDataEx

---

La llamada a función **dsmEndGetDataEx** proporciona el total de bytes fuera de LAN enviados. Es una extensión de la llamada a función **dsmEndGetData**.

## Sintaxis

---

No existen códigos de retorno específicos de esta llamada.

```
dsInt16_t dsmEndGetDataEx (dsmEndGetDataExIn_t * dsmEndGetDataExInP,  
                           dsmEndGetDataExOut_t * dsmEndGetDataExOutP);
```

## Parámetros

---

dsmEndGetDataExIn\_t \*dsmEndGetDataExInP (I)  
Pasa el objeto final dsmHandle que identifica la sesión y la asocia con llamadas subsiguientes.  
dsmEndGetDataExOut\_t \*dsmEndGetDataExOutP (O)  
Esta estructura contiene este parámetro de entrada:

totalLFBytesRecv  
El total de bytes de fuera de la LAN que se han recibido.

## dsmEndGetObj

---

La llamada a función **dsmEndGetObj** finaliza una sesión **dsmGetObj** que obtiene datos para un objeto específico.

Inicia la llamada **dsmEndGetObj** después de que se recibe una finalización de datos del objeto. Esto indica que todos los datos se han recibido, o que no se van a recibir más datos de este objeto. Antes de iniciar otra llamada **dsmGetObj**, debe llamar a **dsmEndGetObj**.

En función del momento en que se invoca **dsmEndGetObj**, es posible que la API deba finalizar el proceso de una corriente de datos parcial antes de que se detenga el proceso. No espere una devolución inmediata de esta llamada.

## Sintaxis

---

```
dsInt16_t dsmEndGetObj (dsUInt32_t dsmHandle);
```

## Parámetros

---

dsUInt32\_t dsmHandle (I)  
El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## Códigos de retorno

---

Los números de código de retorno se proporcionan entre paréntesis ().

Tabla 1. Códigos de retorno para dsmEndGetObj

Código de retorno	Explicación
DSM_RC_NO_MEMORY (102)	No queda RAM para completar la solicitud.

## dsmEndQuery

---

La llamada de función **dsmEndQuery** significa el final de una acción **dsmBeginQuery**. El cliente de la aplicación envía **dsmEndQuery** con objeto de finalizar una consulta. Esta llamada se envía después de obtener todas las respuestas de la consulta a través de **dsmGetNextQObj**, o se envía para finalizar una consulta antes de que se devuelvan todos los datos.

Consejo: En este caso, IBM Spectrum Protect continúa enviando los datos de la consulta desde el servidor al cliente, pero la API descarta cualquier dato restante.



Una vez enviado **dsmBeginQuery**, debe enviarse un **dsmEndQuery** antes de iniciar cualquier otra actividad.

No existen códigos de retorno específicos de esta llamada.

## Sintaxis

```
dsInt16_t dsmEndQuery (dsUInt32_t dsmHandle);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## dsmEndSendObj

La llamada de función **dsmEndSendObj** indica el final de los datos enviados a almacenamiento.

Introduzca la llamada de función **dsmEndSendObj** para indicar el final de los datos de las llamadas **dsmSendObj** y **dsmSendData**. Si esto no se lleva a cabo ocurre una infracción de protocolo. La excepción de la regla se produce si llama a **dsmEndTxn** para finalizar la transacción. Esto elimina todos los datos que se enviaron para la transacción.

## Sintaxis

```
dsInt16_t dsmEndSendObj (dsUInt32_t dsmHandle);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmEndSendObj

Código de retorno	Explicación
DSM_RC_NO_MEMORY (102)	No queda RAM para finalizar la solicitud.

## dsmEndSendObjEx

La llamada de función **dsmEndSendObjEx** proporciona información adicional y el número de bytes que se procesaron. La información incluye: el total de bytes enviados, información de compresión, bytes fuera de la LAN e información sobre la optimización de almacenamiento.

La llamada de función **dsmEndSendObjEx** es una extensión de la llamada de función **dsmEndSendObj**.

## Sintaxis

```
dsInt16_t dsmEndSendObjEx (dsmEndSendObjExIn_t *dsmEndSendObjExInP,  
                           dsmEndSendObjExOut_t *dsmEndSendObjExOutP);
```

## Parámetros

dsmEndSendObjExIn\_t \*dsmEndSendObjExInP (I)

Este parámetro pasa el dsmhandle del objeto de envío final que identifica la sesión y lo asocia con las llamadas posteriores.

dsmEndSendObjExOut\_t \*dsmEndSendObjExOutP (O)

Este parámetro pasa la información de envío final del objeto:

	Nombre	Descripción
	<b>totalBytesSent</b>	El número total de bytes que se leen desde la aplicación.
	<b>objCompressed</b>	Un identificador que muestra si se ha comprimido el objeto.
	<b>totalCompressedSize</b>	El tamaño total en bytes después de la compresión.

	Nombre	Descripción
	<b>totalLFBytesSent</b>	Los bytes sin LAN totales que se enviaron.
	<b>objDeduplicated</b>	Un indicador que muestra si la interfaz de programación de aplicaciones (API) ha realizado una optimización de almacenamiento en el objeto.
	<b>totalDedupSize</b>	Total de bytes enviados durante la optimización de almacenamiento.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ().

Tabla 1. Códigos de retorno para dsmEndSendObjEx

Código de retorno	Explicación
DSM_RC_NO_MEMORY (102)	No queda RAM para finalizar la solicitud.

## dsmEndTxn

La llamada a función dsmEndTxn finaliza una transacción de IBM Spectrum Protect. Empareje la llamada de función dsmEndTxn con dsmBeginTxn para identificar a la llamada o conjunto de llamadas que se consideran una transacción. El cliente de aplicación puede especificar en la llamada dsmEndTxn si se debe confirmar o finalizar la transacción.

Realice todas estas llamadas dentro de los límites de una transacción:

- **dsmSendObj**
- **dsmSendData**
- **dsmEndSendObj**
- **dsmDeleteObj**

## Sintaxis

```
dsInt16_t dsmEndTxn (dsUInt32_t dsmHandle,
                    dsUInt8_t vote,
                    dsUInt16_t *reason);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

dsUInt8\_t vote (I)

Indica si el cliente de aplicación confirma todas las acciones realizadas entre la llamada dsmBeginTxn previa y esta llamada. Son posibles los valores siguientes:

```
DSM_VOTE_COMMIT /* commit current transaction */
DSM_VOTE_ABORT /* roll back current transaction */
```

Utilice DSM\_VOTE\_ABORT únicamente si la aplicación tiene un motivo para detener la transacción.

dsUInt16\_t \*reason (O)

Si la llamada a dsmEndTxn finaliza con un error o el valor de vote no está de acuerdo, este parámetro tiene un código de razón que indica por qué falló el voto. El código de retorno para la llamada puede ser cero, y el código de motivo no. Por lo tanto, el cliente de aplicación debe siempre comprobar los errores tanto en el código de retorno como en el código de motivo (if (rc || reason)) antes de dar por hecho de que la operación ha finalizado correctamente.

Si la aplicación especifica un voto de DSM\_VOTE\_ABORT, el código de razón es DSM\_RS\_ABORT\_BY\_CLIENT (3). Consulte Archivo de origen de códigos de retorno de la API: dsmsrc.h para obtener una lista de los códigos de motivo posibles. Los números del 1 al 50 de la lista de códigos de retorno están reservados para los códigos de motivo. Si el servidor finaliza la transacción, el código de retorno es DSM\_RC\_CHECK\_REASON\_CODE. En este caso, el valor de motivo contiene más información sobre la causa de la anulación.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ().

Tabla 1. Códigos de retorno para dsmEndTxn

Código de retorno	Explicación
DSM_RC_ABORT_CRC_FAILED (236)	El CRC que se recibió del servidor no coincide con el CRC calculado por el cliente.
DSM_RC_INVALID_VOTE (2011)	El valor que se especificó para <code>vote</code> no es válido.
DSM_RC_CHECK_REASON_CODE (2302)	La transacción se anuló. Compruebe el campo de motivo.
DSM_RC_ABORT_STGPOOL_COPY_CONT_NO (241)	La grabación a una de las agrupaciones de almacenamiento de copia ha fallado, y la opción de agrupación de almacenamiento IBM Spectrum Protect de COPYCONTINUE se establece en NO. La transacción finaliza.
DSM_RC_ABORT_RETRY_SINGLE_TXN (242)	Este código de anulación indica que la transacción actual fue anulada debido a un problema durante la operación de almacenamiento. El problema puede resolverse enviando cada uno de los archivos en una transacción separada. Este error es típico en las siguientes circunstancias: <ul style="list-style-type: none"> <li>La siguiente agrupación de almacenamiento tiene una lista de agrupación de almacenamiento de copias diferente.</li> <li>La operación se conmuta a esta agrupación a la mitad de una transacción.</li> </ul>

## dsmEndTxnEx

La llamada de función **dsmEndTxnEx** proporciona la información de ID de objeto de líder de grupo para que se utilice con la llamada de función **dsmGroupHandler**. Es una extensión de llamada a función **dsmEndTxn**.

## Sintaxis

```
dsInt16_t dsmEndTxnEx (dsmEndTxnExIn_t *dsmEndTxnExInP
                     dsmEndTxnExOut_t *dsmEndTxnExOutP);
```

## Parámetros

dsmEndTxnExIn\_t \*dsmEndTxnExInP (I)

Esta estructura contiene los siguientes parámetros:

dsmHandle

El manejador que identifica la sesión y la asocia con llamadas IBM Spectrum Protect subsiguientes.

dsUInt8\_t vote (I)

Indica si el cliente de la aplicación compromete todas las acciones que se realizan entre la llamada `dsmBeginTxn` previa y esta llamada. Los valores posibles son:

```
DSM_VOTE_COMMIT    /* commit current transaction */
DSM_VOTE_ABORT     /* roll back current transaction */
```

Utilice `DSM_VOTE_ABORT` únicamente si la aplicación tiene un motivo para detener la transacción.

dsmEndTxnExOut\_t \*dsmEndTxnExOutP (O)

Esta estructura contiene los siguientes parámetros:

dsUInt16\_t \*reason (O)

Si la llamada a **dsmEndTxnEx** finaliza con un error o el valor de `vote` no está de acuerdo, este parámetro tiene un código de motivo que indica por qué el voto ha fallado.

Consejo: El código de retorno para la llamada puede ser cero, y el código de motivo no. Por lo tanto, el cliente de aplicación siempre debe comprobar los errores, tanto en el código de retorno como en el código de motivo (`if (rc || reason)`), antes de presuponer que la operación ha finalizado correctamente.

Si la aplicación especifica un voto de `DSM_VOTE_ABORT`, el código de motivo es `DSM_RS_ABORT_BY_CLIENT` (3). Consulte Archivo de origen de códigos de retorno de la API: `dsmrc.h` para obtener una lista de los códigos de motivo posibles. Los números del 1 al 50 de la lista de códigos de retorno están reservados para los códigos de motivo. Si el servidor finaliza la transacción, el código de retorno es `DSM_RC_CHECK_REASON_CODE`. En este caso, el valor de motivo contiene más información sobre la causa de la anulación.

groupLeaderObjId

El ID del objeto líder del grupo que se devuelve cuando se utiliza el indicador DSM\_ACTION\_OPEN con la llamada **dsmGroupHandler**.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmEndTxnEx

Código de retorno	Explicación
DSM_RC_INVALID_VOTE (2011)	El valor que se especificó para el voto no es válido.
DSM_RC_CHECK_REASON_CODE (2302)	La transacción se anuló. Compruebe el campo de motivo.
DSM_RC_ABORT_STGPOOL_COPY_CONT_NO (241)	La grabación a una de las agrupaciones de almacenamiento de copia ha fallado, y la opción COPYCONTINUE de agrupación de almacenamiento IBM Spectrum Protect se ha configurado en NO. La transacción termina.
DSM_RC_ABORT_RETRY_SINGLE_TXN (242)	Durante una operación de grabación simultánea, un objeto en la transacción va a un destino con diferentes agrupaciones de almacenamiento de copia. Finalice la transacción actual y envíe cada uno de los objetos de nuevo en su propia transacción.

## dsmGetData

La llamada de función **dsmGetData** obtiene una corriente de byte de datos de IBM Spectrum Protect y la coloca en el almacenamiento intermedio del llamador. El cliente de la aplicación llama a **dsmGetData** cuando hay más datos para recibir de una llamada previa **dsmGetObj** o **dsmGetData**.

## Sintaxis

```
dsInt16_t dsmGetData (dsUInt32_t dsmHandle,  
DataBlk *dataBlkPtr);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

DataBlk \*dataBlkPtr (I/O)

Apunta a una estructura que incluye tanto un puntero al almacenamiento intermedio de los datos que se reciben como el tamaño del almacenamiento intermedio. Cuando se devuelven los datos, esta estructura contiene el número de bytes que se han transferido. Consulte Archivos de origen de definiciones de tipo de API para obtener más información sobre la definición del tipo.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmGetData

Código de retorno	Explicación
DSM_RC_ABORT_INVALID_OFFSET (33)	El desplazamiento especificado durante la recuperación de un objeto parcial es mayor que la longitud del objeto.
DSM_RC_ABORT_INVALID_LENGTH (34)	La longitud que se especificó durante la recuperación de un objeto parcial es mayor que la longitud del objeto, o el desplazamiento y la longitud se extienden más allá del final del objeto.
DSM_RC_FINISHED (121)	Proceso finalizado. Se ha recibido el último almacenamiento intermedio. Compruebe la cantidad de datos en numBytes y a continuación llame a IBM Spectrum ProtectdsmEndGetObj.
DSM_RC_NULL_DATABLKPTR (2001)	El puntero de bloqueo de datos es nulo.
DSM_RC_ZERO_BUFLLEN (2008)	La longitud del almacenamiento intermedio es cero en el puntero del bloque de datos.
DSM_RC_NULL_BUFPTR (2009)	El puntero del almacenamiento intermedio es nulo en el puntero de bloque de datos.

Código de retorno	Explicación
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es diferente de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_MORE_DATA (2200)	Quedan más datos por obtener.

## dsmGetBufferData

La llamada a función **dsmGetBufferData** recibe una secuencia de bytes de datos de IBM Spectrum Protect a través de un almacenamiento intermedio. Después de cada llamada la aplicación necesita copiar los datos y liberar el almacenamiento intermedio a través de una llamada a **dsmReleaseBuffer**. Si el número de almacenamientos intermedios que retiene la aplicación es igual al `numTsmBuffers` especificado en la llamada **dsmInitEx**, se bloquea la función **dsmGetBufferData** hasta que se invoque **dsmReleaseBuffer**.

### Sintaxis

```
dsInt16_t dsmGetBufferData (getDataExIn_t *dsmGetBufferDataExInP,
                           getDataExOut_t *dsmGetBufferDataExOutP) ;
```

### Parámetros

`getDataExIn_t * dsmGetBufferDataExInP (I)`

Esta estructura contiene los siguientes parámetros de entrada.

`dsUInt32_t dsmHandle`

El manejador que identifica la sesión y la asocia con una llamada **dsmInitEx** previa.

`getDataExOut_t * dsmGetBufferDataExOutP (O)`

Esta estructura contienen los siguientes parámetros de salida.

`dsUInt8_t tsmBufferHandle(O)`

El manejador que identifica el almacenamiento intermedio recibido.

`char *dataPtr(O)`

La dirección en la que se escriben los datos.

`dsUInt32_t numBytes(O)`

El número real de bytes grabados por IBM Spectrum Protect.

### Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmGetBufferData

Código de retorno	Explicación
DSM_RC_BAD_CALL_SEQUENCE (2041)	La llamada no se ha emitido en el estado adecuado.
DSM_RC_OBJ_ENCRYPTED (2049)	Esta función no se puede utilizar en objetos cifrados.
DSM_RC_OBJ_COMPRESSED (2048)	Esta función no se puede utilizar en objetos comprimidos.
DSM_RC_BUFF_ARRAY_ERROR (2045)	Se ha producido un error de agrupación de almacenamiento intermedio.

## dsmGetNextQObj

La llamada a función **dsmGetNextQObj** obtiene la siguiente respuesta de consulta de una llamada **dsmBeginQuery** y coloca la respuesta en el almacenamiento intermedio del interlocutor.

La llamada **dsmGetNextQObj** se invoca una o más veces. Cada vez que se llama a una función, se recupera un único registro de consulta o un error o se devuelve un código de razón `DSM_RC_FINISHED`. Si se devuelve `DSM_RC_FINISHED`, no hay más datos a procesar. Cuando se recuperan todos los datos de consulta, o si no se necesitan más datos de consulta, envíe la llamada **dsmEndQuery** para finalizar el proceso de consulta.

El parámetro `dataBlkPtr` debe apuntar a un almacenamiento intermedio definido con el tipo de estructura `qryResp*Data`. El contexto en el que se llama a **dsmGetNextQObj** determina el tipo de estructura que se especifica en la respuesta de la consulta.

## Sintaxis

```
dsInt16_t dsmGetNextQObj (dsUInt32_t dsmHandle,
    DataBlk *dataBlkPtr);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

DataBlk \*dataBlkPtr (I/O)

Apunta a una estructura que incluye tanto un puntero al almacenamiento intermedio de los datos que se reciben como el tamaño del almacenamiento intermedio. Este almacenamiento intermedio es la estructura de respuesta de qryResp\*Data. A cambio, esta estructura contiene el número de bytes que se han transferido. Esta estructura que está asociada con cada tipo de consulta se describe en la tabla siguiente. Para obtener más información acerca de la definición de tipo deDataBlk, consulte el tema siguiente: Archivos de origen de definiciones de tipo de API.

Tabla 1. estructura de puntero DataBlk

Consulta	Estructura de respuesta	Campos de interés
qtArchive	qryRespArchiveData	<p>sizeEstimate Contiene el valor que se pasa en una llamada previa dsmSendObj.</p> <p>mediaClass Puede tener un valor de MEDIA_FIXED si el objeto está en el disco, o MEDIA_LIBRARY si el objeto está en la cinta.</p> <p>clientDeduplicated Indica si este objeto está duplicado por el cliente.</p>
qtBackup	qryRespBackupData	<p>restoreOrderExt Es de tipo dsUInt16_t. Ordene este campo cuando se restauran varios objetos en una llamada dsmBeginGetData. En el ejemplo de API, dapiqry.c, se muestra cómo clasificar el código para esta llamada. Para ver un ejemplo de clasificación, consulte el tema siguiente: Figura 1.</p> <p>sizeEstimate Contiene el valor que se pasa en una llamada previa dsmSendObj.</p> <p>mediaClass Puede tener un valor de MEDIA_FIXED si el objeto está en el disco, o MEDIA_LIBRARY si el objeto está en la cinta.</p> <p>clientDeduplicated Indica si este objeto está duplicado por el cliente.</p>
qtBackupActive	qryARespBackupData	
qtBackupGroups	qryRespBackupData	<p>dsBool_t isGroupLeader Si es verdadero, significa que este objeto es un líder de grupo.</p>
qtOpenGroups	qryRespBackupData	<p>dsBool_t isOpenGroup; Si es verdadero, significa que este grupo es abierto y no está completo.</p>

Consulta	Estructura de respuesta	Campos de interés
qtFilespace	qryRespFSData	backStartDate Contiene la indicación de fecha y hora del servidor cuando el espacio de archivo está actualizado con la acción backStartDate. backCompleteDate Contiene la indicación de fecha y hora del servidor cuando el espacio de archivo está actualizado con la acción backCompleteDate. lastReplStartDate Contiene la indicación de fecha y hora de la última vez que se inició una réplica en el servidor. lastReplCmpltDate Contiene la indicación de fecha y hora de la última vez que se completó una réplica, incluso si se produjo un error. lastBackOpDateFromServer Contiene la última indicación de fecha y hora que se guardó en el servidor. lastBackOpDateFromLocal Contiene la última indicación de fecha y hora que se guardó en el cliente.
qtMC	qryRespMCData qryRespMCDetailData	
qtProxyNodeAuth	qryRespProxyNodeData targetNodeName peerNodeName hAddress lAddress	
qtProxyNodePeer	qryRespProaxyNodeData targetNodeName peerNodeName hAddress lAddress	

## Códigos de retorno

La tabla siguiente describe los códigos de retorno de la llamada a función dsmGetNextQObj.

Tabla 2. Códigos de retorno para la llamada a función dsmGetNextQObj

Código de retorno	Número de código de retorno	Descripción
DSM_RC_ABORT_NO_MATCH	2	No se ha solicitado una coincidencia para la consulta.
DSM_RC_FINISHED	121	Proceso finalizado (iniciar dsmEndQuery). No hay más datos para procesar.
DSM_RC_UNKNOWN_FORMAT	122	El archivo que IBM Spectrum Protect ha intentado restaurar o recuperar tiene un formato desconocido.
DSM_RC_COMM_PROTOCOL_ERROR	136	Error del protocolo de comunicaciones.
DSM_RC_NULL_DATA_BLKPTR	2001	El puntero no apunta a un bloque de datos.
DSM_RC_INVALID_MCNAME	2025	Nombre de clase de gestión no válido.
DSM_RC_BAD_CALL_SEQUENCE	2041	La secuencia de llamadas no es válida.
DSM_RC_WRONG_VERSION_PARM	2065	La versión de la API del cliente de aplicación es diferente de la versión de biblioteca de IBM Spectrum Protect.
DSM_RC_MORE_DATA	2200	Quedan más datos por obtener.
DSM_RC_BUFF_TOO_SMALL	2210	El almacenamiento intermedio es demasiado pequeño.

## dsmGetObj

La llamada de función **dsmGetObj** obtiene los datos de objeto solicitados de la corriente de datos IBM Spectrum Protect y los coloca en el almacenamiento intermedio del llamador. La llamada **dsmGetObj** utiliza el ID de objeto para obtener el siguiente objeto u objeto parcial de la corriente de datos.

Los datos del objeto indicado se colocan en el almacenamiento intermedio al que apunta **DataBlk**. Si hay más datos disponibles, debe realizar una o más llamadas a **dsmGetData** con el fin de recibir los datos del objeto restantes hasta que se devuelva un código de retorno DSM\_RC\_FINISHED. Compruebe el campo `numBytes` en **DataBlk** para ver si quedan datos en el almacenamiento intermedio.

Los objetos deben consultarse en el orden en el aparecen en la lista en la llamada **dsmBeginGetData** del parámetro **dsmGetList**. La excepción ocurre cuando el cliente de la aplicación necesita saltarse un objeto en la corriente de datos para obtener un objeto más tarde en la lista. Si el objeto indicado por el ID del objeto no es el siguiente de la corriente, la corriente de datos se procesa hasta que el objeto se localiza o hasta que se finaliza la corriente. Utilice esta función con atención, ya que es posible que sea necesario procesar y descartar grandes cantidades de datos para localizar el objeto solicitado.

Requisito: Si **dsmGetObj** devuelve un código de error (NOT FINISHED o MORE\_DATA), la sesión deberá finalizarse para detener la operación de restauración. Esto es especialmente importante si utiliza cifrado y recibe un RC\_ENC\_WRONG\_KEY. Debe iniciar una nueva sesión con la clave correcta.

## Sintaxis

```
dsInt16_t dsmGetObj (dsUInt32_t dsmHandle,  
    ObjID *objIdP,  
    DataBlk *dataBlkPtr);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

ObjID \*objIdP (I)

Un puntero al ID del objeto que se va a restaurar.

DataBlk \*dataBlkPtr (I/O)

Un puntero al almacenamiento intermedio donde se colocan los datos restaurados.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmGetObj

Código de retorno	Explicación
DSM_RC_ABORT_INVALID_OFFSET (33)	El desplazamiento que se especificó durante la recuperación de un objeto parcial es mayor que la longitud del objeto.
DSM_RC_ABORT_INVALID_LENGTH (34)	La longitud especificada durante la recuperación de un objeto parcial es mayor que la longitud del objeto, o el desplazamiento y la longitud alcanzan más allá del final del objeto.
DSM_RC_FINISHED (121)	Proceso finalizado (iniciar <b>dsmEndGetObj</b> ).
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_MORE_DATA (2200)	Quedan más datos por obtener.
RC_ENC_WRONG_KEY (4580)	La clave que se proporciona en la llamada <b>dsmInitEx</b> , o la clave guardada, no coinciden con la clave que se utilizó para cifrar este objeto. Termine la sesión y proporcione la clave adecuada.

## dsmGroupHandler

La llamada de función **dsmGroupHandler** realiza una acción en un grupo de archivo lógico dependiendo de los datos introducidos. El cliente relaciona un número de objetos con el fin de hacer referencia y administrar el servidor IBM Spectrum Protect como grupo lógico.

Para obtener más información, consulte el apartado Agrupación de archivos.



## Sintaxis

```
dsInt16_t dsmGroupHandler (dsmGroupHandlerIn_t *dsmGroupHandlerInP,  
                           dsmGroupHandlerOut_t *dsmGroupHandlerOutP);
```

## Parámetros

`dsmGroupHandlerIn_t *dsmGroupHandlerInP (I)`

Pasa los atributos del grupo al API.

`groupType`

El tipo de grupo. Los valores incluyen:

- `DSM_GROUPTYPE_PEER` - peer group

`actionType`

La acción que se va a ejecutar. Los valores incluyen:

- `DSM_GROUP_ACTION_OPEN` - crea un grupo nuevo
- `DSM_GROUP_ACTION_CLOSE` - valida y guarda un grupo abierto
- `DSM_GROUP_ACTION_ADD` - añade a un grupo
- `DSM_GROUP_ACTION_ASSIGNTO` - asigna a otro grupo
- `DSM_GROUP_ACTION_REMOVE` - elimina un miembro de un grupo

`memberType.`

El tipo de grupo del objeto. Los valores incluyen:

- `DSM_MEMBERTYPE_LEADER` - líder de grupo
- `DSM_MEMBERTYPE_MEMBER` - miembro de grupo

`*uniqueGroupTagP`

Un ID de cadena único que está asociado a un grupo.

`leaderObjId`

El ID de objeto para el líder del grupo.

`*objNameP`

Un puntero al nombre del objeto del líder del grupo.

`memberObjList`

Una lista de objetos para eliminar o asignar.

`dsmGroupHandlerOut_t *dsmGroupHandlerOutP (O)`

Pasa la dirección de la estructura que completa la API. Se devuelve el número de la versión de la estructura.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para `dsmGroupHandler`

Código de retorno	Explicación
<code>DSM_RC_ABORT_INVALID_GROUP_ACTION (237)</code>	Se intentó realizar una operación no válida en un líder o miembro de grupo.

## dsmInit

La llamada de función **dsmInit** inicia una sesión de la API y conecta al cliente con el almacenamiento IBM Spectrum Protect. El cliente de la aplicación sólo puede tener una sesión activa abierta a la vez. Para abrir otra sesión con parámetros distintos, utilice la llamada **dsmTerminate** primero con objeto de finalizar la sesión actual.

Para permitir la consulta entre nodos y restaurar o recuperar datos, utilice las opciones de cadena *-fromnode* y *-fromowner* . Para obtener más información, consulte el apartado Acceder a objetos de nodos y propietarios.

## Sintaxis

```
dsInt16_t dsmInit (dsUint32_t *dsmHandle,  
                  dsmApiVersion *dsmApiVersionP,  
                  char *clientNodeNameP,
```

```

char      *clientOwnerNameP,
char      *clientPasswordP,
char      *applicationType,
char      *configfile,
char      *options);

```

## Parámetros

---

`dsUInt32_t *dsmHandle` (O)

El manejador que identifica la sesión de iniciación y que la asocia con llamadas subsiguientes IBM Spectrum Protect.

`dsmApiVersion *dsmApiVersionP` (I)

Un puntero a la estructura de datos que identifica la versión de la API que el cliente de la aplicación está utilizando en esta sesión. La estructura contiene los valores de tres constantes, `DSM_API_VERSION`, `DSM_API_RELEASE` y `DSM_API_LEVEL`, que se configuran en el archivo `dsmapiid.h`. Se debe realizar una llamada previa a `dsmQueryApiVersion` para garantizar que hay compatibilidad entre la versión de la interfaz de programación de aplicaciones (API) de la aplicación y la versión de la biblioteca de la API instalada en la estación de trabajo del usuario.

`char *clientNodeNameP` (I)

Este parámetro es un puntero al nodo de la sesión IBM Spectrum Protect. Todas las sesiones deben tener un nombre de nodo asociado con ellas. La constante `DSM_MAX_NODE_LENGTH`, en el archivo `dsmapiid.h` configura el tamaño máximo permitido del nombre del nodo.

El nombre del nodo no distingue entre mayúsculas y minúsculas.

Si este parámetro está configurado en `NULO`, y `passwordaccess` está configurado en `prompt`, la API intenta obtener primero el nombre del nodo de la cadena de opciones que se pasaron. Si no se encuentra allí, entonces la API intenta obtener el nombre del nodo del archivo de configuración o de los archivos de opciones. Si este intento de obtener el nombre de nodo falla, la API de UNIX o Linux utiliza el nombre del host del sistema, mientras que las API de otros sistemas operativos utilizan el código de retorno `DSM_RC_REJECT_ID_UNKNOWN`.

Este parámetro debe ser `NULO` si la opción `passwordaccess` en el archivo `dsm.sys` está configurada en `generate`. La API entonces utiliza el nombre del host del sistema.

`char *clientOwnerNameP` (I)

Este parámetro es un puntero al propietario de la sesión IBM Spectrum Protect. Si el sistema operativo en donde se inicia la sesión es un sistema de varios usuarios, un nombre de propietario de `NULO` (el usuario `root`) tiene la autorización de realizar copias de seguridad, archivar, restaurar o recuperar objetos que pertenecen a la aplicación, independientemente del propietario del objeto.

El nombre del propietario es sensible a mayúsculas y minúsculas.

Este parámetro debe ser `NULO` si la opción `passwordaccess` en el archivo `dsm.sys` está configurada en `generate`. La API entonces utiliza el ID del usuario del inicio de sesión.

Nota: En un sistema operativo de varios usuarios, si `passwordaccess` está configurado en `prompt`, no es necesario que el nombre del propietario se correlacione con el ID de usuario activo de la sesión que ejecuta la aplicación.

`char *clientPasswordP` (I)

Este parámetro es un puntero a la contraseña del nodo en el que se ejecuta la sesión IBM Spectrum Protect. La constante `DSM_MAX_VERIFIER_LENGTH` en el archivo `dsmapiid.h` configura el tamaño máximo permitido de una contraseña.

La contraseña no es sensible a mayúsculas y minúsculas.

Excepto cuando se inicia primero el archivo de contraseña, el valor del este parámetro se ignora si `passwordaccess` está configurado en `generate`.

`char *applicationType` (I)

Este parámetro identifica la aplicación que está ejecutando la sesión. El cliente de la aplicación define el valor.

Cada vez que un cliente de aplicación de la API inicia una sesión con el servidor, el tipo de aplicación (o plataforma) del cliente se actualiza en el servidor. Recomendamos que el valor del tipo de aplicación contenga una abreviatura del sistema operativo porque este valor se introduce en el campo **platform** del servidor. La longitud máxima de la cadena es `DSM_MAX_PLATFORM_LENGTH`.

Para ver el valor actual del tipo de aplicación, llame a `dsmQuerySessInfo`.

`char *configfile` (I)

Este parámetro apunta a una cadena de caracteres que contiene el nombre calificado al completo del archivo de configuración de la API. Las opciones que se especifican en el archivo de configuración de la API modifican sus especificaciones en el archivo de opciones del cliente. Los archivos de opciones se definen cuando se instala IBM Spectrum Protect (cliente o API).

char \*options (I)

Apunta a una cadena de caracteres que puede contener opciones de archivo como:

- *Compressalways*
- *Servname* (UNIX o Linux únicamente)
- *TCPServeraddr*
- *Fromnode*
- *Fromowner*
- *EnableClientEncryptKey*

El cliente de la aplicación puede utilizar la lista de opciones para modificar los valores de estas opciones definidas por el archivo de configuración.

El formato de la opción es:

1. Cada opción que se especifica en la lista de opción empieza con un guión (-) y lo sigue la palabra clave de la opción.
2. A su vez, a la palabra clave le sigue un signo de igual (=) y a continuación el parámetro de la opción.
3. Si el parámetro de la opción contiene un espacio en blanco, cierre el parámetro con comillas sencillas o dobles.
4. Si se especifica más de una opción, separe las opciones con espacios en blanco.

Si las opciones son NULO, los valores de todas las opciones se toman del archivo de opciones del usuario o del archivo de configuración de la API.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno de dsminit

Código de retorno	Explicación
DSM_RC_ABORT_SYSTEM_ERROR (1)	El servidor ha detectado un error del sistema y ha notificado a los clientes.
DSM_RC_REJECT_VERIFIER_EXPIRED (52)	La contraseña ha caducado y debe actualizarse.
DSM_RC_REJECT_ID_UNKNOWN (53)	No se ha encontrado el nombre de nodo.
DSM_RC_AUTH_FAILURE (137)	Ha ocurrido un fallo de autenticación.
DSM_RC_NO_STARTING_DELIMITER (148)	No hay un delimitador de inicio en el patrón.
DSM_RC_NEEDED_DIR_DELIMITER (149)	Se necesita un delimitador de directorio inmediatamente antes y después de la serie de metadatos de "directorios coincidentes" ("...") y no se ha encontrado ninguno.
DSM_RC_NO_PASS_FILE (168)	El archivo de contraseña no está disponible.
DSM_RC_UNMATCHED_QUOTE (177)	En la cadena de opción hay una comilla sin correlacionar.
DSM_RC-NLS_CANT_OPEN_TXT (0610)	No se puede abrir el archivo de texto del mensaje.
DSM_RC_INVALID_OPT (400)	Una entrada en la cadena de opción no es válida.
DSM_RC_INVALID_DS_HANDLE (2014)	Manejador DSM no válido.
DSM_RC_NO_OWNER_REQD (2032)	El parámetro del propietario debe ser NULO cuando <i>passwordaccess</i> está configurado en <i>generate</i> .
DSM_RC_NO_NODE_REQD (2033)	El parámetro del nodo debe ser NULO cuando <i>passwordaccess</i> está configurado en <i>generate</i> .
DSM_RC_WRONG_VERSION (2064)	La versión de la interfaz de programación de aplicaciones (API) de la aplicación tiene un valor más alto que la versión IBM Spectrum Protect.
DSM_RC_PASSWD_TOOLONG (2103)	La contraseña especificada es demasiado larga.
DSM_RC_NO_OPT_FILE (2220)	No se ha encontrado el archivo de configuración.
DSM_RC_INVALID_KEYWORD (2221)	Una palabra clave especificada en una cadena de opciones no es válida.
DSM_RC_PATTERN_TOO_COMPLEX (2222)	El patrón de inclusión/exclusión es demasiado complicado para que lo interprete IBM Spectrum Protect.
DSM_RC_NO_CLOSING_BRACKET (2223)	No hay paréntesis de cierre en el patrón.

Código de retorno	Explicación
DSM_RC_INVALID_SERVER (2225)	En un entorno de varios usuarios, no se ha encontrado el servidor en el archivo de configuración del sistema.
DSM_RC_NO_HOST_ADDR (2226)	No hay información suficiente para conectar con el host.
DSM_RC_MACHINE_SAME (2227)	El nombre de nodo definido en el archivo de opciones no puede ser el mismo que el nombre del host del sistema.
DSM_RC_NO_API_CONFIGFILE (2228)	No puede abrir el archivo de configuración.
DSM_RC_NO_INCLEXCL_FILE (2229)	No se ha encontrado el archivo de inclusión/exclusión.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	No se ha encontrado el archivo dsm.sys o el de inclusión/exclusión.

**Conceptos relacionados:**

Visión general del archivo de opciones del cliente  
Opciones de proceso

## dsmInitEx

La llamada de función dsmInitEx inicia una sesión de la API utilizando los parámetros adicionales para una verificación extendida.

### Sintaxis

```
dsInt16_t dsmInitEx (dsUInt32_t *dsmHandleP,
                    dsmInitExIn_t *dsmInitExInP,
                    dsmInitExOut_t *dsmInitExOutP) ;
```

### Parámetros

dsUInt32\_t \*dsmHandleP (O)

El manejador que identifica la sesión de iniciación y que la asocia con llamadas subsiguientes IBM Spectrum Protect.

dsmInitExIn\_t \*dsmInitExInP

Esta estructura contiene los siguientes parámetros de entrada:

dsmApiVersion \*dsmApiVersionP (I)

Este parámetro es un puntero a la estructura de datos que identifica la versión de la API que el cliente de la aplicación está utilizando en esta sesión. La estructura contiene los valores de las cuatro constantes, DSM\_API\_VERSION, DSM\_API\_RELEASE, DSM\_API\_LEVEL y DSM\_API\_SUBLEVEL que se definen en el archivo dsmapi.h. Invoque dsmQueryApiVersionEx y compruebe que la versión de la API del cliente de aplicación y la versión de la biblioteca de la API instalada en la estación de trabajo del usuario sean compatibles.

char \*clientNodeNameP (I)

Este parámetro es un puntero al nodo de la sesión IBM Spectrum Protect. Todas las sesiones deben estar asociadas con un nombre de nodo. La constante DSM\_MAX\_NODE\_LENGTH del archivo dsmapi.h establece el tamaño máximo de un nombre de nodo.

El nombre del nodo no distingue entre mayúsculas y minúsculas.

Si este parámetro está configurado en NULO, y passwordaccess está configurado en prompt, la API intenta obtener primero el nombre del nodo de la cadena de opciones que se pasaron. Si no se encuentra allí, entonces la API intenta obtener el nombre del nodo del archivo de configuración o de los archivos de opciones. Si este intento de obtener el nombre del nodo falla, la API de UNIX o Linux utiliza el nombre del host del sistema, mientras que las API de otros sistemas operativos devuelven DSM\_RC\_REJECT\_ID\_UNKNOWN.

Este parámetro debe ser NULL si la opción passwordaccess del archivo dsm.sys se define como generate. La API entonces utiliza el nombre del host del sistema.

char \*clientOwnerNameP (I)

Este parámetro es un puntero al propietario de la sesión IBM Spectrum Protect. Si el sistema operativo es una plataforma de varios usuarios, un nombre de propietario de NULO (el usuario root) tiene la autorización de realizar una copia de seguridad, archivar, restaurar o recuperar los objetos que pertenecen a la aplicación, independientemente del propietario del objeto.

El nombre del propietario es sensible a mayúsculas y minúsculas.

Este parámetro debe ser NULL si la opción passwordaccess del archivo dsm.sys se define como generate. La API entonces utiliza el ID del usuario del inicio de sesión.

Consejo: En una plataforma de varios usuarios, si passwordaccess está configurado en prompt, no es necesario que el nombre del propietario se correlacione con el ID del usuario activo de la sesión que ejecuta la aplicación.

char \*clientPasswordP (I)

Un puntero a la contraseña del nodo en donde se ejecuta la sesión IBM Spectrum Protect. La constante DSM\_MAX\_VERIFIER\_LENGTH del archivo dsmapitd.h define el tamaño máximo permitido para una contraseña.

La contraseña no es sensible a mayúsculas y minúsculas.

Excepto cuando se inicia primero el archivo de contraseña, el valor de este parámetro se ignora si passwordaccess está configurado en generate.

char \*userNameP;

Un puntero al nombre de usuario administrativo que tiene la autorización del cliente para este nodo.

char \*userPasswordP;

Un puntero a la contraseña del parámetro userName, si se proporciona un valor.

char \*applicationType (I)

Identifica la aplicación que está ejecutando la sesión IBM Spectrum Protect. El cliente de la aplicación identifica el valor.

Cada vez que un cliente de aplicación de la API inicia una sesión con el servidor, el tipo de aplicación (o sistema operativo) del cliente se actualiza en el servidor. El valor se especifica en el campo platform del servidor. Considere la posibilidad de utilizar un ID de sistema operativo en el valor. La longitud máxima de la cadena se define en la constante DSM\_MAX\_PLATFORM\_LENGTH.

Para ver el valor actual del tipo de la aplicación, llame a dsmQuerySessInfo.

char \*configfile (I)

Apunta a una cadena de caracteres que contiene el nombre completo del archivo de configuración de la API. Las opciones que se especifican en el archivo de configuración de la API modifican sus especificaciones en el archivo de opciones del cliente. Los archivos de opciones se definen cuando se instala IBM Spectrum Protect (cliente o API).

char \*options (I)

Apunta a una cadena de caracteres que puede contener opciones de archivo como:

- Compressalways
- Servername (Solo sistemas UNIX y Linux)
- TCPServeraddr (no para sistemas UNIX)
- Fromnode
- Fromowner

El cliente de la aplicación puede utilizar la lista de opciones para modificar los valores de estas opciones definidas por el archivo de configuración.

Las opciones tienen el formato siguiente:

1. Cada opción que se especifica en la lista de opción empieza con un guión (-) y lo sigue la palabra clave de la opción.
2. A la palabra clave le sigue un signo de igual (=) y a continuación el parámetro de opción.
3. Si el parámetro de la opción contiene un espacio en blanco, cierre el parámetro con comillas simples o dobles.
4. Si se especifica más de una opción, separe las opciones con espacios en blanco.

Si las opciones son NULO, los valores de todas las opciones se toman del archivo de opciones del usuario o del archivo de configuración de la API.

dirDelimiter

El delimitador del directorio se prefija en los nombres del espacio de archivo, alto y bajo rango. Debe especificar el parámetro dirDelimiter sólo si la aplicación altera temporalmente los valores predeterminados del sistema. En un entorno UNIX o Linux, el valor predeterminado es la barra inclinada (/). En un entorno de Windows, el valor predeterminado es la barra invertida (\).

useUnicode

Un indicador booleano que indica si está habilitado Unicode. El distintivo useUnicode debe establecerse en false para la interoperatividad entre plataformas de sistemas UNIX y Windows.

bCrossPlatform

Un distintivo booleano que debe establecerse (bTrue) para la interoperatividad entre plataformas de sistemas UNIX y Windows. Cuando está establecido el distintivo bCrossPlatform, la API se asegura de que los espacios de archivo no sean Unicode y que la aplicación no utilice Unicode. Una aplicación Windows que utiliza Unicode no es compatible con las aplicaciones que utilizan codificaciones no de Unicode. El distintivo bCrossPlatform no se debe establecer para una aplicación Windows que utiliza Unicode.

UseTsmBuffers

Indica si se ha de utilizar la supresión de copia de almacenamiento intermedio.

numTsmBuffers  
El número de almacenamientos intermedios cuando useTsmBuffers=bTrue.

bEncryptKeyEnabled  
Indica si se utiliza el cifrado con una clave gestionada por la aplicación.

encryptionPasswordP  
La contraseña del cifrado.  
Restricción: Cuando encryptkey=save, si existe una clave cifrada, se omite el valor especificado en encryptionPasswordP.

dsmAppVersion \*appVersionP (I)  
Este parámetro apunta a la estructura de datos que identifica la información de la versión de la aplicación que comienza una sesión de API. La estructura contiene los valores de las cuatro constantes, applicationVersion, applicationRelease, applicationLevel y applicationSubLevel, que se definen en el archivo tsmapi.h.

dsmInitExOut\_t \*dsmInitExOut P  
Esta estructura contienen los parámetros de salida.

dsUint32\_t \*dsmHandle (O)  
El manejador que identifica esta sesión de inicialización y que la asocia con llamadas API subsiguientes.

infoRC  
Información adicional acerca del código de retorno. Compruebe el código de retorno de la función y el valor de infoRC. Si el valor de infoRC es DSM\_RC\_REJECT\_LASTSESS\_CANCELED (69), the IBM Spectrum Protect indica que el administrador ha cancelado la última sesión.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno de dsmInitEx

Código de retorno	Explicación
DSM_RC_ABORT_SYSTEM_ERROR (1)	El servidor de IBM Spectrum Protect ha detectado un error del sistema y ha notificado a los clientes.
DSM_RC_REJECT_VERIFIER_EXPIRED (52)	La contraseña ha caducado y debe actualizarse. La siguiente llamada debe ser dsmChangePW con el manejador devuelto en esta llamada.
DSM_RC_REJECT_ID_UNKNOWN (53)	No se ha encontrado el nombre de nodo.
DSM_RC_TA_COMM_DOWN (103)	El vínculo de comunicaciones no funciona.
DSM_RC_AUTH_FAILURE (137)	Ha ocurrido un fallo de autenticación.
DSM_RC_NO_STARTING_DELIMITER (148)	No hay un delimitador de inicio en el patrón.
DSM_RC_NEEDED_DIR_DELIMITER (149)	Se necesita un delimitador de directorio inmediatamente antes y después de "match directories" meta-string ("..."), pero no se ha encontrado.
DSM_RC_NO_PASS_FILE (168)	El archivo de contraseña no está disponible.
DSM_RC_UNMATCHED_QUOTE (177)	En la cadena de opción hay una comilla no coincidente.
DSM_RC-NLS_CANT_OPEN_TXT (0610)	No se puede abrir el archivo de texto del mensaje.
DSM_RC_INVALID_OPT (2013)	Una entrada en la cadena de opción no es válida.
DSM_RC_INVALID_DS_HANDLE (2014)	Manejador DSM no válido.
DSM_RC_NO_OWNER_REQD (2032)	El parámetro del propietario debe ser NULO cuando passwordaccess está configurado en generate.
DSM_RC_NO_NODE_REQD (2033)	El parámetro del nodo debe ser NULL cuando se establece passwordaccess en generate.
DSM_RC_WRONG_VERSION (2064)	La versión de la interfaz de programación de aplicaciones (API) de la aplicación tiene un valor más alto que la versión de IBM Spectrum Protect.
DSM_RC_PASSWD_TOOLONG (2103)	La contraseña especificada es demasiado larga.
DSM_RC_NO_OPT_FILE (2220)	No se ha encontrado un archivo de configuración.
DSM_RC_INVALID_KEYWORD (2221)	Una palabra clave especificada en una cadena de opciones no es válida.
DSM_RC_PATTERN_TOO_COMPLEX (2222)	El patrón de inclusión/exclusión es demasiado complicado para que IBM Spectrum Protect lo interprete.

Código de retorno	Explicación
DSM_RC_NO_CLOSING_BRACKET (2223)	No hay paréntesis de cierre en el patrón.
DSM_RC_INVALID_SERVER (2225)	En un entorno de varios usuarios, no se ha encontrado el servidor en el archivo de configuración del sistema.
DSM_RC_NO_HOST_ADDR (2226)	No hay información suficiente para conectar con el host.
DSM_RC_MACHINE_SAME (2227)	El nombre de nodo definido en el archivo de opciones no puede ser el mismo que el nombre del host del sistema.
DSM_RC_NO_API_CONFIGFILE (2228)	No puede abrir el archivo de configuración.
DSM_RC_NO_INCLEXCL_FILE (2229)	No se ha encontrado el archivo de inclusión/exclusión.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	Bien dsm.sys o el archivo include-exclude no se han encontrado.

**Conceptos relacionados:**

Visión general del archivo de opciones del cliente  
Opciones de proceso

## dsmLogEvent

La llamada de función **dsmLogEvent** registra un mensaje de usuario (ANE4991 I) en el archivo de registro del servidor, en el registro de error local o en ambos. Una estructura de tipo **logInfo** se pasa en la llamada. Esta llamada debe realizarse con el estado **InSession** dentro de una sesión. No debe ejecutarse durante una operación de envío, obtención o consulta. Para recuperar los mensajes registrados en el servidor, utilice el mandato **query actlog** mediante el cliente administrativo.

Consulte el diagrama de estado resumido, Figura 1.

## Sintaxis

```
dsInt16_t dsmLogEvent
(dsUint32_t dsmHandle,
logInfo *logInfoP);
```

## Parámetros

dsUint32\_t dsmHandle(I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

logInfo \*logInfoP (I)

Pasa el mensaje y el destino. El cliente de aplicación es responsable de asignar almacenamiento para la estructura.

Los campos en la estructura **logInfo** son:

mensaje

El texto del mensaje que se va a registrar. Esta debe ser una cadena finalizada en nulo. La longitud máxima es DSM\_MAX\_RC\_MSG\_LENGTH.

dsmLogtype

Especifica dónde registrar el mensaje. Como valores posibles se incluyen: **logServer**, **logLocal**, **logBoth**.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmLogEvent

Código de retorno	Explicación
DSM_RC_STRING_TOO_LONG (2120)	La cadena del mensaje es demasiado larga.

## dsmLogEventEx

La llamada a función **dsmLogEventEx** registra un mensaje en el archivo de registro del servidor, en el registro de errores local o en ambos. Esta llamada debe realizarse con el estado **InSession** dentro de una sesión. La llamada no se puede realizar dentro de una llamada de consulta, envío u obtención.

Diagrama de estado de resumen: Para obtener una descripción general de las interacciones de sesión, consulte el diagrama de estado de resumen en el siguiente tema:

Figura 1

La gravedad determina el número de mensaje IBM Spectrum Protect. Para ver los mensajes que están registrados en el servidor, utilice el mandato `query actlog` a través del cliente administrativo. Utilice la opción de cliente de IBM Spectrum Protect, `errorlogretention`, para borrar el archivo de registro de errores del cliente si la aplicación genera numerosos mensajes de cliente escritos en el registro de cliente, `dsmLogType`, `logLocal` o `logBoth`. Para obtener más información, consulte la documentación del servidor de IBM Spectrum Protect.

## Sintaxis

```
extern dsInt16_t DSMLINKAGE dsmLogEventEx(  
    dsUInt32_t dsmHandle,  
    dsmLogExIn_t *dsmLogExInP,  
    dsmLogExOut_t *dsmLogExOutP  
);
```

## Parámetros

`dsUInt32_t dsmHandle(I)`

El manejador que asocia esta llamada con una llamada `dsmInitEx` anterior.

`dsmLogExIn_t *dsmLogExInP`

Esta estructura contiene los parámetros de entrada.

`dsmLogSeverity severity;`

Este parámetro es la gravedad del evento. Los valores posibles son:

```
logSevInfo,      /* information ANE4990 */  
logSevWarning,  /* warning ANE4991 */  
logSevError,    /* Error ANE4992 */  
logSevSevere   /* severe ANE4993 */
```

`char appMsgID[8];`

Este parámetro es una cadena que sirve para identificar el mensaje de aplicación específico. Un formato adecuado tiene tres caracteres seguidos por cuatro números, por ejemplo: `DSM0250`.

`dsmLogType logType;`

Este parámetro especifica dónde dirigir el evento. El parámetro tiene los siguientes valores posibles:

- `logServer`
- `logLocal`
- `logBoth`

`char *message;`

Este parámetro es el texto del mensaje de evento que se registra. El texto debe ser una serie finalizada en nulo. La longitud máxima es `DSM_MAX_RC_MSG_LENGTH`.

Restricción: Los mensajes que van al servidor deben estar en inglés. Los mensajes que no son en inglés no se muestran correctamente.

`dsmLogExOut_t *dsmLogExOutP`

Esta estructura contienen los parámetros de salida. Actualmente no existen parámetros de salida.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ().

Tabla 1. Códigos de retorno para `dsmLogEventEx`

Código de retorno	Explicación
<code>DSM_RC_STRING_TOO_LONG (2120)</code>	La cadena del mensaje es demasiado larga.

## dsmQueryAccess

La llamada de función **dsmQueryAccess** consulta las reglas de autorización de acceso del servidor en las copias de seguridad de los objetos o en las copias archivadas. Un puntero a una agrupación de reglas de acceso pasa a la llamada, y se devuelve la agrupación rellena. Un puntero al número de reglas pasa para indicar cuántas reglas hay en la agrupación.

No existen códigos de retorno específicos de esta llamada.



## Sintaxis

```
dsInt16_t DSMLINKAGE dsmQueryAccess
                (dsUInt32_t dsmHandle),
                qryRespAccessData **accessListP,
                dsUInt16_t *numberOfRules) ;
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

qryRespAccessData \*\*accessListP (O)

Un puntero a una agrupación de elementos `qryRespAccessData` que asigna la biblioteca API. Cada elemento se corresponde con una regla de acceso. El número de elementos de la agrupación se devuelve en el parámetro **numberOfRules**. La información que se devuelve en cada elemento `qryRespAccessData` incluye los siguientes datos:

	Nombre	Descripción
	<b>ruleNumber</b>	El ID para la regla de acceso. Esto identifica la regla que se ha de suprimir.
	<b>AccessType</b>	El tipo de archivado o copia de seguridad.
	<b>Nodo</b>	El nodo al que se da acceso.
	<b>Propietario</b>	El usuario al que se le da acceso.
	<b>objName</b>	Descriptores de espacio de archivo de alto y bajo rango.

dsUInt32\_t \*numberOfRules (O)

Devuelve el número de reglas en la agrupación `accessList`.

## dsmQueryApiVersion

La llamada de función **dsmQueryApiVersion** realiza una solicitud de consulta de la versión de la biblioteca de la API a la que accede el cliente de aplicación.

Todas las actualizaciones de la API se realizan en un formato compatible con versiones posteriores. Cualquier cliente de la aplicación con una versión API o release inferior o igual a la biblioteca API en la estación de trabajo del usuario final opera sin cambios. Tenga en cuenta que en caso de que la llamada **dsmQueryApiVersion** devuelva una versión o release de la versión más antigua que la del cliente de aplicación algunas llamadas API pueden mejorar de una forma que no es compatible por la versión de la API más antigua del usuario.

El número de la versión API de la aplicación se almacena en el archivo de encabezado `dsmapi.h` como constantes `DSM_API_VERSION`, `DSM_API_RELEASE`, y `DSM_API_LEVEL`.

No existen códigos de retorno específicos de esta llamada.

## Sintaxis

```
void dsmQueryApiVersion (dsmApiVersion *apiVersionP);
```

## Parámetros

dsmApiVersion \*apiVersionP (O)

Este parámetro es un puntero a la estructura que contiene la versión de la biblioteca API, release y los componentes de nivel. Por ejemplo, si la versión de la biblioteca es 1.1.0, entonces, después de volver de la llamada, los campos de la estructura contienen los siguientes valores:

```
dsmApiVersionP->version = 1
dsmApiVersionP->release = 1
dsmApiVersionP->level   = 0
```

## dsmQueryApiVersionEx

La llamada de función **dsmQueryApiVersionEx** realiza una solicitud de consulta de la versión de la biblioteca API a la que accede el cliente de la aplicación.

Todas las actualizaciones al API se llevan a cabo en un formato compatible con la versión superior. Cualquier cliente de la aplicación con una versión API o release inferior o igual a la biblioteca API en la estación de trabajo del usuario final opera sin cambios. Consulte el resumen de los cambios de código en el archivo README\_api\_enu para obtener información sobre las excepciones de compatibilidad superior. Si la llamada **dsmQueryApiVersionEx** devuelve una versión o release de una versión distinta a la del cliente de la aplicación, tenga en cuenta antes de proceder que algunas llamadas API pueden mejorar de una forma que no es soportada por la versión antigua de la API del usuario final.

El número de versión de API de la aplicación se almacena en el archivo de encabezado dsmapi.h como constantes DSM\_API\_VERSION, DSM\_API\_RELEASE, DSM\_API\_LEVEL, y DSM\_API\_SUBLEVEL.

No existen códigos de retorno específicos de esta llamada.

## Sintaxis

```
void dsmQueryApiVersionEx (dsmApiVersionEx *apiVersionP);
```

## Parámetros

dsmApiVersionEx \*apiVersionP (O)

Este parámetro es un puntero a la estructura que contiene la versión, release, nivel y subnivel de los componentes de la biblioteca API. Por ejemplo, si la versión de la biblioteca es 5.5.0.0, entonces, después de volver de la llamada, los campos de la estructura contienen los siguientes valores:

- ApiVersionP->version = 5
- ApiVersionP->release = 5
- ApiVersionP->level = 0
- ApiVersionP->subLevel = 0

## dsmQueryCliOptions

La llamada de función **dsmQueryCliOptions** consulta valores de opción importantes en los archivos de opción del usuario. Una estructura de tipo **optStruct** se pasa en la llamada y contiene la información. Esta llamada se realiza antes de invocar **dsmInitEx**, y determina la configuración antes de la sesión.

No existen códigos de retorno específicos a esta llamada.

## Sintaxis

```
dsInt16_t dsmQueryCliOptions  
(optStruct *optstructP);
```

## Parámetros

optStruct \*optstructP (I/O)

Este parámetro pasa la dirección de la estructura que la API finaliza. El cliente de la aplicación es responsable de asignar almacenamiento para la estructura. Al devolverse correctamente, se introduce la información apropiada en los campos de la estructura.

La siguiente información se devuelve en la estructura **optStruct** :

	Nombre	Descripción
	<b>dsmiDir</b>	El valor de la variable de entorno DSMI_DIR.
	<b>dsmiConfig</b>	El archivo de opciones de cliente, según se especifica en la variable de entorno DSMI_CONFIG.
	<b>serverName</b>	El nombre del servidor IBM Spectrum Protect.
	<b>commMethod</b>	El método de comunicación seleccionado. Consulte #defines para DSM_COMM_* en el archivo.
	<b>serverAddress</b>	La dirección del servidor que se basa en el método de comunicación.
	<b>nodeName</b>	El nombre de nodo de cliente (máquina).
	<b>compression</b>	Este campo proporciona información con respecto a la opción de compresión.
	<b>passwordAccess</b>	Los valores son: <i>bTrue</i> para generate, y <i>bFalse</i> para prompt.

**Conceptos relacionados:**  
Opciones de proceso

## dsmQuerySessInfo

La llamada de función **dsmQuerySessInfo** inicia una solicitud de consulta a IBM Spectrum Protect sobre información relacionada con la operación de la sesión especificada en **dsmHandle**. Una estructura de tipo **ApiSessInfo** se pasa en la llamada, con toda la información relacionada con la sesión disponible. Esta llamada se inicia después de una llamada **dsmInitEx** correcta.

La información que se devuelve en la estructura **ApiSessInfo** incluye lo siguiente:

- Información del servidor: número de puerto, fecha y hora, y tipo
- Valores predeterminados del cliente: tipo de aplicación, permisos de supresión, delimitadores y límites de transacción
- Información de la sesión: ID de inicio de sesión y propietario
- Datos de política: dominio, conjunto de políticas activas y periodo de gracia de retención

Consulte Archivos de origen de definiciones de tipo de API para obtener más información sobre el contenido de la estructura que se pasa y de cada campo de la misma.

## Sintaxis

```
dsInt16_t dsmQuerySessInfo (dsUInt32_t dsmHandle,  
    ApiSessInfo *SessInfoP);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

ApiSessInfo \*SessInfoP (I/O)

Este parámetro pasa la dirección de la estructura que la API introduce. El cliente de la aplicación es responsable de asignar el almacenamiento para la estructura y de completar las entradas de los campos que indican la versión de la estructura que se utiliza. Cuando la operación es correcta, los campos de la estructura se rellenan con la información adecuada. **adsmServerName** es el nombre que se proporciona en el mandato **define server** del servidor IBM Spectrum Protect. Si el valor del campo **archiveRetentionProtection** es true, el servidor está habilitado para la protección de retención.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmQuerySessInfo

Código de retorno	Explicación
DSM_RC_NO_SESS_BLK (2006)	Información de sesión de servidor no bloqueada.
DSM_RC_NO_POLICY_BLK (2007)	La información de la política del servidor no está disponible.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.

## dsmQuerySessOptions

La llamada de función **dsmQuerySessOptions** consulta valores de opción importantes que son válidos en la sesión especificada en **dsmHandle**. Una estructura de tipo **optStruct** se pasa en la llamada y contiene la información.

Esta llamada se inicia después de una llamada **dsmInitEx** correcta. Es posible que los valores que se devuelvan sean distintos de los valores devueltos en una llamada **dsmQueryCliOptions**, depende de los valores pasados a la llamada **dsmInitEx**, principalmente **optString**, y **optFile**. Para obtener más información sobre la opción de precedencia, consulte Conceptos básicos de los archivos de opciones y configuración.

No existen códigos de retorno específicos de esta llamada.

## Sintaxis

```
dsInt16_t dsmQuerySessOptions  
    (dsUInt32_t dsmHandle,  
    optStruct *optstructP);
```

## Parámetros

dsUint32\_t dsmhandle(I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

optStruct \*optstructP (I/O)

Este parámetro pasa la dirección de la estructura que la API finaliza. El cliente de aplicación es responsable de asignar almacenamiento para la estructura. Cuando la operación es correcta, los campos de la estructura se rellenan con la información adecuada.

La información que se devuelve en la estructura optStruct es:

	Nombre	Descripción
	dsmiDir	El valor de la variable de entorno DSMI_DIR.
	dsmiConfig	El archivo dsm.opt que especifica la variable de entorno DSMI_CONFIG.
	serverName	El nombre de la sentencia del servidor IBM Spectrum Protect en el archivo de opciones.
	commMethod	El método de comunicación que fue seleccionado. Consulte #defines para DSM_COMM_* en el archivo dsmapitd.h.
	serverAddress	La dirección del servidor basada en el método de comunicación.
	nodeName	El nombre del nodo del cliente (máquina).
	compression	El valor de la opción de compresión (bTrue=on y bFalse=off).
	compressAlways	El valor de la opción compressalways (bTrue=on y bFalse=off).
	passwordAccess	Valor bTrue para generar y bFalse para solicitud.

### Conceptos relacionados:

Opciones de proceso

## dsmRCMsg

La llamada de función dsmRCMsg obtiene el texto del mensaje asociado con el código de retorno de la API.

El parámetro **msg** muestra el código de retorno del prefijo del mensaje entre paréntesis (), seguido del texto del mensaje. Por ejemplo, una llamada a dsmRCMsg puede devolver lo siguiente:

```
ANS0264E (RC2300) Sólo puede ejecutar el usuario raíz dsmChangePW o dsmDeleteFS.
```

Para algunos idiomas cuyos caracteres son diferentes en ANSI y en páginas de código OEM, es posible que sea necesario convertir cadenas de ANSI a OEM antes de imprimirlas (por ejemplo, en los conjuntos de caracteres de bytes únicos de Europa del este). A continuación se muestra un ejemplo:

```
dsmRCMsg(dsmHandle, rc, msgBuf);
#ifdef WIN32
#endif
CharToOemBuff(msgBuf, msgBuf, strlen(msgBuf));
#endif
printf("
```

## Sintaxis

```
dsInt16_t dsmRCMsg (dsUint32_t dsmHandle,
dsInt16_t dsmRC,
char *msg);
```

## Parámetros

dsUint32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

dsInt16\_t dsmRC (I)

El código de retorno de la API del texto del mensaje asociado. Los códigos de retorno de la API aparecen en una lista en el archivo dsrmc.h. Para obtener más información, consulte el apartado Archivo de origen de códigos de retorno de la API: dsrmc.h.

char \*msg (O)

Este parámetro es el texto del mensaje que está asociado con el código de retorno, dsmRC. El llamador es responsable de asignar espacio suficiente al texto del mensaje.

La longitud máxima para **msg** está definida como DSM\_MAX\_RC\_MSG\_LENGTH.

En plataformas que tienen NLS y la opción de idiomas en archivos de mensaje, la API devuelve una cadena de mensaje en el idioma nacional.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmRCMsg

Código de retorno	Explicación
DSM_RC_NULL_MSG (2002)	El parámetro <b>msg</b> para la llamada dsmRCMsg es un puntero NULO.
DSM_RC_INVALID_RETCODE (2021)	El código de retorno que pasó a la llamada <b>dsmRCMsg</b> no es un código válido.
DSM_RC-NLS_CANT_OPEN_TXT (0610)	No se puede abrir el archivo de texto del mensaje.

## dsmRegisterFS

La llamada de función **dsmRegisterFS** registra un espacio de archivo nuevo con el servidor IBM Spectrum Protect. Registre un espacio de archivo primero antes de realizar ninguna copia de seguridad de éste.

Los clientes de aplicación no deben utilizar los mismos nombres de espacio de archivo que utilizaría un cliente de copia de seguridad/archivado.

- En UNIX o Linux, ejecute el mandato **df** para estos nombres.
- En Windows, estos nombres son por lo general las etiquetas de volumen que están asociadas con las distintas unidad en el sistema.

## Sintaxis

```
dsInt16_t dsmRegisterFS (dsUInt32_t dsmHandle,  
regFSData *regFilespaceP);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

regFSData \*regFilespaceP (I)

Este parámetro pasa el nombre del espacio de archivo y asocia la información que necesita registrar con el servidor IBM Spectrum Protect.

Consejo: El campo *fstype* incluye el prefijo "**API:**". Todas las consultas del espacio de archivo muestran esta cadena. Por ejemplo, si el usuario pasa *myfstype* para *fstype* en **dsmRegisterFS**, se devuelve la cadena de valor real del servidor como *API:myfstype* cuando se realiza una consulta. Este prefijo distingue objetos API de copias de seguridad o archivados de objeto.

El área que se puede utilizar para **fsInfo** es ahora DSM\_MAX\_USER\_FSINFO\_LENGTH.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmRegisterFS

Código de retorno	Explicación
DSM_RC_INVALID_FSNAME (2016)	Nombre de espacio de archivo no válido.
DSM_RC_INVALID_DRIVE_CHAR (2026)	La letra de la unidad no es un carácter alfabético.
DSM_RC_NULL_FSNAME (2027)	Nombre de espacio de archivo nulo.
DSM_RC_FS_ALREADY_REGED (2062)	El espacio de archivo ya está registrado.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_FSINFO_TOOLONG (2106)	La información del espacio de archivo es demasiado larga.

## dsmReleaseBuffer

La función **dsmReleaseBuffer** devuelve un almacenamiento intermedio a IBM Spectrum Protect. La aplicación llama a **dsmReleaseBuffer** después de que se haya llamado a un **dsmGetDataEx** y que la aplicación haya movido todos los datos fuera del almacenamiento intermedio y esté listo para liberarlo. **dsmReleaseBuffer** requiere que **dsmInitEx** se llame con **UseTsmBuffers** configurada en *true* y que se haya proporcionado un valor que no sea cero en *numTsmBuffers*. También se debe invocar **dsmReleaseBuffer** si la aplicación está a punto de invocar **dsmTerminate** y todavía retiene almacenamientos intermedios de datos.

### dsmReleaseBufferSyntax

```
dsInt16_t dsmReleaseBuffer (releaseBufferIn_t *dsmReleaseBufferInP,  
                             releaseBufferOut_t *dsmReleaseBufferOutP) ;
```

### Parámetros

releaseBufferIn\_t \* dsmReleaseBufferInP (I)

Esta estructura contiene los siguientes parámetros de entrada.

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** previa.

dsUInt8\_t tsmBufferHandle(I)

El manejador que identifica este almacenamiento intermedio.

char \*dataPtr(I)

La dirección a la que se graba la aplicación.

### Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmReleaseBuffer

Código de retorno	Explicación
DSM_RC_BAD_CALL_SEQUENCE	La llamada no se ha emitido en el estado adecuado.
DSM_RC_INVALID_TSMBUFFER	El manejador o el valor de <b>dataPtr</b> no son válidos.
DSM_RC_BUFF_ARRAY_ERROR	Se ha producido un error de agrupación de almacenamiento intermedio.

## dsmRenameObj

La llamada de función **dsmRenameObj** renombra el alto y bajo rango del objeto. En copias de seguridad de objetos, pasa el nombre de objeto actual y cambia el nombre de alto rango o el de bajo rango. En objetos archivados, pasa el nombre del espacio de archivo y el ID del objeto y cambia el nombre de alto rango o el de bajo rango. Utilice esta llamada de función dentro de las llamadas **dsmBeginTxn** y **dsmEndTxn**.

El indicador de fusión determina si el nombre de una copia de seguridad de un objeto duplicada se fusiona con las copias de seguridad existentes. Si el nombre nuevo se corresponde con un objeto existente y la fusión ocurre, el objeto actual se transforma con el nombre nuevo y pasa a ser la versión activa del nuevo nombre mientras que el objeto activa que tenía dicho nombre se transforma en la copia más inactiva del objeto. Si el nombre nuevo se corresponde con un objeto existente y no ocurre la fusión, la función devuelve el código de retorno DSM\_RC\_ABORT\_DUPLICATE\_OBJECT.

Restricciones:

- Sólo el propietario del objeto puede cambiar el nombre.
- No se admite la función **dsmRenameObj** si la protección de retención de datos está habilitada en el servidor de IBM Spectrum Protect o si está conectado al servidor de IBM Spectrum Protect para retención de datos.

La llamada de función **dsmRenameObj** prueba estas condiciones de fusión:

- El objeto actual **dsmObjName** y el nuevo objeto de nivel superior o inferior deben coincidir con el propietario, grupo de copia y clase de gestión.
- Debe haberse realizado una copia de seguridad más reciente del **dsmObjName** actual que del objeto activo con el mismo nombre.
- Sólo debe existir una copia activa del **dsmObjName** actual sin copias inactivas.

## Sintaxis

```
dsInt16_t dsmRenameObj (dsmRenameIn_t *dsmRenameInP,  
                        dsmRenameOut_t *dsmRenameOutP);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmRenameIn\_t \*dsmRenameInP

Esta estructura contiene los parámetros de entrada.

dsUInt8\_t repository (I);

Este parámetro indica si el espacio de archivo que se va a eliminar se encuentra en el repositorio de copia de seguridad o en el repositorio de archivado.

dsmObjName \*objNameP (I);

Este parámetro es un puntero a la estructura que contiene el nombre del espacio del archivo, el nombre de nivel superior, el nombre de nivel inferior y el tipo de objeto.

char newHL [DSM\_MAX\_HL\_LENGTH + 1];

Este parámetro especifica el nombre nuevo de nivel superior.

char newLI [DSM\_MAX\_LL\_LENGTH + 1];

Este parámetro especifica el nombre nuevo de nivel inferior.

dsBool\_t merge;

Este parámetro determina si una copia de seguridad se fusiona con objetos nombrados duplicados. Los valores son verdadero o falso.

ObjID;

El ID de objeto de los objetos archivados.

dsmRenameOut\_t \*dsmRnameOutP

Esta estructura contienen los parámetros de salida.

Nota: No hay parámetros de salida.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno de dsmRenameObj

Código de retorno	Explicación
DSM_RC_ABORT_MERGE_ERROR (45)	El servidor ha detectado un error de fusión.
DSM_RC_ABORT_DUPLICATE_OBJECT (32)	El objeto ya existe y la fusión es falsa.
DSM_RC_ABORT_NO_MATCH (2)	No se ha encontrado el objeto.
DSM_RC_REJECT_SERVER_DOWNLEVEL (58)	El servidor IBM Spectrum Protect debe ser de la versión 3.7.4.0 o posterior para que funcione esta función.

## dsmRequestBuffer

La función **dsmRequestBuffer** devuelve un almacenamiento intermedio a IBM Spectrum Protect. La aplicación invoca **dsmRequestBuffer** después de que se haya invocado **dsmGetDataEx** y de que la aplicación haya movido todos los datos fuera del almacenamiento intermedio y esté lista para liberarlo.

**dsmReleaseBuffer** requiere que se haya invocado **dsmInitEx** con la opción *UseTsmBuffers* configurada en *btrue* y que *numTsmBuffers* tenga un valor distinto a cero. También se debe invocar **dsmReleaseBuffer** si la aplicación está a punto de invocar **dsmTerminate** y todavía retiene almacenamientos intermedios de IBM Spectrum Protect.

## Sintaxis

```
dsInt16_t dsmRequestBuffer (getBufferIn_t *getBufferInP,  
                            getBufferOut_t *getBufferOutP,  
                            *dsmRequestBufferInP,  
                            *dsmRequestBufferOutP);
```

## Parámetros

getBufferIn\_t \* dsmRequestBufferInP (I)

Esta estructura contiene los siguientes parámetros de entrada:

dsUInt32\_t dsmHandle

El manejador que identifica la sesión y la asocia con una llamada **dsmInitEx** previa.

getBufferOut\_t \*dsmRequestBufferOut P (0)

Esta estructura contienen los parámetros de salida.

dsUInt8\_t tsmBufferHandle(0)

El manejador que identifica este almacenamiento intermedio.

char \*dataPtr(0)

La dirección a la que se graba la aplicación.

dsUInt32\_t \*bufferLen(0)

Número máximo de bytes que se pueden grabar a este almacenamiento intermedio.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Código de retorno de dsmRequestBuffer

Código de retorno	Explicación
DSM_RC_BAD_CALL_SEQUENCE (33)	La llamada no se ha emitido en el estado adecuado.
DSM_RC_SENDDATA_WITH_ZERO_SIZE (34)	Si el objeto que se está enviando es de longitud 0, no se permiten llamadas a <b>dsmReleaseBuffer</b> .
DSM_RC_BUFF_ARRAY_ERROR (121)	No se ha podido obtener un almacenamiento intermedio válido.

## dsmRetentionEvent

La llamada de función **dsmRetentionEvent** envía una lista de ID de objetos al servidor de IBM Spectrum Protect con una operación de evento de retención para que se realice en estos objetos. Utilice esta llamada de función dentro de las llamadas **dsmBeginTxn** y **dsmEndTxn**.

Nota: El servidor debe ser de la versión 5.2.2.0 o posterior para que funcione esta función.

El número máximo de objetos en una llamada está limitado al valor de *maxObjPerTxn* que se devuelve en la estructura *ApisessInfo* desde una llamada **dsmQuerySessInfo**.

Solo un propietario de un objeto puede enviar un evento en dicho objeto.

Los siguientes eventos son posibles:

eventRetentionActivate

Se pueden emitir sólo en objetos que están vinculados a un evento basado en la clase de gestión. Al enviar este evento se activa el evento para este objeto y el estado de la retención de este objeto cambia de DSM\_ARCH\_RETINIT\_PENDING a DSM\_ARCH\_RETINIT\_STARTED.

eventHoldObj

Este evento emite una retención o una retención de supresión en el objeto, de modo que el objeto no caduque ni se suprima hasta que se libere.

eventReleaseObj

Este evento sólo se puede emitir en un objeto que tiene un valor de DSM\_ARCH\_HELD\_TRUE en el campo *objectHeld* y elimina la retención en el objeto reanudando la política de retención original.

Antes de enviar *dsmRetentionEvent*, envíe la secuencia de la consulta que se describe en Consultas para el sistema IBM Spectrum Protect con el fin de obtener la información del objeto. La llamada a **dsmGetNextQObj** devuelve una estructura de datos llamada **qryRespArchiveData** en consultas de archivado. Esta estructura de datos contiene la información necesaria de **dsmRetentionEvent**.

## Sintaxis

```
extern dsInt16_t DSMLINKAGE dsmRetentionEvent(  
    dsmRetentionEventIn_t          *ddsmRetentionEventInP,  
    dsmRetentionEventOut_t        *dsmRetentionEventOutP  
);
```

## Parámetros



dsmRetentionEventIn\_t \*dsmRetentionEventP

Esta estructura contiene los siguientes parámetros de entrada:

dsUInt16\_t stVersion;

Este parámetro indica la versión de la estructura.

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

dsmEventType\_t eventType (I);

Este parámetro indica el tipo de evento. Consulte el principio de esta sección para obtener información acerca del significado de los valores posibles: **eventRetentionActivate**, **eventHoldObj**, **eventReleaseObj**

dsmObjList\_t objList;

Este parámetro indica una lista de ID de objetos para señalar.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno de dsmRetentionEvent

Código de retorno	Explicación
DSM_RC_ABORT_NODE_NOT_AUTHORIZED (36)	El nodo o usuario no tiene una autorización adecuada.
DSM_RC_ABORT_TXN_LIMIT_EXCEEDED (249)	Hay demasiados objetos en la transacción.
DSM_RC_ABORT_OBJECT_ALREADY_HELD (250)	El objeto ya está retenido, no es posible emitir otra retención.
DSM_RC_REJECT_SERVER_DOWNLEVEL (58)	El servidor debe ser de la V5.2.2.0 o posterior para que funcione esta función.

## dsmSendBufferData

La llamada de función **dsmSendBufferData** envía una corriente de bytes de datos a IBM Spectrum Protect a través de un almacenamiento intermedio proporcionado en una llamada **dsmReleaseBuffer** anterior. El cliente aplicación puede pasar cualquier tipo de datos para que se almacenen en el servidor. Normalmente estos datos son datos de archivos, pero no necesariamente. Puede llamar a **dsmSendBufferData** varias veces, si la corriente de bytes de datos que está enviando es demasiado larga. Independientemente de si la llamada falla o se procesa correctamente, se libera el almacenamiento intermedio.

Restricción: Al utilizar la opción *useTsmBuffers*, aunque se incluya un objeto para compresión, el objeto no se comprime.

## Sintaxis

```
dsInt16_t dsmSendBufferData (sendBufferDataIn_t *dsmSendBufferDataExInP,  
                             sendBufferDataOut_t *dsmSendBufferDataOutP) ;
```

## Parámetros

sendBufferDataIn\_t \* dsmSendBufferDataInP (I)

Esta estructura contiene los siguientes parámetros de entrada.

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsUInt8\_t tsmBufferHandle(I)

El manejador que identifica el almacenamiento intermedio que se va a enviar.

char \*dataPtr(I)

La dirección en la que se graban los datos de la aplicación.

dsUInt32\_t numBytes(I)

El número real de bytes grabados por la aplicación (siempre debe ser menos que el valor proporcionando en **dsmReleaseBuffer**).

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmSendBufferData

Código de retorno	Explicación
-------------------	-------------

Código de retorno	Explicación
DSM_RC_BAD_CALL_SEQUENCE (2041)	La llamada no se ha emitido en el estado adecuado.
DSM_RC_INVALID_TSMBUFFER (2042)	El manejador o el valor de <b>dataPtr</b> no son válidos.
DSM_RC_BUFF_ARRAY_ERROR (2045)	Se ha producido un error de agrupación de almacenamiento intermedio.
DSM_RC_TOO_MANY_BYTES (2043)	El valor de <i>numBytes</i> es mayor que el tamaño del almacenamiento intermedio proporcionado en la llamada <b>dsmReleaseBuffer</b> .

## dsmSendData

La llamada de función **dsmSendData** envía una corriente de bytes de datos a IBM Spectrum Protect a través de un almacenamiento intermedio. El cliente aplicación puede pasar cualquier tipo de datos para que se almacenen en el servidor. Normalmente estos datos son datos de archivos, pero no necesariamente. Puede llamar a **dsmSendData** varias veces, si la corriente de bytes de datos que desea enviar es demasiado larga.

Restricción: El cliente de la aplicación no puede volver a utilizar el almacenamiento intermedio especificado en **dsmSendData** hasta que la llamada **dsmSendData** devuelva los datos.

Consejo: Si IBM Spectrum Protect devuelve el código 157 (DSM\_RC\_WILL\_ABORT), inicie una llamada a **dsmEndSendObj** y a continuación a **dsmEndTxn** con un voto de DSM\_VOTE\_COMMIT. La aplicación recibe entonces el código de retorno 2302 (DSM\_RC\_CHECK\_REASON\_CODE) y vuelve a pasarlo al usuario de la aplicación. Esto informa al usuario acerca del motivo por el que el servidor está finalizando la transacción.

## Sintaxis

```
dsInt16_t dsmSendData (dsUInt32_t dsmHandle,
    DataBlk *dataBlkPtr);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

DataBlk \*dataBlkPtr (I/O)

Este parámetro apunta a una estructura que incluye tanto un puntero al almacenamiento intermedio al que se le van a enviar los datos como el tamaño del almacenamiento intermedio. Cuando se devuelven los datos, esta estructura contiene el número de bytes que se han transferido. Consulte Archivos de origen de definiciones de tipo de API para obtener más información sobre la definición del tipo.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmSendData

Código de retorno	Explicación
DSM_RC_NO_COMPRESS_MEMORY (154)	No hay memoria suficiente disponible para llevar a cabo una compresión o expansión de datos.
DSM_RC_COMPRESS_GREW (155)	Durante la compresión los datos comprimidos crecen en tamaño comparados con los datos originales.
DSM_RC_WILL_ABORT (157)	Ha ocurrido un error desconocido e inesperado, y la transacción se ha detenido.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API de la aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_NEEDTO_ENDTXN (2070)	Necesita finalizar la transacción.
DSM_RC_OBJ_EXCLUDED (2080)	La lista de inclusión/exclusión excluye al objeto.
DSM_RC_OBJ_NOBCG (2081)	El objeto no tiene un grupo de copia de seguridad y no se enviará al servidor.
DSM_RC_OBJ_NOACG (2082)	El objeto no tiene un grupo de archivado y no se enviará al servidor.
DSM_RC_SENDDATA_WITH_ZERO_SIZE (2107)	El objeto no puede enviar datos con un valor <i>sizeEstimate</i> de cero bytes.

## dsmSendObj

La llamada de función **dsmSendObj** inicia una solicitud para enviar un único objeto al almacenamiento. Se pueden realizar varias llamadas **dsmSendObj** y llamadas asociadas **dsmSendData** dentro de los límites de una transacción por motivos de rendimiento.

La llamada **dsmSendObj** procesa los datos del objeto como una corriente de datos de bytes en buffers de memoria. El parámetro **dataBlkPtr** en la llamada **dsmSendObj** permite al cliente de la aplicación:

- Pasar los datos y los atributos (los atributos se pasan a través de **objAttrPtr**) del objeto en una única llamada.
- Especificar parte de los datos del objeto a través de la llamada **dsmSendObj** y el resto de los datos a través de una o más llamadas **dsmSendData**.

Como alternativa, el cliente de la aplicación puede especificar sólo los atributos a través de la llamada **dsmSendObj** y especificar los datos del objeto a través de una o más llamadas a **dsmSendData**. Para este método, configure **dataBlkPtr** en NULO en la llamada **dsmSendObj**.

Consejo: En determinados tipos de objetos, es posible que los datos de la corriente de bytes no se asocien con los datos; por ejemplo, una entrada de directorio sin atributos ampliados.

Antes de llamar a **dsmSendObj**, se debe realiza una llamada **dsmBindMC** previa con el fin de vincular adecuadamente una clase de gestión con el objeto que desea archivar o realizar una copia de seguridad. La API mantiene esta vinculación para que pueda asociar a la clase de gestión adecuada con el objeto cuando se envía al servidor. Si permite que la clase de gestión vinculada a una llamada **dsmSendObj** sea un tipo de objeto del directorio (DSM\_OBJ\_DIRECTORY), es posible que la clase predeterminada no sea la clase de gestión. En su lugar, se utiliza la clase de gestión con mayor tiempo de retención. Si existe más de una clase de gestión con este tiempo de retención, se utiliza la primera que se encuentra.

Siga todos los datos de objeto que se envían al almacenamiento con una llamada **dsmEndSendObj**. Si no tiene datos de objeto para enviar al servidor, o todos los datos se encontraban dentro de la llamada **dsmSendObj**, inicie una llamada **dsmEndSendObj** antes de iniciar otra llamada **dsmSendObj**. Si se requieran varios envíos de datos a través de la llamada **dsmSendData**, **dsmEndSendObj** sigue el último envío para indicar el cambio de estado.

Consejo: Si IBM Spectrum Protect devuelve el código 157 (DSM\_RC\_WILL\_ABORT), inicie una llamada a **dsmEndTxn** con un voto de DSM\_VOTE\_COMMIT. La aplicación recibe el código de retorno 2302 (DSM\_RC\_CHECK\_REASON\_CODE) y se lo vuelve a pasar al usuario de la aplicación. Esto informa al usuario por qué el servidor está terminando la transacción.

Si el código de retorno es 11 (DSM\_RS\_ABORT\_NO\_REPOSIT\_SPACE), es posible que *sizeEstimate* sea demasiado pequeño para la cantidad real de datos. La aplicación necesita determinar un *sizeEstimate* más preciso y volver a enviar los datos.

## Sintaxis

```
dsInt16_t dsmSendObj (dsUInt32_t      dsmHandle,
                    dsmSendType sendType,
                    void          *sendBuff,
                    dsmObjName   *objNameP,
                    ObjAttr     *objAttrPtr,
                    DataBlk     *dataBlkPtr);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmSendType sendType (I)

Este parámetro especifica el tipo de envío que se está realizando. Dentro de los valores posibles se incluyen los siguientes:

Nombre	Descripción
<b>stBackup</b>	Un objeto de copia de seguridad que se envía al servidor.
<b>stArchive</b>	Una objeto de copia archivada que se envía al servidor.
<b>stBackupMountWait</b>	Un objeto de copia de seguridad al que desea que espere el servidor antes de montar el dispositivo necesario, tal como una cinta.
<b>stArchiveMountWait</b>	Una copia de un objeto archivado para el que desea que el servidor espere hasta que el dispositivo necesario, como una cinta, se monte.

Nota: Utilice los tipos **MountWait** si existe alguna posibilidad de que el usuario de la aplicación envíe datos a una cinta.

void \*sendBuff (I)

Este parámetro es un puntero a la estructura que contiene otra información específica a **sendType** en la llamada. Actualmente, sólo un **sendType** de **stArchive** tiene una estructura asociada. Esta estructura se denomina **sndArchiveData** y contiene la

descripción de la copia archivada.

dsmObjName \*objNameP (I)

Este parámetro es un puntero a la estructura que contiene el nombre del espacio del archivo, el nombre de alto y bajo rango y el tipo de objeto. Para obtener más información, consulte el apartado ID y nombres de objeto.

ObjAttr \*objAttrPtr (I)

Este parámetro pasa atributos de objeto de interés a la aplicación. Consulte Archivos de origen de definiciones de tipo de API para obtener más información sobre la definición del tipo.

Los atributos son:

- **owner** se refiere al propietario del objeto. Determinar si el propietario se declara ser un nombre específico o una cadena vacía es importante cuando se obtiene el objeto de vuelta del almacenamiento IBM Spectrum Protect. Para obtener más información, consulte el apartado Acceder a objetos como propietario de sesión.
- **sizeEstimate** es la mejor estimación total del tamaño de los objetos de los datos que se envían al servidor. Es importante que intente ser lo más preciso posible en la estimación de tamaño, porque el servidor utiliza este atributo para optimizar la asignación del espacio y la colocación del objeto dentro de sus recursos de almacenamiento. Si el tamaño estimado que se ha especificado es considerablemente más pequeño que el número real de bytes que se están enviando, es posible que el servidor tenga dificultades para asignar espacio suficiente y finalice la transacción con un código de motivo 11 (DSM\_RS\_ABORT\_NO\_REPOSIT\_SPACE).  
Nota: la estimación de tamaño es del tamaño total del objeto de datos en bytes.

Los objetos con un tamaño más pequeño que DSM\_MIN\_COMPRESS\_SIZE no se comprimen.

Si el objeto no tiene datos de bit (sólo la información de atributo de esta llamada), el **sizeEstimate** debe ser cero.

Nota: Comenzando con la versión 5.1.0, el destino de la copia dentro de una transacción no se comprueba la coherencia en objetos de longitud cero.

- **objCompressed** es un valor booleano que indica si los datos del objeto ya han sido comprimidos o no.

Si el objeto está comprimido (objeto *compressed=bTrue*), IBM Spectrum Protect no intente comprimirlo de nuevo. Si no está comprimido, IBM Spectrum Protect decide si comprimir el objeto, en función del valor de la opción *compression* establecida por el administrador y establecida en los orígenes de configuración de API.

Si la aplicación va a utilizar restauraciones o recuperaciones parciales de objetos, no es posible comprimir los datos mientras los envía. Para implementar esto, configure *ObjAttr.objCompressed* en *bTrue*.

- **objInfo** guarda información acerca del objeto en concreto.  
Restricción: La información no se almacena aquí automáticamente. Cuando se utiliza este atributo, debe establecer el atributo *objInfoLength*, para mostrar la longitud de *objInfo*.
- **mcNameP** contiene el nombre de la clase de gestión que ignora la clase de gestión que se obtiene de **dsmBindMC**.
- **disableDeduplication** es un valor booleano. Cuando se establece en true (verdadero) el cliente no elimina los duplicados de este objeto.

DataBlk \*dataBlkPtr (I/O)

Este parámetro apunta a una estructura que incluye tanto un puntero al almacenamiento intermedio de datos que se van a archivar o realizar una copia de seguridad como el tamaño de dicho almacenamiento intermedio. Este parámetro se aplica únicamente a **dsmSendObj**. Si desea empezar a enviar datos a una llamada **dsmSendData** subsiguiente, en lugar de en la llamada **dsmSendObj**, configure el puntero del almacenamiento intermedio en la estructura DataBlk en NULO. Cuando se devuelven los datos, esta estructura contiene el número de bytes que se han transferido. Consulte Archivos de origen de definiciones de tipo de API para obtener más información sobre la definición del tipo.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmSendObj

Código de retorno	Explicación
DSM_RC_NO_COMPRESS_MEMORY (154)	No hay memoria suficiente disponible para llevar a cabo una compresión o expansión de datos.
DSM_RC_COMPRESS_GREW (155)	Durante la compresión los datos comprimidos crecen en tamaño comparados con los datos originales.
DSM_RC_WILL_ABORT (157)	Ha ocurrido un error desconocido e inesperado, y la transacción se ha detenido.
DSM_RC_TL_NOACG (186)	La clase de gestión para este archivo no cuenta con un grupo de copia válido para el tipo de envío.

Código de retorno	Explicación
DSM_RC_NULL_OBJNAME (2000)	Nombre de objeto nulo.
DSM_RC_NULL_OBJATTRPTR (2004)	Puntero de atributo de objeto nulo.
DSM_RC_INVALID_OBJTYPE (2010)	Tipo de objeto no válido.
DSM_RC_INVALID_OBJOWNER (2019)	Propietario de objeto no válido.
DSM_RC_INVALID_SENDDTYPE (2022)	Tipo de envío no válido.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	Los caracteres comodín no están permitidos.
DSM_RC_FS_NOT_REGISTERED (2061)	El espacio de archivo no está registrado.
DSM_RC_WRONG_VERSION_PARM (2065)	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_NEEDTO_ENDTXN (2070)	Necesita finalizar la transacción.
DSM_RC_OBJ_EXCLUDED (2080)	La lista de inclusión/exclusión excluye al objeto.
DSM_RC_OBJ_NOBCG (2081)	El objeto no tiene un grupo de copia de seguridad y no se enviará al servidor.
DSM_RC_OBJ_NOACG (2082)	El objeto no tiene un grupo de archivado y no se enviará al servidor.
DSM_RC_DESC_TOOLONG (2100)	La descripción es demasiado larga.
DSM_RC_OBJINFO_TOOLONG (2101)	La información del objeto es demasiado larga.
DSM_RC_HL_TOOLONG (2102)	El calificador de alto rango es demasiado largo.
DSM_RC_FILESPACE_TOOLONG (2104)	El nombre del espacio de archivo es demasiado largo.
DSM_RC_LL_TOOLONG (2105)	El calificador de bajo rango es demasiado largo.
DSM_RC_NEEDTO_CALL_BINDMC (2301)	debe llamarse primero a <b>dsmBindMC</b> .

## dsmSetAccess

La llamada de función **dsmSetAccess** da a otros usuarios o nodos acceso a versiones de copia de seguridad o copias archivadas de los objetos, acceso a todos los objetos o acceso a un grupo determinado. Cuando se otorga acceso a otro usuario, dicho usuario puede consultar, restaurar o recuperar los archivos. Este mandato soporta comodines en los siguientes campos: *fs*, *hl*, *ll*, *nodo*, *propietario*.

Nota: No puede conceder acceso a copias de seguridad y copias archivadas con un único mandato. Debe especificar copia de seguridad o archivado.

## Sintaxis

```
dsInt16_t DSMLINKAGE dsmSetAccess
    (dsUInt32_t      dsmHandle,
     dsmSetAccessType  accessType,
     dsmObjName      *objNameP,
     char            *node,
     char            *owner);
```

## Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmAccessType accessType (I)

Este parámetro especifica el tipo de objeto para el que desea dar acceso. Dentro de los valores posibles se incluyen los siguientes:

Nombre	Descripción
<i>atBackup</i>	Especifica que el acceso se configura para copias de seguridad de objetos.
<i>atArchive</i>	Especifica que el acceso se configura para objetos archivados.

dsmObjName \*objNameP (I)

Este parámetro es un puntero a la estructura que contiene el nombre de espacio de archivo, y el nombre de alto y bajo rango del objeto.

Nota: Con el fin de especificar todos los espacios del archivo, utilice un asterisco (\*) en el nombre del espacio del archivo.  
char \*node (I)

Este parámetro es un puntero al nombre del nodo al que se le concede acceso. Para cualquier nodo, especifique un asterisco (\*).  
char \*owner (I)

Este parámetro es un puntero al nombre de usuario en el nodo al que se le concede acceso. Para todos los usuarios, especifique un asterisco (\*).

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ( ).

Tabla 1. Códigos de retorno para dsmSetAccess

Código de retorno	Explicación
DSM_RC_INVALID_ACCESS_TYPE (2110)	Tipo de acceso especificado no válido.
DSM_RC_FILE_SPACE_NOT_FOUND (124)	No se ha encontrado el espacio de archivo especificado en el servidor.
DSM_RC_QUERY_COMM_FAILURE (2111)	Error de comunicación durante la consulta del servidor.
DSM_RC_NO_FILES_BACKUP (2112)	No se realizaron copias de seguridad en este espacio de archivo.
DSM_RC_NO_FILES_ARCHIVE (2113)	No se realizaron archivaciones en este espacio de archivo.
DSM_RC_INVALID_SETACCESS (2114)	Formulación de acceso no válida.

## dsmSetUp

La llamada de función **dsmSetUp** sobrescribe los valores de la variable del entorno. Llame a **dsmSetUp** antes de a **dsmInitEx**. Los valores que se pasan en la estructura **envSetUp** sobrescriben las variables de entorno existentes o predeterminadas. Si especifica NULL en un campo, los valores se toman del entorno. Si no configura un valor, se toman los valores predeterminados.

Requisitos:

1. Si utiliza **dsmSetUp**, siempre llamea **dsmTerminate** antes de **dsmCleanUp**.
2. La instrumentación de la API solo se puede activar si se ha establecido el distintivo de prueba INSTRUMENT: API en el archivo de configuración y se utilizan las llamadas **dsmSetUp** o **dsmCleanUp** en la aplicación.

## Sintaxis

```
dsInt16_t DSMLINKAGE dsmSetUp  
    (dsBool_t      mtFlag,  
     envSetUp     *envSetUpP);
```

## Parámetros

dsBool\_t mtFlag (I)

Este parámetro especifica si la API se utilizará en una hebra única o en un modo de varias hebras. Los valores incluyen:

```
DSM_SINGLETHREAD  
DSM_MULTITHREAD
```

Requisito: El indicador de varias hebras debe estar activado para que se lleve a cabo una transferencia de datos sin LAN.

envSetUp \*envSetUpP(I)

Este parámetro es un puntero a la estructura que retiene los valores de sobrescritura. Especifique NULO si no quiere modificar las variables de entorno existentes. Los campos en la estructura **envSetUp** incluyen:

	Nombre	Descripción
	<b>dsmiDir</b>	Una ruta de directorio calificada al completo que contiene un archivo de mensaje en UNIX o Linux. También especifica los directorios dsm.sys.
	<b>dsmiConfig</b>	El nombre completo del archivo de opciones del cliente.
	<b>dsmiLog</b>	La ruta completa del directorio del registro de errores.

	Nombre	Descripción
	<b>argv</b>	Pase el nombre de argv[0] del programa de llamada si la aplicación debe ejecutarse con autoridad de usuario autorizado. Para obtener más información, consulte el apartado Control del acceso a los archivos de contraseñas.
	<b>logName</b>	El nombre del archivo de un registro de error si la aplicación no utiliza dserror.log.
	<b>inclExclCaseSensitive</b>	Indica si las normas de inclusión/exclusión distinguen o no entre mayúsculas y minúsculas. Este parámetro se puede utilizar únicamente en Windows, se ignora en otros sistemas.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ().

Tabla 1. Códigos de retorno para dsmSetUp

Código de retorno	Explicación
DSM_RC_ACCESS_DENIED (106)	Se ha negado el acceso al archivo o directorio especificado.
DSM_RC_INVALID_OPT (0400)	Se ha encontrado una opción no válida.
DSM_RC_NO_HOST_ADDR (0405)	La TCPSERVERADDRESS de este servidor no está definida en la sección de nombre de servidor del archivo de opciones del sistema.
DSM_RC_NO_OPT_FILE (0406)	No se ha podido encontrar el archivo de opciones especificado por el nombre de archivo.
DSM_RC_MACHINE_SAME (0408)	El NODENAME definido en el archivo de opciones no puede ser el mismo que el del sistema <i>HostName</i> .
DSM_RC_INVALID_SERVER (0409)	El archivo de opciones del sistema no contiene la opción SERVERNAME.
DSM_RC_INVALID_KEYWORD (0410)	Se ha encontrado una palabra clave de opción no válida en el archivo de configuración <b>dsmInitEx</b> , la cadena de opción, dsm.sys o dsm.opt.
DSM_RC_PATTERN_TOO_COMPLEX (0411)	El patrón de inclusión o exclusión emitido es demasiado complicado para que IBM Spectrum Protect lo interprete de forma precisa.
DSM_RC_NO_CLOSING_BRACKET (0412)	El patrón de inclusión o exclusión no está construido correctamente. Falta el paréntesis de cierre.
DSM_RC-NLS_CANT_OPEN_TXT (0610)	El sistema no puede abrir el archivo de texto del mensaje.
DSM_RC-NLS_INVALID_CNTL_REC (0612)	El sistema no es capaz de utilizar el archivo de texto del mensaje.
DSM_RC_NOT_ADSM_AUTHORIZED (0927)	Debe ser el usuario autorizado para tener multihebra y generar <i>passwordaccess</i> .
DSM_RC_NO_INCLEXCL_FILE (2229)	No se ha encontrado el archivo de inclusión/exclusión.
DSM_RC_NO_SYS_OR_INCLEXCL (2230)	No se ha encontrado el dsm.sys o el archivo de inclusión/exclusión.

## dsmTerminate

La llamada de función **dsmTerminate** finaliza una sesión con el servidor IBM Spectrum Protect y limpia el entorno IBM Spectrum Protect.

### Sintaxis

No existen códigos de retorno específicos para esta llamada.

```
dsInt16_t dsmTerminate (dsUInt32_t dsmHandle);
```

### Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

## dsmUpdateFS

La llamada a función dsmUpdateFS actualiza un espacio de archivos en el almacenamiento IBM Spectrum Protect. Esta actualización garantiza que el administrador tenga un registro actualizado de su espacio de archivos.

### Sintaxis

```
dsInt16_t dsmUpdateFS (dsUInt32_t dsmHandle,  
char *fs,  
dsmFSUpd *fsUpdP,  
dsUInt32_t fsUpdAct);
```

### Parámetros

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada dsmInitEx anterior.

char \*fs (I)

Este parámetro es un puntero al nombre del espacio de archivo.

dsmFSUpd \*fsUpdP (I)

Este parámetro es un puntero a la estructura que tiene los campos correctos para la actualización que desea. Complete únicamente aquellos campos que necesitan actualización.

dsUInt32\_t fsUpdAct (I)

Un mapa de 2 bytes que indica cuál de los campos actualizar. Las máscaras de bits tienen los siguientes valores:

- DSM\_FSUPD\_FSTYPE
- DSM\_FSUPD\_FSINFO  
Consejo: Para Windows, el valor de la letra de la unidad de dsmDOSAttrib también se actualiza cuando se selecciona FSINFO.
- DSM\_FSUPD\_OCCUPANCY
- DSM\_FSUPD\_CAPACITY
- DSM\_FSUPD\_BACKSTARTDATE
- DSM\_FSUPD\_BACKCOMPLETEDATE

Para obtener una descripción de estas máscaras de bits, consulte las definiciones de DSM\_FSUPD en el tema siguiente: Archivos de origen de definiciones de tipo de API.

### Códigos de retorno

La tabla siguiente lista los códigos de retorno para la llamada a función dsmUpdateFS.

Tabla 1. Los códigos de retorno de dsmUpdateFS

Código de retorno	Número de código de retorno	Descripción
DSM_RC_FS_NOT_REGISTERED	2061	El nombre del espacio de archivos no está registrado.
DSM_RC_WRONG_VERSION_PARM	2065	La versión de la API del cliente de aplicación es distinta de la versión de la biblioteca de IBM Spectrum Protect.
DSM_RC_FSINFO_TOOLONG	2106	La información del espacio de archivo es demasiado larga.

## dsmUpdateObj

La llamada de función **dsmUpdateObj** actualiza la metainformación asociada con un objeto archivado o copia de seguridad activos que ya está en el servidor. Los datos de bit de la aplicación no se ven afectados. Para actualizar un objeto, debe asignar un nombre específico sin comodines. Para actualizar un objeto archivado, configure **dsmSendType** en **stArchive**. Solo se actualiza el último objeto archivado nombrado.

Sólo puede iniciar la llamada **dsmUpdateObj** en el estado de la sesión; no se puede llamar dentro de una transacción porque realiza su propia transacción. Además, solo se puede actualizar un objeto cada vez.

Restricción: En un sistema operativo UNIX o Linux, si cambia el campo de propietario no puede consultar o restaurar al objeto a no ser que sea el usuario root.



## Sintaxis

```
dsInt16_t dsmUpdateObj
(dsUInt32_t dsmHandle,
 dsmSendType sendType,
 void *sendBuff,
 dsmObjName *objNameP,
 ObjAttr *objAttrPtr, /* objInfo */
 dsUInt16_t objUpdAct); /* action bit vector */
```

## Parámetros

Las descripciones del campo son las mismas que aquellas en **dsmSendObj**, con las siguientes excepciones:

dsmObjName \*objNameP (I)

No puede utilizar un comodín.

ObjAttr \*objAttrPtr (I)

El campo **objCompressed** se ignora para esta llamada.

Otras diferencias son:

- **propietario**. Si especifica un campo **propietario** nuevo, el propietario cambia.
- **sizeEstimate**. Si especifica un valor que no es cero debe ser la cantidad real de datos enviados en bytes. El valor se almacena en los metadatos de IBM Spectrum Protect para su futuro uso.
- **objInfo**. Este atributo contiene la información nueva que se debe colocar en el campo **objInfo**. Configure **objInfoLength** con la longitud del nuevo **objInfo**.

dsUInt16\_t objUpdAct

Las máscaras de bit y las acciones posibles de **objUpdAct** son:

DSM\_BACKUPD\_MC

Actualiza la clase de gestión del objeto.

DSM\_BACKUPD\_OBJINFO

Actualiza **objInfo**, **objInfoLength** y **sizeEstimate**.

DSM\_BACKUPD\_OWNER

Actualiza al propietario del objeto.

DSM\_ARCHUPD\_DESCR

Actualiza el campo **Descripción**. Introduzca el valor de la descripción nueva a través del parámetro **SendBuff**. Consulte el programa de ejemplo para su uso adecuado.

DSM\_ARCHUPD\_OBJINFO

Actualiza **objInfo**, **objInfoLength** y **sizeEstimate**.

DSM\_ARCHUPD\_OWNER

Actualiza al propietario del objeto.

## Códigos de retorno

Los números de código de retorno se proporcionan entre paréntesis ).

Tabla 1. Códigos de retorno para dsmUpdateObj

Código de retorno	Explicación
DSM_RC_INVALID_ACTION (2232)	Acción no válida.
DSM_RC_FS_NOT_REGISTERED (2061)	El espacio de archivo no está registrado.
DSM_RC_BAD_CALL_SEQUENCE (2041)	La secuencia de llamadas no es válida.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	No están permitidos los caracteres comodín.
DSM_RC_ABORT_NO_MATCH (2)	La consulta anterior no coincide.

## dsmUpdateObjEx

La llamada de función **dsmUpdateObjEx** actualiza la meta información que está asociada con los objetos de archivado o las copias de seguridad en el servidor. Los datos de bit de la aplicación no se ven afectados. Para actualizar un objeto, debe asignar un nombre sin comodines o bien especificar el ID del objeto con el fin de actualizar un objeto archivado específico. No se pueden utilizar caracteres comodín cuando se especifica el nombre. Para actualizar un objeto al que se le ha realizado una copia de seguridad, configure el parámetro **dsmSendType** en **stBackup**. Para actualizar un objeto archivado, configure el parámetro **dsmSendType** en **stArchive**.

Sólo puede iniciar la llamada **dsmUpdateObjEx** en el estado de la sesión; no se puede llamar dentro de una transacción porque realiza su propia transacción. Los objetos sólo se pueden actualizar de uno en uno.

Restricción: En un sistema operativo UNIX o Linux, si cambia el campo del propietario no puede consultar o restaurar al objeto a no ser que sea el usuario root. Sólo se puede actualizar la versión activa actual de una copia de seguridad.

## Sintaxis

---

```
dsInt16_t dsmUpdateObjEx  
(dsmUpdateObjExIn_t *dsmUpdateObjExInP,  
 dsmUpdateObjExOut_t *dsmUpdateObjExOutP);
```

## Parámetros

---

dsmUpdateObjExIn\_t \*dsmUpdateObjExInP

Esta estructura contiene los siguientes parámetros de entrada:

dsUInt16\_t stVersion (I)

La versión actual de la estructura que se utiliza.

dsUInt32\_t dsmHandle (I)

El manejador que asocia esta llamada con una llamada **dsmInitEx** anterior.

dsmSendType sendType (I)

El tipo de envío que se está realizando. El valor puede ser:

stBackup

Un objeto de copia de seguridad que se envía al servidor.

stArchive

Una objeto de copia archivada que se envía al servidor.

dsmObjName \*objNameP (I)

Un puntero a la estructura que contiene el nombre del espacio del archivo, el nombre de alto y bajo rango y el tipo de objeto. No puede utilizar un comodín.

ObjAttr \*objAttrPtr (I)

Pasa atributos de objeto a la aplicación. Los valores que se actualizan dependen del indicador en el campo **objUpdAct**. El atributo **objCompressed** se omite en esta llamada.

Los atributos son:

- **owner** cambia el propietario si se especifica un nombre nuevo.
- **sizeEstimate** es la cantidad de datos real que se envía en bytes. El valor se almacena en los metadatos de IBM Spectrum Protect para uso futuro.
- **objCompressed** es un valor booleano que indica si los datos del objeto ya han sido comprimidos o no.
- **objInfo** es un atributo que contiene la información nueva colocada en el campo **objInfo**. Configure **objInfoLength** con la longitud del nuevo **objInfo**.
- **mcNameP** contiene el nombre de la clase de gestión que ignora la clase de gestión que se obtiene de **dsmBindMC**.

dsUInt32\_t objUpdAct

Especifica las máscaras de bit y las acciones de **objUpdAct** son:

DSM\_BACKUPD\_MC

Actualiza la clase de gestión del objeto.

DSM\_BACKUPD\_OBJINFO

Actualiza el objeto de información (**objInfo**), la longitud del objeto de información (**objInfoLength**), y la cantidad de datos que se envían (**sizeEstimate**) en la copia de seguridad del objeto.

DSM\_BACKUPD\_OWNER

Actualiza al propietario de la copia de seguridad del objeto.

DSM\_ARCHUPD\_DESCR

Actualiza el campo **Description** del objeto archivado. Introduzca el valor de la descripción nueva a través del parámetro **sendBuff**.

DSM\_ARCHUPD\_OBJINFO

Actualiza el objeto de la información (**objInfo**), la longitud del objeto de información (**objInfoLength**), y la cantidad de datos que se envían (**sizeEstimate**) en el objeto archivado.

DSM\_ARCHUPD\_OWNER

Actualiza el propietario del objeto archivado.

ObjID archObjId

Especifica el ID del objeto único de un objeto archivado determinado. Debido a que varios objetos archivados pueden tener el mismo nombre, este parámetro identifica uno en concreto. Es posible obtener el ID del objeto utilizando una llamada de consulta de archivado.

dsmUpdateObjExOut\_t \*dsmUpdateObjExOutP

Esta estructura contiene los parámetros de salida:

dsUint16\_t stVersion (I)

La versión actual de la estructura que se utiliza.

## Códigos de retorno

Los números del código de retorno se proporcionan entre paréntesis ( ) en la siguiente tabla.

Tabla 1. Códigos de retorno de dsmUpdateObjEx

Código de retorno	Explicación
DSM_RC_INVALID_ACTION (2012)	Acción no válida.
DSM_RC_FS_NOT_REGISTERED (2061)	El espacio de archivo no está registrado.
DSM_RC_BAD_CALL_SEQUENCE (2041)	La secuencia de llamadas no es válida.
DSM_RC_WILDCHAR_NOTALLOWED (2050)	No están permitidos los caracteres comodín.
DSM_RC_ABORT_NO_MATCH (2)	La consulta anterior no coincide.

## Archivo de origen de códigos de retorno de la API: dsmrc.h

El archivo de cabecera dsmrc.h contiene todos los códigos de retorno que la API puede devolver a una aplicación.

La información que se proporciona aquí ofrece una copia de puntual del archivo dsmrc.h que se distribuye con la API. Vea el archivo en el paquete de distribución de la API para la última versión.

```

/*****
* Tivoli Storage Manager
* API Client Component
*
* (C) Copyright IBM Corporation 1993,2010
*****/

/*****/
/* Header File Name: dsmrc.h */
/*
/* Descriptive-name: Return codes from Tivoli Storage Manager APIs */
/*****/
#ifndef _H_DSMRC
#define _H_DSMRC

#ifndef DSMAPILIB

#ifndef _H_ANSMACH
typedef int RetCode ;
#endif

#endif

#define DSM_RC_SUCCESSFUL 0 /* successful completion */
#define DSM_RC_OK 0 /* successful completion */

#define DSM_RC_UNSUCCESSFUL -1 /* unsuccessful completion */

/* dsmEndTxn reason code */
#define DSM_RS_ABORT_SYSTEM_ERROR 1
#define DSM_RS_ABORT_NO_MATCH 2
#define DSM_RS_ABORT_BY_CLIENT 3
#define DSM_RS_ABORT_ACTIVE_NOT_FOUND 4
#define DSM_RS_ABORT_NO_DATA 5
#define DSM_RS_ABORT_BAD_VERIFIER 6
#define DSM_RS_ABORT_NODE_IN_USE 7
#define DSM_RS_ABORT_EXPDATE_TOO_LOW 8

```

```

#define DSM_RS_ABORT_DATA_OFFLINE 9
#define DSM_RS_ABORT_EXCLUDED_BY_SIZE 10
#define DSM_RS_ABORT_NO_STO_SPACE_SKIP 11
#define DSM_RS_ABORT_NO_REPOSIT_SPACE DSM_RS_ABORT_NO_STO_SPACE_SKIP
#define DSM_RS_ABORT_MOUNT_NOT_POSSIBLE 12
#define DSM_RS_ABORT_SIZEESTIMATE_EXCEED 13
#define DSM_RS_ABORT_DATA_UNAVAILABLE 14
#define DSM_RS_ABORT_RETRY 15
#define DSM_RS_ABORT_NO_LOG_SPACE 16
#define DSM_RS_ABORT_NO_DB_SPACE 17
#define DSM_RS_ABORT_NO_MEMORY 18

#define DSM_RS_ABORT_FS_NOT_DEFINED 20
#define DSM_RS_ABORT_NODE_ALREADY_DEFED 21
#define DSM_RS_ABORT_NO_DEFAULT_DOMAIN 22
#define DSM_RS_ABORT_INVALID_NODENAME 23
#define DSM_RS_ABORT_INVALID_POL_BIND 24
#define DSM_RS_ABORT_DEST_NOT_DEFINED 25
#define DSM_RS_ABORT_WAIT_FOR_SPACE 26
#define DSM_RS_ABORT_NOT_AUTHORIZED 27
#define DSM_RS_ABORT_RULE_ALREADY_DEFED 28
#define DSM_RS_ABORT_NO_STOR_SPACE_STOP 29

#define DSM_RS_ABORT_LICENSE_VIOLATION 30
#define DSM_RS_ABORT_EXTOBJID_ALREADY_EXISTS 31
#define DSM_RS_ABORT_DUPLICATE_OBJECT 32

#define DSM_RS_ABORT_INVALID_OFFSET 33 /* Partial Object Retrieve */
#define DSM_RS_ABORT_INVALID_LENGTH 34 /* Partial Object Retrieve */
#define DSM_RS_ABORT_STRING_ERROR 35
#define DSM_RS_ABORT_NODE_NOT_AUTHORIZED 36
#define DSM_RS_ABORT_RESTART_NOT_POSSIBLE 37
#define DSM_RS_ABORT_RESTORE_IN_PROGRESS 38
#define DSM_RS_ABORT_SYNTAX_ERROR 39

#define DSM_RS_ABORT_DATA_SKIPPED 40
#define DSM_RS_ABORT_EXCEED_MAX_MP 41
#define DSM_RS_ABORT_NO_OBJSET_MATCH 42
#define DSM_RS_ABORT_PVR_ERROR 43
#define DSM_RS_ABORT_BAD_RECOGTOKEN 44
#define DSM_RS_ABORT_MERGE_ERROR 45
#define DSM_RS_ABORT_FSRENAME_ERROR 46
#define DSM_RS_ABORT_INVALID_OPERATION 47
#define DSM_RS_ABORT_STGPOOL_UNDEFINED 48
#define DSM_RS_ABORT_INVALID_DATA_FORMAT 49
#define DSM_RS_ABORT_DATAMOVER_UNDEFINED 50

#define DSM_RS_ABORT_INVALID_MOVER_TYPE 231
#define DSM_RS_ABORT_ITEM_IN_USE 232
#define DSM_RS_ABORT_LOCK_CONFLICT 233
#define DSM_RS_ABORT_SRV_PLUGIN_COMM_ERROR 234
#define DSM_RS_ABORT_SRV_PLUGIN_OS_ERROR 235
#define DSM_RS_ABORT_CRC_FAILED 236
#define DSM_RS_ABORT_INVALID_GROUP_ACTION 237
#define DSM_RS_ABORT_DISK_UNDEFINED 238
#define DSM_RS_ABORT_BAD_DESTINATION 239
#define DSM_RS_ABORT_DATAMOVER_NOT_AVAILABLE 240
#define DSM_RS_ABORT_STGPOOL_COPY_CONT_NO 241
#define DSM_RS_ABORT_RETRY_SINGLE_TXN 242
#define DSM_RS_ABORT_TOC_CREATION_FAIL 243
#define DSM_RS_ABORT_TOC_LOAD_FAIL 244
#define DSM_RS_ABORT_PATH_RESTRICTED 245
#define DSM_RS_ABORT_NO_LANFREE_SCRATCH 246
#define DSM_RS_ABORT_INSERT_NOT_ALLOWED 247
#define DSM_RS_ABORT_DELETE_NOT_ALLOWED 248
#define DSM_RS_ABORT_TXN_LIMIT_EXCEEDED 249
#define DSM_RS_ABORT_OBJECT_ALREADY_HELD 250
#define DSM_RS_ABORT_INVALID_CHUNK_REFERENCE 254
#define DSM_RS_ABORT_DESTINATION_NOT_DEDUP 255
#define DSM_RS_ABORT_DESTINATION_POOL_CHANGED 257
#define DSM_RS_ABORT_NOT_ROOT 258

/* RETURN CODE */

#define DSM_RC_ABORT_SYSTEM_ERROR DSM_RS_ABORT_SYSTEM_ERROR
#define DSM_RC_ABORT_NO_MATCH DSM_RS_ABORT_NO_MATCH

```

```

#define DSM_RC_ABORT_BY_CLIENT DSM_RS_ABORT_BY_CLIENT
#define DSM_RC_ABORT_ACTIVE_NOT_FOUND DSM_RS_ABORT_ACTIVE_NOT_FOUND
#define DSM_RC_ABORT_NO_DATA DSM_RS_ABORT_NO_DATA
#define DSM_RC_ABORT_BAD_VERIFIER DSM_RS_ABORT_BAD_VERIFIER
#define DSM_RC_ABORT_NODE_IN_USE DSM_RS_ABORT_NODE_IN_USE
#define DSM_RC_ABORT_EXPDATE_TOO_LOW DSM_RS_ABORT_EXPDATE_TOO_LOW
#define DSM_RC_ABORT_DATA_OFFLINE DSM_RS_ABORT_DATA_OFFLINE
#define DSM_RC_ABORT_EXCLUDED_BY_SIZE DSM_RS_ABORT_EXCLUDED_BY_SIZE

#define DSM_RC_ABORT_NO_REPOSIT_SPACE DSM_RS_ABORT_NO_STO_SPACE_SKIP
#define DSM_RC_ABORT_NO_STO_SPACE_SKIP DSM_RS_ABORT_NO_STO_SPACE_SKIP

#define DSM_RC_ABORT_MOUNT_NOT_POSSIBLE DSM_RS_ABORT_MOUNT_NOT_POSSIBLE
#define DSM_RC_ABORT_SIZEESTIMATE_EXCEED DSM_RS_ABORT_SIZEESTIMATE_EXCEED
#define DSM_RC_ABORT_DATA_UNAVAILABLE DSM_RS_ABORT_DATA_UNAVAILABLE
#define DSM_RC_ABORT_RETRY DSM_RS_ABORT_RETRY
#define DSM_RC_ABORT_NO_LOG_SPACE DSM_RS_ABORT_NO_LOG_SPACE
#define DSM_RC_ABORT_NO_DB_SPACE DSM_RS_ABORT_NO_DB_SPACE
#define DSM_RC_ABORT_NO_MEMORY DSM_RS_ABORT_NO_MEMORY

#define DSM_RC_ABORT_FS_NOT_DEFINED DSM_RS_ABORT_FS_NOT_DEFINED
#define DSM_RC_ABORT_NODE_ALREADY_DEFED DSM_RS_ABORT_NODE_ALREADY_DEFED
#define DSM_RC_ABORT_NO_DEFAULT_DOMAIN DSM_RS_ABORT_NO_DEFAULT_DOMAIN
#define DSM_RC_ABORT_INVALID_NODENAME DSM_RS_ABORT_INVALID_NODENAME
#define DSM_RC_ABORT_INVALID_POL_BIND DSM_RS_ABORT_INVALID_POL_BIND
#define DSM_RC_ABORT_DEST_NOT_DEFINED DSM_RS_ABORT_DEST_NOT_DEFINED
#define DSM_RC_ABORT_WAIT_FOR_SPACE DSM_RS_ABORT_WAIT_FOR_SPACE
#define DSM_RC_ABORT_NOT_AUTHORIZED DSM_RS_ABORT_NOT_AUTHORIZED
#define DSM_RC_ABORT_RULE_ALREADY_DEFED DSM_RS_ABORT_RULE_ALREADY_DEFED
#define DSM_RC_ABORT_NO_STOR_SPACE_STOP DSM_RS_ABORT_NO_STOR_SPACE_STOP

#define DSM_RC_ABORT_LICENSE_VIOLATION DSM_RS_ABORT_LICENSE_VIOLATION
#define DSM_RC_ABORT_EXTOBJID_ALREADY_EXISTS DSM_RS_ABORT_EXTOBJID_ALREADY_EXISTS
#define DSM_RC_ABORT_DUPLICATE_OBJECT DSM_RS_ABORT_DUPLICATE_OBJECT

#define DSM_RC_ABORT_INVALID_OFFSET DSM_RS_ABORT_INVALID_OFFSET
#define DSM_RC_ABORT_INVALID_LENGTH DSM_RS_ABORT_INVALID_LENGTH

#define DSM_RC_ABORT_STRING_ERROR DSM_RS_ABORT_STRING_ERROR
#define DSM_RC_ABORT_NODE_NOT_AUTHORIZED DSM_RS_ABORT_NODE_NOT_AUTHORIZED
#define DSM_RC_ABORT_RESTART_NOT_POSSIBLE DSM_RS_ABORT_RESTART_NOT_POSSIBLE
#define DSM_RC_ABORT_RESTORE_IN_PROGRESS DSM_RS_ABORT_RESTORE_IN_PROGRESS
#define DSM_RC_ABORT_SYNTAX_ERROR DSM_RS_ABORT_SYNTAX_ERROR

#define DSM_RC_ABORT_DATA_SKIPPED DSM_RS_ABORT_DATA_SKIPPED
#define DSM_RC_ABORT_EXCEED_MAX_MP DSM_RS_ABORT_EXCEED_MAX_MP
#define DSM_RC_ABORT_NO_OBJSET_MATCH DSM_RS_ABORT_NO_OBJSET_MATCH
#define DSM_RC_ABORT_PVR_ERROR DSM_RS_ABORT_PVR_ERROR
#define DSM_RC_ABORT_BAD_RECOGTOKEN DSM_RS_ABORT_BAD_RECOGTOKEN
#define DSM_RC_ABORT_MERGE_ERROR DSM_RS_ABORT_MERGE_ERROR
#define DSM_RC_ABORT_FSRENAME_ERROR DSM_RS_ABORT_FSRENAME_ERROR
#define DSM_RC_ABORT_INVALID_OPERATION DSM_RS_ABORT_INVALID_OPERATION
#define DSM_RC_ABORT_STGPOOL_UNDEFINED DSM_RS_ABORT_STGPOOL_UNDEFINED
#define DSM_RC_ABORT_INVALID_DATA_FORMAT DSM_RS_ABORT_INVALID_DATA_FORMAT
#define DSM_RC_ABORT_DATAMOVER_UNDEFINED DSM_RS_ABORT_DATAMOVER_UNDEFINED

#define DSM_RC_ABORT_INVALID_MOVER_TYPE DSM_RS_ABORT_INVALID_MOVER_TYPE
#define DSM_RC_ABORT_ITEM_IN_USE DSM_RS_ABORT_ITEM_IN_USE
#define DSM_RC_ABORT_LOCK_CONFLICT DSM_RS_ABORT_LOCK_CONFLICT
#define DSM_RC_ABORT_SRV_PLUGIN_COMM_ERROR DSM_RS_ABORT_SRV_PLUGIN_COMM_ERROR
#define DSM_RC_ABORT_SRV_PLUGIN_OS_ERROR DSM_RS_ABORT_SRV_PLUGIN_OS_ERROR
#define DSM_RC_ABORT_CRC_FAILED DSM_RS_ABORT_CRC_FAILED
#define DSM_RC_ABORT_INVALID_GROUP_ACTION DSM_RS_ABORT_INVALID_GROUP_ACTION
#define DSM_RC_ABORT_DISK_UNDEFINED DSM_RS_ABORT_DISK_UNDEFINED
#define DSM_RC_ABORT_BAD_DESTINATION DSM_RS_ABORT_BAD_DESTINATION
#define DSM_RC_ABORT_DATAMOVER_NOT_AVAILABLE DSM_RS_ABORT_DATAMOVER_NOT_AVAILABLE
#define DSM_RC_ABORT_STGPOOL_COPY_CONT_NO DSM_RS_ABORT_STGPOOL_COPY_CONT_NO
#define DSM_RC_ABORT_RETRY_SINGLE_TXN DSM_RS_ABORT_RETRY_SINGLE_TXN
#define DSM_RC_ABORT_TOC_CREATION_FAIL DSM_RS_ABORT_TOC_CREATION_FAIL
#define DSM_RC_ABORT_TOC_LOAD_FAIL DSM_RS_ABORT_TOC_LOAD_FAIL
#define DSM_RC_ABORT_PATH_RESTRICTED DSM_RS_ABORT_PATH_RESTRICTED
#define DSM_RC_ABORT_NO_LANFREE_SCRATCH DSM_RS_ABORT_NO_LANFREE_SCRATCH
#define DSM_RC_ABORT_INSERT_NOT_ALLOWED DSM_RS_ABORT_INSERT_NOT_ALLOWED
#define DSM_RC_ABORT_DELETE_NOT_ALLOWED DSM_RS_ABORT_DELETE_NOT_ALLOWED
#define DSM_RC_ABORT_TXN_LIMIT_EXCEEDED DSM_RS_ABORT_TXN_LIMIT_EXCEEDED
#define DSM_RC_ABORT_OBJECT_ALREADY_HELD DSM_RS_ABORT_OBJECT_ALREADY_HELD
#define DSM_RC_ABORT_INVALID_CHUNK_REFERENCE DSM_RS_ABORT_INVALID_CHUNK_REFERENCE

```

```

#define DSM_RC_ABORT_DESTINATION_NOT_DEDUP    DSM_RS_ABORT_DESTINATION_NOT_DEDUP
#define DSM_RC_ABORT_DESTINATION_POOL_CHANGED DSM_RS_ABORT_DESTINATION_POOL_CHANGED
#define DSM_RC_ABORT_NOT_ROOT                 DSM_RS_ABORT_NOT_ROOT

#define DSM_RC_ABORT_CERTIFICATE_NOT_FOUND    DSM_RS_ABORT_CERTIFICATE_NOT_FOUND

/* Definitions for server signon reject codes */
/* These error codes are in the range (51 to 99) inclusive. */
#define DSM_RC_REJECT_NO_RESOURCES            51
#define DSM_RC_REJECT_VERIFIER_EXPIRED       52
#define DSM_RC_REJECT_ID_UNKNOWN             53
#define DSM_RC_REJECT_DUPLICATE_ID          54
#define DSM_RC_REJECT_SERVER_DISABLED       55
#define DSM_RC_REJECT_CLOSED_REGISTER       56
#define DSM_RC_REJECT_CLIENT_DOWNLEVEL     57
#define DSM_RC_REJECT_SERVER_DOWNLEVEL     58
#define DSM_RC_REJECT_ID_IN_USE            59
#define DSM_RC_REJECT_ID_LOCKED            61
#define DSM_RC_SIGNONREJECT_LICENSE_MAX    62
#define DSM_RC_REJECT_NO_MEMORY            63
#define DSM_RC_REJECT_NO_DB_SPACE          64
#define DSM_RC_REJECT_NO_LOG_SPACE         65
#define DSM_RC_REJECT_INTERNAL_ERROR       66
#define DSM_RC_SIGNONREJECT_INVALID_CLI    67 /* client type not licensed */
#define DSM_RC_CLIENT_NOT_ARCHRETPROT     68
#define DSM_RC_REJECT_LASTSESS_CANCELED    69
#define DSM_RC_REJECT_UNICODE_NOT_ALLOWED  70
#define DSM_RC_REJECT_NOT_AUTHORIZED       71
#define DSM_RC_REJECT_TOKEN_TIMEOUT        72
#define DSM_RC_REJECT_INVALID_NODE_TYPE    73
#define DSM_RC_REJECT_INVALID_SESSIONINIT  74
#define DSM_RC_REJECT_WRONG_PORT           75
#define DSM_RC_CLIENT_NOT_SPMRETPROT      79

#define DSM_RC_USER_ABORT                   101 /* processing aborted by user */
#define DSM_RC_NO_MEMORY                     102 /* no RAM left to complete request */
#define DSM_RC_TA_COMM_DOWN                 2021 /* no longer used */
#define DSM_RC_FILE_NOT_FOUND               104 /* specified file not found */
#define DSM_RC_PATH_NOT_FOUND               105 /* specified path doesn't exist */
#define DSM_RC_ACCESS_DENIED                106 /* denied due to improper permission */
#define DSM_RC_NO_HANDLES                   107 /* no more file handles available */
#define DSM_RC_FILE_EXISTS                  108 /* file already exists */
#define DSM_RC_INVALID_PARM                 109 /* invalid parameter passed. CRITICAL*/
#define DSM_RC_INVALID_HANDLE               110 /* invalid file handle passed */
#define DSM_RC_DISK_FULL                    111 /* out of disk space */
#define DSM_RC_PROTOCOL_VIOLATION           113 /* call protocol violation. CRITICAL */
#define DSM_RC_UNKNOWN_ERROR                114 /* unknown system error. CRITICAL */
#define DSM_RC_UNEXPECTED_ERROR             115 /* unexpected error. CRITICAL */
#define DSM_RC_FILE_BEING_EXECUTED         116 /* No write is allowed */
#define DSM_RC_DIR_NO_SPACE                  117 /* directory can't be expanded */
#define DSM_RC_LOOPED_SYM_LINK              118 /* too many symbolic links were
encountered in translating path. */
#define DSM_RC_FILE_NAME_TOO_LONG           119 /* file name too long */
#define DSM_RC_FILE_SPACE_LOCKED            120 /* filespace is locked by the system */
#define DSM_RC_FINISHED                     121 /* finished processing */
#define DSM_RC_UNKNOWN_FORMAT               122 /* unknown format */
#define DSM_RC_NO_AUTHORIZATION              123 /* server response when the client has
no authorization to read another
host's owner backup/archive data */
#define DSM_RC_FILE_SPACE_NOT_FOUND         124 /* specified file space not found */
#define DSM_RC_TXN_ABORTED                  125 /* transaction aborted */
#define DSM_RC_SUBDIR_AS_FILE               126 /* Subdirectory name exists as file */
#define DSM_RC_PROCESS_NO_SPACE             127 /* process has no more disk space. */
#define DSM_RC_PATH_TOO_LONG                128 /* a directory path being build became
too long */
#define DSM_RC_NOT_COMPRESSED               129 /* file thought to be compressed is
actually not */
#define DSM_RC_TOO_MANY_BITS                130 /* file was compressed using more bits
then the expander can handle */
#define DSM_RC_SYSTEM_ERROR                 131 /* internal system error */
#define DSM_RC_NO_SERVER_RESOURCES          132 /* server out of resources. */
#define DSM_RC_FS_NOT_KNOWN                 133 /* the file space is not known by the
server */
#define DSM_RC_NO_LEADING_DIRSEP            134 /* no leading directory separator */
#define DSM_RC_WILDCARD_DIR                 135 /* wildcard character in directory

```

```

                                path when not allowed          */
#define DSM_RC_COMM_PROTOCOL_ERROR 136 /* communications protocol error */
#define DSM_RC_AUTH_FAILURE 137 /* authentication failure */
#define DSM_RC_TA_NOT_VALID 138 /* TA not a root and/or SUID program */
#define DSM_RC_KILLED 139 /* process killed. */

#define DSM_RC_RETRY 143 /* retry same operation again */

#define DSM_RC_WOULD_BLOCK 145 /* operation would cause the system to
                                block waiting for input. */
#define DSM_RC_TOO_SMALL 146 /* area for compiled pattern small */
#define DSM_RC_UNCLOSED 147 /* no closing bracket in pattern */
#define DSM_RC_NO_STARTING_DELIMITER 148 /* pattern has to start with
                                directory delimiter */
#define DSM_RC_NEEDED_DIR_DELIMITER 149 /* a directory delimiter is needed
                                immediately before and after the
                                "match directories" metastring
                                ("...") and one wasn't found */
#define DSM_RC_UNKNOWN_FILE_DATA_TYPE 150 /* structured file data type is
                                unknown */
#define DSM_RC_BUFFER_OVERFLOW 151 /* data buffer overflow */

#define DSM_RC_NO_COMPRESS_MEMORY 154 /* Compress/Expand out of memory */
#define DSM_RC_COMPRESS_GREW 155 /* Compression grew */
#define DSM_RC_INV_COMM_METHOD 156 /* Invalid comm method specified */
#define DSM_RC_WILL_ABORT 157 /* Transaction will be aborted */
#define DSM_RC_FS_WRITE_LOCKED 158 /* File space is write locked */
#define DSM_RC_SKIPPED_BY_USER 159 /* User wanted file skipped in the
                                case of ABORT_DATA_OFFLINE */
#define DSM_RC_TA_NOT_FOUND 160 /* TA not found in it's directory */
#define DSM_RC_TA_ACCESS_DENIED 161 /* Access to TA is denied */
#define DSM_RC_FS_NOT_READY 162 /* File space not ready */
#define DSM_RC_FS_IS_BAD 163 /* File space is bad */
#define DSM_RC_FIO_ERROR 164 /* File input/output error */
#define DSM_RC_WRITE_FAILURE 165 /* Error writing to file */
#define DSM_RC_OVER_FILE_SIZE_LIMIT 166 /* File over system/user limit */
#define DSM_RC_CANNOT_MAKE 167 /* Could not create file/directory,
                                could be a bad name */
#define DSM_RC_NO_PASS_FILE 168 /* password file needed and user is
                                not root */
#define DSM_RC_VERFILE_OLD 169 /* password stored locally doesn't
                                match the one at the host */
#define DSM_RC_INPUT_ERROR 173 /* unable to read keyboard input */
#define DSM_RC_REJECT_PLATFORM_MISMATCH 174 /* Platform name doesn't match
                                up with what the server says
                                is the platform for the client */
#define DSM_RC_TL_NOT_FILE_OWNER 175 /* User trying to backup a file is not
                                the file's owner. */
#define DSM_RC_COMPRESSED_DATA_CORRUPTED 176 /* Compressed data is corrupted*/
#define DSM_RC_UNMATCHED_QUOTE 177 /* missing starting or ending quote */

#define DSM_RC_SIGNON_FAILOVER_MODE 178 /* Failed over to the replication server,
                                running in failover mode */
#define DSM_RC_FAILOVER_MODE_FUNC_BLOCKED 179 /* function is blocked because
                                session is in failover mode */

/*-----*/
/* Return codes 180-199 are reserved for Policy Set handling */
/*-----*/
#define DSM_RC_PS_MULTBCG 181 /* Multiple backup copy groups in 1 MC*/
#define DSM_RC_PS_MULTACG 182 /* Multiple arch. copy groups in 1 MC*/
#define DSM_RC_PS_NODFLTMC 183 /* Default MC name not in policy set */
#define DSM_RC_TL_NOBCG 184 /* Backup req, no backup copy group */
#define DSM_RC_TL_EXCLUDED 185 /* Backup req, excl. by in/ex filter */
#define DSM_RC_TL_NOACG 186 /* Archive req, no archive copy group */
#define DSM_RC_PS_INVALID_ARCHMC 187 /* Invalid MC name in archive override*/
#define DSM_RC_NO_PS_DATA 188 /* No policy set data on the server */
#define DSM_RC_PS_INVALID_DIRMC 189 /* Invalid directory MC specified in
                                the options file. */
#define DSM_RC_PS_NO_CG_IN_DIR_MC 190 /* No backup copy group in directory MC.
                                Must specify an MC using DirMC
                                option. */

#define DSM_RC_WIN32_UNSUPPORTED_FILE_TYPE 280 /* File is not of
                                Win32 type FILE_TYPE_DISK */

```

```

/*-----*/
/* Return codes for the Trusted Communication Agent */
/*-----*/
#define DSM_RC_TCA_NOT_ROOT 161 /* Access to TA is denied */
#define DSM_RC_TCA_ATTACH_SHR_MEM_ERR 200 /* Error attaching shared memory */
#define DSM_RC_TCA_SHR_MEM_BLOCK_ERR 200 /* Shared memory block error */
#define DSM_RC_TCA_SHR_MEM_IN_USE 200 /* Shared memory block error */
#define DSM_RC_TCA_SHARED_MEMORY_ERROR 200 /* Shared memory block error */
#define DSM_RC_TCA_SEGMENT_MISMATCH 200 /* Shared memory block error */
#define DSM_RC_TCA_FORK_FAILED 292 /* Error forking off TCA process */
#define DSM_RC_TCA_DIED 294 /* TCA died unexpectedly */
#define DSM_RC_TCA_INVALID_REQUEST 295 /* Invalid request sent to TCA */
#define DSM_RC_TCA_SEMGET_ERROR 297 /* Error getting semaphores */
#define DSM_RC_TCA_SEM_OP_ERROR 298 /* Error in semaphore set or wait */
#define DSM_RC_TCA_NOT_ALLOWED 299 /* TCA not allowed (multi thread) */

/*-----*/
/* 400-430 for options */
/*-----*/
#define DSM_RC_INVALID_OPT 400 /* invalid option */
#define DSM_RC_NO_HOST_ADDR 405 /* Not enuf info to connect server */
#define DSM_RC_NO_OPT_FILE 406 /* No default user configuration file*/
#define DSM_RC_MACHINE_SAME 408 /* -MACHINENAME same as real name */
#define DSM_RC_INVALID_SERVER 409 /* Invalid server name from client */
#define DSM_RC_INVALID_KEYWORD 410 /* Invalid option keyword */
#define DSM_RC_PATTERN_TOO_COMPLEX 411 /* Can't match Include/Exclude entry*/
#define DSM_RC_NO_CLOSING_BRACKET 412 /* Missing closing bracket inc/excl */
#define DSM_RC_OPT_CLIENT_NOT_ACCEPTING 417/* Client doesn't accept this option
from the server */
#define DSM_RC_OPT_CLIENT_DOES_NOT_WANT 418/* Client doesn't want this value
from the server */
#define DSM_RC_OPT_NO_INCLEXCL_FILE 419 /* inclexcl file not found */
#define DSM_RC_OPT_OPEN_FAILURE 420 /* can't open file */
#define DSM_RC_OPT_INV_NODENAME 421/* used for Windows if nodename=local
machine when CLUSTERNODE=YES */
#define DSM_RC_OPT_NODENAME_INVALID 423/* generic invalid nodename */
#define DSM_RC_OPT_ERRORLOG_CONFLICT 424/* both logmax & retention specified */
#define DSM_RC_OPT_SCHEDLOG_CONFLICT 425/* both logmax & retention specified */
#define DSM_RC_CANNOT_OPEN_TRACEFILE 426/* cannot open trace file */
#define DSM_RC_CANNOT_OPEN_LOGFILE 427/* cannot open error log file */
#define DSM_RC_OPT_SESSINIT_LF_CONFLICT 428/* both sessioninit=server and
enablelanfree=yes
are specified*/
#define DSM_RC_OPT_OPTION_IGNORE 429/* option will be ignored */
#define DSM_RC_OPT_DEDUP_CONFLICT 430/* cannot open error log file */
#define DSM_RC_OPT_HSMLOG_CONFLICT 431/* both logmax & retention specified */

/*-----*/
/* 600 to 610 for volume label codes */
/*-----*/
#define DSM_RC_DUP_LABEL 600 /* duplicate volume label found */
#define DSM_RC_NO_LABEL 601 /* drive has no label */

/*-----*/
/* Return codes for message file processing */
/*-----*/
#define DSM_RC-NLS_CANT_OPEN_TXT 610 /* error trying to open msg txt file */
#define DSM_RC-NLS_CANT_READ_HDR 611 /* error trying to read header */
#define DSM_RC-NLS_INVALID_CNTL_REC 612 /* invalid control record */
#define DSM_RC-NLS_INVALID_DATE_FMT 613 /* invalid default date format */
#define DSM_RC-NLS_INVALID_TIME_FMT 614 /* invalid default time format */
#define DSM_RC-NLS_INVALID_NUM_FMT 615 /* invalid default number format */

/*-----*/
/* Return codes 620-630 are reserved for log message return codes */
/*-----*/
#define DSM_RC_LOG_CANT_BE_OPENED 620 /* error trying to open error log */
#define DSM_RC_LOG_ERROR_WRITING_TO_LOG 621 /* error occurred writing to
log file */
#define DSM_RC_LOG_NOT_SPECIFIED 622 /* no error log file was specified */

/*-----*/
/* Return codes 900-999 TSM CLIENT ONLY */
/*-----*/
#define DSM_RC_NOT_ADSM_AUTHORIZED 927 /* Must be ADSM authorized to perform*/

```



```

/* action : root user or pwd auth */
#define DSM_RC_REJECT_USERID_UNKNOWN 940 /* userid unknown on server */
#define DSM_RC_FILE_IS_SYMLINK 959 /* errorlog or trace is a symbolic
link
*/

#define DSM_RC_DIRECT_STORAGE_AGENT_UNSUPPORTED 961 /* Direct connection to SA not supported */
#define DSM_RC_FS_NAMESPACE_DOWNLEVEL 963 /* Long namespace has been removed from
from the Netware volume */
#define DSM_RC_CONTINUE_NEW_CONSUMER 972 /* Continue processing using a new consumer */
#define DSM_RC_CONTINUE_NEW_CONSUMER_NODEDUP 973 /* Continue processing using a new consumer no
dedup*/
#define DSM_RC_CONTINUE_NEW_CONSUMER_NOCOMPRESS 976 /* Continue processing using a new consumer no
compression */

#define DSM_RC_SERVER_SUPPORTS_FUNC 994 /* the server supports this function */
#define DSM_RC_SERVER_AND_SA_SUPPORT_FUNC 995 /* Both server and SA support func */
#define DSM_RC_SERVER_DOWNLEVEL_FUNC 996 /* The server is downlevel for func */
#define DSM_RC_STORAGEAGENT_DOWNLEVEL 997 /* the storage agent is downlevel */
#define DSM_RC_SERVER_AND_SA_DOWNLEVEL 998 /* both server and SA downlevel */

/* TCP/IP error codes */
#define DSM_RC_TCPIP_FAILURE -50 /* TCP/IP communications failure */
#define DSM_RC_CONN_TIMEDOUT -51 /* TCP/IP connection attempt timedout */
#define DSM_RC_CONN_REFUSED -52 /* TCP/IP connection refused by host */
#define DSM_RC_BAD_HOST_NAME -53 /* TCP/IP invalid host name specified */
#define DSM_RC_NETWORK_UNREACHABLE -54 /* TCP/IP host name unreachable */
#define DSM_RC_WINSOCK_MISSING -55 /* TCP/IP WINSOCK.DLL missing */
#define DSM_RC_TCPIP_DLL_LOADFAILURE -56 /* Error from LoadLibrary */
#define DSM_RC_TCPIP_LOADFAILURE -57 /* Error from GetProcAddress */
#define DSM_RC_TCPIP_USER_ABORT -58 /* User aborted while in TCP/IP layer */

/*-----*/
/* Return codes (-71)-(-90) are reserved for CommTSM error codes */
/*-----*/
#define DSM_RC_TSM_FAILURE -71 /* TSM communications failure */
#define DSM_RC_TSM_ABORT -72 /* Session aborted abnormally */

/*comm3270 error codes - no longer used*/
#define DSM_RC_COMM_TIMEOUT 2021 /* no longer used */
#define DSM_RC_EMULATOR_INACTIVE 2021 /* no longer used */
#define DSM_RC_BAD_HOST_ID 2021 /* no longer used */
#define DSM_RC_HOST_SESS_BUSY 2021 /* no longer used */
#define DSM_RC_3270_CONNECT_FAILURE 2021 /* no longer used */
#define DSM_RC_NO_ACS3ELKE_DLL 2021 /* no longer used */
#define DSM_RC_EMULATOR_ERROR 2021 /* no longer used */
#define DSM_RC_EMULATOR_BACKLEVEL 2021 /* no longer used */
#define DSM_RC_CKSUM_FAILURE 2021 /* no longer used */

/* The following Return codes are for EHLAPI for Windows */
#define DSM_RC_3270COMMError_DLL 2021 /* no longer used */
#define DSM_RC_3270COMMError_GetProc 2021 /* no longer used */
#define DSM_RC_EHLAPIError_DLL 2021 /* no longer used */
#define DSM_RC_EHLAPIError_GetProc 2021 /* no longer used */
#define DSM_RC_EHLAPIError_HostConnect 2021 /* no longer used */
#define DSM_RC_EHLAPIError_AllocBuff 2021 /* no longer used */
#define DSM_RC_EHLAPIError_SendKey 2021 /* no longer used */
#define DSM_RC_EHLAPIError_PacketChk 2021 /* no longer used */
#define DSM_RC_EHLAPIError_ChkSum 2021 /* no longer used */
#define DSM_RC_EHLAPIError_HostTimeOut 2021 /* no longer used */
#define DSM_RC_EHLAPIError_Send 2021 /* no longer used */
#define DSM_RC_EHLAPIError_Recv 2021 /* no longer used */
#define DSM_RC_EHLAPIError_General 2021 /* no longer used */
#define DSM_RC_PC3270_MISSING_DLL 2021 /* no longer used */
#define DSM_RC_3270COMM_MISSING_DLL 2021 /* no longer used */

/* NETBIOS error codes */
#define DSM_RC_NETB_ERROR -151 /* Could not add node to LAN */
#define DSM_RC_NETB_NO_DLL -152 /* The ACSNETB.DLL could not be loaded*/
#define DSM_RC_NETB_LAN_ERR -155 /* LAN error detected */
#define DSM_RC_NETB_NAME_ERR -158 /* Netbios error on Add Name */
#define DSM_RC_NETB_TIMEOUT -159 /* Netbios send timeout */
#define DSM_RC_NETB_NOTINST -160 /* Netbios not installed - DOS */

```

```

#define DSM_RC_NETB_REBOOT          -161 /* Netbios config err - reboot DOS */

/* Named Pipe error codes */
#define DSM_RC_NP_ERROR              -190

/* CPIC error codes */
#define DSM_RC_CPIC_ALLOCATE_FAILURE 2021 /* no longer used */
#define DSM_RC_CPIC_TYPE_MISMATCH    2021 /* no longer used */
#define DSM_RC_CPIC_PIP_NOT_SPECIFY_ERR 2021 /* no longer used */
#define DSM_RC_CPIC_SECURITY_NOT_VALID 2021 /* no longer used */
#define DSM_RC_CPIC_SYNC_LVL_NO_SUPPORT 2021 /* no longer used */
#define DSM_RC_CPIC_TPN_NOT_RECOGNIZED 2021 /* no longer used */
#define DSM_RC_CPIC_TP_ERROR          2021 /* no longer used */
#define DSM_RC_CPIC_PARAMETER_ERROR   2021 /* no longer used */
#define DSM_RC_CPIC_PROD_SPECIFIC_ERR 2021 /* no longer used */
#define DSM_RC_CPIC_PROGRAM_ERROR     2021 /* no longer used */
#define DSM_RC_CPIC_RESOURCE_ERROR    2021 /* no longer used */
#define DSM_RC_CPIC_DEALLOCATE_ERROR  2021 /* no longer used */
#define DSM_RC_CPIC_SVC_ERROR         2021 /* no longer used */
#define DSM_RC_CPIC_PROGRAM_STATE_CHECK 2021 /* no longer used */
#define DSM_RC_CPIC_PROGRAM_PARAM_CHECK 2021 /* no longer used */
#define DSM_RC_CPIC_UNSUCCESSFUL      2021 /* no longer used */
#define DSM_RC_UNKNOWN_CPIC_PROBLEM   2021 /* no longer used */
#define DSM_RC_CPIC_MISSING_LU        2021 /* no longer used */
#define DSM_RC_CPIC_MISSING_TP        2021 /* no longer used */
#define DSM_RC_CPIC_SNA6000_LOAD_FAIL 2021 /* no longer used */
#define DSM_RC_CPIC_STARTUP_FAILURE    2021 /* no longer used */

/*-----*/
/* Return codes -300 to -307 are reserved for IPX/SPX communications */
/*-----*/
#define DSM_RC_TLI_ERROR              2021 /* no longer used */
#define DSM_RC_IPXSPX_FAILURE         2021 /* no longer used */
#define DSM_RC_TLI_DLL_MISSING        2021 /* no longer used */
#define DSM_RC_DLL_LOADFAILURE        2021 /* no longer used */
#define DSM_RC_DLL_FUNCTION_LOADFAILURE 2021 /* no longer used */
#define DSM_RC_IPXCONN_REFUSED        2021 /* no longer used */
#define DSM_RC_IPXCONN_TIMEDOUT       2021 /* no longer used */
#define DSM_RC_IPXADDR_UNREACHABLE    2021 /* no longer used */
#define DSM_RC_CPIC_MISSING_DLL       2021 /* no longer used */
#define DSM_RC_CPIC_DLL_LOADFAILURE   2021 /* no longer used */
#define DSM_RC_CPIC_FUNC_LOADFAILURE  2021 /* no longer used */

/*=== Shared Memory Protocol error codes ===*/
#define DSM_RC_SHM_TCPIP_FAILURE       -450
#define DSM_RC_SHM_FAILURE             -451
#define DSM_RC_SHM_NOTAUTH            -452

#define DSM_RC_NULL_OBJNAME            2000 /* Object name pointer is NULL */
#define DSM_RC_NULL_DATABLKPTR         2001 /* dataBlkPtr is NULL */
#define DSM_RC_NULL_MSG                2002 /* msg parm in dsmRCMsg is NULL */

#define DSM_RC_NULL_OBJATTRPTR        2004 /* Object Attr Pointer is NULL */

#define DSM_RC_NO_SESS_BLK             2006 /* no server session info */
#define DSM_RC_NO_POLICY_BLK           2007 /* no policy hdr info */
#define DSM_RC_ZERO_BUFLEN             2008 /* bufferLen is zero for dataBlkPtr */
#define DSM_RC_NULL_BUFPTR            2009 /* bufferPtr is NULL for dataBlkPtr */

#define DSM_RC_INVALID_OBJTYPE         2010 /* invalid object type */
#define DSM_RC_INVALID_VOTE            2011 /* invalid vote */
#define DSM_RC_INVALID_ACTION          2012 /* invalid action */
#define DSM_RC_INVALID_DS_HANDLE       2014 /* invalid ADSM handle */
#define DSM_RC_INVALID_REPOS           2015 /* invalid value for repository */
#define DSM_RC_INVALID_FSNAME          2016 /* fs should start with dir delim */
#define DSM_RC_INVALID_OBJNAME         2017 /* invalid full path name */
#define DSM_RC_INVALID_LLNAME          2018 /* ll should start with dir delim */
#define DSM_RC_INVALID_OBJOWNER        2019 /* invalid object owner name */
#define DSM_RC_INVALID_ACTYPE          2020 /* invalid action type */
#define DSM_RC_INVALID_RETCODE         2021 /* dsmRC in dsmRCMsg is invalid */
#define DSM_RC_INVALID_SENDTYPE        2022 /* invalid send type */
#define DSM_RC_INVALID_PARAMETER       2023 /* invalid parameter */
#define DSM_RC_INVALID_OBJSTATE        2024 /* active, inactive, or any match? */
#define DSM_RC_INVALID_MCNAME          2025 /* Mgmt class name not found */
#define DSM_RC_INVALID_DRIVE_CHAR      2026 /* Drive letter is not alphabet */
#define DSM_RC_NULL_FSNAME             2027 /* Filespace name is NULL */
#define DSM_RC_INVALID_HLNAME          2028 /* hl should start with dir delim */

```

```

#define DSM_RC_NUMOBJ_EXCEED      2029 /* BeginGetData num objs exceeded */

#define DSM_RC_NEWPW_REQD        2030 /* new password is required */
#define DSM_RC_OLDPW_REQD        2031 /* old password is required */
#define DSM_RC_NO_OWNER_REQD     2032 /* owner not allowed. Allow default */
#define DSM_RC_NO_NODE_REQD      2033 /* node not allowed w/ pw=generate */
#define DSM_RC_KEY_MISSING       2034 /* key file can't be found */
#define DSM_RC_KEY_BAD           2035 /* content of key file is bad */

#define DSM_RC_BAD_CALL_SEQUENCE 2041 /* Sequence of DSM calls not allowed*/
#define DSM_RC_INVALID_TSMBUFFER 2042 /* invalid value for tsmbuffhandle or dataPtr */
#define DSM_RC_TOO_MANY_BYTES    2043 /* too many bytes copied to buffer */
#define DSM_RC_MUST_RELEASE_BUFFER 2044 /* cant exit app needs to release buffers */
#define DSM_RC_BUFF_ARRAY_ERROR  2045 /* internal buff array error */
#define DSM_RC_INVALID_DATA_BLK   2046 /* using tsmbuff datablk should be null */
#define DSM_RC_ENCR_NOT_ALLOWED   2047 /* when using tsmbuffers encryption not allowed */
#define DSM_RC_OBJ_COMPRESSED     2048 /* Can't restore using tsmBuff on compressed object */
#define DSM_RC_OBJ_ENCRYPTED       2049 /* Cant restore using tsmbuff an encr obj */
#define DSM_RC_WILDCHAR_NOTALLOWED 2050 /* Wild card not allowed for hl,ll */
#define DSM_RC_POR_NOT_ALLOWED    2051 /* Can't use partial object restore with tsmBuffers */
#define DSM_RC_NO_ENCRYPTION_KEY  2052 /* Encryption key not found*/
#define DSM_RC_ENCR_CONFLICT      2053 /* mutually exclusive options */

#define DSM_RC_FSNAME_NOTFOUND    2060 /* Filespace name not found */
#define DSM_RC_FS_NOT_REGISTERED  2061 /* Filespace name not registered */
#define DSM_RC_FS_ALREADY_REGED   2062 /* Filespace already registered */
#define DSM_RC_OBJID_NOTFOUND     2063 /* No object id to restore */
#define DSM_RC_WRONG_VERSION      2064 /* Wrong level of code */
#define DSM_RC_WRONG_VERSION_PARM 2065 /* Wrong level of parameter struct */

#define DSM_RC_NEEDTO_ENDTXN      2070 /* Need to call dsmEndTxn */

#define DSM_RC_OBJ_EXCLUDED       2080 /* Object is excluded by MC */
#define DSM_RC_OBJ_NOBCG          2081 /* Object has no backup copy group */
#define DSM_RC_OBJ_NOACG          2082 /* Object has no archive copy group */

#define DSM_RC_APISYSTEM_ERROR    2090 /* API internal error */

#define DSM_RC_DESC_TOOLONG       2100 /* description is too long */
#define DSM_RC_OBJINFO_TOOLONG    2101 /* object attr objinfo too long */
#define DSM_RC_HL_TOOLONG         2102 /* High level qualifier is too long */
#define DSM_RC_PASSWD_TOOLONG     2103 /* password is too long */
#define DSM_RC_FILESPACE_TOOLONG  2104 /* filespace name is too long */
#define DSM_RC_LL_TOOLONG         2105 /* Low level qualifier is too long */
#define DSM_RC_FSINFO_TOOLONG     2106 /* filespace length is too big */
#define DSM_RC_SENDDATA_WITH_ZERO_SIZE 2107 /* send data w/ zero est */

/*=== new return codes for dsmaccess ===*/
#define DSM_RC_INVALID_ACCESS_TYPE 2110 /* invalid access type */
#define DSM_RC_QUERY_COMM_FAILURE  2111 /* communication error during query */
#define DSM_RC_NO_FILES_BACKUP     2112 /* No backed up files for this fs */
#define DSM_RC_NO_FILES_ARCHIVE    2113 /* No archived files for this fs */
#define DSM_RC_INVALID_SETACCESS   2114 /* invalid set access format */

/*=== new return codes for dsmaccess ===*/
#define DSM_RC_STRING_TOO_LONG     2120 /* String parameter too long */

#define DSM_RC_MORE_DATA           2200 /* There are more data to restore */

#define DSM_RC_BUFF_TOO_SMALL     2210 /* DataBlk buffer too small for qry */

#define DSM_RC_NO_API_CONFIGFILE   2228 /*specified API cfg file not found*/
#define DSM_RC_NO_INCLXCL_FILE     2229 /* specified inclxcl file not found*/
#define DSM_RC_NO_SYS_OR_INCLXCL  2230 /* either dsm.sys or inclxcl file
        specified in dsm.sys not found */
#define DSM_RC_REJECT_NO_POR_SUPPORT 2231 /* server doesn't have POR support*/

#define DSM_RC_NEED_ROOT           2300 /* API caller must be root */
#define DSM_RC_NEEDTO_CALL_BINDMC  2301 /* dsmBindMC must be called first */
#define DSM_RC_CHECK_REASON_CODE   2302 /* check reason code from dsmEndTxn */
#define DSM_RC_NEEDTO_ENDTXN_DEDUP_SIZE_EXCEEDED 2303 /* max dedup bytes exceeded */

/*=== return codes 2400 - 2410 used by lic file see agentrc.h ===*/

/*=== return codes 2410 - 2430 used by Oracle agent see agentrc.h ===*/

```

```

#define DSM_RC_ENC_WRONG_KEY          4580 /* the key provided is incorrect */
#define DSM_RC_ENC_NOT_AUTHORIZED     4582 /* user is not allowed to decrypt */
#define DSM_RC_ENC_TYPE_UNKNOWN       4584 /* encryption type unknown */

/*=====
Return codes (4600)-(4624) are reserved for clustering
=====*/
#define DSM_RC_CLUSTER_INFO_LIBRARY_NOT_LOADED      4600
#define DSM_RC_CLUSTER_LIBRARY_INVALID             4601
#define DSM_RC_CLUSTER_LIBRARY_NOT_LOADED          4602
#define DSM_RC_CLUSTER_NOT_MEMBER_OF_CLUSTER       4603
#define DSM_RC_CLUSTER_NOT_ENABLED                 4604
#define DSM_RC_CLUSTER_NOT_SUPPORTED               4605
#define DSM_RC_CLUSTER_UNKNOWN_ERROR               4606

/*=====
Return codes (5200)-(5600) are reserved for new Server ABORT codes (dsmcomm.h)
=====*/
#define DSM_RS_ABORT_CERTIFICATE_NOT_FOUND         5200

/*=====
Return codes (5701)-(5749) are reserved for proxy
=====*/
#define DSM_RC_PROXY_REJECT_NO_RESOURCES           5702
#define DSM_RC_PROXY_REJECT_DUPLICATE_ID          5705
#define DSM_RC_PROXY_REJECT_ID_IN_USE             5710
#define DSM_RC_PROXY_REJECT_INTERNAL_ERROR        5717
#define DSM_RC_PROXY_REJECT_NOT_AUTHORIZED        5722
#define DSM_RC_PROXY_INVALID_FROMNODE             5746
#define DSM_RC_PROXY_INVALID_SERVERFREE           5747
#define DSM_RC_PROXY_INVALID_CLUSTER              5748
#define DSM_RC_PROXY_INVALID_FUNCTION             5749

/*=====
Return codes 5801 - 5849 are reserved for cryptography/security
=====*/

#define DSM_RC_CRYPTO_ICC_ERROR                   5801
#define DSM_RC_CRYPTO_ICC_CANNOT_LOAD             5802
#define DSM_RC_SSL_NOT_SUPPORTED                  5803
#define DSM_RC_SSL_INIT_FAILED                   5804
#define DSM_RC_SSL_KEYFILE_OPEN_FAILED           5805
#define DSM_RC_SSL_KEYFILE_BAD_PASSWORD          5806
#define DSM_RC_SSL_BAD_CERTIFICATE               5807

/*=====
Return codes 6300 - 6399 are reserved for client-side deduplication
=====*/
#define DSM_RC_DIGEST_VALIDATION_ERROR           6300 /* End-to-end digest validation err */
#define DSM_RC_DATA_FINGERPRINT_ERROR            6301 /* Failure in Rabin fingerprinting */
#define DSM_RC_DATA_DEDUP_ERROR                  6302 /* Error converting data into chunks */

#endif /* _H_DSMRC */

```

### Referencia relacionada:

Códigos de retorno de la API

## Archivos de origen de definiciones de tipo de API

Este apéndice contiene definiciones de estructura, definiciones de tipo y constantes de la API. El primer archivo de cabecera, dsmapitd.h y tsmapitd.h, ilustra las definiciones que son comunes a todos los sistemas operativos.

El segundo archivo de encabezado, dsmapips.h, proporciona un ejemplo de definiciones que son específicas a un sistema operativo particular; en este ejemplo, la plataforma Windows.

El tercer archivo, release.h, incluye la información de versión y release.

La información que se proporciona aquí contiene una copia puntual de los archivos que se distribuyen con la API. Vea los archivos en el paquete de distribución de la API para la última versión.

```

/*****
* Tivoli Storage Manager
* API Client Component
*
*/

```



```

#define DSM_MAX_PLATFORM_LENGTH      16      /* application type      */
#define DSM_MAX_PS_NAME_LENGTH      30      /* policy set name      */
#define DSM_MAX_SERVERTYPE_LENGTH    32      /* server platform type  */
#define DSM_MAX_VERIFIER_LENGTH     64      /* password              */
#define DSM_PATH_MAX                 1024    /* API config file path  */
#define DSM_NAME_MAX                 255    /* API config file name  */
#define DSM_MAX_NODE_LENGTH         64      /* node/machine name     */
#define DSM_MAX_RC_MSG_LENGTH       1024    /* msg parm for dsmRCMsg */
#define DSM_MAX_SERVER_ADDRESS      1024    /* server address */

#define DSM_MAX_MC_DESCR_LENGTH      DSM_MAX_DESCR_LENGTH /* mgmt class */
#define DSM_MAX_SERVERNAME_LENGTH    DSM_MAX_ID_LENGTH /* server name */
#define DSM_MAX_GET_OBJ              4080    /* max objs on BeginGetData */
#define DSM_MAX_PARTIAL_GET_OBJ      1300 /* max partial objs on BeginGetData*/
#define DSM_MAX_COMPRESSTYPE_LENGTH  32      /* max compression algorithm name */

/*-----+
| Minimum field lengths |
+-----*/
#define DSM_MIN_COMPRESS_SIZE 2048 /* minimum number of bytes an object */
/* needs before compression is allowed*/

/*-----+
| Values for mtFlag in dsmSetup call |
+-----*/
#define DSM_MULTITHREAD      bTrue
#define DSM_SINGLETHREAD    bFalse

/*-----+
| Values for object type in dsmObjName structure |
| Note: These values must be kept in sync with dsmcomm.h |
+-----*/
#define DSM_OBJ_FILE          0x01 /*object has attrib info & data*/
#define DSM_OBJ_DIRECTORY    0x02 /*obj has only attribute info */
#define DSM_OBJ_RESERVED1    0x04 /* for future use */
#define DSM_OBJ_RESERVED2    0x05 /* for future use */
#define DSM_OBJ_RESERVED3    0x06 /* for future use */
#define DSM_OBJ_WILDCARD     0xFE /* Any object type */
#define DSM_OBJ_ANY_TYPE     0xFF /* for future use */

/*-----+
| Type definition for compressedState in QryResp |
+-----*/
#define DSM_OBJ_COMPRESSED_UNKNOWN 0
#define DSM_OBJ_COMPRESSED_YES     1
#define DSM_OBJ_COMPRESSED_NO      2

/*-----+
| Definitions for "group type" field in tsmGroupHandlerIn_t |
+-----*/
#define DSM_GROUPTYPE_NONE      0x00 /* Not a group member */
#define DSM_GROUPTYPE_RESERVED1 0x01 /* for future use */
#define DSM_GROUPTYPE_PEER     0x02 /* Peer group */
#define DSM_GROUPTYPE_RESERVED2 0x03 /* for future use */

/*-----+
| Definitions for "member type" field in tsmGroupHandlerIn_t |
+-----*/
#define DSM_MEMBERTYPE_LEADER   0x01 /* group leader */
#define DSM_MEMBERTYPE_MEMBER   0x02 /* group member */

/*-----+
| Definitions for "operation type" field in tsmGroupHandlerIn_t |
+-----*/
#define DSM_GROUP_ACTION_BEGIN  0x01
#define DSM_GROUP_ACTION_OPEN   0x02 /* create new group */
#define DSM_GROUP_ACTION_CLOSE  0x03 /* commit and save an open group */
#define DSM_GROUP_ACTION_ADD     0x04 /* Append to a group */
#define DSM_GROUP_ACTION_ASSIGNTO 0x05 /* Assign to a another group */
#define DSM_GROUP_ACTION_REMOVE  0x06 /* remove a member from a group */

/*-----+
| Values for copySer in DetailCG structures for Query Mgmt Class response |
+-----*/
#define Copy_Serial_Static      1 /*Copy Serialization Static */

```

```

#define Copy_Serial_Shared_Static 2 /*Copy Serialization Shared Static*/
#define Copy_Serial_Shared_Dynamic 3 /*Copy Serialization Shared Dynamic*/
#define Copy_Serial_Dynamic 4 /*Copy Serialization Dynamic */

/*-----+
| Values for copyMode in DetailCG structures for Query Mgmt Class response |
+-----*/
#define Copy_Mode_Modified 1 /*Copy Mode Modified */
#define Copy_Mode_Absolute 2 /*Copy Mode Absolute */

/*-----+
| Values for objState in qryBackupData structure |
+-----*/
#define DSM_ACTIVE 0x01 /* query only active objects */
#define DSM_INACTIVE 0x02 /* query only inactive objects */
#define DSM_ANY_MATCH 0xFF /* query all backup objects */

/*-----+
| Boundary values for dsmDate.year field in qryArchiveData structure |
+-----*/
#define DATE_MINUS_INFINITE 0x0000 /* lowest boundary */
#define DATE_PLUS_INFINITE 0xFFFF /* highest upper boundary */

/*-----+
| Bits masks for update action parameter on dsmUpdateFS() |
+-----*/
#define DSM_FSUPD_FSTYPE ((unsigned) 0x00000002)
#define DSM_FSUPD_FSINFO ((unsigned) 0x00000004)
#define DSM_FSUPD_BACKSTARTDATE ((unsigned) 0x00000008)
#define DSM_FSUPD_BACKCOMPLETEDATE ((unsigned) 0x00000010)
#define DSM_FSUPD_OCCUPANCY ((unsigned) 0x00000020)
#define DSM_FSUPD_CAPACITY ((unsigned) 0x00000040)
#define DSM_FSUPD_RESERVED1 ((unsigned) 0x00000100)

/*-----+
| Bits mask for backup update action parameter on dsmUpdateObj() |
+-----*/
#define DSM_BACKUPD_OWNER ((unsigned) 0x00000001)
#define DSM_BACKUPD_OBJINFO ((unsigned) 0x00000002)
#define DSM_BACKUPD_MC ((unsigned) 0x00000004)

#define DSM_ARCHUPD_OWNER ((unsigned) 0x00000001)
#define DSM_ARCHUPD_OBJINFO ((unsigned) 0x00000002)
#define DSM_ARCHUPD_DESCR ((unsigned) 0x00000004)

/*-----+
| Values for repository parameter on dsmDeleteFS() |
+-----*/
#define DSM_ARCHIVE_REP 0x0A /* archive repository */
#define DSM_BACKUP_REP 0x0B /* backup repository */
#define DSM_REPOS_ALL 0x01 /* all repository types */

/*-----+
| Values for vote parameter on dsmEndTxn() |
+-----*/
#define DSM_VOTE_COMMIT 1 /* commit current transaction */
#define DSM_VOTE_ABORT 2 /* roll back current transaction */

/*-----+
| Values for various flags returned in ApiSessInfo structure. |
+-----*/
/* Client compression field codes */
#define COMPRESS_YES 1 /* client must compress data */
#define COMPRESS_NO 2 /* client must NOT compress data */
#define COMPRESS_CD 3 /* client determined */

/* Archive delete permission codes. */
#define ARCHDEL_YES 1 /* archive delete allowed */
#define ARCHDEL_NO 2 /* archive delete NOT allowed */

/* Backup delete permission codes. */
#define BACKDEL_YES 1 /* backup delete allowed */
#define BACKDEL_NO 2 /* backup delete NOT allowed */

/*-----+
| Values for various flags returned in optStruct structure. |
+-----*/

```

```

-----*/
#define DSM_PASSWD_GENERATE 1
#define DSM_PASSWD_PROMPT 0

#define DSM_COMM_TCP 1 /* tcpip */
#define DSM_COMM_NAMEDPIPE 2 /* Named pipes */
#define DSM_COMM_SHM 3 /* Shared Memory */

/* obsolete commmethods */
#define DSM_COMM_PVM_IUCV 12
#define DSM_COMM_3270 12
#define DSM_COMM_IUCV 12
#define DSM_COMM_PWSCS 12
#define DSM_COMM_SNA_LU6_2 12
#define DSM_COMM_IPXSPX 12 /* For IPX/SPX support */
#define DSM_COMM_NETBIOS 12 /* NETBIOS */
#define DSM_COMM_400COMM 12
#define DSM_COMM_CLIO 12 /* CLIO/S */
/*-----+
| Values for userNameAuthorities in dsmInitEx for future use |
+-----*/
#define DSM_USERAUTH_NONE ((dsInt16_t)0x0000)
#define DSM_USERAUTH_ACCESS ((dsInt16_t)0x0001)
#define DSM_USERAUTH_OWNER ((dsInt16_t)0x0002)
#define DSM_USERAUTH_POLICY ((dsInt16_t)0x0004)
#define DSM_USERAUTH_SYSTEM ((dsInt16_t)0x0008)

/*-----+
| Values for encryptionType on dsmEndSendObjEx, queryResp |
+-----*/
#define DSM_ENCRYPT_NO ((dsUInt8_t)0x00)
#define DSM_ENCRYPT_USER ((dsUInt8_t)0x01)
#define DSM_ENCRYPT_CLIENTENCRKEY ((dsUInt8_t)0x02)
#define DSM_ENCRYPT_DES_56BIT ((dsUInt8_t)0x04)
#define DSM_ENCRYPT_AES_128BIT ((dsUInt8_t)0x08)
#define DSM_ENCRYPT_AES_256BIT ((dsUInt8_t)0x10)

/*-----+
| Definitions for mediaClass field. |
+-----*/
/*
 * The following constants define a hierarchy of media access classes.
 * Lower numbers indicate media which can supply faster access to data.
 */

/* Fixed: represents the class of on-line, fixed media (such as
hard disks). */
#define MEDIA_FIXED 0x10

/* Library: represents the class of mountable media accessible
through a mechanical mounting device. */
#define MEDIA_LIBRARY 0x20

/* future use */
#define MEDIA_NETWORK 0x30

/* future use */
#define MEDIA_SHELF 0x40

/* future use */
#define MEDIA_OFFSITE 0x50

/* future use */
#define MEDIA_UNAVAILABLE 0xF0

/*-----+
| Type definition for partial object data for dsmBeginGetData() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion; /* Structure version */
    dsStruct64_t partialObjOffset; /* offset into object to begin reading*/
    dsStruct64_t partialObjLength; /* amount of object to read */
} PartialObjData; /* partial object data */

#define PartialObjDataVersion 1 /*

```



```

/*-----+
| Type definition for date structure |
+-----*/
typedef struct
{
    dsUInt16_t    year;          /* year, 16-bit integer (e.g., 1990) */
    dsUInt8_t     month;         /* month, 8-bit integer (1 - 12)    */
    dsUInt8_t     day;          /* day. 8-bit integer (1 - 31)     */
    dsUInt8_t     hour;         /* hour, 8-bit integer (0 - 23)    */
    dsUInt8_t     minute;       /* minute, 8-bit integer (0 - 59)  */
    dsUInt8_t     second;       /* second, b-bit integer (0 - 59)  */
}dsmDate ;

/*-----+
| Type definition for Object ID on dsmGetObj() and in dsmGetList structure|
+-----*/
typedef dsStruct64_t  ObjID ;

/*-----+
| Type definition for dsmQueryBuff on dsmBeginQuery() |
+-----*/
typedef void dsmQueryBuff ;

/*-----+
| Type definition for dsmGetType parameter on dsmBeginGetData() |
+-----*/
typedef enum
{
    gtBackup = 0x00,          /* Backup processing type    */
    gtArchive          /* Archive processing type    */
} dsmGetType ;

/*-----+
| Type definition for dsmQueryType parameter on dsmBeginQuery() |
+-----*/
typedef enum
{
    qtArchive = 0x00,        /* Archive query type        */
    qtBackup,              /* Backup query type        */
    qtBackupActive,       /* Fast query for active backup files */
    qtFilespace,         /* Filespace query type    */
    qtMC,                /* Mgmt. class query type  */
    qtReserved1,        /* future use              */
    qtReserved2,        /* future use              */
    qtReserved3,        /* future use              */
    qtReserved4,        /* future use              */
    qtBackupGroups,     /* group leaders in a specific fs */
    qtOpenGroups,       /* Open groups in a specific fs */
    qtReserved5,        /* future use              */
    qtProxyNodeAuth,    /* nodes that his node can proxy to */
    qtProxyNodePeer,    /* Peer nodes with the same target */
    qtReserved6,        /* future use              */
    qtReserved7,        /* future use              */
    qtReserved8         /* future use              */
}dsmQueryType ;

/*-----+
| Type definition sendType parameter on dsmBindMC() and dsmSendObj() |
+-----*/
typedef enum
{
    stBackup = 0x00,          /* Backup processing type    */
    stArchive,              /* Archive processing type    */
    stBackupMountWait,      /* Backup processing with mountwait on */
    stArchiveMountWait     /* Archive processing with mountwait on */
}dsmSendType ;

/*-----+
| Type definition for delType parameter on dsmDeleteObj() |
+-----*/
typedef enum
{
    dtArchive = 0x00,        /* Archive delete type    */
    dtBackup,              /* Backup delete (deactivate) type */
    dtBackupID            /* Backup delete (remove) type */
}dsmDelType ;

```

```

/*-----+
| Type definition sendType parameter on dsmSetAccess() |
+-----*/
typedef enum
{
    atBackup = 0x00,                /* Backup processing type */
    atArchive                       /* Archive processing type */
}dsmAccessType;

/*-----+
| Type definition for API Version on dsmInit() and dsmQueryApiVersion() |
+-----*/
typedef struct
{
    dsUInt16_t version;             /* API version */
    dsUInt16_t release;            /* API release */
    dsUInt16_t level;              /* API level */
}dsmApiVersion;

/*-----+
| Type definition for API Version on dsmInit() and dsmQueryApiVersion() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion;          /* Structure version */
    dsUInt16_t version;           /* API version */
    dsUInt16_t release;           /* API release */
    dsUInt16_t level;             /* API level */
    dsUInt16_t subLevel;          /* API sub level */
    dsmBool_t unicode;           /* API unicode? */
}dsmApiVersionEx;

#define apiVersionExVer    2

/*-----+
| Type definition for Application Version on dsmInit() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion;          /* Structure version */
    dsUInt16_t applicationVersion; /* application version number */
    dsUInt16_t applicationRelease; /* application release number */
    dsUInt16_t applicationLevel;   /* application level number */
    dsUInt16_t applicationSubLevel; /* application sub level number */
} dsmAppVersion;

#define appVersionVer    1

/*-----+
| Type definition for object name used on BindMC, Send, Delete, Query |
+-----*/
typedef struct S_dsmObjName
{
    char fs[DSM_MAX_FSNAME_LENGTH + 1]; /* Filespace name */
    char hl[DSM_MAX_HL_LENGTH + 1];     /* High level name */
    char ll[DSM_MAX_LL_LENGTH + 1];     /* Low level name */
    dsUInt8_t objType;                   /* for object type values, see defines above */
}dsmObjName;

/*-----+
| Type definition for Backup delete info on dsmDeleteObj() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion;             /* structure version */
    dsmObjName *objNameP;             /* object name */
    dsUInt32_t copyGroup;             /* copy group */
}delBack ;

#define delBackVersion    1

/*-----+
| Type definition for Archive delete info on dsmDeleteObj() |
+-----*/

```

```

typedef struct
{
    dsUInt16_t      stVersion ;                /* structure version */
    dsStruct64_t    objId ;                    /* object ID */
}delArch ;

#define delArchVersion 1

/*-----+
| Type definition for Backup ID delete info on dsmDeleteObj() |
+-----*/
typedef struct
{
    dsUInt16_t      stVersion ;                /* structure version */
    dsStruct64_t    objId ;                    /* object ID */
}delBackID;

#define delBackIDVersion 1

/*-----+
| Type definition for delete info on dsmDeleteObj() |
+-----*/
typedef union
{
    delBack  backInfo ;
    delArch  archInfo ;
    delBackID backIDInfo ;
}dsmDelInfo ;

/*-----+
| Type definition for Object Attribute parameter on dsmSendObj() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion; /* Structure version */
    char owner[DSM_MAX_OWNER_LENGTH + 1]; /* object owner */
    dsStruct64_t sizeEstimate; /* Size estimate in bytes of the object */
    dsmBool_t objCompressed; /* Is object already compressed? */
    dsUInt16_t objInfoLength; /* length of object-dependent info */
    char *objInfo; /* object-dependent info */
    char *mcNameP; /* mgmnt class name for override */
    dsmBool_t disableDeduplication; /* force no dedup for this object */
    dsmBool_t useExtObjInfo; /* use ext obj info up to 1536 */
}ObjAttr;

#define ObjAttrVersion 4

/*-----+
| Type definition for mcBindKey returned on dsmBindMC() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion; /* structure version */
    char mcName[DSM_MAX_MC_NAME_LENGTH + 1];
    /* Name of mc bound to object. */
    dsmBool_t backup_cg_exists; /* True/false */
    dsmBool_t archive_cg_exists; /* True/false */
    char backup_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
    /* Backup copy dest. name */
    char archive_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
    /* Arch copy dest.name */
}mcBindKey;

#define mcBindKeyVersion 1

/*-----+
| Type definition for object list on dsmBeginGetData() |
+-----*/
typedef struct
{
    dsUInt16_t stVersion ; /* structure version */
    dsUInt32_t numObjId ; /* number of object IDs in the list */
    ObjID *objId ; /* list of object IDs to restore*/
    PartialObjData *partialObjData; /*list of partial obj data info */

```

```

}dsmGetList ;

#define dsmGetListVersion 2 /* default if not using Partial Obj data */
#define dsmGetListPORVersion 3 /* version if using Partial Obj data */

/*-----+
| Type definition for DataBlk used to Get or Send data |
+-----*/
typedef struct
{
    dsUInt16_t stVersion ; /* structure version */
    dsUInt32_t bufferLen; /* Length of buffer passed below */
    dsUInt32_t numBytes; /* Actual number of bytes read from */
    /* or written to the buffer */
    char *bufferPtr; /* Data buffer */
    dsUInt32_t numBytesCompressed; /* on send actual bytes compressed */
    dsUInt16_t reserved; /* for future use */
}DataBlk;

#define DataBlkVersion 3

/*-----+
| Type definition for Mgmt Class queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct S_qryMCData
{
    dsUInt16_t stVersion; /* structure version */
    char *mcName; /* Mgmt class name */
    /* single name to get one or empty string to get all*/
    dsmBool_t mcDetail; /* Want details or not? */
}qryMCData;

#define qryMCDataVersion 1

/*=== values for RETINIT ===*/
#define ARCH_RETINIT_CREATE 0
#define ARCH_RETINIT_EVENT 1

/*-----+
| Type definition for Archive Copy Group details on Query MC response |
+-----*/
typedef struct S_archDetailCG
{
    char cgName[DSM_MAX_CG_NAME_LENGTH + 1]; /* Copy group name */
    dsUInt16_t frequency; /* Copy (archive) frequency */
    dsUInt16_t retainVers; /* Retain version */
    dsUInt8_t copySer; /* for copy serialization values, see defines */
    dsUInt8_t copyMode; /* for copy mode values, see defines above */
    char destName[DSM_MAX_CG_DEST_LENGTH + 1]; /* Copy dest name */
    dsmBool_t bLanFreeDest; /* Destination has lan free path? */
    dsmBool_t reserved; /* Not currently used */
    dsUInt8_t retainInit; /* possible values see above */
    dsUInt16_t retainMin; /* if retInit is EVENT num of days */
    dsmBool_t bDeduplicate; /* destination has dedup enabled */
}archDetailCG;

/*-----+
| Type definition for Backup Copy Group details on Query MC response |
+-----*/
typedef struct S_backupDetailCG
{
    char cgName[DSM_MAX_CG_NAME_LENGTH + 1]; /* Copy group name */
    dsUInt16_t frequency; /* Backup frequency */
    dsUInt16_t verDataExst; /* Versions data exists */
    dsUInt16_t verDataDltd; /* Versions data deleted */
    dsUInt16_t retXtraVers; /* Retain extra versions */
    dsUInt16_t retOnlyVers; /* Retain only versions */
    dsUInt8_t copySer; /* for copy serialization values, see defines */
    dsUInt8_t copyMode; /* for copy mode values, see defines above */
    char destName[DSM_MAX_CG_DEST_LENGTH + 1]; /* Copy dest name */
    dsmBool_t bLanFreeDest; /* Destination has lan free path? */
    dsmBool_t reserved; /* Not currently used */
    dsmBool_t bDeduplicate; /* destination has dedup enabled */
}backupDetailCG;

```

```

/*-----+
| Type definition for Query Mgmt Class detail response on dsmGetNextQObj() |
+-----*/
typedef struct S_qryRespMCDetailData
{
    dsUInt16_t      stVersion;          /* structure version */
    char            mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    char            mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /*mc description */
    archDetailCG    archDet;           /* Archive copy group detail */
    backupDetailCG  backupDet;         /* Backup copy group detail */
}qryRespMCDetailData;

#define qryRespMCDetailDataVersion 4

/*-----+
| Type definition for Query Mgmt Class summary response on dsmGetNextQObj() |
+-----*/
typedef struct S_qryRespMCData
{
    dsUInt16_t      stVersion;          /* structure version */
    char            mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    char            mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /* mc description */
}qryRespMCData;

#define qryRespMCDataVersion 1

/*-----+
| Type definition for Archive queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct S_qryArchiveData
{
    dsUInt16_t      stVersion;          /* structure version */
    dsmObjName      *objName;          /* Full dsm name of object */
    char            *owner;            /* owner name */
    /* for maximum date boundaries, see defines above */
    dsmDate          insDateLowerBound; /* low bound archive insert date */
    dsmDate          insDateUpperBound; /* hi bound archive insert date */
    dsmDate          expDateLowerBound; /* low bound expiration date */
    dsmDate          expDateUpperBound; /* hi bound expiration date */
    char            *descr;            /* archive description */
} qryArchiveData;

#define qryArchiveDataVersion 1

/*=== values for retentionInitiated field ===*/
#define DSM_ARCH_RETINIT_UNKNOWN 0 /* ret init is unknown (down-level srv) */
#define DSM_ARCH_RETINIT_STARTED 1 /* retention clock is started */
#define DSM_ARCH_RETINIT_PENDING 2 /* retention clock is not started */

/*=== Values for objHeld ===*/
#define DSM_ARCH_HELD_UNKNOWN 0 /* unknown hold status (down-level srv) */
#define DSM_ARCH_HELD_FALSE 1 /* object is NOT in a delete hold state */
#define DSM_ARCH_HELD_TRUE 2 /* object is in a delete hold state */

/*-----+
| Type definition for Query Archive response on dsmGetNextQObj() |
+-----*/
typedef struct S_qryRespArchiveData
{
    dsUInt16_t      stVersion;          /* structure version */
    dsmObjName      objName;           /* Filespace name qualifier */
    dsUInt32_t      copyGroup;         /* copy group number */
    char            mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    char            owner[DSM_MAX_OWNER_LENGTH + 1]; /* owner name */
    dsStruct64_t    objId;             /* Unique copy id */
    dsStruct64_t    reserved;          /* backward compatability */
    dsUInt8_t       mediaClass;        /* media access class */
    dsmDate          insDate;          /* archive insertion date */
    dsmDate          expDate;          /* expiration date for object */
    char            descr[DSM_MAX_DESCR_LENGTH + 1]; /* archive description */
    dsUInt16_t      objInfolen;        /* length of object-dependent info*/
    char            reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
}

```

```

    dsUint160_t    restoreOrderExt; /* restore order */
    dsStruct64_t   sizeEstimate; /* size estimate stored by user*/
    dsUint8_t      compressType; /* Compression flag*/
    dsUint8_t      retentionInitiated; /* object waiting on retention event*/
    dsUint8_t      objHeld; /*object is on retention "hold" see values above*/
    dsUint8_t      encryptionType; /* type of encryption */
    dsmBool_t      clientDeduplicated; /* obj deduplicated by API*/
    char           objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
    char           compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1]; /* compression algorithm name */
}qryRespArchiveData;

#define qryRespArchiveDataVersion 7

/*-----+
| Type definition for Archive sendBuff parameter on dsmSendObj() |
+-----*/
typedef struct S_sndArchiveData
{
    dsUint16_t      stVersion; /* structure version */
    char            *descr; /* archive description */
}sndArchiveData;

#define sndArchiveDataVersion 1

/*-----+
| Type definition for Backup queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct S_qryBackupData
{
    dsUint16_t      stVersion; /* structure version */
    dsmObjName      *objName; /* full dsm name of object */
    char            *owner; /* owner name */
    dsUint8_t       objState; /* object state selector */
    dsmDate         pitDate; /* Date value for point in time restore */
                    /* for possible values, see defines above */
}qryBackupData;

#define qryBackupDataVersion 2

typedef struct
{
    dsUint8_t       reserved1;
    dsStruct64_t    reserved2;
} reservedInfo_t; /* for future use */

/*-----+
| Type definition for Query Backup response on dsmGetNextQObj() |
+-----*/
typedef struct S_qryRespBackupData
{
    dsUint16_t      stVersion; /* structure version */
    dsmObjName      objName; /* full dsm name of object */
    dsUint32_t      copyGroup; /* copy group number */
    char            mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    char            owner[DSM_MAX_OWNER_LENGTH + 1]; /* owner name */
    dsStruct64_t    objId; /* Unique object id */
    dsStruct64_t    reserved; /* backward compatability */
    dsUint8_t       mediaClass; /* media access class */
    dsUint8_t       objState; /* Obj state, active, etc. */
    dsmDate         insDate; /* backup insertion date */
    dsmDate         expDate; /* expiration date for object */
    dsUint16_t      objInfolen; /* length of object-dependent info*/
    char            reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
    dsUint160_t     restoreOrderExt; /* restore order */
    dsStruct64_t    sizeEstimate; /* size estimate stored by user */
    dsStruct64_t    baseObjId;
    dsUint16_t      baseObjInfolen; /* length of base object-dependent info*/
    dsUint8_t       baseObjInfo[DSM_MAX_OBJINFO_LENGTH]; /* base object-dependent info */
    dsUint160_t     baseRestoreOrder; /* restore order */
    dsUint32_t      fsID;
    dsUint8_t       compressType;
    dsmBool_t       isGroupLeader;
    dsmBool_t       isOpenGroup;
    dsUint8_t       reserved1; /* for future use */
    dsmBool_t       reserved2; /* for future use */
    dsUint16_t      reserved3; /* for future use */
    reservedInfo_t  *reserved4; /* for future use */
}

```

```

    dsUInt8_t      encryptionType;                /* type of encryption */
    dsmBool_t      clientDeduplicated;            /* obj deduplicated by API */
    char           objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
    char           compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1]; /* compression algorithm name */
}qryRespBackupData;

#define qryRespBackupDataVersion 8

/*-----+
| Type definition for Active Backup queryBuffer on dsmBeginQuery()
|
| Notes: For the active backup query, only the fs (filesystem) and objType
|        fields of objName need be set. objType can only be set to
|        DSM_OBJ_FILE or DSM_OBJ_DIRECTORY. DSM_OBJ_ANY_TYPE will not
|        find a match on the query.
+-----*/
typedef struct S_qryABackupData
{
    dsUInt16_t     stVersion;                      /* structure version */
    dsmObjName     *objName;                      /* Only fs and objtype used */
}qryABackupData;

#define qryABackupDataVersion 1

/*-----+
| Type definition for Query Active Backup response on dsmGetNextQObj()
+-----*/
typedef struct S_qryARespBackupData
{
    dsUInt16_t     stVersion;                      /* structure version */
    dsmObjName     objName;                      /* full dsm name of object */
    dsUInt32_t     copyGroup;                    /* copy group number */
    char           mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /*management class name*/
    char           owner[DSM_MAX_OWNER_LENGTH + 1]; /* owner name */
    dsmDate        insDate;                      /* backup insertion date */
    dsUInt16_t     objInfoLen;                   /* length of object-dependent info*/
    char           reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
    char           objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
}qryARespBackupData;

#define qryARespBackupDataVersion 2

/*-----+
| Type definition for Backup queryBuffer on dsmBeginQuery()
+-----*/
typedef struct qryBackupGroups
{
    dsUInt16_t     stVersion;                      /* structure version */
    dsUInt8_t      groupType;
    char           *fsName;
    char           *owner;
    dsStruct64_t   groupLeaderObjId;
    dsUInt8_t      objType;
    dsmBool_t      noRestoreOrder;
    dsmBool_t      noGroupInfo;
    char           *hl;
}qryBackupGroups;

#define qryBackupGroupsVersion 3

/*-----+
| Type definition for proxynode queryBuffer on dsmBeginQuery()
+-----*/
typedef struct qryProxyNodeData
{
    dsUInt16_t     stVersion;                      /* structure version */
    char           *targetNodeName;              /* target node name */
}qryProxyNodeData;

#define qryProxyNodeDataVersion 1

/*-----+
| Type definition for qryRespProxyNodeData parameter used on dsmGetNextQObj()
+-----*/

typedef struct

```

```

{
    dsUInt16_t      stVersion ;                /* structure version */
    char            targetNodeName[DSM_MAX_ID_LENGTH+1]; /* target node name */
    char            peerNodeName[DSM_MAX_ID_LENGTH+1]; /* Peer node name */
    char            hlAddress[DSM_MAX_ID_LENGTH+1];     /* peer hlAddress */
    char            llAddress[DSM_MAX_ID_LENGTH+1];     /* peer hlAddress */
}qryRespProxyNodeData;

#define qryRespProxyNodeDataVersion 1

/*-----+
| Type definition for WINNT and OS/2 Filespace attributes |
+-----*/
typedef struct
{
    char            driveLetter ;              /* drive letter for filespace */
    dsUInt16_t      fsInfoLength;             /* fsInfo length used */
    char            fsInfo[DSM_MAX_FSINFO_LENGTH]; /* caller-determined data */
}dsmDosFSAttrib ;

/*-----+
| Type definition for UNIX Filespace attributes |
+-----*/
typedef struct
{
    dsUInt16_t      fsInfoLength;             /* fsInfo length used */
    char            fsInfo[DSM_MAX_FSINFO_LENGTH]; /* caller-determined data */
}dsmUnixFSAttrib ;

/*-----+
| Type definition for NetWare Filespace attributes |
+-----*/
typedef dsmUnixFSAttrib dsmNetwareFSAttrib;

/*-----+
| Type definition for Filespace attributes on all Filespace calls |
+-----*/
typedef union
{
    dsmNetwareFSAttrib netwareFSAttr;
    dsmUnixFSAttrib    unixFSAttr ;
    dsmDosFSAttrib     dosFSAttr ;
}dsmFSAttr ;

/*-----+
| Type definition for fsUpd parameter on dsmUpdateFS() |
+-----*/
typedef struct S_dsmFSUpd
{
    dsUInt16_t      stVersion ;                /* structure version */
    char            *fsType ;                  /* filespace type */
    dsStruct64_t    occupancy ;                /* occupancy estimate */
    dsStruct64_t    capacity ;                 /* capacity estimate */
    dsmFSAttr       fsAttr ;                  /* platform specific attributes */
}dsmFSUpd ;

#define dsmFSUpdVersion 1

/*-----+
| Type definition for Filespace queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct S_qryFSData
{
    dsUInt16_t      stVersion;                /* structure version */
    char            *fsName;                  /* File space name */
}qryFSData;

#define qryFSDataVersion 1

/*-----+
| Type definition for Query Filespace response on dsmGetNextQObj() |
+-----*/
typedef struct S_qryRespFSData
{
    dsUInt16_t      stVersion;                /* structure version */
    char            fsName[DSM_MAX_FSNAME_LENGTH + 1]; /* Filespace name */
}

```



```

char          fsType[DSM_MAX_FSTYPE_LENGTH + 1] ;          /* Filespace type */
dsStruct64_t  occupancy;                                   /* Occupancy est. in bytes.*/
dsStruct64_t  capacity;                                   /* Capacity est. in bytes.*/
dsmFSAttr     fsAttr ;                                   /* platform specific attributes */
dsmDate       backStartDate;                             /* start backup date      */
dsmDate       backCompleteDate;                         /* end backup Date       */
dsmDate       reserved1;                                /* For future use        */
dsmDate       lastReplStartDate;                        /* The last time replication was started */
dsmDate       lastReplCmpltDate;                       /* The last time replication completed */
/* (could have had a failure, */
/* but it still completes) */
dsmDate       lastBackOpDateFromServer;                /* The last store time stamp the client */
/* saved on the server */
dsmDate       lastArchOpDateFromServer;                /* The last store time stamp the client */
/* saved on the server */
dsmDate       lastSpMgOpDateFromServer;                /* The last store time stamp the client */
/* saved on the server */
dsmDate       lastBackOpDateFromLocal;                 /* The last store time stamp the client */
/* saved on the Local */
dsmDate       lastArchOpDateFromLocal;                 /* The last store time stamp the client */
/* saved on the Local */
dsmDate       lastSpMgOpDateFromLocal;                 /* The last store time stamp the client */
/* saved on the Local */
dsInt32_t     failOverWriteDelay;                      /* Minutes for client to wait before allowed */
/* to store to this Repl svr, Specail codes: */
/* NO_ACCESS (-1), ACCESS_RDONLY (-2) */

}qryRespFSData;

#define qryRespFSDataVersion 4

/*-----+
| Type definition for regFilespace parameter on dsmRegisterFS()
+-----*/
typedef struct S_regFSData
{
    dsUInt16_t    stVersion;                            /* structure version */
    char          *fsName;                              /* Filespace name */
    char          *fsType;                              /* Filespace type */
    dsStruct64_t  occupancy;                            /* Occupancy est. in bytes. */
    dsStruct64_t  capacity;                            /* Capacity est. in bytes. */
    dsmFSAttr     fsAttr ;                            /* platform specific attributes */
}regFSData;

#define regFSDataVersion 1

/*-----+
| Type definition for dedupType used in apisessInfo
+-----*/
typedef enum
{
    dedupServerOnly= 0x00,                            /* dedup only done on server */
    dedupClientOrServer                               /* dedup can be done on client or server */
}dsmDedupType ;

/*-----+
| Type definition for fail over configuration and status
+-----*/
typedef enum
{
    failOvrNotConfigured = 0x00,
    failOvrConfigured,
    failOvrConnectedToReplServer
}dsmFailOvrCfgType ;

/*-----+
| Type definition for session info response on dsmQuerySessionInfo()
+-----*/
typedef struct
{
    dsUInt16_t    stVersion;                            /* Structure version */
    /*-----+
    /* Server information
    +-----*/
    char          serverHost[DSM_MAX_SERVERNAME_LENGTH+1];
    /* Network host name of DSM server */
    dsUInt16_t    serverPort;                            /* Server comm port on host */
    dsmDate       serverDate;                            /* Server's date/time */

```

```

char          serverType[DSM_MAX_SERVERTYPE_LENGTH+1];
              /* Server's execution platform          */
dsUint16_t    serverVer;          /* Server's version number          */
dsUint16_t    serverRel;         /* Server's release number          */
dsUint16_t    serverLev;         /* Server's level number            */
dsUint16_t    serverSubLev;      /* Server's sublevel number         */
/*-----*/
/*          Client Defaults          */
/*-----*/
char          nodeType[DSM_MAX_PLATFORM_LENGTH+1]; /*node/application type*/
char          fsdelim;           /* File space delimiter             */
char          hldelim;           /* Delimiter betw highlev & lowlev */
dsUint8_t     compression;      /* Compression flag                 */
dsUint8_t     archDel;          /* Archive delete permission        */
dsUint8_t     backDel;          /* Backup delete permission         */
dsUint32_t    maxBytesPerTxn;    /* for future use                   */
dsUint16_t    maxObjPerTxn;     /* The max objects allowed in a txn */
/*-----*/
/*          Session Information      */
/*-----*/
char          id[DSM_MAX_ID_LENGTH+1]; /* Sign-in id node name            */
char          owner[DSM_MAX_OWNER_LENGTH+1]; /* Sign-in owner                    */
              /* (for multi-user platforms)     */
char          confFile[DSM_PATH_MAX + DSM_NAME_MAX +1];
              /* len is platform dep            */
              /* dsInit name of appl config file */
dsUint8_t     opNoTrace;         /* dsInit option - NoTrace = 1     */
/*-----*/
/*          Policy Data              */
/*-----*/
char          domainName[DSM_MAX_DOMAIN_LENGTH+1]; /* Domain name                      */
char          policySetName[DSM_MAX_PS_NAME_LENGTH+1];
              /* Active policy set name          */
dsmDate       polActDate;        /* Policy set activation date       */
char          dfltMCName[DSM_MAX_MC_NAME_LENGTH+1]; /* Default Mgmt Class              */
dsUint16_t    gpBackRetn;       /* Grace-period backup retention    */
dsUint16_t    gpArchRetn;      /* Grace-period archive retention   */
char          adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* adsm server name */
dsmBool_t     archiveRetentionProtection; /* is server Retention protection enabled */
dsStruct64_t  maxBytesPerTxn_64; /* for future use                   */
dsmBool_t     lanFreeEnabled;    /* lan free option is set          */
dsmDedupType  dedupType;        /* server or clientOrServer        */
char          accessNode[DSM_MAX_ID_LENGTH+1]; /* as node node name                */
/*-----*/
/*          Replication and fail over information      */
/*-----*/
dsmFailOvrCfgType failOverCfgType; /* status of fail over */
char          replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* repl server name */
char          homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* home server name */
char          replServerHost[DSM_MAX_SERVERNAME_LENGTH+1]; /* Network host name of DSM server */
dsInt32_t     replServerPort;     /* Server comm port on host        */

}ApiSessInfo;

#define ApiSessInfoVersion 6

/*-----+
| Type definition for Query options response on dsmQueryCliOptions() |
| and dsmQuerySessOptions() |
+-----*/

typedef struct
{
    char          dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX +1];
    char          dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
    char          serverName[DSM_MAX_SERVERNAME_LENGTH+1];
    dsInt16_t     commMethod;
    char          serverAddress[DSM_MAX_SERVER_ADDRESS];
    char          nodeName[DSM_MAX_NODE_LENGTH+1];
    dsmBool_t     compression;
    dsmBool_t     compressalways;
    dsmBool_t     passwordAccess;
}optStruct ;

```

```

/*-----+
| Type definition for LogType used in logInfo                                     |
+-----*/
typedef enum
{
    logServer = 0x00,          /* log msg only to server      */
    logLocal,                 /* log msg only to local error log */
    logBoth,                  /* log msg to server and to local error log */
    logNone
}dsmLogType ;

/*-----+
| Type definition for logInfo parameter used on dsmLogEvent()                 |
+-----*/

typedef struct
{
    char          *message;    /* text of message to be logged */
    dsmLogType    logType;    /* log type : local, server, both */
}logInfo;

/*-----+
| Type definition for qryRespAccessData parameter used on dsmQueryAccess()    |
+-----*/

typedef struct
{
    dsUint16_t    stVersion ;          /* structure version      */
    char          node[DSM_MAX_ID_LENGTH+1]; /* node name            */
    char          owner[DSM_MAX_OWNER_LENGTH+1]; /* owner                */
    dsmObjName    objName ;           /* object name           */
    dsmAccessType accessType;        /* archive or backup     */
    dsUint32_t    ruleNumber ;        /* Access rule id       */
}qryRespAccessData;

#define qryRespAccessDataVersion 1

/*-----+
| Type definition for envSetUp parameter on dsmSetUp()                       |
+-----*/
typedef struct S_envSetUp
{
    dsUint16_t    stVersion;          /* structure version      */
    char          dsmdir[DSM_PATH_MAX + DSM_NAME_MAX +1];
    char          dsmdirConfig[DSM_PATH_MAX + DSM_NAME_MAX +1];
    char          dsmdirLog[DSM_PATH_MAX + DSM_NAME_MAX +1];
    char          **argv; /* for executables name argv[0] */
    char          logName[DSM_NAME_MAX +1];
    dsmBool_t     reserved1; /* for future use */
    dsmBool_t     reserved2; /* for future use */
}envSetUp;

#define envSetUpVersion 4

/*-----+
| Type definition for dsmInitExIn_t                                         |
+-----*/
typedef struct dsmInitExIn_t
{
    dsUint16_t    stVersion;          /* structure version      */
    dsmApiVersionEx *apiVersionExP;
    char          *clientNodeNameP;
    char          *clientOwnerNameP;
    char          *clientPasswordP;
    char          *userNameP;
    char          *userPasswordP;
    char          *applicationTypeP;
    char          *configfile;
    char          *options;
    char          dirDelimiter;
    dsmBool_t     useUnicode;
    dsmBool_t     bCrossPlatform;
    dsmBool_t     bService;
    dsmBool_t     bEncryptKeyEnabled;
    char          *encryptionPasswordP;
    dsmBool_t     useTsmBuffers;
    dsUint8_t     numTsmBuffers;
}

```

```

    dsmAppVersion      *appVersionP;
}dsmInitExIn_t;

#define dsmInitExInVersion 5

/*-----+
| Type definition for dsmInitExOut_t
+-----*/
typedef struct dsmInitExOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsInt16_t       userNameAuthorities;
    dsInt16_t       infoRC;            /* error return code if encountered */
    char            adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1];
    dsUInt16_t      serverVer;         /* Server's version number */
    dsUInt16_t      serverRel;        /* Server's release number */
    dsUInt16_t      serverLev;        /* Server's level number */
    dsUInt16_t      serverSubLev;     /* Server's sublevel number */

    dsmBool_t       bIsFailOverMode; /* true if failover has occurred */
    char            replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* repl server name */
    char            homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* home server name */
}dsmInitExOut_t;

#define dsmInitExOutVersion 3

/*-----+
| Type definition for LogType used in logInfo
+-----*/
typedef enum
{
    logSevInfo = 0x00,      /* information ANE4991 */
    logSevWarning,         /* warning ANE4992 */
    logSevError,           /* Error ANE4993 */
    logSevSevere,          /* severe ANE4994 */
    logSevLicense,         /* License ANE4995 */
    logSevTryBuy           /* try Buy ANE4996 */
}dsmLogSeverity ;

/*-----+
| Type definition for dsmLogExIn_t
+-----*/
typedef struct dsmLogExIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsmLogSeverity  severity;
    char            appMsgID[8];
    dsmLogType      logType;           /* log type : local, server, both */
    char            *message;          /* text of message to be logged */
    char            appName[DSM_MAX_PLATFORM_LENGTH];
    char            osPlatform[DSM_MAX_PLATFORM_LENGTH];
    char            appVersion[DSM_MAX_PLATFORM_LENGTH];
}dsmLogExIn_t;

#define dsmLogExInVersion 2

/*-----+
| Type definition for dsmLogExOut_t
+-----*/
typedef struct dsmLogExOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
}dsmLogExOut_t;

#define dsmLogExOutVersion 1

/*-----+
| Type definition for dsmRenameIn_t
+-----*/
typedef struct dsmRenameIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsUInt32_t      dsmHandle;          /* handle for session */
    dsUInt8_t       repository;         /* Backup or Archive */
    dsmObjName      *objNameP ;        /* object name */
}

```

```

    char          newHl[DSM_MAX_HL_LENGTH + 1]; /* new High level name */
    char          newLl[DSM_MAX_LL_LENGTH + 1]; /* new Low level name */
    dsmBool_t     merge;                        /* merge into existing name*/
    ObjID         objId;                       /* objId for Archive */
}dsmRenameIn_t;

#define dsmRenameInVersion 1

/*-----+
| Type definition for dsmRenameOut_t
+-----*/
typedef struct dsmRenameOut_t
{
    dsUint16_t     stVersion;                  /* structure version */
}dsmRenameOut_t;

#define dsmRenameOutVersion 1

/*-----+
| Type definition for dsmEndSendObjExIn_t
+-----*/
typedef struct dsmEndSendObjExIn_t
{
    dsUint16_t     stVersion;                  /* structure version */
    dsUint32_t     dsmHandle;                 /* handle for session */
}dsmEndSendObjExIn_t;

#define dsmEndSendObjExInVersion 1

/*-----+
| Type definition for dsmEndSendObjExOut_t
+-----*/
typedef struct dsmEndSendObjExOut_t
{
    dsUint16_t     stVersion;                  /* structure version */
    dsStruct64_t   totalBytesSent;            /* total bytes read from app */
    dsmBool_t      objCompressed;             /* was object compressed */
    dsStruct64_t   totalCompressSize;         /* total size after compress */
    dsStruct64_t   totalLFBytesSent;         /* total bytes sent Lan Free */
    dsUint8_t      encryptionType;           /* type of encryption used */
    dsmBool_t      objDeduplicated;           /* was object processed for dist. data dedup */
    dsStruct64_t   totalDedupSize;           /* total size after de-dup */
}dsmEndSendObjExOut_t;

#define dsmEndSendObjExOutVersion 3

/*-----+
| Type definition for dsmGroupHandlerIn_t
+-----*/
typedef struct dsmGroupHandlerIn_t
{
    dsUint16_t     stVersion;                  /* structure version */
    dsUint32_t     dsmHandle;                 /* handle for session */
    dsUint8_t      groupType;                 /* Type of group */
    dsUint8_t      actionType;                /* Type of group operation */
    dsUint8_t      memberType;                /* Type of member: Leader or member */
    dsStruct64_t   leaderObjId;               /* OBJID of the groupleader when manipulating a member */
    char           *uniqueGroupTagP;          /* Unique group identifier */
    dsmObjName     *objNameP ;                /* group leader object name */
    dsmGetList     memberObjList;            /* list of objects to remove, assign */
}dsmGroupHandlerIn_t;

#define dsmGroupHandlerInVersion 1

/*-----+
| Type definition for dsmGroupHandlerExOut_t
+-----*/
typedef struct dsmGroupHandlerOut_t
{
    dsUint16_t     stVersion;                  /* structure version */
}dsmGroupHandlerOut_t;

#define dsmGroupHandlerOutVersion 1

/*-----+
| Type definition for dsmEndTxnExIn_t
+-----*/
typedef struct dsmEndTxnExIn_t

```

```

{
    dsUint16_t      stVersion;          /* structure version */
    dsUint32_t      dsmHandle;         /* handle for session */
    dsUint8_t       vote;
}dsmEndTxnExIn_t;

#define dsmEndTxnExInVersion 1

/*-----+
| Type definition for dsmEndTxnExOut_t
+-----*/
typedef struct dsmEndTxnExOut_t
{
    dsUint16_t      stVersion;          /* structure version */
    dsUint16_t      reason;             /* reason code */
    dsStruct64_t    groupLeaderObjId;   /* groupLeader obj id returned on */
                                         /* DSM_ACTION_OPEN */
    dsUint8_t       reserved1;         /* future use */
    dsUint16_t      reserved2;         /* future use */
}dsmEndTxnExOut_t;

#define dsmEndTxnExOutVersion 1

/*-----+
| Type definition for dsmEndGetDataExIn_t
+-----*/
typedef struct dsmEndGetDataExIn_t
{
    dsUint16_t      stVersion;          /* structure version */
    dsUint32_t      dsmHandle;         /* handle for session */
}dsmEndGetDataExIn_t;

#define dsmEndGetDataExInVersion 1

/*-----+
| Type definition for dsmEndGetDataExOut_t
+-----*/
typedef struct dsmEndGetDataExOut_t
{
    dsUint16_t      stVersion;          /* structure version */
    dsUint16_t      reason;             /* reason code */
    dsStruct64_t    totalLFBytesRecv;   /* total lan free bytes recieved */
}dsmEndGetDataExOut_t;

#define dsmEndGetDataExOutVersion 1

/*-----+
| Type definition for object list on dsmRetentionEvent()
+-----*/
typedef struct dsmObjList
{
    dsUint16_t      stVersion;          /* structure version */
    dsUint32_t      numObjId;          /* number of object IDs in the list */
    ObjID           *objId;           /* list of object IDs to signal */
}dsmObjList_t ;

#define dsmObjlistVersion 1

/*-----+
| Type definition eventType used on dsmRetentionEvent
+-----*/
typedef enum
{
    eventRetentionActivate = 0x00,     /* signal the server that the event has occurred */
    eventHoldObj,                     /* suspend delete/expire of the object */
    eventReleaseObj                    /* Resume normal delete/expire processing */
}dsmEventType_t;

/*-----+
| Type definition for on dsmRetentionEvent()
+-----*/
typedef struct dsmRetentionEventIn_t
{
    dsUint16_t      stVersion;          /* structure version */
    dsUint32_t      dsmHandle;         /* session Handle */
    dsmEventType_t  eventType;         /* Event type */
    dsmObjList_t    objList;          /* object ID */
}

```

```

}dsmRetentionEventIn_t;

#define dsmRetentionEventInVersion 1

/*-----+
| Type definition for on dsmRetentionEvent() |
+-----*/
typedef struct dsmRetentionEventOut_t
{
    dsUInt16_t      stVersion ;                /* structure version */
}dsmRetentionEventOut_t;

#define dsmRetentionEventOutVersion 1

/*-----+
| Type definition for on dsmRequestBuffer() |
+-----*/
typedef struct requestBufferIn_t
{
    dsUInt16_t      stVersion;                /* structure version */
    dsUInt32_t      dsmHandle;                /* session Handle */
}requestBufferIn_t;

#define requestBufferInVersion 1

/*-----+
| Type definition for on dsmRequestBuffer() |
+-----*/
typedef struct requestBufferOut_t
{
    dsUInt16_t      stVersion ;                /* structure version */
    dsUInt8_t       tsmBufferHandle;          /* handle to tsm Data buffer */
    char            *dataPtr;                 /* Address to write data to */
    dsUInt32_t      bufferLen;                /* Max length of data to be written */
}requestBufferOut_t;

#define requestBufferOutVersion 1

/*-----+
| Type definition for on dsmReleaseBuffer() |
+-----*/
typedef struct releaseBufferIn_t
{
    dsUInt16_t      stVersion;                /* structure version */
    dsUInt32_t      dsmHandle;                /* session Handle */
    dsUInt8_t       tsmBufferHandle;          /* handle to tsm Data buffer */
    char            *dataPtr;                 /* Address to write data to */
}releaseBufferIn_t;

#define releaseBufferInVersion 1

/*-----+
| Type definition for on dsmReleaseBuffer() |
+-----*/
typedef struct releaseBufferOut_t
{
    dsUInt16_t      stVersion ;                /* structure version */
}releaseBufferOut_t;

#define releaseBufferOutVersion 1

/*-----+
| Type definition for on dsmGetBufferData() |
+-----*/
typedef struct getBufferDataIn_t
{
    dsUInt16_t      stVersion;                /* structure version */
    dsUInt32_t      dsmHandle;                /* session Handle */
}getBufferDataIn_t;

#define getBufferDataInVersion 1

/*-----+
| Type definition for on dsmGetBufferData() |
+-----*/
typedef struct getBufferDataOut_t

```

```

{
    dsUInt16_t      stVersion ;                /* structure version */
    dsUInt8_t      tsmBufferHandle;          /* handle to tsm Data buffer */
    char           *dataPtr;                 /* Address of actual data to read */
    dsUInt32_t     numBytes;                 /* Actual number of bytes to read from dataPtr*/
}getBufferDataOut_t;

#define getBufferDataOutVersion 1

/*-----+
| Type definition for on dsmSendBufferData() |
+-----*/
typedef struct sendBufferDataIn_t
{
    dsUInt16_t      stVersion;                /* structure version */
    dsUInt32_t      dsmHandle;                /* session Handle */
    dsUInt8_t       tsmBufferHandle;         /* handle to tsm Data buffer */
    char           *dataPtr;                 /* Address of actual data to send */
    dsUInt32_t     numBytes;                 /* Actual number of bytes to send from dataPtr*/
}sendBufferDataIn_t;

#define sendBufferDataInVersion 1

/*-----+
| Type definition for on dsmSendBufferData() |
+-----*/
typedef struct sendBufferDataOut_t
{
    dsUInt16_t      stVersion ;                /* structure version */
}sendBufferDataOut_t;

#define sendBufferDataOutVersion 1

/*-----+
| Type definition for dsmUpdateObjExIn_t    |
+-----*/
typedef struct dsmUpdateObjExIn_t
{
    dsUInt16_t      stVersion;                /* structure version */
    dsUInt32_t      dsmHandle;                /* session Handle */
    dsmSendType     sendType;                 /* send type back/arch */
    char           *descrP;                   /* archive description */
    dsmObjName      *objNameP;               /* objName */
    ObjAttr         *objAttrPtr;             /* attribute */
    dsUInt32_t      objUpdAct;                /* update action */
    ObjID           archObjId;               /* objId for archive */
}dsmUpdateObjExIn_t;

#define dsmUpdateObjExInVersion 1

/*-----+
| Type definition for dsmUpdateObjExOut_t   |
+-----*/
typedef struct dsmUpdateObjExOut_t
{
    dsUInt16_t      stVersion;                /* structure version */
}dsmUpdateObjExOut_t;

#define dsmUpdateObjExOutVersion 1

#if ( _OPSYS_TYPE == DS_WINNT) && !defined( _WIN64)
#pragma pack()
#endif

#ifdef _MAC
#pragma options align=reset
#endif
#endif /* _H_DSMAPITD */

/*****
* Tivoli Storage Manager
* API Client Component
*
* (C) Copyright IBM Corporation 1993,2010
*****/

```



```

/*****
* Header File Name: tsmapi.h
*
* Environment: *****
*               ** This is a platform-independent source file **
*
*               *****
*
* Design Notes: This file contains basic data types and constants
*               includable by all client source files. The constants
*               within this file should be set properly for the
*               particular machine and operating system on which the
*               client software is to be run.
*
*               Platform specific definitions are included in dsmapi.h
*
* Descriptive-name: Definitions for Tivoli Storage manager API constants
*-----*/

#ifndef _H_TSMAPITD
#define _H_TSMAPITD

/*=== set the structure alignment to pack the structures ===*/
#if _OPSYS_TYPE == DS_WINNT
#define _WIN64
#pragma pack(8)
#else
#pragma pack(1)
#endif
#endif

#ifdef _MAC
#pragma options align = packed
#endif

/*=====
Win32 applications using the tsm interface must use the
-DUNICODE flag during compilation.
=====*/
#if _OPSYS_TYPE == DS_WINNT && !defined(DSMAPILIB)
#ifndef UNICODE
#error "Win32 applications using the TSM interface MUST be compiled with the -DUNICODE flag"
#endif
#endif

/*=====
Mac OS X applications using the tsm interface must use the
-DUNICODE flag during compilation.
=====*/
#if _OPSYS_TYPE == DS_MACOS && !defined(DSMAPILIB)
#ifndef UNICODE
#error "Mac OS X applications using the TSM interface MUST be compiled with the -DUNICODE flag"
#endif
#endif

/*-----+
| Type definition for dsmGetType parameter on tsmBeginGetData() |
+-----*/
typedef enum
{
    gtTsmBackup = 0x00,          /* Backup processing type */
    gtTsmArchive          /* Archive processing type */
} tsmGetType ;

/*-----+
| Type definition for dsmQueryType parameter on tsmBeginQuery() |
+-----*/
typedef enum
{
    qtTsmArchive = 0x00,          /* Archive query type */
    qtTsmBackup,                /* Backup query type */
    qtTsmBackupActive,          /* Fast query for active backup files */
    qtTsmFilespace,            /* Filespace query type */
    qtTsmMC,                    /* Mgmt. class query type */
    qtTsmReserved1,            /* future use */
}

```

```

    qtTsmReserved2,                /* future use */
    qtTsmReserved3,                /* future use */
    qtTsmReserved4,                /* future use */
    qtTsmBackupGroups,            /* All group leaders in a specific filespace */
    qtTsmOpenGroups,              /* All group members associated with a leader */
    qtTsmReserved5,                /* future use */
    qtTsmProxyNodeAuth,           /* nodes that this node can proxy to */
    qtTsmProxyNodePeer,           /* peer nodes under this target node */
    qtTsmReserved6,                /* future use */
    qtTsmReserved7,                /* future use */
    qtTsmReserved8                 /* future use */
} tsmQueryType ;

/*-----+
| Type definition sendType parameter on tsmBindMC() and tsmSendObj() |
+-----*/
typedef enum
{
    stTsmBackup = 0x00,             /* Backup processing type */
    stTsmArchive,                  /* Archive processing type */
    stTsmBackupMountWait,          /* Backup processing with mountwait on */
    stTsmArchiveMountWait         /* Archive processing with mountwait on */
} tsmSendType ;

/*-----+
| Type definition for delType parameter on tsmDeleteObj() |
+-----*/
typedef enum
{
    dtTsmArchive = 0x00,           /* Archive delete type */
    dtTsmBackup,                  /* Backup delete (deactivate) type */
    dtTsmBackupID                 /* Backup delete (remove) type */
} tsmDelType ;

/*-----+
| Type definition sendType parameter on tsmSetAccess() |
+-----*/
typedef enum
{
    atTsmBackup = 0x00,           /* Backup processing type */
    atTsmArchive                  /* Archive processing type */
} tsmAccessType;

/*-----+
| Type definition for Overwrite parameter on tsmSendObj() |
+-----*/
typedef enum
{
    owIGNORE = 0x00,
    owYES,
    owNO
} tsmOwType;

/*-----+
| Type definition for API Version on tsmInit() and tsmQueryApiVersion() |
+-----*/
typedef struct
{
    dsUint16_t stVersion;          /* Structure version */
    dsUint16_t version;           /* API version */
    dsUint16_t release;           /* API release */
    dsUint16_t level;             /* API level */
    dsUint16_t subLevel;          /* API sub level */
    dsMBool_t unicode;           /* API unicode? */
} tsmApiVersionEx;

#define tsmApiVersionExVer 2

/*-----+
| Type definition for Application Version on tsmInit() |
+-----*/
typedef struct
{
    dsUint16_t stVersion;          /* Structure version */
    dsUint16_t applicationVersion; /* application version number */
    dsUint16_t applicationRelease; /* application release number */
}

```

```

    dsUint16_t  applicationLevel;    /* application level number */
    dsUint16_t  applicationSubLevel; /* application sub level number */
} tsmAppVersion;

#define tsmAppVersionVer    1

/*-----+
| Type definition for object name used on BindMC, Send, Delete, Query |
+-----*/

typedef struct tsmObjName
{
    dsChar_t    fs[DSM_MAX_FSNAME_LENGTH + 1]; /* Filespace name */
    dsChar_t    hl[DSM_MAX_HL_LENGTH + 1];    /* High level name */
    dsChar_t    ll[DSM_MAX_LL_LENGTH + 1];    /* Low level name */
    dsUint8_t   objType; /* for object type values, see defines above */
    dsChar_t    dirDelimiter;
} tsmObjName;

/*-----+
| Type definition for Backup delete info on dsmDeleteObj() |
+-----*/

typedef struct tsmDelBack
{
    dsUint16_t   stVersion; /* structure version */
    tsmObjName   *objNameP; /* object name */
    dsUint32_t   copyGroup; /* copy group */
} tsmDelBack;

#define tsmDelBackVersion    1

/*-----+
| Type definition for Archive delete info on dsmDeleteObj() |
+-----*/

typedef struct
{
    dsUint16_t   stVersion; /* structure version */
    dsStruct64_t objId; /* object ID */
} tsmDelArch;

#define tsmDelArchVersion    1

/*-----+
| Type definition for Backup ID delete info on dsmDeleteObj() |
+-----*/

typedef struct
{
    dsUint16_t   stVersion; /* structure version */
    dsStruct64_t objId; /* object ID */
} tsmDelBackID;

#define tsmDelBackIDVersion    1

/*-----+
| Type definition for delete info on dsmDeleteObj() |
+-----*/

typedef union
{
    tsmDelBack   backInfo;
    tsmDelArch   archInfo;
    tsmDelBackID backIDInfo;
} tsmDelInfo;

/*-----+
| Type definition for Object Attribute parameter on dsmSendObj() |
+-----*/

typedef struct tsmObjAttr
{
    dsUint16_t   stVersion; /* Structure version */
    dsChar_t     owner[DSM_MAX_OWNER_LENGTH + 1]; /* object owner */
    dsStruct64_t sizeEstimate; /* Size estimate in bytes of the object */
    dsmBool_t    objCompressed; /* Is object already compressed? */
    dsUint16_t   objInfoLength; /* length of object-dependent info */
    char         *objInfo; /* object-dependent info byte buffer */
    dsChar_t     *mcNameP; /* mgmnt class name for override */
}

```

```

    tsmOwType    reserved1;                /* for future use */
    tsmOwType    reserved2;                /* for future use */
    dsmBool_t    disableDeduplication;     /* force no dedup for this object */
    dsmBool_t    useExtObjInfo;           /* use ext objinfo up to 1536 */
} tsmObjAttr;

#define tsmObjAttrVersion 5

/*-----+
| Type definition for mcBindKey returned on dsmBindMC() |
+-----*/
typedef struct tsmMcBindKey
{
    dsUInt16_t    stVersion;                /* structure version */
    dsChar_t      mcName[DSM_MAX_MC_NAME_LENGTH + 1];
    /* Name of mc bound to object. */
    dsmBool_t     backup_cg_exists;        /* True/false */
    dsmBool_t     archive_cg_exists;      /* True/false */
    dsChar_t      backup_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
    /* Backup copy dest. name */
    dsChar_t      archive_copy_dest[DSM_MAX_CG_DEST_LENGTH + 1];
    /* Arch copy dest.name */
} tsmMcBindKey;

#define tsmMcBindKeyVersion 1

/*-----+
| Type definition for Mgmt Class queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct tsmQryMCData
{
    dsUInt16_t    stVersion;                /* structure version */
    dsChar_t      *mcName;                  /* Mgmt class name */
    /* single name to get one or empty string to get all*/
    dsmBool_t     mcDetail;                 /* Want details or not? */
} tsmQryMCData;

#define tsmQryMCDataVersion 1

/*-----+
| Type definition for Archive Copy Group details on Query MC response |
+-----*/
typedef struct tsmArchDetailCG
{
    dsChar_t      cgName[DSM_MAX_CG_NAME_LENGTH + 1];    /* Copy group name */
    dsUInt16_t    frequency;                            /* Copy (archive) frequency */
    dsUInt16_t    retainVers;                           /* Retain version */
    dsUInt8_t     copySer;                               /* for copy serialization values, see defines */
    dsUInt8_t     copyMode;                             /* for copy mode values, see defines above */
    dsChar_t      destName[DSM_MAX_CG_DEST_LENGTH + 1];  /* Copy dest name */
    dsmBool_t     bLanFreeDest;                         /* Destination has lan free path? */
    dsmBool_t     reserved;                             /* Not currently used */
    dsUInt8_t     retainInit;                           /* possible values see dsmapi.h */
    dsUInt16_t    retainMin;                            /* if retInit is EVENT num of days */
    dsmBool_t     bDeduplicate;                        /* destination has dedup enabled */
} tsmArchDetailCG;

/*-----+
| Type definition for Backup Copy Group details on Query MC response |
+-----*/
typedef struct tsmBackupDetailCG
{
    dsChar_t      cgName[DSM_MAX_CG_NAME_LENGTH + 1];    /* Copy group name */
    dsUInt16_t    frequency;                            /* Backup frequency */
    dsUInt16_t    verDataExst;                          /* Versions data exists */
    dsUInt16_t    verDataDltd;                          /* Versions data deleted */
    dsUInt16_t    retXtraVers;                          /* Retain extra versions */
    dsUInt16_t    retOnlyVers;                         /* Retain only versions */
    dsUInt8_t     copySer;                               /* for copy serialization values, see defines */
    dsUInt8_t     copyMode;                             /* for copy mode values, see defines above */
    dsChar_t      destName[DSM_MAX_CG_DEST_LENGTH + 1];  /* Copy dest name */
    dsmBool_t     bLanFreeDest;                         /* Destination has lan free path? */
    dsmBool_t     reserved;                             /* Not currently used */
    dsmBool_t     bDeduplicate;                        /* destination has dedup enabled */
} tsmBackupDetailCG;

```

```

/*-----+
| Type definition for Query Mgmt Class detail response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryRespMCDetailData
{
    dsUInt16_t      stVersion;          /* structure version */
    dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    dsChar_t        mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /*mc description */
    archDetailCG    archDet;           /* Archive copy group detail */
    backupDetailCG  backupDet;        /* Backup copy group detail */
} tsmQryRespMCDetailData;

#define tsmQryRespMCDetailDataVersion 4

/*-----+
| Type definition for Query Mgmt Class summary response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryRespMCData
{
    dsUInt16_t      stVersion;          /* structure version */
    dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    dsChar_t        mcDesc[DSM_MAX_MC_DESCR_LENGTH + 1]; /* mc description */
} tsmQryRespMCData;

#define tsmQryRespMCDataVersion 1

/*-----+
| Type definition for Archive queryBuffer on tsmBeginQuery() |
+-----*/
typedef struct tsmQryArchiveData
{
    dsUInt16_t      stVersion;          /* structure version */
    tsmObjName      *objName;          /* Full dsm name of object */
    dsChar_t        *owner;            /* owner name */
    /* for maximum date boundaries, see defines above */
    dsmDate         insDateLowerBound; /* low bound archive insert date */
    dsmDate         insDateUpperBound; /* hi bound archive insert date */
    dsmDate         expDateLowerBound; /* low bound expiration date */
    dsmDate         expDateUpperBound; /* hi bound expiration date */
    dsChar_t        *descr;            /* archive description */
} tsmQryArchiveData;

#define tsmQryArchiveDataVersion 1

/*-----+
| Type definition for Query Archive response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryRespArchiveData
{
    dsUInt16_t      stVersion;          /* structure version */
    tsmObjName      objName;           /* Filespace name qualifier */
    dsUInt32_t      copyGroup;         /* copy group number */
    dsChar_t        mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    dsChar_t        owner[DSM_MAX_OWNER_LENGTH + 1]; /* owner name */
    dsStruct64_t    objId;             /* Unique copy id */
    dsStruct64_t    reserved;          /* backward compatability */
    dsUInt8_t       mediaClass;        /* media access class */
    dsmDate         insDate;           /* archive insertion date */
    dsmDate         expDate;           /* expiration date for object */
    dsChar_t        descr[DSM_MAX_DESCR_LENGTH + 1]; /* archive description */
    dsUInt16_t      objInfolen;        /* length of object-dependent info*/
    dsUInt8_t       reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
    dsUInt160_t     restoreOrderExt;   /* restore order */
    dsStruct64_t    sizeEstimate;      /* size estimate stored by user*/
    dsUInt8_t       compressType;      /* Compression flag */
    dsUInt8_t       retentionInitiated; /* object waiting on retention event*/
    dsUInt8_t       objHeld;           /* object is on "hold" see dsmapi.h for values */
    dsUInt8_t       encryptionType;    /* type of encryption */
    dsmBool_t       clientDeduplicated; /* obj deduplicated by API*/
    dsUInt8_t       objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
    dsChar_t        compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1]; /* compression algorithm name */
} tsmQryRespArchiveData;

#define tsmQryRespArchiveDataVersion 7

```

```

/*-----+
| Type definition for Archive sendBuff parameter on dsmSendObj() |
+-----*/
typedef struct tsmSndArchiveData
{
    dsUInt16_t    stVersion;          /* structure version */
    dsChar_t     *descr;             /* archive description */
} tsmSndArchiveData;

#define tsmSndArchiveDataVersion 1

/*-----+
| Type definition for Backup queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct tsmQryBackupData
{
    dsUInt16_t    stVersion;          /* structure version */
    tsmObjName   *objName;           /* full dsm name of object */
    dsChar_t     *owner;             /* owner name */
    dsUInt8_t    objState;           /* object state selector */
    dsmDate      pitDate;            /* Date value for point in time restore */
    /* for possible values, see defines above */
    dsUInt32_t   reserved1;
    dsUInt32_t   reserved2;
} tsmQryBackupData;

#define tsmQryBackupDataVersion 3

/*-----+
| Type definition for Query Backup response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryRespBackupData
{
    dsUInt16_t    stVersion;          /* structure version */
    tsmObjName   objName;            /* full dsm name of object */
    dsUInt32_t    copyGroup;          /* copy group number */
    dsChar_t     mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /* mc name */
    dsChar_t     owner[DSM_MAX_OWNER_LENGTH + 1]; /* owner name */
    dsStruct64_t objId;               /* Unique object id */
    dsStruct64_t reserved;            /* backward compatability */
    dsUInt8_t    mediaClass;          /* media access class */
    dsUInt8_t    objState;            /* Obj state, active, etc. */
    dsmDate      insDate;             /* backup insertion date */
    dsmDate      expDate;             /* expiration date for object */
    dsUInt16_t   objInfolen;          /* length of object-dependent info*/
    dsUInt8_t    reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
    dsUInt160_t  restoreOrderExt;     /* restore order */
    dsStruct64_t sizeEstimate;        /* size estimate stored by user */
    dsStruct64_t baseObjId;
    dsUInt16_t   baseObjInfolen;      /* length of base object-dependent info*/
    dsUInt8_t    baseObjInfo[DSM_MAX_OBJINFO_LENGTH]; /* base object-dependent info */
    dsUInt160_t  baseRestoreOrder;    /* restore order */
    dsUInt32_t   fsID;
    dsUInt8_t    compressType;
    dsmBool_t    isGroupLeader;
    dsmBool_t    isOpenGroup;
    dsUInt8_t    reserved1;           /* for future use */
    dsmBool_t    reserved2;           /* for future use */
    dsUInt16_t   reserved3;           /* for future use */
    reservedInfo_t *reserved4;        /* for future use */
    dsUInt8_t    encryptionType;      /* type of encryption */
    dsmBool_t    clientDeduplicated;  /* obj deduplicated by API*/
    dsUInt8_t    objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
    dsChar_t     compressAlg[DSM_MAX_COMPRESSTYPE_LENGTH + 1]; /* compression algorithm name */
} tsmQryRespBackupData;

#define tsmQryRespBackupDataVersion 8

/*-----+
| Type definition for Active Backup queryBuffer on dsmBeginQuery() |
| |
| Notes: For the active backup query, only the fs (filesystem) and objType |
| fields of objName need be set. objType can only be set to |
| DSM_OBJ_FILE or DSM_OBJ_DIRECTORY. DSM_OBJ_ANY_TYPE will not |
| find a match on the query. |
+-----*/
typedef struct tsmQryABackupData
{

```

```

    dsUint16_t    stVersion;          /* structure version */
    tsmObjName    *objName;          /* Only fs and objtype used */
} tsmQryABackupData;

#define tsmQryABackupDataVersion 1

/*-----+
| Type definition for Query Active Backup response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryARespBackupData
{
    dsUint16_t    stVersion;          /* structure version */
    tsmObjName    objName;            /* full dsm name of object */
    dsUint32_t    copyGroup;          /* copy group number */
    dsChar_t      mcName[DSM_MAX_MC_NAME_LENGTH + 1]; /*management class name*/
    dsChar_t      owner[DSM_MAX_OWNER_LENGTH + 1];    /* owner name */
    dsmDate       insDate;            /* backup insertion date */
    dsUint16_t    objInfoLen;         /* length of object-dependent info*/
    dsUint8_t     reservedObjInfo[DSM_MAX_OBJINFO_LENGTH]; /*object-dependent info */
    dsUint8_t     objInfo[DSM_MAX_EXT_OBJINFO_LENGTH]; /*object-dependent info */
} tsmQryARespBackupData;

#define tsmQryARespBackupDataVersion 2

/*-----+
| Type definition for Backup queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct tsmQryBackupGroups
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint8_t     groupType;
    dsChar_t      *fsName;
    dsChar_t      *owner;
    dsStruct64_t  groupLeaderObjId;
    dsUint8_t     objType;
    dsUint32_t    reserved1;
    dsUint32_t    reserved2;
    dsmBool_t     noRestoreOrder;
    dsmBool_t     noGroupInfo;
    dsChar_t      *hl;
} tsmQryBackupGroups;

#define tsmQryBackupGroupsVersion 4

/*-----+
| Type definition for proxynode queryBuffer on tsmBeginQuery() |
+-----*/
typedef struct tsmQryProxyNodeData
{
    dsUint16_t    stVersion;          /* structure version */
    dsChar_t      *targetNodeName;    /* target node name */
} tsmQryProxyNodeData;

#define tsmQryProxyNodeDataVersion 1

/*-----+
| Type definition for qryRespProxyNodeData parameter used on tsmGetNextQObj() |
+-----*/

typedef struct tsmQryRespProxyNodeData
{
    dsUint16_t    stVersion ;          /* structure version */
    dsChar_t      targetNodeName[DSM_MAX_ID_LENGTH+1]; /* target node name */
    dsChar_t      peerNodeName[DSM_MAX_ID_LENGTH+1]; /* peer node name */
    dsChar_t      hlAddress[DSM_MAX_ID_LENGTH+1]; /* peer hlAddress */
    dsChar_t      llAddress[DSM_MAX_ID_LENGTH+1]; /* peer llAddress */
} tsmQryRespProxyNodeData;

#define tsmQryRespProxyNodeDataVersion 1

/*-----+
| Type definition for WINNT and OS/2 Filespace attributes |
+-----*/
typedef struct tsmDosFSAttrib
{
    osChar_t      driveLetter ;        /* drive letter for filespace */
    dsUint16_t    fsInfoLength;        /* fsInfo length used */
}

```

```

    osChar_t      fsInfo[DSM_MAX_FSINFO_LENGTH];/*caller-determined data */
} tsmDosFSAttrib ;

/*-----+
| Type definition for UNIX Filespace attributes |
+-----*/
typedef struct tsmUnixFSAttrib
{
    dsUInt16_t    fsInfoLength;          /* fsInfo length used          */
    osChar_t      fsInfo[DSM_MAX_FSINFO_LENGTH];/*caller-determined data */
} tsmUnixFSAttrib ;

/*-----+
| Type definition for NetWare Filespace attributes |
+-----*/
typedef tsmUnixFSAttrib tsmNetwareFSAttrib;

/*-----+
| Type definition for Filespace attributes on all Filespace calls |
+-----*/
typedef union
{
    tsmNetwareFSAttrib  netwareFSAttr;
    tsmUnixFSAttrib     unixFSAttr ;
    tsmDosFSAttrib      dosFSAttr ;
} tsmFSAttr ;

/*-----+
| Type definition for fsUpd parameter on dsmUpdateFS() |
+-----*/
typedef struct    tsmFSUpd
{
    dsUInt16_t     stVersion ;                /* structure version          */
    dsChar_t       *fsType ;                  /* filespace type            */
    dsStruct64_t   occupancy ;                /* occupancy estimate        */
    dsStruct64_t   capacity ;                 /* capacity estimate         */
    tsmFSAttr      fsAttr ;                  /* platform specific attributes */
} tsmFSUpd ;

#define tsmFSUpdVersion 1

/*-----+
| Type definition for Filespace queryBuffer on dsmBeginQuery() |
+-----*/
typedef struct tsmQryFSData
{
    dsUInt16_t     stVersion;                /* structure version          */
    dsChar_t       *fsName;                  /* File space name           */
} tsmQryFSData;

#define tsmQryFSDataVersion 1

/*-----+
| Type definition for Query Filespace response on dsmGetNextQObj() |
+-----*/
typedef struct tsmQryRespFSData
{
    dsUInt16_t     stVersion;                /* structure version          */
    dsChar_t       fsName[DSM_MAX_FSNAME_LENGTH + 1]; /* Filespace name          */
    dsChar_t       fsType[DSM_MAX_FSTYPE_LENGTH + 1]; /* Filespace type          */
    dsStruct64_t   occupancy;                /* Occupancy est. in bytes. */
    dsStruct64_t   capacity;                 /* Capacity est. in bytes.  */
    tsmFSAttr      fsAttr ;                  /* platform specific attributes */
    dsmDate        backStartDate;            /* start backup date         */
    dsmDate        backCompleteDate;         /* end backup date           */
    dsmDate        reserved1 ;               /* For future use           */
    dsmBool_t      bIsUnicode;
    dsUInt32_t     fsID;
    dsmDate        lastReplStartDate;         /* The last time replication was started */
    dsmDate        lastReplCmpltDate;        /* The last time replication completed   */
    /* (could have had a failure,          */
    /* but it still completes)            */
    dsmDate        lastBackOpDateFromServer; /* The last store time stamp the client  */
    /* saved on the server                 */
    dsmDate        lastArchOpDateFromServer; /* The last store time stamp the client  */
    /* saved on the server                 */
    dsmDate        lastSpMgOpDateFromServer; /* The last store time stamp the client  */
}

```



```

        dsmDate      lastBackOpDateFromLocal; /* saved on the server */
        dsmDate      lastArchOpDateFromLocal; /* The last store time stamp the client
        /* saved on the Local */
        dsmDate      lastSpMgOpDateFromLocal; /* The last store time stamp the client
        /* saved on the Local */
        dsInt32_t    failOverWriteDelay; /* Minutes for client to wait before allowed
        /* to store to this Repl srvr, Specail codes:
        /* NO_ACCESS(-1), ACCESS_RDONLY (-2)
    } tsmQryRespFSData;

#define tsmQryRespFSDataVersion 5

/*-----+
| Type definition for regFilespace parameter on dsmRegisterFS()
+-----*/
typedef struct tsmRegFSData
{
    dsUInt16_t      stVersion; /* structure version */
    dsChar_t        *fsName; /* Filespace name */
    dsChar_t        *fsType; /* Filespace type */
    dsStruct64_t    occupancy; /* Occupancy est. in bytes. */
    dsStruct64_t    capacity; /* Capacity est. in bytes. */
    tsmFSAttr      fsAttr ; /* platform specific attributes */
} tsmRegFSData;

#define tsmRegFSDataVersion 1

/*-----+
| Type definition for session info response on dsmQuerySessionInfo()
+-----*/
typedef struct
{
    dsUInt16_t      stVersion; /* Structure version */
    /*-----+
    /* Server information */
    /*-----+
    dsChar_t        serverHost[DSM_MAX_SERVERNAME_LENGTH+1];
    /* Network host name of DSM server */
    dsUInt16_t      serverPort; /* Server comm port on host */
    dsmDate         serverDate; /* Server's date/time */
    dsChar_t        serverType[DSM_MAX_SERVERTYPE_LENGTH+1];
    /* Server's execution platform */
    dsUInt16_t      serverVer; /* Server's version number */
    dsUInt16_t      serverRel; /* Server's release number */
    dsUInt16_t      serverLev; /* Server's level number */
    dsUInt16_t      serverSubLev; /* Server's sublevel number */
    /*-----+
    /* Client Defaults */
    /*-----+
    dsChar_t        nodeType[DSM_MAX_PLATFORM_LENGTH+1]; /*node/application type*/
    dsChar_t        fsdelim; /* File space delimiter */
    dsChar_t        hldelim; /* Delimiter betw highlev & lowlev */
    dsUInt8_t       compression; /* Compression flag */
    dsUInt8_t       archDel; /* Archive delete permission */
    dsUInt8_t       backDel; /* Backup delete permission */
    dsUInt32_t      maxBytesPerTxn; /* for future use */
    dsUInt16_t      maxObjPerTxn; /* The max objects allowed in a txn */
    /*-----+
    /* Session Information */
    /*-----+
    dsChar_t        id[DSM_MAX_ID_LENGTH+1]; /* Sign-in id node name */
    dsChar_t        owner[DSM_MAX_OWNER_LENGTH+1]; /* Sign-in owner */
    /* (for multi-user platforms) */
    dsChar_t        confFile[DSM_PATH_MAX + DSM_NAME_MAX +1];
    /* len is platform dep */
    /* dsInit name of appl config file */
    dsUInt8_t       opNoTrace; /* dsInit option - NoTrace = 1 */
    /*-----+
    /* Policy Data */
    /*-----+
    dsChar_t        domainName[DSM_MAX_DOMAIN_LENGTH+1]; /* Domain name */
    dsChar_t        policySetName[DSM_MAX_PS_NAME_LENGTH+1];
    /* Active policy set name */
    dsmDate         polActDate; /* Policy set activation date */
    dsChar_t        dfltMCName[DSM_MAX_MC_NAME_LENGTH+1]; /* Default Mgmt Class */

```

```

    dsUInt16_t    gpBackRetn;          /* Grace-period backup retention */
    dsUInt16_t    gpArchRetn;         /* Grace-period archive retention */
    dsChar_t      adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* adsm server name */
    dsmBool_t     archiveRetentionProtection; /* is server Retention protection enabled */
    dsUInt64_t    maxBytesPerTxn_64;   /* for future use */
    dsmBool_t     lanFreeEnabled;      /* lan free option is set */
    dsmDedupType  dedupType;          /* server or clientOrServer */
    dsChar_t      accessNode[DSM_MAX_ID_LENGTH+1]; /* as node node name */

/*-----*/
/*          Replication and fail over information          */
/*-----*/
    dsmFailOvrCfgType failOverCfgType; /* status of fail over */
    dsChar_t      replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* repl server name */
    dsChar_t      homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* home server name */
    dsChar_t      replServerHost[DSM_MAX_SERVERNAME_LENGTH+1]; /* Network host name of DSM server */
    dsInt32_t     replServerPort;     /* Server comm port on host */
} tsmApiSessInfo;

#define tsmApiSessInfoVersion 6

/*-----+
| Type definition for Query options response on dsmQueryCliOptions() |
| and dsmQuerySessOptions() |
+-----*/

typedef struct
{
    dsUInt16_t    stVersion;
    dsChar_t      dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX + 1];
    dsChar_t      dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX + 1];
    dsChar_t      serverName[DSM_MAX_SERVERNAME_LENGTH+1];
    dsInt16_t     commMethod;
    dsChar_t      serverAddress[DSM_MAX_SERVER_ADDRESS];
    dsChar_t      nodeName[DSM_MAX_NODE_LENGTH+1];
    dsmBool_t     compression;
    dsmBool_t     compressalways;
    dsmBool_t     passwordAccess;
} tsmOptStruct ;

#define tsmOptStructVersion 1

/*-----+
| Type definition for qryRespAccessData parameter used on dsmQueryAccess() |
+-----*/

typedef struct
{
    dsUInt16_t    stVersion ;          /* structure version */
    dsChar_t      node[DSM_MAX_ID_LENGTH+1]; /* node name */
    dsChar_t      owner[DSM_MAX_OWNER_LENGTH+1]; /* owner */
    tsmObjName     objName ;          /* object name */
    dsmAccessType  accessType;        /* archive or backup */
    dsUInt32_t    ruleNumber ;        /* Access rule id */
} tsmQryRespAccessData;

#define tsmQryRespAccessDataVersion 1

/*-----+
| Type definition for envSetUp parameter on dsmSetUp() |
+-----*/

typedef struct tsmEnvSetUp
{
    dsUInt16_t    stVersion;          /* structure version */
    dsChar_t      dsmiDir[DSM_PATH_MAX + DSM_NAME_MAX + 1];
    dsChar_t      dsmiConfig[DSM_PATH_MAX + DSM_NAME_MAX + 1];
    dsChar_t      dsmiLog[DSM_PATH_MAX + DSM_NAME_MAX + 1];
    char          **argv; /* for executables name argv[0] */
    dsChar_t      logName[DSM_NAME_MAX + 1];
    dsmBool_t     reserved1; /* for future use */
    dsmBool_t     reserved2; /* for future use */
} tsmEnvSetUp;

#define tsmEnvSetUpVersion 4

```

```

/*-----+
| Type definition for dsmInitExIn_t
+-----*/
typedef struct tsmInitExIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    tsmApiVersionEx *apiVersionExp;
    dsChar_t        *clientNodeNameP;
    dsChar_t        *clientOwnerNameP;
    dsChar_t        *clientPasswordP;
    dsChar_t        *userNameP;
    dsChar_t        *userPasswordP;
    dsChar_t        *applicationTypeP;
    dsChar_t        *configfile;
    dsChar_t        *options;
    dsChar_t        dirDelimiter;
    dsmBool_t       useUnicode;
    dsmBool_t       bCrossPlatform;
    dsmBool_t       bService;
    dsmBool_t       bEncryptKeyEnabled;
    dsChar_t        *encryptionPasswordP;
    dsmBool_t       useTsmBuffers;
    dsUInt8_t       numTsmBuffers;
    tsmAppVersion   appVersionP;
} tsmInitExIn_t;

#define tsmInitExInVersion 5

/*-----+
| Type definition for dsmInitExOut_t
+-----*/
typedef struct tsmInitExOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsInt16_t       userNameAuthorities;
    dsInt16_t       infoRC;             /* error return code if encountered */
    /* adsm server name */
    dsChar_t        adsmServerName[DSM_MAX_SERVERNAME_LENGTH+1];
    dsUInt16_t      serverVer;          /* Server's version number */
    dsUInt16_t      serverRel;         /* Server's release number */
    dsUInt16_t      serverLev;         /* Server's level number */
    dsUInt16_t      serverSubLev;      /* Server's sublevel number */
    dsmBool_t       bIsFailOverMode; /* true if failover has occurred */
    dsChar_t        replServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* repl server name */
    dsChar_t        homeServerName[DSM_MAX_SERVERNAME_LENGTH+1]; /* home server name */
} tsmInitExOut_t;

#define tsmInitExOutVersion 3

/*-----+
| Type definition for dsmLogExIn_t
+-----*/
typedef struct tsmLogExIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsmLogSeverity  severity;
    dsChar_t        appMsgID[8];
    dsmLogType      logType;           /* log type : local, server, both */
    dsChar_t        *message;         /* text of message to be logged */
    dsChar_t        appName[DSM_MAX_PLATFORM_LENGTH];
    dsChar_t        osPlatform[DSM_MAX_PLATFORM_LENGTH];
    dsChar_t        appVersion[DSM_MAX_PLATFORM_LENGTH];
} tsmLogExIn_t;

#define tsmLogExInVersion 2

/*-----+
| Type definition for dsmLogExOut_t
+-----*/
typedef struct tsmLogExOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
} tsmLogExOut_t;

#define tsmLogExOutVersion 1

```

```

/*-----+
| Type definition for dsmRenameIn_t
+-----*/
typedef struct tsmRenameIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsUInt32_t      tsmHandle;         /* handle for session */
    dsUInt8_t       repository;        /* Backup or Archive */
    tsmObjName      *objNameP;        /* object name */
    dsChar_t        newHl[DSM_MAX_HL_LENGTH + 1]; /* new High level name */
    dsChar_t        newLl[DSM_MAX_LL_LENGTH + 1]; /* new Low level name */
    dsmBool_t       merge;             /* merge into existing name*/
    ObjID           objId;             /* objId for Archive */
} tsmRenameIn_t;

#define tsmRenameInVersion 1

/*-----+
| Type definition for dsmRenameOut_t
+-----*/
typedef struct tsmRenameOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
} tsmRenameOut_t;

#define tsmRenameOutVersion 1

/*-----+
| Type definition for tsmEndSendObjExIn_t
+-----*/
typedef struct tsmEndSendObjExIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsUInt32_t      tsmHandle;         /* handle for session */
} tsmEndSendObjExIn_t;

#define tsmEndSendObjExInVersion 1

/*-----+
| Type definition for dsmEndSendObjExOut_t
+-----*/
typedef struct tsmEndSendObjExOut_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsStruct64_t    totalBytesSent;     /* total bytes read from app */
    dsmBool_t       objCompressed;     /* was object compressed */
    dsStruct64_t    totalCompressSize; /* total size after compress */
    dsStruct64_t    totalLFBytesSent;  /* total bytes sent Lan Free */
    dsUInt8_t       encryptionType;   /* type of encryption used */
    dsmBool_t       objDeduplicated;   /* was object processed for dist. data dedup */
    dsStruct64_t    totalDedupSize;    /* total size after de-dup */
} tsmEndSendObjExOut_t;

#define tsmEndSendObjExOutVersion 3

/*-----+
| Type definition for tsmGroupHandlerIn_t
+-----*/
typedef struct tsmGroupHandlerIn_t
{
    dsUInt16_t      stVersion;          /* structure version */
    dsUInt32_t      tsmHandle;         /* handle for session */
    dsUInt8_t       groupType;        /* Type of group */
    dsUInt8_t       actionType;       /* Type of group operation */
    dsUInt8_t       memberType;       /* Type of member: Leader or member */
    dsStruct64_t    leaderObjId;      /* OBJID of the groupleader */
    dsChar_t        *uniqueGroupTagP; /* Unique group identifier */
    tsmObjName      *objNameP;        /* group leader object name */
    dsmGetList      memberObjList;    /* list of objects to remove, assign */
} tsmGroupHandlerIn_t;

#define tsmGroupHandlerInVersion 1

/*-----+
| Type definition for tsmGroupHandlerExOut_t
+-----*/
typedef struct tsmGroupHandlerOut_t

```

```

{
    dsUint16_t    stVersion;          /* structure version */
} tsmGroupHandlerOut_t;

#define tsmGroupHandlerOutVersion 1

/*-----+
| Type definition for tsmEndTxnExIn_t
+-----*/
typedef struct tsmEndTxnExIn_t
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint32_t    tsmHandle;         /* handle for session */
    dsUint8_t     vote;
} tsmEndTxnExIn_t;

#define tsmEndTxnExInVersion 1

/*-----+
| Type definition for tsmEndTxnExOut_t
+-----*/
typedef struct tsmEndTxnExOut_t
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint16_t    reason;             /* reason code */
    dsStruct64_t  groupLeaderObjId;   /* groupLeader obj id returned on */
    /* DSM_ACTION_OPEN */
    dsUint8_t     reserved1;         /* future use */
    dsUint16_t    reserved2;         /* future use */
} tsmEndTxnExOut_t;

#define tsmEndTxnExOutVersion 1

/*-----+
| Type definition for tsmEndGetDataExIn_t
+-----*/
typedef struct tsmEndGetDataExIn_t
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint32_t    tsmHandle;         /* handle for session */
} tsmEndGetDataExIn_t;

#define tsmEndGetDataExInVersion 1

/*-----+
| Type definition for tsmEndGetDataExOut_t
+-----*/
typedef struct tsmEndGetDataExOut_t
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint16_t    reason;             /* reason code */
    dsStruct64_t  totalLFBytesRecv;  /* total lan free bytes recieved */
} tsmEndGetDataExOut_t;

#define tsmEndGetDataExOutVersion 1

/*-----+
| Type definition for on tsmRetentionEvent()
+-----*/
typedef struct tsmRetentionEventIn_t
{
    dsUint16_t    stVersion;          /* structure version */
    dsUint32_t    tsmHandle;         /* session Handle */
    dsmEventType_t eventType;        /* Event type */
    dsmObjList_t  objList;          /* object ID */
} tsmRetentionEventIn_t;

#define tsmRetentionEventInVersion 1

/*-----+
| Type definition for on tsmRetentionEvent()
+-----*/
typedef struct tsmRetentionEventOut_t
{
    dsUint16_t    stVersion ;          /* structure version */
} tsmRetentionEventOut_t;

```



```

/* support for linkage */
#include <windows.h>
#define DSMLINKAGE WINAPI

#define DS_WINNT 22
#define _OPSYS_TYPE DS_WINNT

typedef signed char dsInt8_t;
typedef unsigned char dsUInt8_t;
typedef signed short dsInt16_t;
typedef unsigned short dsUInt16_t;
typedef signed long dsInt32_t;
typedef unsigned long dsUInt32_t;

/*=== Character and string types ===*/
#ifdef UNICODE
typedef wchar_t dsChar_t;
#define dsTEXT(x) L##x
#else
typedef char dsChar_t;
#define dsTEXT(x) x
#endif /* !UNICODE */

/*=== Common typedefs and defines derived from dsChar_t ===*/
typedef dsChar_t *dsString_t;

/* added for the extended restore order */
typedef struct
{
    dsUInt32_t top;
    dsUInt32_t hi_hi;
    dsUInt32_t hi_lo;
    dsUInt32_t lo_hi;
    dsUInt32_t lo_lo;
} dsUInt160_t ;

#ifdef _LONG_LONG
typedef __int64 dsInt64_t;
typedef unsigned __int64 dsUInt64_t;
/*=== A "true" unsigned 64-bit integer ===*/
typedef __int64 dsLongLong_t;
#else
typedef struct tagUINT64_t
{
    dsUInt32_t hi; /* Most significant 32 bits. */
    dsUInt32_t lo; /* Least significant 32 bits. */
} dsUInt64_t;
#endif

/*-----+
| Type definition for bool_t |
+-----*/
/*
 * Had to create a Boolean type that didn't clash with any other predefined
 * version in any operating system or windowing system.
 */
typedef enum
{
    dsmFalse = 0x00,
    dsmTrue = 0x01
}dsmBool_t ;

/*=== for backward compatability ===*/
#define uint8 dsUInt8_t
#define int8 dsInt8_t
#define uint16 dsUInt16_t
#define int16 dsInt16_t
#define uint32 dsUInt32_t
#define int32 dsInt32_t
#define uint64 dsStruct64_t
#define bool_t dsBool_t
#define dsBool_t dsmBool_t
#define bTrue dsmTrue
#define bFalse dsmFalse

```

```

typedef struct
{
    dsUint32_t hi;          /* Most significant 32 bits. */
    dsUint32_t lo;        /* Least significant 32 bits. */
}dsStruct64_t ;

#endif /* DSMAPILIB */

#ifdef _WIN64
#pragma pack()
#endif
#endif /* _H_DSMAPIPS */

/*****
 * IBM Spectrum Protect *
 * Common Source Component *
 * *
 * (C) Copyright IBM Corporation 1993,2016 *
 *****/

/*****
 * Header File Name: release.h
 *
 * Environment: *****
 * ** This is a platform-independent source file **
 * *****
 *
 * Design Notes: This file contains the common information about
 * the actual version.release.level.sublevel
 *
 * Descriptive-name: Definitions for Tivoli Storage manager version
 *
 * Note: This file should contain no LOG or CMVC information. It is
 * shipped with the API code.
 *
 *-----*/

#ifdef _H_RELEASE
#define _H_RELEASE

#define COMMON_VERSION 8
#define COMMON_RELEASE 1
#define COMMON_LEVEL 2
#define COMMON_SUBLEVEL 0
#define COMMON_DRIVER dsTEXT("")

#define COMMON_VERSIONTXT "8.1.2.0"

#define SHIPYEARTXT "2017"
#define SHIPYEARTXTW dsTEXT("2017")
#define TSMPRODTXT "IBM Spectrum Protect"

/*=====
The following string definitions are used for VERSION information
and should not be converted to dsTEXT or osTEXT. They are used
only at link time.

These are also used when the Jar file is built on Unix. See the
the perl script tools/unx/mzbuild/createReleaseJava
=====*/
#define COMMON_VERSION_STR "8"
#define COMMON_RELEASE_STR "1"
#define COMMON_LEVEL_STR "2"
#define COMMON_SUBLEVEL_STR "0"
#define COMMON_DRIVER_STR ""

/*=== product names definitions ===*/
#define COMMON_NAME_DFDSM 1
#define COMMON_NAME_ADSM 2
#define COMMON_NAME_TSM 3
#define COMMON_NAME_ITSM 4
#define COMMON_NAME COMMON_NAME_ITSM

/*=====

```



Internal version, release, and level (build) version. This should be unique for every version+release+ptf of a product. This information is recorded in the file attributes and data stream for diagnostic purposes.

NOTE: DO NOT MODIFY THESE VALUES. YOU CAN ONLY ADD NEW ENTRIES!

```
=====*/
#define COMMON_BUILD_TSM_510 1
#define COMMON_BUILD_TSM_511 2
#define COMMON_BUILD_TSM_515 3
#define COMMON_BUILD_TSM_516 4
#define COMMON_BUILD_TSM_520 5
#define COMMON_BUILD_TSM_522 6
#define COMMON_BUILD_TSM_517 7
#define COMMON_BUILD_TSM_523 8
#define COMMON_BUILD_TSM_530 9
#define COMMON_BUILD_TSM_524 10
#define COMMON_BUILD_TSM_532 11
#define COMMON_BUILD_TSM_533 12
#define COMMON_BUILD_TSM_525 13
#define COMMON_BUILD_TSM_534 14
#define COMMON_BUILD_TSM_540 15
#define COMMON_BUILD_TSM_535 16
#define COMMON_BUILD_TSM_541 17
#define COMMON_BUILD_TSM_550 18
#define COMMON_BUILD_TSM_542 19
#define COMMON_BUILD_TSM_551 20
#define COMMON_BUILD_TSM_610 21
#define COMMON_BUILD_TSM_552 22
#define COMMON_BUILD_TSM_611 23
#define COMMON_BUILD_TSM_543 24
#define COMMON_BUILD_TSM_620 25
#define COMMON_BUILD_TSM_612 26
#define COMMON_BUILD_TSM_553 27
#define COMMON_BUILD_TSM_613 28
#define COMMON_BUILD_TSM_621 29
#define COMMON_BUILD_TSM_622 30
#define COMMON_BUILD_TSM_614 31
#define COMMON_BUILD_TSM_623 32
#define COMMON_BUILD_TSM_630 33
#define COMMON_BUILD_TSM_615 34
#define COMMON_BUILD_TSM_624 35
#define COMMON_BUILD_TSM_631 36
#define COMMON_BUILD_TSM_640 37
#define COMMON_BUILD_TSM_710 38
#define COMMON_BUILD_TSM_625 39
#define COMMON_BUILD_TSM_641 40
#define COMMON_BUILD_TSM_711 41
#define COMMON_BUILD_TSM_712 42
#define COMMON_BUILD_TSM_713 43
#define COMMON_BUILD_TSM_714 44
#define COMMON_BUILD_TSM_720 45
#define COMMON_BUILD_TSM_721 46
#define COMMON_BUILD_TSM_642 47
#define COMMON_BUILD_TSM_643 48
#define COMMON_BUILD_TSM_715 49
#define COMMON_BUILD_TSM_716 50
#define COMMON_BUILD_TSM_810 51
#define COMMON_BUILD_TSM_811 52
#define COMMON_BUILD_TSM_812 53
#define COMMON_BUILD COMMON_BUILD_TSM_812

/*=== define VRL as an Int for bitmap version compares ===*/
static const int VRL_712 = 712;
static const int VRL_713 = 713;
static const int VRL_714 = 714;
static const int VRL_715 = 715;
static const int VRL_716 = 716;
static const int VRL_810 = 810;
static const int VRL_811 = 811;
static const int VRL_812 = 812;

#define TDP4VE_PLATFORM_STRING_MBCS "TDP VMware"
#define TDP4VE_PLATFORM_STRING dsTEXT("TDP VMware")

#define TDP4HYPERV_PLATFORM_STRING_MBCS "TDP HyperV"
#define TDP4HYPERV_PLATFORM_STRING dsTEXT("TDP HyperV")
```

```
#endif /* _H_RELEASE */
```

## Archivo de origen de las definiciones de la función de la API

---

Este apéndice contiene el archivo de encabezado dsmapifp.h para poder ver las definiciones de la función de API.

Nota: DSMLINKAGE se define de forma distinta en cada sistema operativo. Consulte en el archivo dsmapi.h las definiciones que se corresponden con su sistema operativo específico.

La información que se proporciona aquí contiene una copia puntual de los archivos que se distribuyen con la API. Vea los archivos en el paquete de distribución de la API para la última versión.

```
/******  
* Tivoli Storage Manager *  
* API Client Component *  
* * *  
* (C) Copyright IBM Corporation 1993,2002 *  
*****/  
  
/******/  
/* Header File Name: dsmapifp.h */  
/* */  
/* Descriptive-name: Tivoli Storage Manager API function prototypes */  
/******/  
#ifndef _H_DSMAIFP  
#define _H_DSMAIFP  
  
#if defined(__cplusplus)  
extern "C" {  
#endif  
  
#ifdef DYNALOAD_DSMAPI  
  
/* function will be dynamically loaded */  
#include "dsmapidl.h"  
  
#else  
  
/* functions will be implicitly loaded from library */  
  
/*=====*/  
/* PUBLIC FUNCTIONS */  
/*=====*/  
  
extern dsInt16_t DSMLINKAGE dsmBeginGetData(  
    dsUInt32_t dsmHandle,  
    dsBool_t mountWait,  
    dsmGetType getType,  
    dsmGetList *dsmGetObjListP  
);  
  
extern dsInt16_t DSMLINKAGE dsmBeginQuery(  
    dsUInt32_t dsmHandle,  
    dsmQueryType queryType,  
    dsmQueryBuff *queryBuffer  
);  
  
extern dsInt16_t DSMLINKAGE dsmBeginTxn(  
    dsUInt32_t dsmHandle  
);  
  
extern dsInt16_t DSMLINKAGE dsmBindMC(  
    dsUInt32_t dsmHandle,  
    dsmObjName *objNameP,  
    dsmSendType sendType,  
    mcBindKey *mcBindKeyP  
);  
  
extern dsInt16_t DSMLINKAGE dsmChangePW(  
    dsUInt32_t dsmHandle,  
    char *oldPW,  
    char *newPW  
);
```

```

extern dsInt16_t DSMLINKAGE dsmCleanUp (
    dsBool_t          mtFlag
);

extern dsInt16_t DSMLINKAGE dsmDeleteAccess (
    dsUInt32_t        dsmHandle,
    dsUInt32_t        ruleNum
);

extern dsInt16_t DSMLINKAGE dsmDeleteObj (
    dsUInt32_t        dsmHandle,
    dsmDelType        delType,
    dsmDelInfo        delInfo
);

extern dsInt16_t DSMLINKAGE dsmDeleteFS (
    dsUInt32_t        dsmHandle,
    char              *fsName,
    dsUInt8_t         repository
);

extern dsInt16_t DSMLINKAGE dsmEndGetData (
    dsUInt32_t        dsmHandle
);

extern dsInt16_t DSMLINKAGE dsmEndGetDataEx (
    dsmEndGetDataExIn_t *dsmEndGetDataExInP,
    dsmEndGetDataExOut_t *dsmEndGetDataExOutP
);

extern dsInt16_t DSMLINKAGE dsmEndGetObj (
    dsUInt32_t        dsmHandle
);

extern dsInt16_t DSMLINKAGE dsmEndQuery (
    dsUInt32_t        dsmHandle
);

extern dsInt16_t DSMLINKAGE dsmEndSendObj (
    dsUInt32_t        dsmHandle
);

extern dsInt16_t DSMLINKAGE dsmEndSendObjEx (
    dsmEndSendObjExIn_t *dsmEndSendObjExInP,
    dsmEndSendObjExOut_t *dsmEndSendObjExOutP
);

extern dsInt16_t DSMLINKAGE dsmEndTxnEx (
    dsmEndTxnExIn_t   *dsmEndTxnExInP,
    dsmEndTxnExOut_t  *dsmEndTxnExOutP
);

extern dsInt16_t DSMLINKAGE dsmEndTxn (
    dsUInt32_t        dsmHandle,
    dsUInt8_t         vote,
    dsUInt16_t        *reason
);

extern dsInt16_t DSMLINKAGE dsmGetData (
    dsUInt32_t        dsmHandle,
    DataBlk           *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE dsmGetBufferData (
    getBufferDataIn_t *dsmGetBufferDataInP,
    getBufferDataOut_t *dsmGetBufferDataOutP
);

extern dsInt16_t DSMLINKAGE dsmGetNextQObj (
    dsUInt32_t        dsmHandle,
    DataBlk           *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE dsmGetObj (
    dsUInt32_t        dsmHandle,

```

```

        ObjID          *objIdP,
        DataBlk       *dataBlkPtr
    );

extern dsInt16_t DSMLINKAGE dsmGroupHandler(
        dsmGroupHandlerIn_t *dsmGroupHandlerInP,
        dsmGroupHandlerOut_t *dsmGroupHandlerOutP
    );

extern dsInt16_t DSMLINKAGE dsmInit(
        dsUInt32_t *dsmHandle,
        dsmApiVersion *dsmApiVersionP,
        char *clientNodeNameP,
        char *clientOwnerNameP,
        char *clientPasswordP,
        char *applicationType,
        char *configfile,
        char *options
    );

extern dsInt16_t DSMLINKAGE dsmInitEx(
        dsUInt32_t *dsmHandleP,
        dsmInitExIn_t *dsmInitExInP,
        dsmInitExOut_t *dsmInitExOutP
    );

extern dsInt16_t DSMLINKAGE dsmLogEvent(
        dsUInt32_t dsmHandle,
        logInfo *lopInfoP
    );

extern dsInt16_t DSMLINKAGE dsmLogEventEx(
        dsUInt32_t dsmHandle,
        dsmLogExIn_t *dsmLogExInP,
        dsmLogExOut_t *dsmLogExOutP
    );

extern dsInt16_t DSMLINKAGE dsmQueryAccess(
        dsUInt32_t dsmHandle,
        qryRespAccessData **accessListP,
        dsUInt16_t *numberOfRules
    );

extern void DSMLINKAGE dsmQueryApiVersion(
        dsmApiVersion *apiVersionP
    );

extern void DSMLINKAGE dsmQueryApiVersionEx(
        dsmApiVersionEx *apiVersionP
    );

extern dsInt16_t DSMLINKAGE dsmQueryCliOptions(
        optStruct *optstructP
    );

extern dsInt16_t DSMLINKAGE dsmQuerySessInfo(
        dsUInt32_t dsmHandle,
        ApiSessInfo *SessInfoP
    );

extern dsInt16_t DSMLINKAGE dsmQuerySessOptions(
        dsUInt32_t dsmHandle,
        optStruct *optstructP
    );

extern dsInt16_t DSMLINKAGE dsmRCMsg(
        dsUInt32_t dsmHandle,
        dsInt16_t dsmRC,
        char *msg
    );

extern dsInt16_t DSMLINKAGE dsmRegisterFS(
        dsUInt32_t dsmHandle,
        regFSData *regFilespaceP
    );

```

```

extern dsInt16_t DSMLINKAGE dsmReleaseBuffer (
    releaseBufferIn_t      *dsmReleaseBufferInP,
    releaseBufferOut_t     *dsmReleaseBufferOutP
);

extern dsInt16_t DSMLINKAGE dsmRenameObj (
    dsmRenameIn_t         *dsmRenameInP,
    dsmRenameOut_t        *dsmRenameOutP
);

extern dsInt16_t DSMLINKAGE dsmRequestBuffer (
    requestBufferIn_t     *dsmRequestBufferInP,
    requestBufferOut_t    *dsmRequestBufferOutP
);

extern dsInt16_t DSMLINKAGE dsmRetentionEvent (
    dsmRetentionEventIn_t *dsmRetentionEventInP,
    dsmRetentionEventOut_t *dsmRetentionEventOutP
);

extern dsInt16_t DSMLINKAGE dsmSendBufferData (
    sendBufferDataIn_t    *dsmSendBufferDataInP,
    sendBufferDataOut_t   *dsmSendBufferDataOutP
);

extern dsInt16_t DSMLINKAGE dsmSendData (
    dsUInt32_t            dsmHandle,
    DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE dsmSendObj (
    dsUInt32_t            dsmHandle,
    dsmSendType           sendType,
    void                  *sendBuff,
    dsmObjName            *objNameP,
    ObjAttr               *objAttrPtr,
    DataBlk               *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE dsmSetAccess (
    dsUInt32_t            dsmHandle,
    dsmAccessType         accessType,
    dsmObjName            *objNameP,
    char                  *node,
    char                  *owner
);

extern dsInt16_t DSMLINKAGE dsmSetUp (
    dsBool_t              mtFlag,
    envSetUp               *envSetUpP
);

extern dsInt16_t DSMLINKAGE dsmTerminate (
    dsUInt32_t            dsmHandle
);

extern dsInt16_t DSMLINKAGE dsmUpdateFS (
    dsUInt32_t            dsmHandle,
    char                  *fs,
    dsmFSUpd              *fsUpdP,
    dsUInt32_t            fsUpdAct
);

extern dsInt16_t DSMLINKAGE dsmUpdateObj (
    dsUInt32_t            dsmHandle,
    dsmSendType           sendType,
    void                  *sendBuff,
    dsmObjName            *objNameP,
    ObjAttr               *objAttrPtr,
    dsUInt32_t            objUpdAct
);

extern dsInt16_t DSMLINKAGE dsmUpdateObjEx (
    dsmUpdateObjExIn_t    *dsmUpdateObjExInP,
    dsmUpdateObjExOut_t   *dsmUpdateObjExOutP
);

```

```
#endif /* ifdef DYNALOAD */

#if defined(__cplusplus)
}
#endif

#endif /* _H_DSMAPIFP */
```

Esta sección contiene las definiciones de función de API. Es una copia del archivo de encabezado de tsmapifp.h.  
 Nota: DSMLINKAGE se define de forma distinta para cada sistema operativo. Consulte las definiciones en el archivo tsmapi.h para el sistema operativo específico.

```

/*****
 * Tivoli Storage Manager
 * API Client Component
 *
 * (C) Copyright IBM Corporation 1993,2002
 *****/

/*****
/* Header File Name: tsmapifp.h
/*
/* Descriptive-name: Tivoli Storage Manager API function prototypes
*****/
#endif
#define _H_DSMAPIFP

#if defined(__cplusplus)
extern "C" {
#endif

#ifdef DYNALOAD_DSMAPI

/* function will be dynamically loaded */
#include "dsmapi.h"

#else

/* functions will be implicitly loaded from library */

/*=====
/* P U B L I C F U N C T I O N S
/*=====

typedef void tsmQueryBuff;

extern dsInt16_t DSMLINKAGE tsmBeginGetData(
    dsUInt32_t tsmHandle,
    dsBool_t mountWait,
    tsmGetType getType,
    dsmGetList *dsmGetObjListP
);

extern dsInt16_t DSMLINKAGE tsmBeginQuery(
    dsUInt32_t tsmHandle,
    tsmQueryType queryType,
    tsmQueryBuff *queryBuffer
);

extern dsInt16_t DSMLINKAGE tsmBeginTxn(
    dsUInt32_t tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmBindMC(
    dsUInt32_t tsmHandle,
    tsmObjName *objNameP,
    tsmSendType sendType,
    tsmMcBindKey *mcBindKeyP
);

extern dsInt16_t DSMLINKAGE tsmChangePW(
    dsUInt32_t tsmHandle,
    dsChar_t *oldPW,
    dsChar_t *newPW

```

```

);

extern dsInt16_t DSMLINKAGE tsmCleanUp(
    dsBool_t          mtFlag
);

extern dsInt16_t DSMLINKAGE tsmDeleteAccess(
    dsUInt32_t        tsmHandle,
    dsUInt32_t        ruleNum
);

extern dsInt16_t DSMLINKAGE tsmDeleteObj(
    dsUInt32_t        tsmHandle,
    tsmDelType        delType,
    tsmDelInfo        delInfo
);

extern dsInt16_t DSMLINKAGE tsmDeleteFS(
    dsUInt32_t        tsmHandle,
    dsChar_t          *fsName,
    dsUInt8_t         repository
);

extern dsInt16_t DSMLINKAGE tsmEndGetData(
    dsUInt32_t        tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmEndGetDataEx(
    tsmEndGetDataExIn_t *tsmEndGetDataExInP,
    tsmEndGetDataExOut_t *tsmEndGetDataExOutP
);

extern dsInt16_t DSMLINKAGE tsmEndGetObj(
    dsUInt32_t        tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmEndQuery(
    dsUInt32_t        tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmEndSendObj(
    dsUInt32_t        tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmEndSendObjEx(
    tsmEndSendObjExIn_t *tsmEndSendObjExInP,
    tsmEndSendObjExOut_t *tsmEndSendObjExOutP
);

extern dsInt16_t DSMLINKAGE tsmEndTxn(
    dsUInt32_t        tsmHandle,
    dsUInt8_t         vote,
    dsUInt16_t        *reason
);

extern dsInt16_t DSMLINKAGE tsmEndTxnEx(
    tsmEndTxnExIn_t   *tsmEndTxnExInP,
    tsmEndTxnExOut_t  *tsmEndTxnExOutP
);

extern dsInt16_t DSMLINKAGE tsmGetData(
    dsUInt32_t        tsmHandle,
    DataBlk*dataBlkPtr
);

extern dsInt16_t DSMLINKAGE tsmGetBufferData(
    getBufferDataIn_t *tsmGetBufferDataInP,
    getBufferDataOut_t *tsmGetBufferDataOutP
);

extern dsInt16_t DSMLINKAGE tsmGetNextQObj(
    dsUInt32_t        tsmHandle,
    DataBlk*dataBlkPtr
);

extern dsInt16_t DSMLINKAGE tsmGetObj(

```

```

        dsUint32_t          tsmHandle,
        ObjID              *objIdP,
        DataBlk            *dataBlkPtr
    );

extern dsInt16_t DSMLINKAGE tsmGroupHandler(
    tsmGroupHandlerIn_t   *tsmGroupHandlerInP,
    tsmGroupHandlerOut_t  *tsmGroupHandlerOutP
);

extern dsInt16_t DSMLINKAGE tsmInitEx(
    dsUint32_t            *tsmHandleP,
    tsmInitExIn_t         *tsmInitExInP,
    tsmInitExOut_t        *tsmInitExOutP
);

extern dsInt16_t DSMLINKAGE tsmLogEventEx(
    dsUint32_t            tsmHandle,
    tsmLogExIn_t          *tsmLogExInP,
    tsmLogExOut_t         *tsmLogExOutP
);

extern dsInt16_t DSMLINKAGE tsmQueryAccess(
    dsUint32_t            tsmHandle,
    tsmQryRespAccessData **accessListP,
    dsUint16_t            *numberOfRules
);

extern void DSMLINKAGE      tsmQueryApiVersionEx(
    tsmApiVersionEx        *apiVersionP
);

extern dsInt16_t DSMLINKAGE tsmQueryCliOptions(
    tsmOptStruct            *optstructP
);

extern dsInt16_t DSMLINKAGE tsmQuerySessInfo(
    dsUint32_t              tsmHandle,
    tsmApiSessInfo          *SessInfoP
);

extern dsInt16_t DSMLINKAGE tsmQuerySessOptions(
    dsUint32_t              tsmHandle,
    tsmOptStruct            *optstructP
);

extern dsInt16_t DSMLINKAGE tsmRCMsg(
    dsUint32_t              tsmHandle,
    dsInt16_t               tsmRC,
    dsChar_t                *msg
);

extern dsInt16_t DSMLINKAGE tsmRegisterFS(
    dsUint32_t              tsmHandle,
    tsmRegFSData            *regFilespaceP
);

extern dsInt16_t DSMLINKAGE tsmReleaseBuffer(
    releaseBufferIn_t       *tsmReleaseBufferInP,
    releaseBufferOut_t      *tsmReleaseBufferOutP
);

extern dsInt16_t DSMLINKAGE tsmRenameObj(
    tsmRenameIn_t           *tsmRenameInP,
    tsmRenameOut_t          *tsmRenameOutP
);

extern dsInt16_t DSMLINKAGE tsmRequestBuffer(
    requestBufferIn_t        *tsmRequestBufferInP,
    requestBufferOut_t       *tsmRequestBufferOutP
);

extern dsInt16_t DSMLINKAGE tsmRetentionEvent(
    tsmRetentionEventIn_t   *tsmRetentionEventInP,
    tsmRetentionEventOut_t  *tsmRetentionEventOutP
);

```



```

);

extern dsInt16_t DSMLINKAGE tsmSendBufferData(
    sendBufferDataIn_t *tsmSendBufferDataInP,
    sendBufferDataOut_t *tsmSendBufferDataOutP
);

extern dsInt16_t DSMLINKAGE tsmSendData(
    dsUInt32_t tsmHandle,
    DataBlk *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE tsmSendObj(
    dsUInt32_t tsmHandle,
    tsmSendType sendType,
    void *sendBuff,
    tsmObjName *objNameP,
    tsmObjAttr *objAttrPtr,
    DataBlk *dataBlkPtr
);

extern dsInt16_t DSMLINKAGE tsmSetAccess(
    dsUInt32_t tsmHandle,
    tsmAccessType accessType,
    tsmObjName *objNameP,
    dsChar_t *node,
    dsChar_t *owner
);

extern dsInt16_t DSMLINKAGE tsmSetUp(
    dsBool_t mtFlag,
    tsmEnvSetUp *envSetUpP
);

extern dsInt16_t DSMLINKAGE tsmTerminate(
    dsUInt32_t tsmHandle
);

extern dsInt16_t DSMLINKAGE tsmUpdateFS(
    dsUInt32_t tsmHandle,
    dsChar_t *fs,
    tsmFSUpd *fsUpdP,
    dsUInt32_t fsUpdAct
);

extern dsInt16_t DSMLINKAGE tsmUpdateObj(
    dsUInt32_t tsmHandle,
    tsmSendType sendType,
    void *sendBuff,
    tsmObjName *objNameP,
    tsmObjAttr *objAttrPtr,
    dsUInt32_t objUpdAct
);

extern dsInt16_t DSMLINKAGE tsmUpdateObjEx(
    tsmUpdateObjExIn_t *tsmUpdateObjExInP,
    tsmUpdateObjExOut_t *tsmUpdateObjExOutP
);

#endif /* ifdef DYNALOAD */

#if defined(__cplusplus)
}
#endif

#endif /* _H_TSMAPIFP */

```

## Documentación de interfaz de programación de aplicaciones en archivos PDF

La información acerca de la API (interfaz de programación de aplicaciones) de IBM Spectrum Protect que está disponible en IBM Knowledge Center también está disponible en archivos PDF.

- Uso de la interfaz de programación de aplicaciones
- Códigos de retorno de la interfaz de programación de aplicaciones y mensajes del cliente

**Información relacionada:**

Soluciones de desarrollo con interfaz de programación de aplicaciones

## Rendimiento

---

Existen muchos factores que afectan el rendimiento del servidor y de los clientes, incluyendo sistemas operativos, sistema de hardware, configuraciones de red, tipos de dispositivos de almacenamiento y tamaños y números de archivos de cliente. Las interacciones entre estos factores pueden hacer que la optimización del rendimiento sea compleja.

En este release no se incluye una versión actualizada del componente de rendimiento. Para obtener la documentación que trata sobre el rendimiento, consulte la Versión 8.1.0.

## Resolución de problemas

---


Hay procedimientos de resolución de problemas disponibles para el diagnóstico y la resolución de problemas.

Este release no incluye una versión actualizada del componente de resolución de problemas. Para obtener la documentación que trata sobre la resolución de problemas, consulte la Versión 8.1.0.

## Mensajes, códigos de retorno y códigos de error

---

Hay disponibles explicaciones y acciones recomendadas para los mensajes emitidos por los componentes de IBM Spectrum Protect.

- Introducción a los mensajes
- Códigos de retorno de IBM Global Security Kit  
El servidor y el cliente utilizan el proceso de IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre el servidor y el cliente de archivado y copia de seguridad. Algunos mensajes que se emiten para el proceso de SSL incluyen códigos de retorno de GSKit.
- ANE: eventos del cliente registrados en el servidor
- ANR: mensajes comunes del servidor y específicos de la plataforma
- ANS: mensajes del cliente
- Códigos de retorno de API
- Descripciones de código de error de E/S en mensajes de servidor
- Códigos de error de dispositivo en el registro de errores del sistema AIX
-  Resolución de problemas (V8.1.0 es la publicación más reciente)

## Introducción a los mensajes

---

Los mensajes, códigos de error y códigos de retorno son emitidos por el servidor y los clientes de IBM Spectrum Protect.

Los mensajes y los códigos pueden aparecer en la consola del servidor, el cliente administrativo, una terminal del operador, la interfaz gráfica de usuario administrativa, el cliente de archivado y copia de seguridad o el cliente de gestión de almacenamiento jerárquico (cliente HSM).

IBM Spectrum Protect proporciona anotaciones de actividades para ayudar al administrador a hacer un seguimiento de la actividad del servidor y a supervisar el sistema. Las anotaciones de actividad contienen los mensajes que genera el servidor, y están almacenadas en la base de datos. El servidor elimina automáticamente los mensajes de las anotaciones de actividad una vez expirado el período de retención. Los mensajes de error enviados a la consola del servidor se almacenan en las anotaciones de actividades. Ejemplos de tipos de mensajes almacenados en las anotaciones de actividades incluyen:

- Cuándo se inician o finalizan las sesiones de cliente.
- Cuándo se inicia o finaliza la migración.
- Cuándo han caducado los archivos de copia de seguridad del almacenamiento del servidor
- Cualquier salida generada desde los procesos de fondo

Algunos mensajes no tienen explicaciones y no se publican. El cliente puede enviar estadísticas al servidor que proporciona la información sobre una copia de seguridad o restauración. Esas estadísticas son mensajes informativos que pueden activarse o desactivarse en los varios receptores de anotaciones de eventos. Estos mensajes no se publican.

- Formato de los mensajes de cliente y servidor de IBM Spectrum Protect
- Interpretación de los mensajes de código de retorno

**Tareas relacionadas:**

↳ Uso del registro de actividad (V7.1.1)

## Formato de los mensajes de cliente y servidor de IBM Spectrum Protect

Los mensajes de cliente y servidor IBM Spectrum Protect constan de los siguientes elementos:

- Un prefijo de tres letras. Los mensajes tiene distintos prefijos que ayudan a identificar el componente IBM Spectrum Protect que emite el mensaje. Generalmente, todos los mensajes de un componente tienen el mismo prefijo. A veces un componente emite mensajes con dos o tres prefijos diferentes.

Por ejemplo, los clientes de archivado y copia de seguridad emiten mensajes con el prefijo ANS. Los eventos de cliente de archivado y copia de seguridad que se registran en el servidor tienen el prefijo ANE. Los mensajes comunes del servidor y específicos de la plataforma del servidor tienen el prefijo ANR.

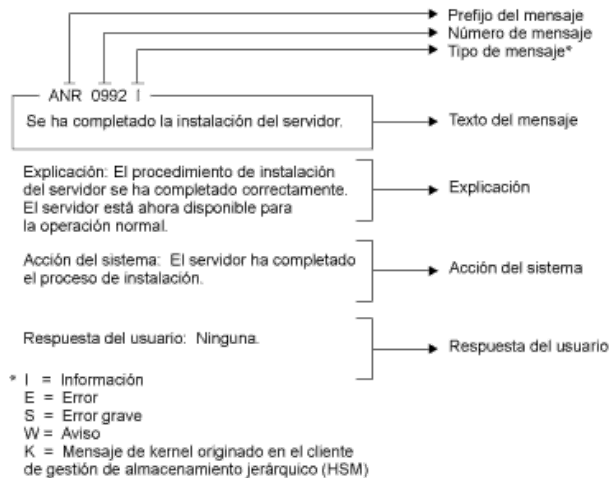
- Identificador de mensaje numérico.
- Un código de gravedad de una letra. Los códigos siguientes indican la gravedad de la acción que ha generado el mensaje:

Código	Gravedad	Significado
S	Grave	El producto o una función del producto no puede continuar. Es necesaria una respuesta del usuario.
E	Error	Se ha encontrado un error durante el proceso. El proceso puede llegar a detenerse. Puede ser necesaria una respuesta del usuario.
Sem	Aviso	El proceso continúa, pero pueden producirse problemas más adelante como resultado del aviso.
I	Información	El proceso continúa. No es necesaria ninguna respuesta por parte del usuario.

- Un mensaje de texto que se muestra en pantalla y está escrito en las anotaciones de mensajes.
- Textos Explicación, Acción del sistema, y Respuesta del usuario. Estos textos se profundizan en el texto de mensaje y están disponibles en las publicaciones de mensajes de producto y en la ayuda de línea de mandatos.

La imagen siguiente presenta un mensaje de servidor de IBM Spectrum Protect típico.

Los globos identifican cada elemento del mensaje.



Las variables de mensaje del texto del mensaje aparecen en cursiva.

## Interpretación de los mensajes de código de retorno

Muchos mandatos distintos pueden generar el mismo *código de retorno*. Los siguientes ejemplos son ilustraciones de dos mandatos distintos emitidos que producen el mismo código de retorno; por lo tanto, debe leer el *mensaje descriptivo* para el mandato.

En estos ejemplos, dos mandatos diferentes proporcionan el mismo código de retorno, pero también devuelven mensajes descriptivos que son únicos para cada mandato. Los dos mandatos son `q event standard dddd def vol cstg05 primary`. Ambos proporcionan un mensaje genérico con un código de retorno:

ANS5102I: Código de retorno 11.

Pero el primer mandato también proporciona un mensaje descriptivo:

ANR2034I: QUERY EVENT: No se ha encontrado coincidencia para esta consulta.

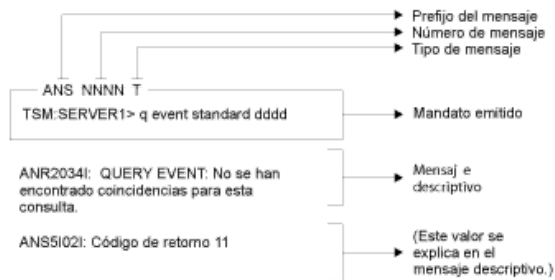
Y el segundo mandato también proporciona un mensaje único descriptivo:

ANRxxxx: DEFINE VOLUME: No se ha definido la agrupación de almacenamiento CSTG05.

- Ejemplo uno para el mandato QUERY EVENT
- Ejemplo dos para el mandato DEFINE VOLUME

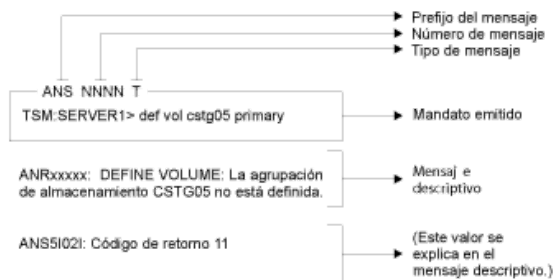
## Ejemplo uno para el mandato QUERY EVENT

---



## Ejemplo dos para el mandato DEFINE VOLUME

---



## Mensajes de ANE

---

El servidor emite los mensajes de ANE. Todos los mensajes con prefijo ANE son sucesos de cliente registrados en el servidor.

- Lista de mensajes de ANE

## Mensajes de ANR

---

El servidor emite los mensajes de ANR. Algunos mensajes ANR son comunes para todos los sistemas operativos, y algunos son específicos a un único sistema operativo.

- Lista de mensajes de ANR

## Mensajes ANS 0000-9999

---

Los mensajes ANS con números de mensaje en el rango 0000-9999 los emiten los siguientes clientes de IBM Spectrum Protect:

- Clientes de administración

- Clientes de interfaz de programación de aplicaciones
- Clientes del archivo de copia de seguridad
- IBM Spectrum Protect para los clientes de Space Management (HSM)

Hay disponible una lista de mensajes nuevos y modificados desde el nivel de modificación del producto anterior en el archivo `client_message.chg` del directorio de instalación de productos. Las listas de los mensajes del cliente nuevos y modificados para V8.1.2 y posteriores también están disponibles en la wiki de IBM developerWorks.

- Lista de mensajes de ANS

## Códigos de retorno API

En la lista se muestran los códigos de retorno de la API de IBM Spectrum Protect V8.1.2. Se describe el formato de los códigos de retorno.

Adicionalmente, algunos mensajes emitidos por el proceso de SSL incluyen códigos de retorno de GSKit. Consulte [Códigos de retorno de IBM Global Security Kit](#) para obtener más detalles.

- Formato de códigos de retorno API
- Códigos de retorno API

## Formato de códigos de retorno API

En esta sección se describe el formato del código de retorno API (Interfaz de programación de aplicación). Se suministra la siguiente información para cada código de retorno:

- El número del código de retorno. Este número corresponde al número del archivo de cabecera **dsmrc.h**.
- El código de gravedad. Esta letra es una indicación de la gravedad que ha generado el código de retorno. Los códigos de gravedad y sus significados son:

<b>S</b>	Error grave	El proceso no puede continuar.
<b>E</b>	Error	El proceso no puede continuar.
<b>W</b>	Aviso	El proceso puede continuar, pero es posible que posteriormente se generen problemas. Debería proceder con cautela.
<b>I</b>	Información	El proceso continúa. No es necesaria ninguna respuesta por parte del usuario.

- El nombre simbólico. Este nombre corresponde a la definición del archivo de cabecera **dsmrc.h**. *Utilice siempre el nombre simbólico para un código de retorno en lugar del número del código de retorno.*
- La descripción. Este campo explica las circunstancias bajo las que es posible que se genere este código de retorno.
- La acción del sistema. Este campo describe la acción que IBM Spectrum Protect va a emprender en respuesta al código de retorno.
- La respuesta del usuario. Este campo explica cómo debe responder ante la acción del sistema.

Muchos códigos de retorno describen errores que provocan que el proceso se detenga. Puede enviar un mensaje al usuario final que describa el problema y sugerirle una línea de actuación. Para identificar distintos mensajes, utilice estos valores de código de retorno o desarrolle su propio sistema de numeración.

## Códigos de retorno API

Los códigos de retorno de la API de IBM Spectrum Protect V8.1.2 API se muestran en la lista en orden numérico ascendente. Se documenta el código de retorno completo.

- -452 E  
DSM\_RC\_SHM\_NOTAUTH Autorización insuficiente para conectarse a la región de memoria compartida
- -451 E  
DSM\_RC\_SHM\_FAILURE Se ha producido un error al utilizar el protocolo de memoria compartida
- -450 E  
DSM\_RC\_SHM\_TCPIP\_FAILURE Sesión rechazada: ha fallado la conexión TCP/IP para la Memoria compartida
- -190 E  
DSM\_RC\_NP\_ERROR Sesión rechazada: ha fallado la conexión de Named Pipes.
- -057 E  
DSM\_RC\_TCPIP\_LOADFAILURE La función de carga del TCP/IP ha fallado.
- -056 E  
DSM\_RC\_TCPIP\_DLL\_LOADFAILURE Se ha producido un error al cargar una biblioteca.

- -055 E  
DSM\_RC\_WINSOCK\_MISSING No se puede encontrar el archivo TCP/IP WINSOCK.DLL.
- -054 E  
DSM\_RC\_NETWORK\_UNREACHABLE El nombre de host TCP/IP especificado es inalcanzable
- -053 E  
DSM\_RC\_BAD\_HOST\_NAME Se ha especificado una dirección del TCP/IP no correcta.
- -052 E  
DSM\_RC\_CONN\_REFUSED El host ha rechazado un intento de establecer una conexión de TCP/IP
- -051 E  
DSM\_RC\_CONN\_TIMEDOUT El intento de establecer una conexión TCP/IP ha excedido el tiempo de espera antes de que se realizara la conexión.
- -050 E  
DSM\_RC\_TCPIP\_FAILURE Sesión rechazada: Error de conexión con TCP/IP.
- 0000 I  
DSM\_RC\_OK Se ha realizado satisfactoriamente.
- 0001 E  
DSM\_RC\_ABORT\_SYSTEM\_ERROR Esta operación no puede continuar debido a un error en el servidor IBM Spectrum Protect. Póngase en contacto con el administrador del servidor IBM Spectrum Protect para obtener ayuda.
- 0002 E  
DSM\_RC\_ABORT\_NO\_MATCH No hay objetos en el servidor que coincidan con la consulta
- 0003 E  
DSM\_RC\_ABORT\_BY\_CLIENT El cliente ha finalizado la transacción
- 0004 W  
DSM\_RC\_ABORT\_ACTIVE\_NOT\_FOUND No se ha encontrado ninguna versión de copia de seguridad activa.
- 0005 E  
DSM\_RC\_ABORT\_NO\_DATA El servidor IBM Spectrum Protect no tiene datos para el objeto.
- 0006 E  
DSM\_RC\_ABORT\_BAD\_VERIFIER Ha entrado una contraseña incorrecta.
- 0007 E  
DSM\_RC\_ABORT\_NODE\_IN\_USE El nodo está en uso
- 0008 E  
DSM\_RC\_ABORT\_EXPIRATE\_TOO\_LOW La fecha de caducidad debe ser posterior a la fecha de hoy
- 0009 W  
DSM\_RC\_ABORT\_DATA\_OFFLINE Los datos solicitados están fuera de línea.
- 0010 E  
DSM\_RC\_ABORT\_EXCLUDED\_BY\_SIZE El objeto es demasiado grande para los límites del servidor
- 0011 E  
DSM\_RC\_ABORT\_NO\_REPOSIT\_SPACE El servidor se ha quedado sin espacio de almacenamiento de datos
- 0012 E  
DSM\_RC\_ABORT\_MOUNT\_NOT\_POSSIBLE No es posible el montaje de soportes del servidor
- 0013 E  
DSM\_RC\_ABORT\_SIZEESTIMATE\_EXCEED Se ha excedido el tamaño estimado
- 0014 E  
DSM\_RC\_ABORT\_DATA\_UNAVAILABLE En este momento no hay datos del archivo disponibles en el servidor
- 0015 E  
DSM\_RC\_ABORT\_RETRY Solicitud de reintento inesperada. El servidor IBM Spectrum Protect ha encontrado un error al grabar los datos.
- 0016 E  
DSM\_RC\_ABORT\_NO\_LOG\_SPACE El servidor no tiene suficiente espacio de registro de recuperación para continuar la operación actual
- 0017 E  
DSM\_RC\_ABORT\_NO\_DB\_SPACE El servidor no tiene suficiente espacio de base de datos para continuar la operación actual
- 0018 E  
DSM\_RC\_ABORT\_NO\_MEMORY El servidor no tiene suficiente memoria para continuar con la operación actual
- 0020 E  
DSM\_RC\_ABORT\_FS\_NOT\_DEFINED El espacio de archivos especificado no existe en el servidor. Es posible que el espacio de archivos haya sido suprimido por otro cliente o un administrador.
- 0021 S  
DSM\_RC\_ABORT\_NODE\_ALREADY\_DEFINED El registro abierto ha fallado porque el nombre de nodo especificado está definido en el servidor
- 0022 S  
DSM\_RC\_ABORT\_NO\_DEFAULT\_DOMAIN El registro abierto ha fallado porque no existe ningún dominio predeterminado
- 0023 S  
DSM\_RC\_ABORT\_INVALID\_NODENAME El registro abierto ha fallado porque se ha especificado un nombre de nodo que no es



- válido
- 0024 S  
DSM\_RC\_ABORT\_INVALID\_POL\_BIND Se ha producido un problema de gestión de políticas en el servidor IBM Spectrum Protect.
- 0024 E  
DSM\_RC\_ABORT\_NO\_INVALID\_POL\_BIND Se ha enlazado un objeto de la transacción a una clase de gestión que no es válida.
- 0025 E  
DSM\_RC\_ABORT\_DEST\_NOT\_DEFINED Problema del servidor: Destino no definido.
- 0026 S  
DSM\_RC\_ABORT\_WAIT\_FOR\_SPACE El servidor IBM Spectrum Protect no tiene actualmente espacio en la agrupación de almacenamiento para este archivo. Puede tratarse de una condición temporal.
- 0027 E  
DSM\_RC\_ABORT\_NOT\_AUTHORIZED No se puede suprimir el espacio de archivos debido a que este nodo no tiene permiso para suprimir datos archivados o de copia de seguridad.
- 0028 E  
DSM\_RS\_ABORT\_RULE\_ALREADY\_DEFED Ya se ha definido la regla de acceso 'regla\_acceso' para el nodo 'nodo '. Es necesario suprimir la regla antigua para que se pueda definir una nueva.
- 0029 S  
DSM\_RC\_ABORT\_NO\_STOR\_SPACE\_STOP El servidor se ha quedado sin espacio de almacenamiento de datos
- 0030 E  
DSM\_RC\_ABORT\_LICENSE\_VIOLATION La operación no está permitida debido a los valores de las licencias del servidor
- 0032 E  
DSM\_RC\_ABORT\_DUPLICATE\_OBJECT Se ha encontrado un objeto duplicado, la operación no se puede completar.
- 0033 E  
DSM\_RC\_ABORT\_INVALID\_OFFSET El valor de partialObjOffset para la recuperación de objeto parcial no es válido.
- 0034 E  
DSM\_RC\_ABORT\_INVALID\_LENGTH El valor de partialObjLength para la recuperación de objetos parcial no es válido.
- 0036 E  
DSM\_RC\_END\_NODE\_NOT\_AUTHORIZED El nodo o usuario no tiene la autorización adecuada para realizar esta operación
- 0041 E  
DSM\_RC\_ABORT\_EXCEED\_MAX\_MP Este nodo ha excedido su número máximo de puntos de montaje.
- 0045 E  
DSM\_RC\_ABORT\_MERGE\_ERROR Los objetos especificados han fallado la prueba de fusión.
- 0047 E  
DSM\_RC\_ABORT\_INVALID\_OPERATION Se ha intentado una operación no válida en un nodo
- 0048 E  
DSM\_RC\_ABORT\_STGPOOL\_UNDEFINED La agrupación de almacenamiento de destino especificada no se ha definido.
- 0049 E  
DSM\_RC\_ABORT\_INVALID\_DATA\_FORMAT Una agrupación de almacenamiento de destino no tiene el formato de datos correcto para el tipo de nodo proporcionado.
- 0050 E  
DSM\_RC\_ABORT\_DATAMOVER\_UNDEFINED No se ha definido ningún transportador de datos asociado para el nodo especificado.
- 0051 E  
DSM\_RC\_REJECT\_NO\_RESOURCES Sesión rechazada: Todas las sesiones de servidor están en uso en este momento
- 0052 E  
DSM\_RC\_REJECT\_VERIFIER\_EXPIRED Se ha rechazado la sesión. Su contraseña ha caducado.
- 0053 E  
DSM\_RC\_REJECT\_ID\_UNKNOWN Sesión rechazada: El ID de usuario es incorrecto, no tiene autorización de administrador o el servidor no lo conoce
- 0054 E  
DSM\_RC\_REJECT\_DUPLICATE\_ID Sesión rechazada: Se ha especificado un ID duplicado
- 0055 E  
DSM\_RC\_REJECT\_SERVER\_DISABLED Sesión rechazada: Servidor inhabilitado.
- 0056 E  
DSM\_RC\_REJECT\_CLOSED\_REGISTER El servidor no está configurado para permitir una inscripción abierta
- 0057 S  
DSM\_RC\_REJECT\_CLIENT\_DOWNLEVEL Sesión rechazada: Versión de código de cliente de nivel inferior
- 0058 S  
DSM\_RC\_REJECT\_SERVER\_DOWNLEVEL Sesión rechazada: Versión de código de servidor de nivel inferior
- 0059 E  
DSM\_RC\_REJECT\_ID\_IN\_USE Sesión rechazada: el nombre de nodo especificado está actualmente en uso
- 0061 E  
DSM\_RC\_REJECT\_ID\_LOCKED Sesión rechazada: El nombre de nodo especificado está bloqueado actualmente.

- 0062 S  
DSM\_RC\_SIGNONREJECT\_LICENSE\_MAX SLM LICENSE EXCEEDED: Las licencias de cliente para IBM Spectrum Protect se han superado. Consulte con el administrador del sistema.
- 0063 E  
DSM\_RC\_REJECT\_NO\_MEMORY Sesión rechazada: El servidor no tiene suficiente memoria para permitir que se establezca una conexión.
- 0064 E  
DSM\_RC\_REJECT\_NO\_DB\_SPACE Sesión rechazada: El servidor no tiene suficiente espacio de base de datos para permitir que se establezca una conexión.
- 0065 E  
DSM\_RC\_REJECT\_NO\_LOG\_SPACE Sesión rechazada: El servidor no tiene suficiente espacio de registro de recuperación para permitir que se establezca una conexión.
- 0066 E  
DSM\_RC\_REJECT\_INTERNAL\_ERROR Se ha rechazado la sesión. El servidor IBM Spectrum Protect tiene un error interno.
- 0067 S  
DSM\_RC\_SIGNONREJECT\_INVALID\_CLI Sesión rechazada: El servidor no tiene licencia para este tipo de plataforma. Consulte con el administrador del sistema.
- 0068 E  
DSM\_RC\_CLIENT\_NOT\_ARCHRETPROT Se ha rechazado la sesión. El servidor no permite un inicio de sesión de un cliente que no tenga activada la protección de retención de copia archivada.
- 0069 E  
DSM\_RC\_SESSION\_CANCELED Sesión rechazada: El administrador del sistema canceló la sesión.
- 0073 E  
DSM\_RC\_REJECT\_INVALID\_NODE\_TYPE Se ha detectado una incoherencia entre el nodo de cliente y el nodo que está registrado en el servidor IBM Spectrum Protect.
- 0074 E  
DSM\_RC\_REJECT\_INVALID\_SESSIONINIT El servidor no permite conexiones iniciadas por el cliente para este nodo.
- 0075 E  
DSM\_RC\_REJECT\_WRONG\_PORT Puerto de servidor incorrecto.
- 0079 E  
DSM\_RC\_CLIENT\_NOT\_SPMRETPROT Se ha rechazado la sesión. El servidor no permite un inicio de sesión de un cliente que no tenga activada la protección de retención gestionada por espacios.
- 0101 W  
DSM\_RC\_USER\_ABORT El usuario ha detenido la operación.
- 0102 E  
DSM\_RC\_NO\_MEMORY nombre archivo(número línea) El sistema operativo ha rechazado una solicitud de IBM Spectrum Protect de asignación de memoria.
- 0104 E  
DSM\_RC\_FILE\_NOT\_FOUND No se ha encontrado el archivo durante el proceso de copia de seguridad, archivado o migración
- 0105 E  
DSM\_RC\_PATH\_NOT\_FOUND No se ha encontrado la vía de acceso de directorio especificada 'vía-acceso'.
- 0106 E  
DSM\_RC\_ACCESS\_DENIED Se ha denegado el acceso al archivo o directorio especificado
- 0106 E  
DSM\_RC\_ACCESS\_DENIED El archivo especificado está siendo utilizado por otro proceso
- 0107 E  
DSM\_RC\_NO\_HANDLES No hay descriptores de contexto de archivo disponibles
- 0108 E  
DSM\_RC\_FILE\_EXISTS El archivo sale y no se puede sobrescribir.
- 0109 E  
DSM\_RC\_INVALID\_PARM Se ha encontrado un parámetro no válido.
- 0110 E  
DSM\_RC\_INVALID\_HANDLE Se ha especificado un descriptor de contexto de archivo que no es válido; error del sistema.
- 0111 E  
DSM\_RC\_DISK\_FULL El proceso se ha detenido; El disco está lleno
- 0113 E  
DSM\_RC\_PROTOCOL\_VIOLATION Violación de protocolo
- 0114 E  
DSM\_RC\_UNKNOWN\_ERROR Se ha producido un error de sistema desconocido del que IBM Spectrum Protect no se puede recuperar.
- 0115 E  
DSM\_RC\_UNEXPECTED\_ERROR Se ha producido un error inesperado.
- 0116 E  
DSM\_RC\_FILE\_BEING\_EXECUTED El archivo está en uso; Permiso de escritura denegado.

- 0117 E  
DSM\_RC\_DIR\_NO\_SPACE No se pueden restaurar o recuperar más archivos porque el directorio de destino está lleno.
- 0118 E  
DSM\_RC\_LOOPED\_SYM\_LINK Se han detectado demasiados vínculos simbólicos mientras se resolvía el nombre
- 0119 E  
DSM\_RC\_FILE\_NAME\_TOO\_LONG El nombre de archivo es demasiado largo y IBM Spectrum Protect no lo puede procesar
- 0120 E  
DSM\_RC\_FILE\_SPACE\_LOCKED El sistema de archivos está bloqueado por el sistema
- 0121 I  
DSM\_RC\_FINISHED La operación ha finalizado.
- 0122 E  
DSM\_RC\_UNKNOWN\_FORMAT El archivo tiene un formato desconocido.
- 0123 E  
DSM\_RC\_NO\_AUTHORIZATION No autorizado a restaurar los datos del otro nodo.
- 0124 E  
DSM\_RC\_FILE\_SPACE\_NOT\_FOUND El espacio de archivos 'nombre\_espacio\_archivos' no existe
- 0125 E  
DSM\_RC\_TXN\_ABORTED La transacción ha terminado anormalmente
- 0126 E  
DSM\_RC\_SUBDIR\_AS\_FILE IBM Spectrum Protect no puede crear una vía de acceso del directorio porque existe un archivo con el mismo nombre que el directorio.
- 0127 E  
DSM\_RC\_PROCESS\_NO\_SPACE Se ha alcanzado el límite de espacio de disco para este proceso
- 0128 E  
DSM\_RC\_PATH\_TOO\_LONG La longitud de la vía de acceso de directorio de destino supera el máximo del sistema
- 0129 E  
DSM\_RC\_NOT\_COMPRESSED El archivo no está comprimido; Anomalía del sistema.
- 0130 E  
DSM\_RC\_TOO\_MANY\_BITS El archivo se ha comprimido en una máquina cliente distinta que tiene más memoria
- 0131 E  
DSM\_RC\_COMPRESSED\_DATA\_CORRUPTED El archivo comprimido está dañado y no se puede expandir correctamente.
- 0131 S  
DSM\_RC\_SYSTEM\_ERROR Se ha producido un error de programa interno.
- 0132 E  
DSM\_RC\_NO\_SERVER\_RESOURCES El servidor IBM Spectrum Protect se ha quedado sin recursos.
- 0133 E  
DSM\_RC\_FS\_NOT\_KNOWN No se ha podido encontrar el espacio de archivos para el dominio 'nombre-dominio' en el servidor de IBM Spectrum Protect.
- 0134 E  
DSM\_RC\_NO\_LEADING\_DIRSEP El campo objName no tiene un separador de directorio.
- 0135 E  
DSM\_RC\_WILDCARD\_DIR No se permiten caracteres comodín en la vía de acceso de directorio de objName.
- 0136 E  
DSM\_RC\_COMM\_PROTOCOL\_ERROR Se ha rechazado la sesión: se ha producido un error en el protocolo de comunicaciones.
- 0137 E  
DSM\_RC\_AUTH\_FAILURE Sesión rechazada: Error de autenticación
- 0138 E  
DSM\_RC\_TA\_NOT\_VALID Los permisos de ejecución/propietario de dsmtca no son válidos.
- 0139 S  
DSM\_RC\_KILLED Proceso interrumpido.
- 0145 S  
DSM\_RC\_WOULD\_BLOCK dsmtca bloqueará la operación.
- 0146 S  
DSM\_RC\_TOO\_SMALL El área para el patrón de inclusión/exclusión es demasiado pequeña.
- 0147 S  
DSM\_RC\_UNCLOSED No hay ningún corchete de cierre en el patrón.
- 0148 S  
DSM\_RC\_NO\_STARTING\_DELIMITER El patrón inclusión/exclusión debe comenzar con un delimitador de directorio
- 0149 S  
DSM\_RC\_NEEDED\_DIR\_DELIMITER Falta el delimitador de directorio de comienzo o finalización del patrón Incluir/Excluir.
- 0151 S  
DSM\_RC\_BUFFER\_OVERFLOW El almacenamiento intermedio de datos se ha desbordado.
- 0154 E  
DSM\_RC\_NO\_COMPRESS\_MEMORY No hay memoria suficiente para la compresión/expansión del archivo

- 0155 T  
DSM\_RC\_COMPRESS\_GREW Crecimiento de datos comprimidos
- 0156 E  
DSM\_RC\_INV\_COMM\_METHOD Se ha especificado un método de comunicaciones no admitido.
- 0157 S  
DSM\_RC\_WILL\_ABORT La transacción terminará anormalmente.
- 0158 E  
DSM\_RC\_FS\_WRITE\_LOCKED El archivo o el directorio destino está bloqueado contra grabación
- 0159 I  
DSM\_RC\_SKIPPED\_BY\_USER Se ha omitido un archivo durante una operación de restauración porque el archivo está fuera de línea y la aplicación ha elegido no esperar un montaje de cinta.
- 0160 E  
DSM\_RC\_TA\_NOT\_FOUND No se encuentra el módulo dsmtca.
- 0162 E  
DSM\_RC\_FS\_NOT\_READY El sistema/unidad de archivos no está preparado
- 0164 E  
DSM\_RC\_FIO\_ERROR Error de la entrada/salida del archivo
- 0165 E  
DSM\_RC\_WRITE\_FAILURE Error al grabar el archivo
- 0166 E  
DSM\_RC\_OVER\_FILE\_SIZE\_LIMIT El archivo supera los límites del archivo del sistema/usuario
- 0167 E  
DSM\_RC\_CANNOT\_MAKE No es posible crear archivo/directorio
- 0168 E  
DSM\_RC\_NO\_PASS\_FILE El archivo de contraseña no está disponible.
- 0169 E  
DSM\_RC\_VERFILE\_OLD PASSWORDACCESS es GENERATE, pero se necesita la contraseña para el servidor 'nombre\_servidor'. La contraseña no está almacenada localmente, o se cambió en el servidor.
- 0173 E  
DSM\_RC\_INPUT\_ERROR El proceso se está ejecutando en un modo no interactivo, pero requiere la entrada del usuario.
- 0174 E  
DSM\_RC\_REJECT\_PLATFORM\_MISMATCH Sesión rechazada: el tipo de nodo no coincide
- 0175 E  
DSM\_RC\_TL\_NOT\_FILE\_OWNER No es el propietario del archivo
- 0177 S  
DSM\_RC\_UNMATCHED\_QUOTE Las comillas no coinciden
- 0184 E  
DSM\_RC\_TL\_NOBCG La clase de gestión de este archivo no tiene un grupo de copia de seguridad válido. No se realizará la copia de seguridad de este archivo.
- 0185 W  
DSM\_RC\_TL\_EXCLUDED El archivo 'nombre\_archivo nombre\_archivonombre\_archivo' se ha excluido por una lista de inclusión/exclusión
- 0186 E  
DSM\_RC\_TL\_NOACG La clase de gestión para este archivo no tiene un grupo de copia de archivado especificado. Este archivo no se archivará.
- 0187 E  
DSM\_RC\_PS\_INVALID\_ARCHMC Se ha especificado una clase de gestión que no es válida
- 0188 S  
DSM\_RC\_NO\_PS\_DATA Bien el nodo no existe en el servidor o bien no hay un conjunto de políticas activas para el nodo.
- 0189 S  
DSM\_RC\_PS\_INVALID\_DIRMC La clase de gestión asignada a los directorios no existe.
- 0190 S  
DSM\_RC\_PS\_NO\_CG\_IN\_DIR\_MC No hay ningún grupo de copia de seguridad en la clase de gestión utilizada para los directorios.
- 0231 E  
DSM\_RC\_ABORT\_MOVER\_TYPE Tipo Remote Mover desconocido
- 0232 E  
DSM\_RC\_ABORT\_ITEM\_IN\_USE Una operación para el nodo y el espacio de archivos solicitados ya está en curso.
- 0233 E  
DSM\_RC\_ABORT\_LOCK\_CONFLICT Recurso de sistema en uso
- 0234 E  
DSM\_RC\_ABORT\_SRV\_PLUGIN\_COMM\_ERROR Error de comunicación del conector del servidor.
- 0235 E  
DSM\_RC\_ABORT\_SRV\_PLUGIN\_OS\_ERROR El plug-in de servidor ha detectado un sistema operativo de gestor de archivos NAS no soportado.

- 0236E  
DSM\_RC\_ABORT\_CRC\_FAILED El CRC recibido del servidor no coincide con el CRC calculado por el cliente.
- 0237E  
DSM\_RC\_ABORT\_INVALID\_GROUP\_ACTION Se ha intentado una operación no válida en un líder de grupo o miembro de grupo.
- 0238E  
DSM\_RC\_ABORT\_DISK\_UNDEFINED Disco remoto no definido.
- 0239E  
DSM\_RC\_ABORT\_BAD\_DESTINATION El destino de entrada no coincide con el destino esperado.
- 0240E  
DSM\_RC\_ABORT\_DATAMOVER\_NOT\_AVAILABLE El transportador de datos no está disponible.
- 0241E  
DSM\_RC\_ABORT\_STGPOOL\_COPY\_CONT\_NO La operación ha fallado porque la opción de copia continua se ha establecido en NO.
- 0242E  
DSM\_RC\_ABORT\_RETRY\_SINGLE\_TXN La transacción ha fallado debido a un problema ocurrido durante una operación de almacenamiento.
- 0245 E  
DSM\_RC\_ABORT\_PATH\_RESTRICTED La configuración de cliente actual no cumple con el valor de la opción de servidor DATAWRITEPATH o DATAREADPATH para este nodo.
- 0247 E  
DSM\_RC\_ABORT\_INSERT\_NOT\_ALLOWED Este servidor no admite operaciones de copia de seguridad.
- 0248 E  
DSM\_RC\_ABORT\_DELETE\_NOT\_ALLOWED Suprimiendo este objeto: "fshlll" no están permitidos.
- 0249 E  
DSM\_RC\_ABORT\_TXN\_LIMIT\_EXCEEDED El número de objetos de esta transacción ha excedido los valores de TXNGROUPMAX.
- 0250 E  
DSM\_RC\_ABORT\_OBJECT\_ALREADY\_HELD fshlll ya está en retención.
- 0292 E  
DSM\_RC\_TCA\_FORK\_FAILED Error al iniciar el proceso de dsmtca o dsmenc.
- 0295 E  
DSM\_RC\_TCA\_INVALID\_REQUEST El módulo dsmtca de IBM Spectrum Protect ha recibido una solicitud no válida.
- 0296 E  
DSM\_RC\_TCA\_NOT\_ROOT Esta acción necesita autorización administrativa de IBM Spectrum Protect en este sistema.
- 0297 E  
DSM\_RC\_TCA\_SEMGET\_ERROR Error al asignar semáforos.
- 0298 E  
DSM\_RC\_TCA\_SEM\_OP\_ERROR Error al establecer el valor de los semáforos o al esperar por un semáforo.
- 0400 E  
DSM\_RC\_INVALID\_OPT Se ha encontrado una opción no válida durante el análisis de opción.
- 0405 E  
DSM\_RC\_NO\_HOST\_ADDR TCPSERVERADDRESS no definido por este servidor en el Archivo de opciones del sistema
- 0406 S  
DSM\_RC\_NO\_OPT\_FILE o se ha podido encontrar el archivo de opciones 'file-name' o no puede leerse.
- 0408 E  
DSM\_RC\_MACHINE\_SAME Un nombre de nodo virtual no debe ser igual a un nombre de nodo o al nombre de host del sistema.
- 0409 E  
DSM\_RC\_INVALID\_SERVER No se ha encontrado el nombre del servidor en el archivo de opciones del sistema
- 0410 E  
DSM\_RC\_INVALID\_KEYWORD Se ha encontrado una palabra clave de opción no válida durante el análisis de opción.
- 0411 S  
DSM\_RC\_PATTERN\_TOO\_COMPLEX No se puede analizar el patrón de inclusión o exclusión.
- 0412 S  
DSM\_RC\_NO\_CLOSING\_BRACKET El patrón Inclusión/Exclusión ha perdido un paréntesis de cierre
- 0426 E  
DSM\_RC\_CANNOT\_OPEN\_TRACEFILE Las funciones de inicialización no pueden abrir el archivo de seguimiento especificado.
- 0427 E  
DSM\_RC\_CANNOT\_OPEN\_LOGFILE Las funciones de inicialización no pueden abrir el archivo de registro de errores especificado.
- 0600 E  
DSM\_RC\_DUP\_LABEL Hay una etiqueta de volumen duplicada. La operación no puede continuar.
- 0601 E  
DSM\_RC\_NO\_LABEL La unidad no tiene etiqueta. La operación no puede continuar.
- 0610 E  
DSM\_RC-NLS\_CANT\_OPEN\_TXT No se puede abrir el archivo de texto de mensajes.

- 0611 E  
DSM\_RC-NLS\_CANT\_READ\_HDR No se puede utilizar el archivo de texto de mensajes.
- 0612 E  
DSM\_RC-NLS\_INVALID\_CNTL\_REC No se puede utilizar el archivo de texto de mensaje.
- 0613 E  
DSM\_RC-NLS\_INVALID\_DATE\_FMT Se ha especificado un valor no válido para DATEFORMAT.
- 0614 E  
DSM\_RC-NLS\_INVALID\_TIME\_FMT Se ha especificado un valor no válido para TIMEFORMAT.
- 0615 E  
DSM\_RC-NLS\_INVALID\_NUM\_FMT Se ha especificado un valor no válido para NUMBERFORMAT.
- 0620 E  
DSM\_RC\_LOG\_CANT\_BE\_OPENED No se puede abrir el archivo de registro de errores.
- 0621 E  
DSM\_RC\_LOG\_ERROR\_WRITING\_TO\_LOG No se puede escribir en el archivo de registro.
- 0622 E  
DSM\_RC\_LOG\_NOT\_SPECIFIED No se ha especificado el nombre de archivo de registro.
- 0927 E  
DSM\_RC\_NOT\_ADSM\_AUTHORIZED Sólo un usuario autorizado de IBM Spectrum Protect puede realizar esta acción.
- 961 E  
DSM\_RC\_DIRECT\_STORAGE\_AGENT\_UNSUPPORTED No se permite la conexión directa con el agente de almacenamiento.
- 963 E  
DSM\_RC\_FS\_NAMESPACE\_DOWNLEVEL El espacio de nombres largos se ha eliminado del espacio de archivos local. Si desea continuar con la operación de copia de seguridad y archivado, renombre el espacio de archivos en el servidor.
- 0996 E  
DSM\_RC\_SERVER\_DOWNLEVEL\_FUNC El servidor IBM Spectrum Protect es de un nivel inferior y no soporta la función solicitada. Consulte las anotaciones de errores para la información de versión.
- 0997 E  
DSM\_RC\_STORAGEAGENT\_DOWNLEVEL El agente de almacenamiento de IBM Spectrum Protect es de un nivel inferior y no soporta la función solicitada. Consulte las anotaciones de errores para la información de versión.
- 0998 E  
DSM\_RC\_SERVER\_AND\_SA\_DOWNLEVEL El servidor de IBM Spectrum Protect y el agente de almacenamiento de IBM Spectrum Protect son de un nivel inferior y no soportan la función solicitada. Consulte las anotaciones de errores para la información de versión.
- 1376 E  
DSM\_RC\_DIGEST\_VALIDATION\_ERROR Se ha producido un error al procesar 'nombre espacio de archivosnombre-vía acceso nombre-archivos'; ha fallado la validación de procesamiento de punto a punto.
- 2000 E  
DSM\_RC\_NULL\_OBJNAME El puntero de nombre de objeto es NULL.
- 2001 E  
DSM\_RC\_NULL\_DATA\_BLKPTR El puntero de bloque de datos es NULL.
- 2002 E  
DSM\_RC\_NULL\_MSG El parámetro de mensaje para dsmRCMsg es un puntero NULL.
- 2004 E  
DSM\_RC\_NULL\_OBJATTRPTR El puntero de atributo de objeto es NULL.
- 2006 E  
DSM\_RC\_NO\_SESS\_BLK No hay información de sesión con el servidor.
- 2007 E  
DSM\_RC\_NO\_POLICY\_BLK No hay información de política de servidor.
- 2008 E  
DSM\_RC\_ZERO\_BUFLLEN El valor de dataBlk bufferLen es cero.
- 2009 E  
DSM\_RC\_NULL\_BUFPTR dataBlk bufferPtr es NULL.
- 2010 E  
DSM\_RC\_INVALID\_OBJTYPE El objType no es válido.
- 2011 E  
DSM\_RC\_INVALID\_VOTE El voto dsmEndTxn no es válido.
- 2012 E  
DSM\_RC\_INVALID\_ACTION La acción de actualización no es válida.
- 2014 E  
DSM\_RC\_INVALID\_DS\_HANDLE Ha habido un error en la estructura interna de la API de IBM Spectrum Protect.
- 2015 E  
DSM\_RC\_INVALID\_REPOS El tipo de repositorio no es válido.
- 2016 E  
DSM\_RC\_INVALID\_FSNAME El nombre de espacio de archivo debe empezar con el delimitador de directorio.

- 2017 E  
DSM\_RC\_INVALID\_OBJNAME El nombre de objeto es una serie vacía o no tiene delimitador inicial.
- 2018 E  
DSM\_RC\_INVALID\_LLNAME RL calificador de bajo nivel del nombre de objeto debe empezar con el delimitador de directorio.
- 2019 E  
DSM\_RC\_INVALID\_OBJOWNER El propietario de objeto no es válido.
- 2020 E  
DSM\_RC\_INVALID\_ACTYPE dsmBindMC sendType no es válido.
- 2021 E  
DSM\_RC\_INVALID\_RETCODE No hay texto disponible para este código de retorno.
- 2022 E  
DSM\_RC\_INVALID\_SENDDTYPE dsmSendObj sendType no es válido.
- 2023 E  
DSM\_RC\_INVALID\_PARAMETER dsmDeleteObj delType no es válido.
- 2024 E  
DSM\_RC\_INVALID\_OBJSTATE La consulta Backup objState no es válida.
- 2025 E  
DSM\_RC\_INVALID\_MCNAME No se ha encontrado el nombre de clase de gestión.
- 2026 E  
DSM\_RC\_INVALID\_DRIVE\_CHAR La letra de unidad no es un carácter alfabético.
- 2027 E  
DSM\_RC\_NULL\_FSNAME El nombre de espacio de archivo de registro es NULL.
- 2028 E  
DSM\_RC\_INVALID\_HLNAME El calificador de alto nivel del nombre de objeto debe empezar con el delimitador de directorio.
- 2029 E  
DSM\_RC\_NUMOBJ\_EXCEED El número de objetos en dsmBeginGetData supera DSM\_MAX\_GET\_OBJ | DSM\_MAX\_PARTIAL\_GET\_OBJ.
- 2030 E  
DSM\_RC\_NEWPW\_REQD El nuevo valor de contraseña es NULL o está en blanco.
- 2031 E  
DSM\_RC\_OLDPW\_REQD El valor anterior de contraseña es NULL o está en blanco.
- 2032 E  
DSM\_RC\_NO\_OWNER\_REQD En dsmInit, no se permite establecer sesión al propietario cuando PASSWORDACCESS=generate.
- 2033 E  
DSM\_RC\_NO\_NODE\_REQD En dsmInit, el nodo no está permitido si PASSWORDACCESS=generate.
- 2034 E  
DSM\_RC\_KEY\_MISSING Falta el archivo de claves.
- 2035 E  
DSM\_RC\_KEY\_BAD El contenido del archivo de claves no es válido.
- 2041 E  
DSM\_RC\_BAD\_CALL\_SEQUENCE La secuencia de llamadas no es válida.
- 2042 E  
DSM\_RC\_INVALID\_TSMBUFFER tsmBuffHandle no es válido o el valor de dataPtr no es válido.
- 2043 E  
DSM\_RC\_TOO\_MANY\_BYTES El número de bytes copiados en tsmBuffer es mayor que el valor permitido.
- 2044 E  
DSM\_RC\_MUST\_RELEASE\_BUFFER dsmTerminate no puede finalizar debido a que la aplicación se mantiene en uno o más tsmBuffers.
- 2045 E  
DSM\_RC\_BUFF\_ARRAY\_ERROR Se ha producido un error interno en la matriz de tsmBuffer.
- 2046 E  
DSM\_RC\_INVALID\_DATA\_BLK Al utilizar useTsmBuffers, dataBlk debe ser NULL en las llamadas a dsmSendObj y dsmGetObj.
- 2047 E  
DSM\_RC\_ENCR\_NOT\_ALLOWED No se permite el cifrado al utilizar useTsmBuffers.
- 2048 E  
DSM\_RC\_OBJ\_COMPRESSED Este objeto no se puede restaurar/recuperar mediante useTsmBuffers porque está comprimido.
- 2049 E  
DSM\_RC\_OBJ\_ENCRYPTED Este objeto no se puede restaurar/recuperar mediante useTsmBuffers porque está cifrado.
- 2050 E  
DSM\_RC\_WILDCHAR\_NOTALLOWED En dsmSendObj, no se permiten caracteres comodín para objName.
- 2051 E  
DSM\_RC\_POR\_NOT\_ALLOWED Al utilizar useTsmBuffers, no se permite una restauración/recuperación con restauración de objetos parcial.

- 2052 E  
DSM\_RC\_NO\_ENCRYPTION\_KEY No se ha encontrado ninguna clave de cifrado. Si está utilizando -encryptkey=prompt asegúrese de que hay un valor en el campo encryptionPasswordP y que bEncryptKeyEnabled está establecido en verdadero.
- 2053 E  
DSM\_RC\_ENCR\_CONFLICT Se han especificado opciones de clave de cifrado conflictivas.
- 2060 E  
DSM\_RC\_FSNAME\_NOTFOUND No se puede encontrar el espacio de archivos para suprimir/establecer el acceso.
- 2061 E  
DSM\_RC\_FS\_NOT\_REGISTERED En dsmSendObj, dsmDeleteObj o dsmUpdateFS, el espacio de archivos no se ha registrado.
- 2062 W  
DSM\_RC\_FS\_ALREADY\_REGED en dsmRegisterFS el espacio de archivos ya se ha registrado.
- 2063 E  
DSM\_RC\_OBJID\_NOTFOUND En dsmBeginGetData, el objID es NULL.
- 2064 E  
DSM\_RC\_WRONG\_VERSION En dsmInit, la versión de la API del emisor de la llamada es distinta de la versión de la biblioteca de IBM Spectrum Protect.
- 2065 E  
DSM\_RC\_WRONG\_VERSION\_PARM La versión de estructura del interlocutor es diferente de la versión de biblioteca de IBM Spectrum Protect.
- 2070 E  
DSM\_RC\_NEEDTO\_ENDTXN Emita dsmEndTxn y, a continuación, empiece una sesión de transacción nueva.
- 2080 E  
DSM\_RC\_OBJ\_EXCLUDED El objeto de archivado o copia de seguridad se excluye del proceso.
- 2081 E  
DSM\_RC\_OBJ\_NOBCG El objeto de copia de seguridad no tiene un grupo de copias.
- 2082 E  
DSM\_RC\_OBJ\_NOACG El objeto de archivado no tiene un grupo de copias.
- 2090 E  
DSM\_RC\_APISYSTEM\_ERROR La memoria utilizada por la API de IBM Spectrum Protect se ha dañado.
- 2100 E  
DSM\_RC\_DESC\_TOOLONG La descripción de archivado de sendObj es demasiado larga.
- 2101 E  
DSM\_RC\_OBJINFO\_TOOLONG sendObj ObjAttr.objInfo es demasiado largo.
- 2102 E  
DSM\_RC\_HL\_TOOLONG The sendObj dsmObjName.hl es demasiado largo.
- 2103 E  
DSM\_RC\_PASSWD\_TOOLONG La contraseña o la serie encryptionPassword proporcionada es demasiado larga.
- 2104 E  
DSM\_RC\_FILESPACE\_TOOLONG sendObj dsmObjName.fs es demasiado largo.
- 2105 E  
DSM\_RC\_LL\_TOOLONG sendObj dsmObjName.ll es demasiado largo.
- 2106 E  
DSM\_RC\_FSINFO\_TOOLONG en RegisterFS o UpdateFS el fsInfo de fsAttr es demasiado largo.
- 2107 E  
DSM\_RC\_SENDDATA\_WITH\_ZERO\_SIZE No se pueden enviar datos con un sizeEstimate de byte cero.
- 2110 E  
DSM\_RC\_INVALID\_ACCESS\_TYPE El tipo de acceso dsmSetAccess no es válido.
- 2111 E  
DSM\_RC\_QUERY\_COMM\_FAILURE Error de comunicaciones con el servidor durante la consulta de objeto
- 2112 E  
DSM\_RC\_NO\_FILES\_BACKUP No se ha realizado anteriormente ninguna copia de seguridad de los archivos para este nombre de archivo/espacio de archivo.
- 2113 E  
DSM\_RC\_NO\_FILES\_ARCHIVE No se han archivado anteriormente ningún archivo para este nombre de archivo/espacio de archivo.
- 2114 E  
DSM\_RC\_INVALID\_SETACCESS Formato no válido para el mandato Set Access.
- 2120 E  
DSM\_RC\_STRING\_TOO\_LONG El mensaje siguiente era demasiado largo para anotarlo en el servidor: 'mensaje abreviado con número de mensaje'
- 2200 I  
DSM\_RC\_MORE\_DATA En dsmGetNextQObj o dsmGetData hay más datos disponibles.
- 2210 E  
DSM\_RC\_BUFF\_TOO\_SMALL El almacenamiento intermedio dataBlk es demasiado pequeño para la respuesta de consulta.



- 2228 E  
DSM\_RC\_NO\_API\_CONFIGFILE No se puede abrir el archivo de configuración especificado en dsmInit.
- 2229 E  
DSM\_RC\_NO\_INCLEXCL\_FILE No se ha encontrado el archivo de definición Include/Exclude.
- 2230 E  
DSM\_RC\_NO\_SYS\_OR\_INCLEXCL El archivo dsm.sys no se ha encontrado o el archivo Inclexcl especificado en dsm.sys no se ha encontrado.
- 2231 E  
DSM\_RC\_REJECT\_NO\_POR\_SUPPORT No se soporta la recuperación de objetos parcial en este servidor.
- 2300 E  
DSM\_RC\_NEED\_ROOT Solo un usuario root de UNIX puede ejecutar dsmChangePW o dsmDeleteFS.
- 2301 E  
DSM\_RC\_NEEDTO\_CALL\_BINDMC Debe emitir dsmBindMC antes que dsmSendObj.
- 2302 I  
DSM\_RC\_CHECK\_REASON\_CODE El voto de dsmEndTxn es ABORT, de modo que compruebe el campo de razón.
- 2400 E  
DSM\_RC\_ALMGR\_OPEN\_FAIL No se ha podido abrir el archivo de licencia.
- 2401 E  
DSM\_RC\_ALMGR\_READ\_FAIL Anomalía de lectura en el archivo de licencia.
- 2402 E  
DSM\_RC\_ALMGR\_WRITE\_FAIL Anomalía de escritura en el archivo de licencia.
- 2403 E  
DSM\_RC\_\_ALMGR\_DATA\_FMT Los datos del archivo de licencia no están en un formato válido.
- 2404 E  
DSM\_RC\_ALMGR\_CKSUM\_BAD La suma de comprobación del archivo de licencia no coincide con la serie del registro de licencia.
- 2405 E  
DSM\_RC\_ALMGR\_TRIAL\_EXPRD Esta licencia de prueba ha caducado.
- 4580 E  
DSM\_RC\_ENC\_WRONG\_KEY Error al procesar 'nombre de espacio de archivosnombre de rutanombre de archivo'; clave de cifrado no válida
- 4582 E  
DSM\_RC\_ENC\_NOT\_AUTHORIZED El usuario no está autorizado para cifrar archivo-nombre de espaciodirectorio\_rutanombre\_archivo.
- 4584 E  
DSM\_RC\_ENC\_TYPE\_UNKOWN Error al procesar 'nombre de espacio de archivosnombre de rutanombre de archivo': tipo de cifrado no admitido.
- 4600 E  
DSM\_RC\_CLUSTER\_INFO\_LIBRARY\_NOT\_LOADED CLUSTERNODE se ha establecido en YES pero el daemon de información de clúster no se ha iniciado.
- 4601 E  
DSM\_RC\_CLUSTER\_LIBRARY\_INVALID CLUSTERNODE está establecido en YES pero la biblioteca de carga de clúster no es válida.
- 4602 E  
DSM\_RC\_CLUSTER\_LIBRARY\_NOT\_LOADED CLUSTERNODE se ha establecido en YES pero el software de clúster no está disponible en este sistema.
- 4603 E  
DSM\_RC\_CLUSTER\_NOT\_MEMBER\_OF\_CLUSTER CLUSTERNODE se ha establecido en YES pero esta máquina no es miembro de un clúster.
- 4604 E  
DSM\_RC\_CLUSTER\_NOT\_ENABLED CLUSTERNODE está establecido en YES pero el servicio de clúster no está habilitado en este sistema.
- 4605 E  
DSM\_RC\_CLUSTER\_NOT\_SUPPORTED No se admite la opción CLUSTERNODE en este sistema.
- 4606 E  
DSM\_RC\_CLUSTER\_UNKNOWN\_ERROR Se ha producido un error inesperado (código\_ret) mientras el programa intentaba obtener el nombre de clúster del sistema.
- 5200 E  
DSM\_RC\_ABORT\_CERTIFICATE\_NOT\_FOUND NOT\_FOUND El nodo remoto no está correctamente configurado en el servidor de IBM Spectrum Protect.
- 5702 E  
DSM\_RC\_PROXY\_REJECT\_NO\_RESOURCES Proxy rechazado: El servidor de IBM Spectrum Protect se ha quedado sin memoria.
- 5705 E  
DSM\_RC\_PROXY\_REJECT\_DUPLICATE\_ID Proxy rechazado: las opciones ASNODENAME y NODENAME tienen el mismo valor.

- 5710 E  
DSM\_RC\_PROXY\_REJECT\_ID\_IN\_USE Se ha rechazado el proxy: El nombre de nodo especificado en la opción ASNODENAME está bloqueado.
- 5717 E  
DSM\_RC\_PROXY\_REJECT\_INTERNAL\_ERROR Se ha rechazado el proxy: Se ha producido un error interno en el servidor.
- 5722 E  
DSM\_RC\_PROXY\_REJECT\_NOT\_AUTHORIZED Se ha rechazado el proxy: No se ha otorgado autorización de proxy a este nodo.
- 5746 E  
DSM\_RC\_PROXY\_INVALID\_FROMNODE La opción ASNODENAME no es válida con la opción FROMNODE.
- 5748 E  
DSM\_RC\_PROXY\_INVALID\_CLUSTER No se puede utilizar la opción ASNODENAME con la opción CLUSTERNODE.
- 5749 E  
DSM\_RC\_PROXY\_INVALID\_FUNCTION No se puede invocar la operación que se está intentando con la opción ASNODENAME.
- 5801 E  
DSM\_RC\_CRYPTO\_ICC\_ERROR Error inesperado en la biblioteca de cifrado.

## **-452 E DSM\_RC\_SHM\_NOTAUTH Autorización insuficiente para conectarse a la región de memoria compartida**

---

### **Explicación**

El usuario que emite el mandato no tiene autoridad para conectarse al segmento de memoria compartida. Cuando el servidor crea el segmento de memoria compartida, será propiedad del ID de usuario efectivo del proceso del servidor (dsmserv). Sólo los procesos que se ejecuten con este ID de usuario o raíz podrán conectarse al segmento (y por lo tanto al servidor).

### **Acción del Sistema**

Se rechaza la sesión y el proceso se detiene.

### **Respuesta del Usuario**

Ejecute el mandato con el ID de usuario del proceso que ejecuta dsmserv si es posible. De lo contrario, póngase en contacto con el administrador del sistema para obtener más ayuda.

## **-451 E DSM\_RC\_SHM\_FAILURE Se ha producido un error al utilizar el protocolo de memoria compartida**

---

### **Explicación**

Se ha producido un error al leer o grabar datos mediante el protocolo de comunicaciones de memoria compartida.

### **Acción del Sistema**

IBM Spectrum Protect no puede completar la operación solicitada.

### **Respuesta del Usuario**

Compruebe las anotaciones de rastreo para obtener más información e intente de nuevo la operación. Si el problema continúa, consulte al administrador del sistema para obtener ayuda adicional.

## **-450 E DSM\_RC\_SHM\_TCPIP\_FAILURE Sesión rechazada: ha fallado la conexión TCP/IP para la Memoria compartida**

---

### **Explicación**

Ha fallado un intento de conexión al servidor local utilizando el protocolo de memoria compartida durante las comunicaciones TCP/IP iniciales. Este error puede producirse si el servidor no está conectado al puerto correcto o si se cae el servidor.

### **Acción del Sistema**

Se ha rechazado la sesión. El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación o espere hasta que el servidor vuelva a estar activo y reintente la operación. Si el problema continúa, consulte al administrador del sistema para obtener ayuda adicional.

## **-190 E DSM\_RC\_NP\_ERROR Sesión rechazada: ha fallado la conexión de Named Pipes.**

---

### **Explicación**

Ha fallado el intento de conexión con el servidor utilizando las comunicaciones de Named Pipes. Esto podría haber ocurrido si se especificara un NAMEDPIPE\_NAME incorrecto en el archivo de opciones o si su administrador del sistema cancelara una operación de copia de seguridad.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación o espere hasta que el servidor vuelva a estar activo y reintente la operación. Asegúrese de que el valor especificado en la opción NAMEDPIPE\_NAME es el mismo que el utilizado por el servidor. Si el problema continúa, consulte al administrador del sistema para obtener ayuda adicional.

## **-057 E DSM\_RC\_TCPIP\_LOADFAILURE La función de carga del TCP/IP ha fallado.**

---

### **Explicación**

Se ha producido un error al localizar una función. Ha fallado la función de carga del TCP/IP.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Verificar la instalación del TCP/IP.

## **-056 E DSM\_RC\_TCPIP\_DLL\_LOADFAILURE Se ha producido un error al cargar una biblioteca.**

---

### **Explicación**

Se ha producido un error al cargar una biblioteca. Ha fallado la carga del DLL TCP/IP DLL.

### **Acción del Sistema**

El proceso se ha detenido.

### Respuesta del Usuario

Verificar la instalación del TCP/IP.

## **-055 E DSM\_RC\_WINSOCK\_MISSING No se puede encontrar el archivo TCP/IP WINSOCK.DLL.**

---

### Explicación

No se ha encontrado el archivo TCP/IP WINSOCK.DLL.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Verificar la instalación del TCP/IP.

## **-054 E DSM\_RC\_NETWORK\_UNREACHABLE El nombre de host TCP/IP especificado es inalcanzable**

---

### Explicación

No se puede alcanzar el nombre de host TCP/IP especificado en la sentencia TCPSERVERADDRESS.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Compruebe el archivo de opciones para la sentencia TCPSERVERADDRESS correcta. Consulte a su administrador el nombre correcto del servidor.

## **-053 E DSM\_RC\_BAD\_HOST\_NAME Se ha especificado una dirección del TCP/IP no correcta.**

---

### Explicación

La dirección TCP/IP especificada por el valor TCPSERVERADDRESS del cliente IBM Spectrum Protect no se ha podido encontrar en la red. Las razones comunes para este error incluyen:

- La opción de cliente TCPSERVERADDRESS especifica la dirección del TCP/IP errónea para el servidor" IBM Spectrum Protect .
- La máquina que contiene el servidor IBM Spectrum Protect no está en la red.
- Un problema de red impide al cliente IBM Spectrum Protect alcanzar la máquina que contiene el servidor IBM Spectrum Protect .

### Acción del Sistema

el proceso se detiene.

### Respuesta del Usuario

Verifique que los valores TCPSEVERADDRESS y TCPPOINT tienen los valores correctos para el servidor IBM Spectrum Protect. Utilice el programa de utilidad "ping" (o similar) del sistema operativo para asegurarse de que la máquina puede localizar la máquina que contiene el servidor IBM Spectrum Protect en la red. Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## **-052 E DSM\_RC\_CONN\_REFUSED El host ha rechazado un intento de establecer una conexión de TCP/IP**

---

### **Explicación**

El servidor ha rechazado un intento de establecer conexión al TCP/IP.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

El servidor no se ha inicializado completamente, no se está ejecutando en este momento, no se ha habilitado para comunicaciones TCP/IP, o se ha especificado un número de puerto del TCP/IP incorrecto. Si el problema continúa, consulte al administrador del sistema.

## **-051 E DSM\_RC\_CONN\_TIMEDOUT El intento de establecer una conexión TCP/IP ha excedido el tiempo de espera antes de que se realizara la conexión.**

---

### **Explicación**

El intento del objeto de la conexión no ha respondido durante el tiempo de espera asignado. En el caso del cliente B/A, este mensaje aparece antepuesto en dsmerror.log por el mensaje ANS5216E que proporciona detalles de la conexión que ha fallado. Esta condición puede ser temporal.

### **Acción del Sistema**

el proceso se detiene.

### **Respuesta del Usuario**

- Reinicie el cliente IBM Spectrum Protect y vuelva a intentar la operación.
- Compruebe el archivo de opciones de cliente y verifique que TCPSEVERADDRESS y TCPPOINT especifican la dirección TCP/IP y el número de puerto correctos para el servidor de IBM Spectrum Protect.
- Verifique que existe conectividad de red entre la máquina cliente de IBM Spectrum Protect y la máquina del servidor de IBM Spectrum Protect.
- Si el problema persiste, pregunte a su administrador IBM Spectrum Protect para obtener más ayuda.

## **-050 E DSM\_RC\_TCPIP\_FAILURE Sesión rechazada: Error de conexión con TCP/IP.**

---

### **Explicación**

Ha fallado el intento de conexión con el servidor utilizando las comunicaciones TCP/IP. Esto puede ser debido a que los valores de la opción TCP/IP en el archivo de opciones del cliente son incorrectos. Este error también se puede producir si la conexión de la LAN se ha inactivado o si el administrador ha cancelado una operación de copia de seguridad.

### **Acción del Sistema**

Se ha rechazado la sesión. El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación o espere hasta que el servidor vuelva a estar activo y reintente la operación. Si el problema continúa, consulte al administrador del sistema para obtener ayuda adicional.

## **0000 I DSM\_RC\_OK Se ha realizado satisfactoriamente.**

---

### **Explicación**

La operación se ha completado satisfactoriamente.

### **Acción del Sistema**

Ninguna.

### **Respuesta del Usuario**

Ninguna.

## **0001 E DSM\_RC\_ABORT\_SYSTEM\_ERROR Esta operación no puede continuar debido a un error en el servidor IBM Spectrum Protect. Póngase en contacto con el administrador del servidor IBM Spectrum Protect para obtener ayuda.**

---

### **Explicación**

El servidor IBM Spectrum Protect ha encontrado una condición de error que impide que la operación de cliente IBM Spectrum Protect continúe. El administrador de servidor IBM Spectrum Protect puede revisar el registro de actividad del servidor IBM Spectrum Protect para obtener más detalles sobre el error.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del servidor IBM Spectrum Protect para obtener ayuda. El administrador puede revisar el registro de actividad del servidor IBM Spectrum Protect para obtener más información sobre las condiciones que han llevado a este error.

## **0002 E DSM\_RC\_ABORT\_NO\_MATCH No hay objetos en el servidor que coincidan con la consulta**

---

### **Explicación**

Ningún objeto del servidor coincide con la operación de consulta que se está realizando. Si este objeto forma parte de un juego de copias de seguridad generado en un nodo y se cambia el nombre de nodo en el servidor, los objetos del juego de copias de seguridad generados antes del cambio de nombre no coincidirán con el nuevo nombre de nodo.

### **Acción del Sistema**

El proceso se ha detenido.

## Respuesta del Usuario

Asegúrese de que los nombres se han escrito correctamente. Si el objeto forma parte de un juego de copias de seguridad generado antes de un cambio de nombre de nodo, asegúrese de que el nombre del nodo es el mismo que el nodo para el que se generó el juego de copias de seguridad.

## **0003 E DSM\_RC\_ABORT\_BY\_CLIENT El cliente ha finalizado la transacción**

---

### Explicación

El sistema cliente ha finalizado la operación con el servidor y ha finalizado la transacción actual.

### Acción del Sistema

El proceso se ha detenido.

## Respuesta del Usuario

Reinicie la sesión.

## **0004 W DSM\_RC\_ABORT\_ACTIVE\_NOT\_FOUND No se ha encontrado ninguna versión de copia de seguridad activa.**

---

### Explicación

Se ha intentado hacer caducar un objeto, pero el servidor IBM Spectrum Protect no ha podido encontrar una versión de copia de seguridad activa del objeto. Este mensaje va precedido del mensaje ANS1228E que especifica nombre de objeto.

Por ejemplo, este mensaje podría emitirse si dos procesos de cliente distintos están realizando una copia de seguridad del mismo sistema de archivos a la vez. Si uno de los procesos hace caducar un archivo, el servidor IBM Spectrum Protect hará que el archivo quede inactivo. Si el segundo proceso intenta hacer caducar posteriormente el mismo archivo, el servidor IBM Spectrum Protect no encontrará una versión activa del archivo, por lo tanto, el segundo proceso emitirá este mensaje para ese archivo.

### Acción del Sistema

El objeto no caduca. El proceso continúa con el objeto siguiente.

## Respuesta del Usuario

- Revise la salida de la consola, las anotaciones de planificación o las anotaciones de errores y busque el mensaje ANS1228E que sigue a este mensaje. ANS1228E identificará el objeto que no se ha podido caducar.
- Examine las condiciones en las que se ha producido el problema y valore si dichas condiciones explican la aparición de este mensaje. Por ejemplo, este mensaje podría aparecer si varias instancias del cliente intentan realizar una copia de seguridad del sistema de archivos a la vez.
- Si no se puede determinar la razón de este mensaje y vuelve a aparecer al intentar de nuevo la operación, póngase en contacto con el soporte técnico de IBM para obtener ayuda. Intente también buscar este número de mensajes en <http://www.ibm.com> para encontrar una solución.

## **0005 E DSM\_RC\_ABORT\_NO\_DATA El servidor IBM Spectrum Protect no tiene datos para el objeto.**

---

### Explicación

IBM Spectrum Protect ha intentado restaurar o recuperar un objeto que no tiene datos asociados. Si hay alguna acción correctiva posible, es con el servidor IBM Spectrum Protect.

## Acción del Sistema

IBM Spectrum Protect finaliza la operación actual.

## Respuesta del Usuario

Pida al administrador de IBM Spectrum Protect que busque en el registro de actividad de IBM Spectrum Protect mensajes relacionados con este error que puedan ayudarle a identificar el problema.

## 0006 E DSM\_RC\_ABORT\_BAD\_VERIFIER Ha entrado una contraseña incorrecta.

---

### Explicación

Ha especificado una contraseña actual incorrecta o una nueva contraseña que no cumple los requisitos de longitud de contraseñas del servidor.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar iniciar la sesión con la contraseña correcta. Si esto falla o ha olvidado la contraseña, solicite al administrador de IBM Spectrum Protect que asigne una contraseña nueva.

## 0007 E DSM\_RC\_ABORT\_NODE\_IN\_USE El nodo está en uso

---

### Explicación

Otra operación del servidor está utilizando el nodo que se está ejecutando. Podría deberse a otro cliente o actividad del servidor.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar la operación o consulte al administrador del sistema para ver qué otras operaciones se están ejecutando en el nodo.

## 0008 E DSM\_RC\_ABORT\_EXPDATE\_TOO\_LOW La fecha de caducidad debe ser posterior a la fecha de hoy

---

### Explicación

La fecha de caducidad de archivado está demasiado próxima o debe ser posterior a la fecha de hoy.

### Acción del Sistema

IBM Spectrum Protect ha cancelado la operación actual.

### Respuesta del Usuario

Vuelva a intentar la operación especificando una fecha de caducidad posterior a la fecha de hoy.



## 0009 W DSM\_RC\_ABORT\_DATA\_OFFLINE Los datos solicitados están fuera de línea.

---

### Explicación

Para la operación de restauración o recuperación, se debe recuperar uno o varios de los archivos solicitados del soporte de almacenamiento fuera de línea (generalmente una cinta). El tiempo de espera depende de las políticas de gestión de almacenamiento fuera de línea del sitio.

### Acción del Sistema

IBM Spectrum Protect espera que el soporte de almacenamiento fuera de línea esté disponible para continuar.

### Respuesta del Usuario

Ninguna.

## 0010 E DSM\_RC\_ABORT\_EXCLUDED\_BY\_SIZE El objeto es demasiado grande para los límites del servidor

---

### Explicación

El objeto es demasiado grande. La configuración del servidor no tiene ningún espacio de almacenamiento de datos que acepte el objeto.

### Acción del Sistema

El archivo se omite.

### Respuesta del Usuario

Consulte al administrador del sistema para determinar el tamaño máximo de archivo (objeto) para el que está configurado el servidor de su sitio.

## 0011 E DSM\_RC\_ABORT\_NO\_REPOSIT\_SPACE El servidor se ha quedado sin espacio de almacenamiento de datos

---

### Explicación

El servidor no tiene espacio disponible para almacenar el objeto.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Puede realizar una de las siguientes acciones:

- Solicitar al administrador del sistema que añada espacio a la agrupación de almacenamiento.
- Para el cliente de IBM Spectrum Protect, establezca COMPRESSALWAYS=NO y COMPRESSIon=YES en el archivo de opciones (DSM.OPT) y el archivo se reenviará sin comprimir si crece durante la compresión.
- En aplicaciones de la API, consulte la documentación de la aplicación para leer recomendaciones acerca de la compresión.
- Desconecte la función de caché del disco en la agrupación de almacenamiento de disco y emita los mandatos MOVE DATA en cada volumen de agrupación de discos para borrar los bitfiles con función de caché.

## 0012 E DSM\_RC\_ABORT\_MOUNT\_NOT\_POSSIBLE No es posible el montaje de soportes del servidor

---

### Explicación

No es posible el montaje de soportes del servidor. El servidor ha excedido el tiempo de espera para el montaje de un volumen fuera de línea.

### Acción del Sistema

El archivo se omite.

### Respuesta del Usuario

Vuelva a intentarlo más tarde cuando los volúmenes del servidor puedan montarse. Asegúrese de que el valor de MAXNUMMP (número máximo de puntos de montaje) definido en el servidor para este nodo es mayor de 0.

## 0013 E DSM\_RC\_ABORT\_SIZEESTIMATE\_EXCEED Se ha excedido el tamaño estimado

---

### Explicación

La cantidad total de datos para una operación de copia de seguridad o archivado supera el tamaño estimado enviado originalmente al servidor para asignar espacio de almacenamiento de datos. Esto sucede cuando muchos archivos crecen en grandes cantidades durante la operación de copia de seguridad o archivado.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar la operación. Si el problema continúa, compruebe qué otros procesos se están ejecutando en la máquina cliente que generan grandes cantidades de datos. Inhabilite esas operaciones mientras se realiza la operación de copia de seguridad o archivado.

## 0014 E DSM\_RC\_ABORT\_DATA\_UNAVAILABLE En este momento no hay datos del archivo disponibles en el servidor

---

### Explicación

Los datos del archivo no están disponibles en el servidor en este momento. Se ha intentado realizar una operación de recuperación o restauración. Las posibles causas son las siguientes:

- Los datos estaban dañados en el servidor.
- El servidor ha detectado un error de lectura.
- El archivo está implicado temporalmente en una operación de reclamación en el servidor.
- El servidor ha solicitado un volumen de cinta que estaba marcado como no disponible.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador del sistema para determinar el problema desde la consola del servidor o de las anotaciones de actividad. Compruebe si se ha realizado alguna solicitud para un volumen de cinta que no estaba disponible. Es posible que un volumen de cinta estuviera marcado como no disponible si se detectaron errores de lectura anteriores o se extrae el volumen de la biblioteca de cintas.

## **0015 E DSM\_RC\_ABORT\_RETRY Solicitud de reintento inesperada. El servidor IBM Spectrum Protect ha encontrado un error al grabar los datos.**

---

### **Explicación**

Ninguna.

### **Acción del Sistema**

Si la operación actual admite otro intento, el cliente vuelve a intentar la operación. Si no, el proceso se detiene.

### **Respuesta del Usuario**

Ninguna.

## **0016 E DSM\_RC\_ABORT\_NO\_LOG\_SPACE El servidor no tiene suficiente espacio de registro de recuperación para continuar la operación actual**

---

### **Explicación**

El servidor se ha quedado sin espacio en las anotaciones de recuperación.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Este error es un problema temporal. Vuelva a intentar la operación o consulte al administrador del sistema.

## **0017 E DSM\_RC\_ABORT\_NO\_DB\_SPACE El servidor no tiene suficiente espacio de base de datos para continuar la operación actual**

---

### **Explicación**

El servidor se ha quedado sin espacio en la base de datos.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0018 E DSM\_RC\_ABORT\_NO\_MEMORY El servidor no tiene suficiente memoria para continuar con la operación actual**

---

### **Explicación**

El servidor se ha quedado sin memoria.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Es un problema temporal. Vuelva a intentar la operación o consulte al administrador del sistema.

## **0020 E DSM\_RC\_ABORT\_FS\_NOT\_DEFINED El espacio de archivos especificado no existe en el servidor. Es posible que el espacio de archivos haya sido suprimido por otro cliente o un administrador.**

---

### **Explicación**

El espacio de archivos especificado no existe en el servidor. El administrador del sistema ha suprimido el espacio de archivos u otro cliente que utiliza el nombre de nodo del cliente lo ha suprimido.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Compruebe el nombre del espacio de archivos para asegurarse de que es correcto y vuelva a intentar la operación.

## **0021 S DSM\_RC\_ABORT\_NODE\_ALREADY\_DEFED El registro abierto ha fallado porque el nombre de nodo especificado está definido en el servidor**

---

### **Explicación**

El registro abierto ha fallado porque el nombre de nodo especificado está definido en el servidor con el mismo nombre.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Reinténtelo con otro nombre de nodo.

## **0022 S DSM\_RC\_ABORT\_NO\_DEFAULT\_DOMAIN El registro abierto ha fallado porque no existe ningún dominio predeterminado**

---

### **Explicación**

El registro abierto ha fallado porque no existe ningún dominio de políticas predeterminado donde colocar el nodo.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0023 S DSM\_RC\_ABORT\_INVALID\_NODENAME El registro abierto ha fallado porque se ha especificado un nombre de nodo que no es válido**

---

### **Explicación**

El registro abierto ha fallado porque el nombre de nodo especificado contiene caracteres que no son válidos.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Vuelva a intentar la operación con otro nombre de nodo válido.

## **0024 S DSM\_RC\_ABORT\_INVALID\_POL\_BIND Se ha producido un problema de gestión de políticas en el servidor IBM Spectrum Protect.**

---

### **Explicación**

El registro de errores del cliente y el registro de actividad del servidor de IBM Spectrum Protect pueden contener información adicional sobre este error.

### **Acción del Sistema**

El proceso se detiene.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema persiste, examine el registro de errores del cliente y el registro de actividades del servidor de IBM Spectrum Protect para obtener información adicional sobre este error. Si no se puede resolver el problema, obtenga un rastreo de servicio que capture el problema y póngase en contacto con el soporte técnico de IBM para obtener ayuda adicional. El administrador de IBM Spectrum Protect puede ayudarle a configurar el rastreo.

## **0024 E DSM\_RC\_ABORT\_NO\_INVALID\_POL\_BIND Se ha enlazado un objeto de la transacción a una clase de gestión que no es válida.**

---

### **Explicación**

Se ha vinculado no de los objetos de la transacción a una clase de gestión que no es parte de esta política del nodo, o el tipo de clase de gestión no está admitido para este nivel de cliente.

### **Acción del Sistema**

La actual operación termina.

## Respuesta del Usuario

Asegúrese de que todos los objetos están enlazados a una clase de gestión válida o actualice el cliente al nivel adecuado.

## 0025 E DSM\_RC\_ABORT\_DEST\_NOT\_DEFINED Problema del servidor: Destino no definido.

---

### Explicación

Problema del servidor: Destino no definido.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Solicite al representante del servicio que compruebe las anotaciones de errores.

## 0026 S DSM\_RC\_ABORT\_WAIT\_FOR\_SPACE El servidor IBM Spectrum Protect no tiene actualmente espacio en la agrupación de almacenamiento para este archivo. Puede tratarse de una condición temporal.

---

### Explicación

Este mensaje se suele emitir cuando la agrupación de almacenamiento en la que se colocan los datos no tiene espacio suficiente, pero pronto estará disponible. Por ejemplo, es posible que la migración de una agrupación de almacenamiento libere suficiente espacio para almacenar los datos.

### Acción del Sistema

La operación actual se ha cancelado.

### Respuesta del Usuario

Intente la operación más tarde. Si falla de nuevo, solicite al administrador de IBM Spectrum Protect más espacio en la agrupación de almacenamiento.

## 0027 E DSM\_RC\_ABORT\_NOT\_AUTHORIZED No se puede suprimir el espacio de archivos debido a que este nodo no tiene permiso para suprimir datos archivados o de copia de seguridad.

---

### Explicación

No puede suprimir los datos del espacio de archivos a menos que el administrador de IBM Spectrum Protect haya autorizado al nodo a hacerlo. La autorización le permite suprimir datos de copia de seguridad, datos archivados o ambos.

### Acción del Sistema

El proceso de suprimir ha fallado.

### Respuesta del Usuario

Utilice el mandato DSMC QUERY SESSION para verificar su autorización. Solicite al administrador de IBM Spectrum Protect que proporcione la autorización necesaria o que suprima el espacio de archivos.

## **0028 E DSM\_RS\_ABORT\_RULE\_ALREADY\_DEFED Ya se ha definido la regla de acceso 'regla\_acceso' para el nodo 'nodo '. Es necesario suprimir la regla antigua para que se pueda definir una nueva.**

---

### **Explicación**

Está intentando definir la autorización para el nodo especificado, que ya ha definido la autorización.

### **Acción del Sistema**

IBM Spectrum Protect no redefinió la autorización para el nodo especificado.

### **Respuesta del Usuario**

Actualice la autorización, o suprima la regla antigua y defina una nueva, o utilice la autorización actual.

## **0029 S DSM\_RC\_ABORT\_NO\_STOR\_SPACE\_STOP El servidor se ha quedado sin espacio de almacenamiento de datos**

---

### **Explicación**

El servidor no tiene espacio disponible para almacenar el objeto.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

informa al administrador del sistema de que una agrupación de almacenamiento del servidor está llena.

## **0030 E DSM\_RC\_ABORT\_LICENSE\_VIOLATION La operación no está permitida debido a los valores de las licencias del servidor**

---

### **Explicación**

El nodo o usuario está intentando realizar una operación que bien sobrepasa los valores de licencia o que no tiene licencia.

### **Acción del Sistema**

Se ha rechazado la sesión o se ha cancelado la transacción, finalizando la operación actual.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0032 E DSM\_RC\_ABORT\_DUPLICATE\_OBJECT Se ha encontrado un objeto duplicado, la operación no se puede completar.**

---

## Explicación

Se ha encontrado un objeto duplicado, la operación no se puede completar.

## Acción del Sistema

La operación solicitada no ha podido realizarse.

## Respuesta del Usuario

Pruebe la operación con una especificación de archivo diferente.

## **0033 E DSM\_RC\_ABORT\_INVALID\_OFFSET El valor de partialObjOffset para la recuperación de objeto parcial no es válido.**

---

### Explicación

El valor partialObjOffset para la recuperación parcial de objetos no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Especifique un valor válido.

## **0034 E DSM\_RC\_ABORT\_INVALID\_LENGTH El valor de partialObjLength para la recuperación de objetos parcial no es válido.**

---

### Explicación

El valor partialObjLength para la recuperación parcial de objetos no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Especifique un valor válido.

## **0036 E DSM\_RC\_END\_NODE\_NOT\_AUTHORIZED El nodo o usuario no tiene la autorización adecuada para realizar esta operación**

---

### Explicación

El nodo o usuario no tiene la autorización adecuada para realizar esta operación.

### Acción del Sistema

La transacción ha finalizado.

### Respuesta del Usuario



Compruebe la autorización para el objeto específico.

## **0041 E DSM\_RC\_ABORT\_EXCEED\_MAX\_MP Este nodo ha excedido su número máximo de puntos de montaje.**

---

### **Explicación**

No se permiten puntos de montaje secuenciales de disco o de cinta para esta operación, o ya se está utilizando el número máximo de puntos de montaje permitidos. No se puede finalizar la operación. El administrador de IBM Spectrum Protect define el número máximo de puntos de montaje con la propiedad MAXNUMMP de la definición de nodo.

### **Acción del Sistema**

El objeto se pasa por alto.

### **Respuesta del Usuario**

Si está realizando otras operaciones que puede que utilicen puntos de montaje, espere a que finalicen esas operaciones e intente de nuevo la operación anómala. De lo contrario, póngase en contacto con el administrador de IBM Spectrum Protect para obtener más ayuda

## **0045 E DSM\_RC\_ABORT\_MERGE\_ERROR Los objetos especificados han fallado la prueba de fusión.**

---

### **Explicación**

Los objetos específicos fallaron la prueba de fusión, la operación no se ha podido completar.

### **Acción del Sistema**

La operación solicitada no ha podido realizarse.

### **Respuesta del Usuario**

Consulte la documentación para obtener información completa sobre los parámetros de prueba de fusión.

## **0047 E DSM\_RC\_ABORT\_INVALID\_OPERATIONSe ha intentado una operación no válida en un nodo**

---

### **Explicación**

La operación no es válida.

### **Acción del Sistema**

La operación actual ha finalizado.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del sistema para obtener más información.

## **0048 E DSM\_RC\_ABORT\_STGPOOL\_UNDEFINED La agrupación de almacenamiento de destino especificada no se ha definido.**

---

## Explicación

No se ha definido la agrupación de almacenamiento.

## Acción del Sistema

La operación actual ha finalizado.

## Respuesta del Usuario

Póngase en contacto con el administrador del sistema para obtener más información.

**0049 E DSM\_RC\_ABORT\_INVALID\_DATA\_FORMAT Una agrupación de almacenamiento de destino no tiene el formato de datos correcto para el tipo de nodo proporcionado.**

---

## Explicación

Sin comentarios

## Acción del Sistema

La operación actual ha finalizado.

## Respuesta del Usuario

Póngase en contacto con el administrador del sistema para obtener más información.

**0050 E DSM\_RC\_ABORT\_DATAMOVER\_UNDEFINED No se ha definido ningún transportador de datos asociado para el nodo especificado.**

---

## Explicación

Sin comentarios

## Acción del Sistema

La operación actual ha finalizado.

## Respuesta del Usuario

Póngase en contacto con el administrador del sistema para obtener más información.

**0051 E DSM\_RC\_REJECT\_NO\_RESOURCES Sesión rechazada: Todas las sesiones de servidor están en uso en este momento**

---

## Explicación

IBM Spectrum Protect tiene todas las sesiones disponibles en uso y no puede aceptar una nueva en este momento.

## Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Vuelva a intentar la operación. Si el problema continúa, consulte al administrador del sistema para aumentar el número de sesiones activas simultáneamente en el servidor.

## 0052 E DSM\_RC\_REJECT\_VERIFIER\_EXPIRED Se ha rechazado la sesión. Su contraseña ha caducado.

---

### Explicación

La contraseña para el ID de usuario de IBM Spectrum Protect ha caducado. Puede tratarse de la contraseña del nombre de nodo de IBM Spectrum Protect o la contraseña del ID de usuario administrativo, o ambas.

### Acción del Sistema

La operación actual se ha cancelado. No tiene permiso para conectarse al servidor hasta que se actualice la contraseña.

## Respuesta del Usuario

Actualice su contraseña. Es posible que tenga que actualizar la contraseña del nombre de nodo, la contraseña del ID administrativo correspondiente o ambas. Puede utilizar el mandato SET PASSWORD o solicitar al administrador de IBM Spectrum Protect que actualice el nodo o su ID administrativo.

## 0053 E DSM\_RC\_REJECT\_ID\_UNKNOWN Sesión rechazada: El ID de usuario es incorrecto, no tiene autorización de administrador o el servidor no lo conoce

---

### Explicación

El servidor no conoce el ID de usuario, que es el nombre de usuario o el ID de usuario de administración de IBM Spectrum Protect. Entre las causas posibles se encuentran las siguientes:

- Su nombre de nodo no está registrado con el servidor de IBM Spectrum Protect
- El nombre de nodo es correcto pero no tiene un ID administrativo correspondiente con el mismo nombre ni autorización de propietario de cliente
- está intentando acceder al archivo migrado a un nodo diferente.

### Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Realice las siguientes comprobaciones:

- Compruebe que el ID de usuario de IBM Spectrum Protect se ha especificado correctamente.
- Compruebe el ID administrativo asociado con el nodo de IBM Spectrum Protect y verifique que el nombre de nodo de IBM Spectrum Protect tiene un ID administrativo coincidente con autorización de propietario de cliente para el nodo. Si no es así, el administrador de IBM Spectrum Protect deberá crearlo.
- Compruebe que el servidor esté utilizando el registro cerrado y que el nombre de nodo esté registrado en el servidor.
- Si se intenta acceder a un archivo migrado, el nombre de nodo debe ser el mismo nodo que ha migrado el archivo.

## 0054 E DSM\_RC\_REJECT\_DUPLICATE\_ID Sesión rechazada: Se ha especificado un ID duplicado

---

### Explicación

Otro proceso que utiliza este nombre de nodo está activo en el servidor.

### **Acción del Sistema**

IBM Spectrum Protect no puede conectarse al servidor. La operación actual se ha cancelado.

### **Respuesta del Usuario**

Si está ejecutando un sistema basado en UNIX, asegúrese de que otro proceso no está activo en IBM Spectrum Protect con el mismo nombre. Asegúrese también de que su nombre de nodo es único en el servidor de modo que no pueda utilizarlo otra persona. Consulte al administrador del sistema para identificar al propietario de ese nombre de nodo.

## **0055 E DSM\_RC\_REJECT\_SERVER\_DISABLED Sesión rechazada: Servidor inhabilitado.**

---

### **Explicación**

El servidor está inhabilitado y no se puede acceder a él para llevar a cabo una actividad normal.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

En el servidor IBM Spectrum Protect, ejecute el mandato administrativo ENABLE SESSIONS. Vuelva a intentar la operación después de que el servidor regrese a un estado activado. Si el problema continúa, consulte al administrador del sistema.

## **0056 E DSM\_RC\_REJECT\_CLOSED\_REGISTER El servidor no está configurado para permitir una inscripción abierta**

---

### **Explicación**

No hay autorización. El administrador del sistema necesita registro. El servidor no está configurado para permitir registro abierto.

### **Acción del Sistema**

No se ha iniciado la sesión.

### **Respuesta del Usuario**

Debe obtener un nodo y contraseña de IBM Spectrum Protect del administrador del sistema.

## **0057 S DSM\_RC\_REJECT\_CLIENT\_DOWNLEVEL Sesión rechazada: Versión de código de cliente de nivel inferior**

---

### **Explicación**

La versión del servidor y la versión del cliente no coinciden. El código de cliente es de nivel inferior.

### **Acción del Sistema**

La operación actual se ha cancelado.

## Respuesta del Usuario

Consulte al administrador del sistema para saber qué versión de IBM Spectrum Protect debe ejecutar en su ubicación.

## **0058 S DSM\_RC\_REJECT\_SERVER\_DOWNLEVEL Sesión rechazada: Versión de código de servidor de nivel inferior**

---

### Explicación

La versión del servidor y la versión del cliente no coinciden. El código de servidor es de nivel inferior.

### Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Consulte al administrador del sistema para saber qué versión de IBM Spectrum Protect debe ejecutar en su ubicación.

## **0059 E DSM\_RC\_REJECT\_ID\_IN\_USE Sesión rechazada: el nombre de nodo especificado está actualmente en uso**

---

### Explicación

El nombre de nodo que ha especificado está en uso en el servidor.

### Acción del Sistema

No se ha iniciado la sesión.

## Respuesta del Usuario

Es posible que el servidor esté realizando una tarea que impide que su nodo establezca una sesión. Vuelva a intentar la operación o consulte al administrador del sistema.

## **0061 E DSM\_RC\_REJECT\_ID\_LOCKED Sesión rechazada: El nombre de nodo especificado está bloqueado actualmente.**

---

### Explicación

El nombre de nodo que ha especificado está bloqueado en el servidor en este momento.

### Acción del Sistema

No se ha iniciado la sesión.

## Respuesta del Usuario

Pregunte al administrador del sistema por qué está bloqueado su nombre de nodo.

## **0062 S DSM\_RC\_SIGNONREJECT\_LICENSE\_MAX SLM LICENSE EXCEEDED: Las licencias de cliente para IBM Spectrum Protect se han superado. Consulte con el administrador del sistema.**

---

## Explicación

La adición de una nueva inscripción excederá el número de licencias de producto de IBM Spectrum Protect.

## Acción del Sistema

La ejecución de la inscripción del cliente o la solicitud de conexión finaliza.

## Respuesta del Usuario

Consulte con el administrador del sistema.

## **0063 E DSM\_RC\_REJECT\_NO\_MEMORY Sesión rechazada: El servidor no tiene suficiente memoria para permitir que se establezca una conexión.**

---

### Explicación

El servidor no tiene suficiente memoria para permitir que el cliente establezca una conexión.

### Acción del Sistema

No se ha iniciado la sesión.

### Respuesta del Usuario

Vuelva a intentar la operación o consulte al administrador del sistema.

## **0064 E DSM\_RC\_REJECT\_NO\_DB\_SPACE Sesión rechazada: El servidor no tiene suficiente espacio de base de datos para permitir que se establezca una conexión.**

---

### Explicación

El servidor se ha quedado sin espacio en la base de datos.

### Acción del Sistema

No se ha iniciado la sesión.

### Respuesta del Usuario

Consulte con el administrador del sistema.

## **0065 E DSM\_RC\_REJECT\_NO\_LOG\_SPACE Sesión rechazada: El servidor no tiene suficiente espacio de registro de recuperación para permitir que se establezca una conexión.**

---

### Explicación

El servidor se ha quedado sin espacio en las anotaciones de recuperación.

### **Acción del Sistema**

No se ha iniciado la sesión.

### **Respuesta del Usuario**

Este error es un problema temporal. Vuelva a intentar la operación o consulte al administrador del sistema.

## **0066 E DSM\_RC\_REJECT\_INTERNAL\_ERROR Se ha rechazado la sesión. El servidor IBM Spectrum Protect tiene un error interno.**

---

### **Explicación**

El cliente no puede establecer una conexión con el servidor de IBM Spectrum Protect debido a un error interno del servidor.

### **Acción del Sistema**

La sesión no se ha iniciado.

### **Respuesta del Usuario**

Informe al administrador de IBM Spectrum Protect de este error.

## **0067 S DSM\_RC\_SIGNONREJECT\_INVALID\_CLI Sesión rechazada: El servidor no tiene licencia para este tipo de plataforma. Consulte con el administrador del sistema.**

---

### **Explicación**

El servidor no tiene licencia para el tipo de cliente que realiza la solicitud.

### **Acción del Sistema**

La ejecución de la inscripción del cliente o la solicitud de conexión finaliza.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0068 E DSM\_RC\_CLIENT\_NOT\_ARCHRETPROT Se ha rechazado la sesión. El servidor no permite un inicio de sesión de un cliente que no tenga activada la protección de retención de copia archivada.**

---

### **Explicación**

El cliente no puede establecer una conexión con el servidor porque el servidor tiene activada la protección de retención de copia archivada y el cliente no.

### **Acción del Sistema**

La sesión no se ha iniciado.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0069 E DSM\_RC\_SESSION\_CANCELED Sesión rechazada: El administrador del sistema canceló la sesión.**

---

### **Explicación**

El administrador del servidor ha cancelado la sesión actual del cliente.

### **Acción del Sistema**

La ejecución de la solicitud de conexión del cliente finaliza.

### **Respuesta del Usuario**

Consulte con el administrador del sistema.

## **0073 E DSM\_RC\_REJECT\_INVALID\_NODE\_TYPE Se ha detectado una incoherencia entre el nodo de cliente y el nodo que está registrado en el servidor IBM Spectrum Protect.**

---

### **Explicación**

Es posible que el usuario haya codificado la opción de nodo de forma incorrecta. Por ejemplo, el nodo que está registrado en el servidor IBM Spectrum Protect puede ser un tipo de NAS, pero el nodo en realidad es un cliente no de NAS.

### **Acción del Sistema**

La operación finaliza.

### **Respuesta del Usuario**

Asegúrese de que el nombre de nodo es correcto en el archivo de opciones del cliente. Utilice un nodo de tipo NAS únicamente con la opción nasnodename.

## **0074 E DSM\_RC\_REJECT\_INVALID\_SESSIONINIT El servidor no permite conexiones iniciadas por el cliente para este nodo.**

---

### **Explicación**

El nodo no tiene permiso para iniciar conexiones debido a los parámetros de configuración de este nodo en el servidor. El servidor puede iniciar conexiones con el planificador del cliente ejecutándose en modalidad por solicitud.

### **Acción del Sistema**

La operación de IBM Spectrum Protect finaliza.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del sistema para habilitar sesiones iniciadas por el cliente en su nodo o actualizar la opción SESSIONINITIATION y ejecutar el planificador del cliente.

## **0075 E DSM\_RC\_REJECT\_WRONG\_PORT Puerto de servidor incorrecto.**

---



## Explicación

Está intentando abrir una sesión del cliente de copia de seguridad/archivado en la configuración del puerto del servidor sólo para sesiones de administración.

## Acción del Sistema

La operación de IBM Spectrum Protect finaliza.

## Respuesta del Usuario

Póngase en contacto con el administrador del sistema y/o utilice los valores correctos para el puerto TCP y el puerto de administración TCP.

## **0079 E DSM\_RC\_CLIENT\_NOT\_SPMRETPROT Se ha rechazado la sesión. El servidor no permite un inicio de sesión de un cliente que no tenga activada la protección de retención gestionada por espacios.**

---

## Explicación

El cliente no puede establecer una conexión con el servidor porque el servidor tiene activada la protección de retención de gestión de espacio y el cliente no.

## Acción del Sistema

La sesión no se ha iniciado.

## Respuesta del Usuario

Consulte con el administrador del sistema.

## **0101 W DSM\_RC\_USER\_ABORT El usuario ha detenido la operación.**

---

## Explicación

La operación se ha detenido a petición del usuario. Esto suele ocurrir cuando se pulsa la tecla 'Q' dos veces.

## Acción del Sistema

El proceso se ha detenido.

## Respuesta del Usuario

Ninguna.

## **0102 E DSM\_RC\_NO\_MEMORY nombre archivo(número línea) El sistema operativo ha rechazado una solicitud de IBM Spectrum Protect de asignación de memoria.**

---

## Explicación

IBM Spectrum Protect requiere acceder a la memoria para almacenar información durante el proceso. En este caso, se ha solicitado más memoria de la que podía asignar el sistema operativo. Las posibles razones son:

- El sistema dispone de poca memoria.
- El proceso en el que se ejecuta el programa ha excedido la memoria máxima asignada.
- Se ha producido alguna otra condición de error. No hay memoria disponible.

### Acción del Sistema

IBM Spectrum Protect no puede completar la operación solicitada.

### Respuesta del Usuario

Cierre todas las aplicaciones que no sean necesarias y repita la operación. Si la operación sigue sin poder efectuarse, intente dividir la tarea en varias unidades más pequeñas. Por ejemplo, si una especificación de archivo contiene varios directorios de alto nivel, ejecute la tarea de IBM Spectrum Protect secuencialmente para cada directorio. Si la tarea de IBM Spectrum Protect es una copia de seguridad incremental, utilice la opción "-memoryefficientbackup=yes".

Para sistemas UNIX que admiten límites de recursos, puede comprobar si el límite de recurso de memoria es demasiado pequeño; para ello, utilice este mandato: `ulimit -a`

En función de los datos que obtenga, puede solicitar al usuario root del sistema UNIX que aumente el límite de recursos por encima del límite predeterminado actual. El usuario root del sistema UNIX tiene autorización para aumentar los límites de recursos.

## 0104 E DSM\_RC\_FILE\_NOT\_FOUND No se ha encontrado el archivo durante el proceso de copia de seguridad, archivado o migración

---

### Explicación

El archivo de la operación de copia de seguridad, archivado o migración ya no existe en el cliente. Otro proceso ha suprimido el archivo antes de que IBM Spectrum Protect pudiera hacer una copia de seguridad, archivarlo o migrarlo.

### Acción del Sistema

El archivo se omite.

### Respuesta del Usuario

Ninguna.

## 0105 E DSM\_RC\_PATH\_NOT\_FOUND No se ha encontrado la vía de acceso de directorio especificada '*vía-acceso*'.

---

### Explicación

Se ha especificado una vía de acceso de directorio que no es válida o no se puede alcanzar.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar la operación con una vía de acceso de directorio válida.

## 0106 E DSM\_RC\_ACCESS\_DENIED Se ha denegado el acceso al archivo o directorio especificado

---

### Explicación

Se ha denegado el acceso al archivo o directorio especificado. Ha intentado leer o grabar datos en un archivo y no dispone de autorización para acceder al archivo o al directorio.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que haya especificado el nombre de archivo o directorio correcto, corrija las autorizaciones o especifique una nueva ubicación.

## **0106 E DSM\_RC\_ACCESS\_DENIED El archivo especificado está siendo utilizado por otro proceso**

---

### **Explicación**

Otro proceso está utilizando el archivo especificado. Ha intentado leer o grabar en un archivo que actualmente utiliza otro proceso.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que haya especificado el nombre de archivo o directorio correcto, corrija las autorizaciones o especifique una nueva ubicación.

## **0107 E DSM\_RC\_NO\_HANDLES No hay descriptores de contexto de archivo disponibles**

---

### **Explicación**

Todos los descriptores de contexto de archivo del sistema están en uso en este momento. No hay más disponibles.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Libere algunos descriptores de contexto de archivo finalizando otros procesos o modifique la configuración del sistema de modo que se puedan abrir más archivos al mismo tiempo.

## **0108 E DSM\_RC\_FILE\_EXISTS El archivo sale y no se puede sobrescribir.**

---

### **Explicación**

El archivo que se está restaurando o recuperando ya existe y no se puede sobrescribir debido a una falta de autoridad o permisos de acceso.

### **Acción del Sistema**

El archivo se pasa por alto.

## Respuesta del Usuario

Verifique que tiene permisos de acceso suficientes para sobrescribir el archivo y vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador del sistema o el administrador de IBM Spectrum Protect para obtener ayuda adicional.

## **0109 E DSM\_RC\_INVALID\_PARM Se ha encontrado un parámetro no válido.**

---

### Explicación

El sistema ha detectado un error de programa interno debido a un parámetro no válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Solicite al representante del servicio que compruebe las anotaciones de errores.

## **0110 E DSM\_RC\_INVALID\_HANDLE Se ha especificado un descriptor de contexto de archivo que no es válido; error del sistema.**

---

### Explicación

Se ha producido un error interno del sistema: No se ha podido llevar a cabo una operación de archivo porque se ha especificado un descriptor de contexto de archivos que no es válido.

### Acción del Sistema

el proceso se detiene.

## Respuesta del Usuario

Vuelva a intentar la operación. Si la anomalía persiste, obtenga un rastreo de servicio que capture el problema y póngase en contacto con el soporte técnico de IBM para obtener ayuda adicional. El administrador de IBM Spectrum Protect puede ayudarle a configurar el rastreo.

## **0111 E DSM\_RC\_DISK\_FULL El proceso se ha detenido; El disco está lleno**

---

### Explicación

No se pueden restaurar ni recuperar más archivos porque el disco de destino está lleno.

### Acción del Sistema

El proceso se ha detenido.

## Respuesta del Usuario

Deje libre espacio del disco, o restaure o recupere el archivo en otro disco.

## **0113 E DSM\_RC\_PROTOCOL\_VIOLATION Violación de protocolo**

---

### Explicación

Se ha producido un error de protocolo de comunicaciones. El subsistema de comunicación no se ha definido correctamente o es erróneo.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Verifique que los procesos de comunicación funcionan correctamente y vuelva a intentar la operación.

## **0114 E DSM\_RC\_UNKNOWN\_ERROR Se ha producido un error de sistema desconocido del que IBM Spectrum Protect no se puede recuperar.**

---

### **Explicación**

Se ha producido un error desconocido. Podría ser un error del sistema de bajo nivel o de comunicación del que no se puede recuperar IBM Spectrum Protect.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema persiste, revise las anotaciones de errores de IBM Spectrum Protect para buscar mensajes relacionados. Obtenga un rastreo de servicio que capture el problema y póngase en contacto con el soporte técnico de IBM para obtener ayuda adicional. El administrador de IBM Spectrum Protect puede ayudarle a configurar el rastreo.

## **0115 E DSM\_RC\_UNEXPECTED\_ERROR Se ha producido un error inesperado.**

---

### **Explicación**

Esto lo produce normalmente un error de sistema de bajo nivel o un error de comunicación del que IBM Spectrum Protect no se puede recuperar.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Examine las anotaciones de errores del cliente para consultar otros mensajes relacionados con este problema. Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el soporte técnico de IBM Spectrum Protect para obtener más ayuda.

## **0116 E DSM\_RC\_FILE\_BEING\_EXECUTED El archivo está en uso; Permiso de escritura denegado.**

---

### **Explicación**

El archivo actual no puede abrirse para grabar en él porque está utilizándose actualmente en otra aplicación.

### **Acción del Sistema**

El archivo se omite.

### Respuesta del Usuario

Detenga la operación que está ejecutando el archivo y vuelva a intentar la operación, o restaure o recupere el archivo con otro nombre o en otro directorio.

## 0117 E DSM\_RC\_DIR\_NO\_SPACE No se pueden restaurar o recuperar más archivos porque el directorio de destino está lleno.

---

### Explicación

No se pueden restaurar ni recuperar más archivos porque el disco de destino está lleno.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Deje libre espacio del disco, o restaure o recupere el archivo en otro disco.

## 0118 E DSM\_RC\_LOOPED\_SYM\_LINK Se han detectado demasiados vínculos simbólicos mientras se resolvía el nombre

---

### Explicación

Al intentar resolver el nombre de archivo, se han encontrado demasiados vínculos simbólicos.

### Acción del Sistema

El archivo se omite.

### Respuesta del Usuario

Asegúrese de no tener ningún vínculo simbólico en bucle para el archivo.

## 0119 E DSM\_RC\_FILE\_NAME\_TOO\_LONG El nombre de archivo es demasiado largo y IBM Spectrum Protect no lo puede procesar

---

### Explicación

El límite del tamaño de archivo de los nombres de archivos puede variar dependiendo del sistema operativo. El límite más común es de 256 caracteres. El nombre de archivo que se está procesando excede el límite soportado por IBM Spectrum Protect en este sistema.

### Acción del Sistema

El archivo se pasa por alto.

### Respuesta del Usuario

Especifique HELP FILE SPEC o consulte el manual del cliente del sistema operativo en el que está recibiendo este error. La sección del manual "Sintaxis de especificación de archivo" explica las longitudes de nombre de archivo soportadas por IBM Spectrum Protect.

## 0120 E DSM\_RC\_FILE\_SPACE\_LOCKED El sistema de archivos está bloqueado por el sistema

---

### Explicación

No se puede acceder al sistema de archivos porque el sistema lo ha bloqueado.

### Acción del Sistema

La operación no puede completarse.

### Respuesta del Usuario

Consulte con el administrador del sistema.

## 0121 I DSM\_RC\_FINISHED La operación ha finalizado.

---

### Explicación

La operación finaliza.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Proceda con la siguiente llamada a función.

## 0122 E DSM\_RC\_UNKNOWN\_FORMAT El archivo tiene un formato desconocido.

---

### Explicación

El proceso ha intentado restaurar o recuperar un archivo, pero tenía un formato desconocido.

### Acción del Sistema

El archivo se pasa por alto.

### Respuesta del Usuario

Otra aplicación ha realizado una copia de seguridad del archivo o los datos no son válidos. Si el archivo pertenece a este sistema, vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el soporte técnico de IBM para obtener más ayuda.

## 0123 E DSM\_RC\_NO\_AUTHORIZATION No autorizado a restaurar los datos del otro nodo.

---

### Explicación

El cliente no está autorizado a restaurar los datos de otro nodo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Consiga autorización de otro nodo.

## 0124 E DSM\_RC\_FILE\_SPACE\_NOT\_FOUND El espacio de archivos '*nombre\_espacio\_archivos*' no existe

---

### Explicación

El espacio de archivos (dominio) especificado es incorrecto o no existe en la máquina.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Vuelva a intentar la operación especificando un dominio existente (letra de unidad o nombre de sistema de archivos).

## 0125 E DSM\_RC\_TXN\_ABORTED La transacción ha terminado anormalmente

---

### Explicación

Se ha detenido la transacción actual entre el servidor y el cliente. Se no puede recuperar una anomalía de servidor, cliente o comunicación.

### Acción del Sistema

La operación actual se ha cancelado.

### Respuesta del Usuario

Vuelva a intentar la operación. Si el problema continúa, consulte al administrador del sistema para identificar el problema.

## 0126 E DSM\_RC\_SUBDIR\_AS\_FILE IBM Spectrum Protect no puede crear una vía de acceso del directorio porque existe un archivo con el mismo nombre que el directorio.

---

### Explicación

Ninguna.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario



Suprima o cambie el nombre al archivo que tiene el mismo nombre que el directorio. De lo contrario, puede restaurar el directorio en una ubicación distinta.

## **0127 E DSM\_RC\_PROCESS\_NO\_SPACE Se ha alcanzado el límite de espacio de disco para este proceso**

---

### **Explicación**

El espacio de disco asignado para el propietario cliente está lleno.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Libere espacio de disco y vuelva a intentar la operación de restauración o recuperación.

## **0128 E DSM\_RC\_PATH\_TOO\_LONG La longitud de la vía de acceso de directorio de destino supera el máximo del sistema**

---

### **Explicación**

El nombre de vía de acceso especificado más el nombre de vía de acceso del nombre del archivo restaurado forman un nombre cuya longitud excede la máxima permitida por el sistema.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Especifique una vía de acceso de destino que, combinada, tenga una longitud inferior a la máxima permitida por el sistema.

## **0129 E DSM\_RC\_NOT\_COMPRESSED El archivo no está comprimido; Anomalía del sistema.**

---

### **Explicación**

Un archivo que tenía el distintivo de compresión no lo estaba y se ha producido una anomalía en el sistema.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del sistema para notificarle del problema. Este error se debe a una anomalía del sistema.

## **0130 E DSM\_RC\_TOO\_MANY\_BITS El archivo se ha comprimido en una máquina cliente distinta que tiene más memoria**

---

### **Explicación**

Está intentando restaurar un archivo del que se hizo una copia de seguridad y se comprimió en otra estación de trabajo cliente que tenía más memoria que su estación de trabajo cliente. No puede restaurar este archivo. Al restaurarse el archivo, éste se expande y su estación de trabajo no dispone de suficiente memoria.

### Acción del Sistema

La operación actual se ha cancelado.

### Respuesta del Usuario

Consiga una máquina con más memoria y vuelva a intentar la operación.

## 0131 E DSM\_RC\_COMPRESSED\_DATA\_CORRUPTED El archivo comprimido está dañado y no se puede expandir correctamente.

---

### Explicación

El archivo comprimido no puede expandirse correctamente debido a uno de los motivos siguientes:

- Existe un problema en la cinta.
- Existe un problema de comunicaciones.
- El archivo comprimido estaba dañado en el servidor de IBM Spectrum Protect.

### Acción del Sistema

El archivo se omite.

### Respuesta del Usuario

1) El archivo comprimido está dañado porque existe un problema en la cinta. Para saber si este es el problema, ejecute el comando siguiente en el servidor IBM Spectrum Protect: `audit volume <nombre_volumen> fix=no` Si se informa de algún problema, podría mover los datos desde ese volumen a otro nuevo (consulte el comando `MOVE DATA`) y volver a intentar la restauración. 2) Existen problemas de comunicación entre el servidor de IBM Spectrum Protect y el cliente de IBM Spectrum Protect y el resultado es que el archivo se ha dañado durante la transmisión. Si utiliza un adaptador de Ethernet de un gigabit en el servidor, actualice el controlador de la tarjeta (plataforma AIX) o añada cambios sugeridos proporcionados por SUN a algunas opciones de red del sistema que han resuelto este problema (plataforma SUN). 3) Verifique con el soporte de red si durante la restauración existe algún problema entre el cliente/servidor de IBM Spectrum Protect que esté causando los daños del archivos.

## 0131 S DSM\_RC\_SYSTEM\_ERROR Se ha producido un error de programa interno.

---

### Explicación

Se ha encontrado una condición inesperada y la operación no puede continuar. Esto podría ser un error de programación.

### Acción del Sistema

el proceso se detiene.

### Respuesta del Usuario

Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador de IBM Spectrum Protect o el soporte técnico de IBM para obtener más ayuda.

## 0132 E DSM\_RC\_NO\_SERVER\_RESOURCES El servidor IBM Spectrum Protect se ha quedado sin recursos.

---

## Explicación

La falta de recursos de almacenamiento o una condición de valor máximo no le permite ninguna actividad nueva.

## Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Vuelva a intentar la operación más adelante. Si el problema continúa, póngase en contacto con el administrador de IBM Spectrum Protect para aislar el recurso que no esté disponible. El administrador de IBM Spectrum Protect puede comprobar las anotaciones de actividad del servidor IBM Spectrum Protect para mensajes que podrían explicar el problema.

## 0133 E DSM\_RC\_FS\_NOT\_KNOWN No se ha podido encontrar el espacio de archivos para el dominio '*nombre-dominio*' en el servidor de IBM Spectrum Protect.

---

### Explicación

Se esperaba encontrar el espacio de archivos especificado en el servidor, pero ya no existe. Es posible que se haya emitido un mandato para suprimir el espacio de archivos del servidor mientras la operación actual estaba en proceso.

### Acción del Sistema

El proceso de IBM Spectrum Protect se detiene.

### Respuesta del Usuario

Vuelva a intentar la operación. Si se repite el problema, compruebe las anotaciones de errores para otros mensajes que puedan indicar la razón de la anomalía. Intente corregir todos los problemas indicados y vuelva a ejecutar la operación. Si el problema persiste, póngase en contacto con el soporte técnico de IBM para obtener más ayuda.

## 0134 E DSM\_RC\_NO\_LEADING\_DIRSEP El campo objName no tiene un separador de directorio.

---

### Explicación

El campo objName no tiene un separador de directorio.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Corrija el valor para objName.

## 0135 E DSM\_RC\_WILDCARD\_DIR No se permiten caracteres comodín en la vía de acceso de directorio de objName.

---

### Explicación

No se permiten caracteres comodín en la vía de acceso de directorios objName.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Corrija el valor para objName.

## **0136 E DSM\_RC\_COMM\_PROTOCOL\_ERROR Se ha rechazado la sesión: se ha producido un error en el protocolo de comunicaciones.**

---

### Explicación

El cliente ha recibido un mensaje de red inesperado. Podría deberse a problemas de red o a un error de programación.

## Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Verifique que la vía de acceso de comunicación funciona correctamente y vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## **0137 E DSM\_RC\_AUTH\_FAILURE Sesión rechazada: Error de autenticación**

---

### Explicación

Error de autenticación. Ha especificado un ID de usuario o contraseña incorrectos.

## Acción del Sistema

La operación actual se ha cancelado.

## Respuesta del Usuario

Especifique el nombre de usuario y contraseña correctos. Si no puede recordar el id de usuario o contraseña correctos, consulte con el administrador del sistema para que le asigne nuevas credenciales para el nombre de nodo.

## **0138 E DSM\_RC\_TA\_NOT\_VALID Los permisos de ejecución/propietario de dsmtca no son válidos.**

---

### Explicación

Los permisos de ejecución/propietario de dsmtca no son válidos.

## Acción del Sistema

El proceso se ha detenido.

## Respuesta del Usuario

Solicite al administrador del sistema que consulte las instrucciones de instalación del cliente para asegurarse de que los permisos de dsmtca se han establecido correctamente.

## **0139 S DSM\_RC\_KILLED Proceso interrumpido.**

---

### **Explicación**

El proceso se ha detenido. Es un error de programación, y el programa cliente finaliza.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema continúa, póngase en contacto con el administrador del sistema.

## **0145 S DSM\_RC\_WOULD\_BLOCK dsmtca bloqueará la operación.**

---

### **Explicación**

dsmtca bloquea la operación. Es un error de programación, y el programa cliente finaliza.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema continúa, póngase en contacto con el administrador del sistema.

## **0146 S DSM\_RC\_TOO\_SMALL El área para el patrón de inclusión/exclusión es demasiado pequeña.**

---

### **Explicación**

El área para el patrón inclusión/exclusión es demasiado pequeña. Es un error de programación, y el programa cliente finaliza.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema continúa, póngase en contacto con el administrador del sistema.

## **0147 S DSM\_RC\_UNCLOSED No hay ningún corchete de cierre en el patrón.**

---

### **Explicación**

No hay corchetes de cierre en el patrón. Es un error de programación, y el programa cliente finaliza.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema continúa, póngase en contacto con el administrador del sistema.

## **0148 S DSM\_RC\_NO\_STARTING\_DELIMITER El patrón inclusión/exclusión debe comenzar con un delimitador de directorio**

---

### **Explicación**

El patrón inclusión/exclusión debe comenzar con un delimitador de directorio.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Corrija la sintaxis del patrón.

## **0149 S DSM\_RC\_NEEDED\_DIR\_DELIMITER Falta el delimitador de directorio de comienzo o finalización del patrón Incluir/Excluir.**

---

### **Explicación**

1. El patrón inclusión/exclusión tiene un '!' sin delimitador de directorio de comienzo o finalización.
2. Para Windows, el separador de unidad no está seguido inmediatamente por un delimitador de directorio.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Corrija la sintaxis del patrón.

## **0151 S DSM\_RC\_BUFFER\_OVERFLOW El almacenamiento intermedio de datos se ha desbordado.**

---

### **Explicación**

El almacenamiento intermedio de datos se desbordó. Es un error de programación, y el programa cliente finaliza.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema continúa, póngase en contacto con el administrador del sistema.

## **0154 E DSM\_RC\_NO\_COMPRESS\_MEMORY No hay memoria suficiente para la compresión/expansión del archivo**

---

### **Explicación**

No hay suficiente memoria disponible para hacer compresión o ampliación de datos. Para una restauración o recuperación, no se puede recuperar archivo desde el servidor hasta que haya más almacenamiento disponible. Para una copia de seguridad o archivado, intente ejecutar sin compresión si no hay almacenamiento disponible.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Libere almacenamiento extra para que la operación continúe, o ejecute el proceso de copia de seguridad o archivado sin la compresión activa.

## **0155 T DSM\_RC\_COMPRESS\_GREW Crecimiento de datos comprimidos**

---

### **Explicación**

El tamaño del archivo después de la compresión es mayor que antes.

### **Acción del Sistema**

Aunque el tamaño del archivo comprimido ha aumentado el archivo está comprimido.

### **Respuesta del Usuario**

Ninguna.

## **0156 E DSM\_RC\_INV\_COMM\_METHOD Se ha especificado un método de comunicaciones no admitido.**

---

### **Explicación**

Ninguna.

### **Acción del Sistema**

el proceso se detiene.

### **Respuesta del Usuario**

Especifique una interfaz de comunicaciones que esté soportada por el cliente de IBM Spectrum Protect en el sistema operativo. Consulte el manual del cliente de IBM Spectrum Protect para su sistema operativo para obtener más información sobre la configuración de las comunicaciones del cliente de IBM Spectrum Protect.

## **0157 S DSM\_RC\_WILL\_ABORT La transacción terminará anormalmente.**

---

### **Explicación**

El servidor ha detectado un error y terminará la transacción anormalmente.

### **Acción del Sistema**

La transacción se cancelará. El código de razón se ha especificado en la llamada dsmEndTxn.

### **Respuesta del Usuario**

Emita dsmEndTxn con un voto de DSM\_VOTE\_COMMIT y examine el código de razón.

## **0158 E DSM\_RC\_FS\_WRITE\_LOCKED El archivo o el directorio destino está bloqueado contra grabación**

---

### **Explicación**

No se puede grabar en el archivo o directorio que se está restaurando o recuperando desde el servidor porque el destino está bloqueado contra grabación. Puede que otra operación tenga abierto el archivo y no deje que se actualice.

### **Acción del Sistema**

El archivo se omite.

### **Respuesta del Usuario**

Determine qué operación tiene el archivo bloqueado contra grabación o restaure el archivo con otro nombre o en otra ubicación.

## **0159 I DSM\_RC\_SKIPPED\_BY\_USER Se ha omitido un archivo durante una operación de restauración porque el archivo está fuera de línea y la aplicación ha elegido no esperar un montaje de cinta.**

---

### **Explicación**

Se ha omitido un archivo durante una operación de restauración porque el archivo está desactivado y la aplicación ha elegido no esperar el montaje de la cinta.

### **Acción del Sistema**

El archivo se omite.

### **Respuesta del Usuario**

Verifique que la aplicación establece el valor mountWait correctamente en dsmBeginGetData.

## **0160 E DSM\_RC\_TA\_NOT\_FOUND No se encuentra el módulo dsmtca.**

---

### **Explicación**

IBM Spectrum Protect no encuentra el módulo dsmtca en el directorio especificado.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Asegúrese de que el módulo dsmtca esté en el directorio especificado por DSMI\_DIR.

## **0162 E DSM\_RC\_FS\_NOT\_READY El sistema/unidad de archivos no está preparado**

---

### **Explicación**



El sistema de archivos o la unidad no están preparados para que se pueda acceder a ellos.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que la unidad esté disponible y vuelva a intentar la operación.

## **0164 E DSM\_RC\_FIO\_ERROR Error de la entrada/salida del archivo**

---

### **Explicación**

Se ha detectado un error al leer o grabar datos en el archivo.

### **Acción del Sistema**

El archivo o sistema de archivos se pasa por alto.

### **Respuesta del Usuario**

Compruebe el sistema para asegurarse de que está funcionando correctamente. En OS/2, ejecute CHKDSK /F para la unidad que genera el error, que puede localizarse en el archivo dsmerror.log.

## **0165 E DSM\_RC\_WRITE\_FAILURE Error al grabar el archivo**

---

### **Explicación**

Se ha detectado un error al grabar datos en el archivo.

### **Acción del Sistema**

El archivo se omite.

### **Respuesta del Usuario**

Compruebe el sistema para asegurarse de que está funcionando correctamente.

## **0166 E DSM\_RC\_OVER\_FILE\_SIZE\_LIMIT El archivo supera los límites del archivo del sistema/usuario**

---

### **Explicación**

Un archivo que se está restaurando o recuperando supera los límites establecidos por el sistema para este usuario.

### **Acción del Sistema**

El archivo se omite.

### **Respuesta del Usuario**

Asegúrese de que los límites del sistema estén bien definidos.

## **0167 E DSM\_RC\_CANNOT\_MAKE No es posible crear archivo/directorio**

---

## Explicación

No se puede crear la vía de acceso del directorio para los archivos que se están restaurando o recuperando.

## Acción del Sistema

El archivo se omite.

## Respuesta del Usuario

Asegúrese de que dispone de la autorización apropiada para crear el directorio del archivo que se está restaurando o recuperando.  
Asegúrese de que tiene acceso de grabación.

## 0168 E DSM\_RC\_NO\_PASS\_FILE El archivo de contraseña no está disponible.

---

### Explicación

El archivo que contiene la contraseña almacenada para el *nombre de servidor* especificado no está disponible.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

El usuario root debe establecer y almacenar una contraseña nueva.

## 0169 E DSM\_RC\_VERFILE\_OLD PASSWORDACCESS es GENERATE, pero se necesita la contraseña para el servidor '*nombre\_servidor*'. La contraseña no está almacenada localmente, o se cambió en el servidor.

---

### Explicación

La contraseña no está almacenada localmente, o se cambió en el servidor.

### Acción del Sistema

IBM Spectrum Protect le solicita la contraseña si IBM Spectrum Protect se está ejecutando en primer plano.

### Respuesta del Usuario

Si IBM Spectrum Protect se estaba ejecutando como proceso subordinado, emita cualquier mandato de IBM Spectrum Protect desde primer plano. Escriba la contraseña en respuesta a la solicitud. Después, intente de nuevo el mandato de IBM Spectrum Protect en segundo plano.

## 0173 E DSM\_RC\_INPUT\_ERROR El proceso se está ejecutando en un modo no interactivo, pero requiere la entrada del usuario.

---

### Explicación

Este proceso requiere una entrada de teclado, pero los procesos no interactivos no pueden leer la entrada desde el teclado.

### Acción del Sistema

el proceso se detiene.

### Respuesta del Usuario

Realice las siguientes acciones para resolver este error:

- Ejecute el producto en modo interactivo.
- Asegúrese de que su contraseña está configurada correctamente.

## 0174 E DSM\_RC\_REJECT\_PLATFORM\_MISMATCH Sesión rechazada: el tipo de nodo no coincide

---

### Explicación

El nombre de nodo está asociado con un tipo diferente de sistema operativo y no puede utilizarse en este sistema.

### Acción del Sistema

La operación actual se ha cancelado.

### Respuesta del Usuario

Si necesita un nombre de nodo nuevo, consulte al administrador del sistema para que le asigne uno nuevo. Por lo general, tiene un nombre de nodo para cada par de máquina y sistema operativo que necesita acceder al servidor.

## 0175 E DSM\_RC\_TL\_NOT\_FILE\_OWNER No es el propietario del archivo

---

### Explicación

No se puede hacer copia de seguridad del archivo porque el cliente no es el propietario del archivo.

### Acción del Sistema

El archivo se pasa por alto.

### Respuesta del Usuario

Ninguna.

## 0177 S DSM\_RC\_UNMATCHED\_QUOTE Las comillas no coinciden

---

### Explicación

Las comillas especificadas en el patrón no son iguales y no van a juego.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Corrija el patrón utilizando comillas que coincidan en la sintaxis.

## 0184 E DSM\_RC\_TL\_NOBCG La clase de gestión de este archivo no tiene un grupo de copia de seguridad válido.

## No se realizará la copia de seguridad de este archivo.

---

### Explicación

La clase de gestión para este archivo no tiene un grupo de copia de seguridad especificado. No se realizará la copia de seguridad de este archivo.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Añada un grupo de copia de seguridad válido a la clase de gestión, y vuelva a intentar la operación.

## 0185 W DSM\_RC\_TL\_EXCLUDED El archivo '*nombre\_archivo nombre\_archivo*' se ha excluido por una lista de inclusión/exclusión

---

### Explicación

No puede hacer copias de seguridad, archivar o migrar archivos que están excluidos.

### Acción del Sistema

El archivo no puede procesarse.

### Respuesta del Usuario

Si el archivo está excluido de forma intencionada, este mensaje se puede ignorar. De lo contrario, modifique la lista inclusión/exclusión, reinicie el cliente, y vuelva a intentar la operación. Póngase en contacto con el administrador de IBM Spectrum Protect para obtener más ayuda.

## 0186 E DSM\_RC\_TL\_NOACG La clase de gestión para este archivo no tiene un grupo de copia de archivado especificado. Este archivo no se archivará.

---

### Explicación

La clase de gestión para este archivo no tiene un grupo de copia de archivado especificado. Este archivo no se archivará.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Añada un grupo de copia de archivado válido a la clase de gestión, y vuelva a intentar la operación.

## 0187 E DSM\_RC\_PS\_INVALID\_ARCHMC Se ha especificado una clase de gestión que no es válida

---

## Explicación

Ha introducido una clase de gestión no válida.

## Acción del Sistema

La operación solicitada no es posible.

## Respuesta del Usuario

Vuelva a intentar la operación utilizando una clase de gestión válida.

## **0188 S DSM\_RC\_NO\_PS\_DATA Bien el nodo no existe en el servidor o bien no hay un conjunto de políticas activas para el nodo.**

---

### Explicación

Se produce este error cuando intenta acceder a los datos de otro nodo. Bien el nodo no está registrado con el servidor IBM Spectrum Protect, o bien no hay un conjunto de políticas activas para el nodo.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Verifique que el nodo a cuyos datos está intentando acceder está registrado con el servidor IBM Spectrum Protect. Si tiene más de un servidor de IBM Spectrum Protect, asegúrese de que se está conectando al servidor correcto y, a continuación, intente la operación de nuevo. Si el problema persiste, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## **0189 S DSM\_RC\_PS\_INVALID\_DIRMC La clase de gestión asignada a los directorios no existe.**

---

### Explicación

La clase de gestión nombrada en la opción DIRMC no existe en su conjunto de políticas asignado en el servidor. Las anotaciones de errores contienen una entrada que muestra un nombre de clase de gestión no válido.

### Acción del Sistema

el proceso se detiene.

### Respuesta del Usuario

Suprima la opción DIRMC actual del archivo de opciones del cliente, después ejecute DSMC QUERY MGMTCLASS -DETAIL para ver la información sobre las clases de gestión disponibles. Asegúrese de que la clase de gestión que selecciona tiene un grupo de copia de seguridad. Si tiene más de un servidor de IBM Spectrum Protect, asegúrese de que se está conectado al servidor correcto. Si no puede encontrar una clase de gestión adecuada, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## **0190 S DSM\_RC\_PS\_NO\_CG\_IN\_DIR\_MC No hay ningún grupo de copia de seguridad en la clase de gestión utilizada para los directorios.**

---

### Explicación

La opción DIRMC asigna un nombre a la clase de gestión que no contiene un grupo de copia de seguridad.

## Acción del Sistema

el proceso se detiene.

## Respuesta del Usuario

Suprima la opción DIRMC actual del archivo de opciones del cliente, después ejecute DSMC QUERY MGMTCLASS -DETAIL para ver la información sobre las clases de gestión disponibles. Asegúrese de que la clase de gestión que selecciona tiene un grupo de copia de seguridad. Si tiene más de un servidor de IBM Spectrum Protect, asegúrese de que se está conectado al servidor correcto. Si no puede encontrar una clase de gestión adecuada, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## **0231 E DSM\_RC\_ABORT\_MOVER\_TYPE Tipo Remote Mover desconocido**

---

### Explicación

El tipo Remote Mover especificado es desconocido.

### Acción del Sistema

La operación actual ha finalizado.

### Respuesta del Usuario

Póngase en contacto con el administrador del sistema para obtener más información.

## **0232 E DSM\_RC\_ABORT\_ITEM\_IN\_USE Una operación para el nodo y el espacio de archivos solicitados ya está en curso.**

---

### Explicación

Se ha realizado una solicitud para utilizar un transportador de datos para ejecutar una operación para el nodo y el espacio de archivos indicados. Como la operación para este nodo y este espacio de archivos ya está en curso, la nueva operación no puede ejecutarse.

### Acción del Sistema

La operación actual ha finalizado.

### Respuesta del Usuario

Vuelva a intentar la operación más tarde.

## **0233 E DSM\_RC\_ABORT\_LOCK\_CONFLICT Recurso de sistema en uso**

---

### Explicación

Un recurso necesario está siendo utilizado por otro mandato o proceso.

### Acción del Sistema

La operación actual ha finalizado.

### Respuesta del Usuario

Vuelva a intentar la operación más tarde.

## **0234 E DSM\_RC\_ABORT\_SRV\_PLUGIN\_COMM\_ERROR** Error de comunicación del conector del servidor.

---

### **Explicación**

La comunicación entre un módulo de plug-in del servidor y un filtro NAS ha fallado.

### **Acción del Sistema**

La operación actual ha finalizado.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del sistema para obtener más información.

## **0235 E DSM\_RC\_ABORT\_SRV\_PLUGIN\_OS\_ERROR** El plug-in de servidor ha detectado un sistema operativo de gestor de archivos NAS no soportado.

---

### **Explicación**

Un módulo de plug-in ha detectado que un archivador NAS está ejecutando un sistema operativo o un nivel de sistema operativo no admitido.

### **Acción del Sistema**

La operación actual ha finalizado.

### **Respuesta del Usuario**

Póngase en contacto con el administrador del sistema para obtener más información.

## **0236E DSM\_RC\_ABORT\_CRC\_FAILED** El CRC recibido del servidor no coincide con el CRC calculado por el cliente.

---

### **Explicación**

El servidor envió un CRC para un almacenamiento intermedio. El cliente calculó un CRC para el mismo almacenamiento intermedio. No coinciden. La discrepancia indica un fallo en la comunicación.

### **Acción del Sistema**

En algunos casos, el cliente puede indicar un fallo el servidor y volver a intentar la operación.

### **Respuesta del Usuario**

Compruebe las anotaciones de rastreo para obtener más información e intente de nuevo la operación. Si el problema continúa, consulte al administrador del sistema.

## **0237E DSM\_RC\_ABORT\_INVALID\_GROUP\_ACTION** Se ha intentado una operación no válida en un líder de grupo o miembro de grupo.

---

### **Explicación**

Se ha intentado una operación no válida en un grupo lógico.

### **Acción del Sistema**

La operación actual se detiene.

### **Respuesta del Usuario**

Vuelva a intentar la operación válida.

## **0238E DSM\_RC\_ABORT\_DISK\_UNDEFINED Disco remoto no definido.**

---

### **Explicación**

Se ha intentado una operación en un disco remoto que no está definido.

### **Acción del Sistema**

La operación actual se detiene.

### **Respuesta del Usuario**

Defina el disco remoto adecuado.

## **0239E DSM\_RC\_ABORT\_BAD\_DESTINATION El destino de entrada no coincide con el destino esperado.**

---

### **Explicación**

El destino de entrada no coincide con el destino previsto.

### **Acción del Sistema**

La operación actual se detiene.

### **Respuesta del Usuario**

Vuelva a intentar la operación con un destino adecuado.

## **0240E DSM\_RC\_ABORT\_DATAMOVER\_NOT\_AVAILABLE El transportador de datos no está disponible.**

---

### **Explicación**

El transportador de datos no está disponible.

### **Acción del Sistema**

La operación actual se detiene.

### **Respuesta del Usuario**

Vuelva a intentar la operación con un transportador de datos adecuado.



## **0241E DSM\_RC\_ABORT\_STGPOOL\_COPY\_CONT\_NO La operación ha fallado porque la opción de copia continua se ha establecido en NO.**

---

### **Explicación**

La operación ha fallado porque la opción de copia continua estaba establecida en NO.

### **Acción del Sistema**

La operación actual se detiene.

### **Respuesta del Usuario**

Este código de cancelación indica que una operación de almacenamiento, tal como una operación de copia de seguridad o archivado ha fallado debido a que la opción de copia continua se ha establecido en NO. El administrador del sistema, sysadmin, deberá resolver el problema en el servidor.

## **0242E DSM\_RC\_ABORT\_RETRY\_SINGLE\_TXN La transacción ha fallado debido a un problema ocurrido durante una operación de almacenamiento.**

---

### **Explicación**

La transacción ha fallado debido a un problema durante una operación de almacenamiento. Este error suele producirse cuando la siguiente agrupación de almacenamiento tiene una lista de agrupación de almacenamiento de copia distinta y se cambia a esta agrupación en mitad de una transacción.

### **Acción del Sistema**

La transacción se ha cancelado.

### **Respuesta del Usuario**

Vuelva a enviar los objetos en transacciones separadas.

## **0245 E DSM\_RC\_ABORT\_PATH\_RESTRICTED La configuración de cliente actual no cumple con el valor de la opción de servidor DATAWRITEPATH o DATAREADPATH para este nodo.**

---

### **Explicación**

Los valores de las opciones del servidor DATAWRITEPATH y DATAREADPATH especifican a dónde se le permite al servidor enviar datos, y desde dónde se leen esos datos. Los valores para el nombre de nodo especificado debería corresponder a la configuración del cliente. Por ejemplo, obtendrá este mensaje de error si DATAWRITEPATH contiene un valor LAN y el cliente está configurado para utilizar un protocolo fuera de la LAN, o viceversa.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Compruebe las anotaciones de cliente, servidor y agente de almacenamiento para determinar porqué el cliente no pudo enviar datos fuera de la LAN. Asegúrese de que la configuración de cliente y las opciones de servidor son compatibles.

## 0247 E DSM\_RC\_ABORT\_INSERT\_NOT\_ALLOWED Este servidor no admite operaciones de copia de seguridad.

---

### Explicación

Este servidor sólo admite operaciones de archivado, no se admiten operaciones de copia de seguridad.

### Acción del Sistema

La actual operación termina.

### Respuesta del Usuario

Realice únicamente operaciones de archivado en este servidor.

## 0248 E DSM\_RC\_ABORT\_DELETE\_NOT\_ALLOWED Suprimiendo este objeto: "fshlll" no están permitidos.

---

### Explicación

El objeto está retenido y no puede suprimirse o está en un servidor habilitado con protección de retención y no ha caducado.

### Acción del Sistema

El objeto se salta y el proceso continúa.

### Respuesta del Usuario

Compruebe el estado del objeto mediante una consulta para saber si está retenido o cuándo caduca.

## 0249 E DSM\_RC\_ABORT\_TXN\_LIMIT\_EXCEEDED El número de objetos de esta transacción ha excedido los valores de TXNGROUPMAX.

---

### Explicación

Hay demasiados objetos en esta transacción.

### Acción del Sistema

La actual operación termina.

### Respuesta del Usuario

Vuelva a intentar la operación con menos objetos en la transacción o aumente el valor de TXNGROUPMAX en el servidor.

## 0250 E DSM\_RC\_ABORT\_OBJECT\_ALREADY\_HELD fshlll ya está en retención.

---

### Explicación

Uno de los objetos de la transacción El objeto especificado ya está retenido y no se puede volver a retener.

### Acción del Sistema

La operación actual finaliza. Este objeto se salta y el proceso continúa.

### Respuesta del Usuario

Emita una consulta para comprobar el estado de los objetos y vuelva a intentar la operación sin el objeto retenido.

## 0292 E DSM\_RC\_TCA\_FORK\_FAILED Error al iniciar el proceso de dsmtca o dsmenc.

---

### Explicación

Se ha producido un error al iniciar el proceso de dsmtca o dsmenc; en concreto, ha fallado la función `fork()`.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Probable error del sistema. Si el problema persiste, reinicie la estación de trabajo.

## 0295 E DSM\_RC\_TCA\_INVALID\_REQUEST El módulo dsmtca de IBM Spectrum Protect ha recibido una solicitud no válida.

---

### Explicación

El cliente de archivado y copia de seguridad ha invocado el proceso de dsmtca o dsmenc y ha recibido un argumento de solicitud desconocido en la llamada.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Es posible que un proceso distinto del cliente de archivado y copia de seguridad haya invocado por error el proceso de dsmtca o dsmenc. Si no es el caso, se trata de un error interno. Si el problema persiste, póngase en contacto con el representante de servicio de IBM.

## 0296 E DSM\_RC\_TCA\_NOT\_ROOT Esta acción necesita autorización administrativa de IBM Spectrum Protect en este sistema.

---

### Explicación

Se ha intentado llevar a cabo una actividad que debe realizar el administrador de IBM Spectrum Protect (por ejemplo, un registro abierto, una supresión de espacio de archivos o una actualización de contraseña).

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Si la actividad es necesaria, debe realizarla el administrador del sistema.

## 0297 E DSM\_RC\_TCA\_SEMGET\_ERROR Error al asignar semáforos.

---

### Explicación

Se ha producido un error debido a que los semáforos que está intentando asignar son insuficientes.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Consulte al administrador del sistema para obtener ayuda y que aumente el número de semáforos del sistema.

## 0298 E DSM\_RC\_TCA\_SEM\_OP\_ERROR Error al establecer el valor de los semáforos o al esperar por un semáforo.

---

### Explicación

Se ha producido un error al intentar establecer o esperar por un semáforo.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Probable error del sistema. Si el problema persiste, reinicie la estación de trabajo.

## 0400 E DSM\_RC\_INVALID\_OPT Se ha encontrado una opción no válida durante el análisis de opción.

---

### Explicación

Se ha encontrado una opción que no es válida.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique las opciones en dsm.opt, dsm.sys, y en la serie de opciones. Consulte las anotaciones de errores para obtener información detallada acerca del error. En la plataforma AS/400, verifique las opciones en \*LIB/QOPTIBM Spectrum Protect(APIOPT).

## 0405 E DSM\_RC\_NO\_HOST\_ADDR TCPSERVERADDRESS no definido por este servidor en el Archivo de opciones del sistema

---

### Explicación

El TCPSERVERADDRESS para este servidor no está definido en la sección de nombre de servidor en el archivo de opciones del sistema.

### Acción del Sistema

La inicialización de IBM Spectrum Protect falla y el programa finaliza.

## Respuesta del Usuario

Consulte el administrador de IBM Spectrum Protect para el sistema y asegúrese de que el servidor al que está intentando conectarse, tiene una TCPSEVERADDRESS válida definida en el archivo de opciones del sistema.

## 0406 S DSM\_RC\_NO\_OPT\_FILE o se ha podido encontrar el archivo de opciones '*file-name*' o no puede leerse.

---

### Explicación

Las razones comunes para este error incluyen:

- El archivo de opciones predeterminado no existe.
- Especifique la opción -OPTFILE cuando inicie el cliente de IBM Spectrum Protect , pero el archivo de opciones que proporcionó no existe.
- La variable de entorno DSM\_CONFIG (o DSMI\_CONFIG si está utilizando la API de IBM Spectrum Protect ) especifica un archivo de opciones que no existe.
- Ha especificado la opción -OPTFILE al iniciar el cliente de IBM Spectrum Protect pero el archivo de opciones proporcionado no está en el cifrado de archivo estándar del sistema. Por ejemplo, en Windows el cifrado de archivo es ANSI.
- La especificado la opción -OPTFILE cuando se instala el cliente de IBM Spectrum Protect pero el archivo de opciones proporcionado no tiene derechos de lectura apropiados para el usuario que está ejecutando la operación.

### Acción del Sistema

El cliente de IBM Spectrum Protect detiene el proceso.

## Respuesta del Usuario

Compruebe que el archivo de opciones que desea utilizar existe, tiene los derechos de lectura establecidos para el usuario que está ejecutando la operación, y está en el cifrado de archivo estándar del sistema. Por ejemplo, en Windows el cifrado de archivo es ANSI. Revise la información de configuración en el manual del cliente de IBM Spectrum Protect específica para su sistema operativo. Si el problema persiste, póngase en contacto con el administrador de IBM Spectrum Protect para obtener ayuda.

## 0408 E DSM\_RC\_MACHINE\_SAME Un nombre de nodo virtual no debe ser igual a un nombre de nodo o al nombre de host del sistema.

---

### Explicación

Se ha especificado la opción VIRTUALNODENAME con un nombre igual al de una opción NODENAME o al nombre de host del sistema.

### Acción del Sistema

La inicialización falla y el programa finaliza.

## Respuesta del Usuario

Si el nombre de nodo virtual introducido era el mismo que el nombre de host, elimine la opción de nombre de nodo virtual. Si es el mismo que la opción de nombre de nodo, puede eliminar uno, en función del uso deseado. El nombre de nodo se utiliza para asignar un nombre alternativo para su sistema. El nombre de nodo virtual se utiliza para acceder a los datos del servidor de otro sistema.

## 0409 E DSM\_RC\_INVALID\_SERVER No se ha encontrado el nombre del servidor en el archivo de opciones del sistema

---

### Explicación

El archivo de opciones del sistema no contiene la opción SERVERNAME.

### **Acción del Sistema**

La inicialización de IBM Spectrum Protect falla y el programa finaliza.

### **Respuesta del Usuario**

Consulte el administrador de IBM Spectrum Protect para su sistema, y asegúrese de que el archivo de opciones del sistema contiene el nombre del servidor.

## **0410 E DSM\_RC\_INVALID\_KEYWORD Se ha encontrado una palabra clave de opción no válida durante el análisis de opción.**

---

### **Explicación**

Se ha encontrado una palabra clave de opción no válida en el archivo de configuración dsmInit, la serie de opciones, dsm.sys, o dsm.opt.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Corrija la ortografía de las palabras claves de opción. Verifique que el archivo de configuración dsmInit solamente tiene un subconjunto de las opciones dsm.sys. Consulte las anotaciones de errores para obtener información detallada acerca del error.

## **0411 S DSM\_RC\_PATTERN\_TOO\_COMPLEX No se puede analizar el patrón de inclusión o exclusión.**

---

### **Explicación**

El patrón se ha formateado incorrectamente o es demasiado complejo para interpretarse.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Verifique que se ha especificado correctamente el patrón de inclusión o de exclusión. Si el patrón es correcto, póngase en contacto con el soporte técnico de IBM para obtener más ayuda.

## **0412 S DSM\_RC\_NO\_CLOSING\_BRACKET El patrón Inclusión/Exclusión ha perdido un paréntesis de cierre**

---

### **Explicación**

El patrón de inclusión o de exclusión está construido de forma incorrecta. Falta el paréntesis de cierre.

### **Acción del Sistema**

El proceso se ha detenido.

## Respuesta del Usuario

Corrija la sintaxis del patrón.

## 0426 E DSM\_RC\_CANNOT\_OPEN\_TRACEFILE Las funciones de inicialización no pueden abrir el archivo de seguimiento especificado.

---

### Explicación

No se ha podido abrir el archivo durante la inicialización. Es posible que la vía de acceso especificada sea incorrecta. También es posible que el usuario actual no tenga permiso para grabar en el archivo de rastreo en el directorio especificado. O que no haya espacio disponible en la ubicación del archivo de rastreo.

### Acción del Sistema

El proceso se ha detenido.

## Respuesta del Usuario

Asegúrese de que la opción del archivo de rastreo hace referencia a una vía de acceso válida y que el usuario tiene los permisos adecuados para grabar en el archivo especificado.

## 0427 E DSM\_RC\_CANNOT\_OPEN\_LOGFILE Las funciones de inicialización no pueden abrir el archivo de registro de errores especificado.

---

### Explicación

El archivo de registro de errores no se puede abrir durante la inicialización. La vía de acceso especificada puede ser incorrecta. También es posible que el usuario actual no tenga permiso para grabar en el archivo de registro en el directorio especificado. O que no haya espacio disponible en la ubicación del archivo de registro indicado.

### Acción del Sistema

El proceso finaliza.

## Respuesta del Usuario

Asegúrese de que la opción del archivo de registro hace referencia a una vía de acceso válida y que el usuario tiene los permisos adecuados para grabar en el archivo especificado.

## 0600 E DSM\_RC\_DUP\_LABEL Hay una etiqueta de volumen duplicada. La operación no puede continuar.

---

### Explicación

Para los medios extraíbles, IBM Spectrum Protect utiliza la etiqueta de volumen como el nombre de espacio de archivos. Para evitar que los datos de volúmenes diferentes se almacenen en el mismo espacio de archivos del servidor IBM Spectrum Protect, no se permite la copia de seguridad o el archivado de volúmenes de soportes extraíbles que tienen etiquetas de volumen duplicadas.

### Acción del Sistema

La operación solicitada no se ejecuta.

## Respuesta del Usuario

Cambie las etiquetas de volumen de los volúmenes de medios extraíbles para que no haya etiquetas duplicadas. Después, reinicie IBM Spectrum Protect y vuelva a intentar la operación.

## **0601 E DSM\_RC\_NO\_LABEL La unidad no tiene etiqueta. La operación no puede continuar.**

---

### **Explicación**

Para la copia de seguridad o archivado de medios extraíbles es necesario que los medios tengan una etiqueta de volumen. Se ha intentado hacer copia de seguridad o archivar datos en un volumen extraíble que no tiene etiqueta.

### **Acción del Sistema**

La operación solicitada no se ejecuta.

### **Respuesta del Usuario**

Cree una etiqueta de volumen en un medio extraíble, a continuación, vuelva a intentar la operación.

## **0610 E DSM\_RC-NLS\_CANT\_OPEN\_TXT No se puede abrir el archivo de texto de mensajes.**

---

### **Explicación**

El sistema no puede abrir el archivo de txt de mensajes (dscenu.txt o dsmclientV3.cat para AIX). En la plataforma AS/400 este archivo es QANSAPI/QAANSENU(TXT).

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique que el archivo dscenu.txt está en el directorio al que hace referencia DSMI\_DIR. En AIX, verifique que el archivo dsmclientV3.cat tiene un enlace simbólico a /usr/lib/nls/msg/<locale>/dsmclientV3.cat .

## **0611 E DSM\_RC-NLS\_CANT\_READ\_HDR No se puede utilizar el archivo de texto de mensajes.**

---

### **Explicación**

El sistema no puede utilizar el archivo de texto de mensajes (dscenu.txt o dsmclientV3.cat para AIX) debido a una cabecera no válida. En la plataforma AS/400 este archivo es QANSAPI/QAANSENU(TXT).

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Vuelva a instalar el archivo de texto de mensajes.

## **0612 E DSM\_RC-NLS\_INVALID\_CNTL\_REC No se puede utilizar el archivo de texto de mensaje.**

---



## Explicación

El sistema no puede utilizar el archivo txt de mensajes (dscenu.txt o dsmclientV3.cat para AIX) debido a un registro de control no válido. En la plataforma AS/400 este archivo es QANSAPI/QAANSENU(TXT).

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Vuelva a instalar el archivo de texto de mensajes.

## 0613 E DSM\_RC-NLS\_INVALID\_DATE\_FMT Se ha especificado un valor no válido para DATEFORMAT.

---

### Explicación

Se ha especificado un valor no válido para DATEFORMAT.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Especifique un valor válido.

## 0614 E DSM\_RC-NLS\_INVALID\_TIME\_FMT Se ha especificado un valor no válido para TIMEFORMAT.

---

### Explicación

Se ha especificado un valor no válido para TIMEFORMAT.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Especifique un valor válido.

## 0615 E DSM\_RC-NLS\_INVALID\_NUM\_FMT Se ha especificado un valor no válido para NUMBERFORMAT.

---

### Explicación

Se ha especificado un valor no válido para NUMBERFORMAT.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Especifique un valor válido.

## 0620 E DSM\_RC\_LOG\_CANT\_BE\_OPENED No se puede abrir el archivo de registro de errores.

---

### Explicación

El sistema no puede abrir el archivo de registro de errores.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique el valor y el permiso de acceso de DSMI\_LOG. En la plataforma AS/400, verifique el valor especificado para ERRORLOGNAME en el archivo de opciones de la API.

## 0621 E DSM\_RC\_LOG\_ERROR\_WRITING\_TO\_LOG No se puede escribir en el archivo de registro.

---

### Explicación

Se ha producido un error al escribir en el archivo de registro.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique el valor y el permiso de acceso de DSMI\_LOG. En la plataforma AS/400, verifique el valor especificado para ERRORLOGNAME en el archivo de opciones de la API.

## 0622 E DSM\_RC\_LOG\_NOT\_SPECIFIED No se ha especificado el nombre de archivo de registro.

---

### Explicación

El sistema no puede abrir el archivo de registro de errores.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique el valor y el permiso de acceso de DSMI\_LOG. En la plataforma AS/400, verifique el valor especificado para ERRORLOGNAME en el archivo de opciones de la API.

## 0927 E DSM\_RC\_NOT\_ADSM\_AUTHORIZED Sólo un usuario autorizado de IBM Spectrum Protect puede realizar esta acción.

---

### Explicación

El usuario debe ser un usuario autorizado de IBM Spectrum Protect para realizar esta acción. El usuario no tiene autorización de contraseña y esta acción requiere información.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

El usuario debe ser un usuario root, o el usuario debe ser el propietario del ejecutable y el bit del id de usuario efectivo del conjunto está configurado en 'on' (bit 's').

## 961 E DSM\_RC\_DIRECT\_STORAGE\_AGENT\_UNSUPPORTED No se permite la conexión directa con el agente de almacenamiento.

---

### Explicación

No puede conectarse directamente al agente de almacenamiento.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Para realizar operaciones libres de Lan mediante el agente de almacenamiento, especifique la opción ENABLELANFREE en el archivo de opciones, y vuelva a iniciar el proceso.

## 963 E DSM\_RC\_FS\_NAMESPACE\_DOWNLEVEL El espacio de nombres largos se ha eliminado del espacio de archivos local. Si desea continuar con la operación de copia de seguridad y archivado, renombre el espacio de archivos en el servidor.

---

### Explicación

El proceso ha detectado que el espacio de nombres del servidor es NTW:LONG, pero el volumen local no tiene soporte de nombres largos. Si desea realizar una copia de seguridad del volumen utilizando los nombres abreviados, renombre el espacio de archivos en el servidor. Si quiere hacer copia de seguridad del volumen utilizando nombres cortos, añada el soporte de espacio de nombres largos de vuelta al volumen en cuestión.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Añada el soporte de espacio de nombres largos al volumen o renombre (elimine) el espacio de archivos del servidor correspondiente.

## **0996 E DSM\_RC\_SERVER\_DOWNLEVEL\_FUNC El servidor IBM Spectrum Protect es de un nivel inferior y no soporta la función solicitada. Consulte las anotaciones de errores para la información de versión.**

---

### **Explicación**

La función que se está utilizando precisa un servidor IBM Spectrum Protect más actual.

### **Acción del Sistema**

La operación falla.

### **Respuesta del Usuario**

Actualice el servidor IBM Spectrum Protect a un nivel que admita esta función. Consulte las anotaciones de errores para la información de versión.

## **0997 E DSM\_RC\_STORAGEAGENT\_DOWNLEVEL El agente de almacenamiento de IBM Spectrum Protect es de un nivel inferior y no soporta la función solicitada. Consulte las anotaciones de errores para la información de versión.**

---

### **Explicación**

La función que se está utilizando precisa un agente de almacenamiento IBM Spectrum Protect más actual.

### **Acción del Sistema**

La operación falla.

### **Respuesta del Usuario**

Actualice el agente de almacenamiento IBM Spectrum Protect a un nivel que admita esta función. Consulte las anotaciones de errores para la información de versión.

## **0998 E DSM\_RC\_SERVER\_AND\_SA\_DOWNLEVEL El servidor de IBM Spectrum Protect y el agente de almacenamiento de IBM Spectrum Protect son de un nivel inferior y no soportan la función solicitada. Consulte las anotaciones de errores para la información de versión.**

---

### **Explicación**

La función que se está utilizando precisa un servidor IBM Spectrum Protect y de un agente de almacenamiento IBM Spectrum Protect más actual.

### **Acción del Sistema**

La operación falla.

### **Respuesta del Usuario**

Actualice el servidor IBM Spectrum Protect y el un agente de almacenamiento IBM Spectrum Protect a un nivel que admita esta función. Consulte las anotaciones de errores para la información de versión.

## **1376 E DSM\_RC\_DIGEST\_VALIDATION\_ERROR Se ha producido un error al procesar '*nombre espacio de archivosnombre-vía acceso nombre-archivos*'; ha fallado la validación de procesamiento de punto a punto.**

---

### **Explicación**

El procesamiento mediante cifrado de los datos restaurados o recuperados no coincide con el procesamiento generado durante la operación de copia de seguridad o archivado. Entre las causas posibles se encuentra el error de transmisión, la corrupción de datos o la colisión de hash.

### **Acción del Sistema**

Se detiene el proceso.

### **Respuesta del Usuario**

Intente restaurar la operación de nuevo. Si el problema persiste, póngase en contacto con el soporte técnico de IBM para obtener ayuda adicional.

## **2000 E DSM\_RC\_NULL\_OBJNAME El puntero de nombre de objeto es NULL.**

---

### **Explicación**

No se ha proporcionado ningún valor para el puntero del nombre del objeto.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Proporcione una dirección para la estructura dsmObjName.

## **2001 E DSM\_RC\_NULL\_DATA\_BLKPTR El puntero de bloque de datos es NULL.**

---

### **Explicación**

No se ha proporcionado ningún valor para el puntero del bloque de datos.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Proporcione una dirección para la estructura DataBlk.

## **2002 E DSM\_RC\_NULL\_MSG El parámetro de mensaje para dsmRCMsg es un puntero NULL.**

---

## Explicación

El parámetro del mensaje para dsmRCMsg es un puntero NULL.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Asigne espacio suficiente para el parámetro mensaje.

## 2004 E DSM\_RC\_NULL\_OBJATTRPTR El puntero de atributo de objeto es NULL.

---

## Explicación

No se ha proporcionado ningún valor para el puntero del atributo del objeto.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Proporcione una dirección para la estructura ObjAttr.

## 2006 E DSM\_RC\_NO\_SESS\_BLK No hay información de sesión con el servidor.

---

## Explicación

El servidor no responde con la información de sesión.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Compruebe el estado del servidor.

## 2007 E DSM\_RC\_NO\_POLICY\_BLK No hay información de política de servidor.

---

## Explicación

El servidor no responde con la información de la política.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Compruebe las definiciones de la política del servidor.

## **2008 E DSM\_RC\_ZERO\_BUFLEN El valor de dataBlk bufferLen es cero.**

---

### **Explicación**

El valor para dataBlk bufferLen es cero.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Proporcione un valor que no sea cero para bufferLen.

## **2009 E DSM\_RC\_NULL\_BUFPTR dataBlk bufferPtr es NULL.**

---

### **Explicación**

No se ha proporcionado ningún valor para dataBlk bufferPtr.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Proporcione una dirección para bufferPtr.

## **2010 E DSM\_RC\_INVALID\_OBJTYPE El objType no es válido.**

---

### **Explicación**

El valor para objType bufferLen no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El valor para dsmObjName.objType debe ser:

- DSM\_OBJ\_FILE o DSM\_OBJ\_DIRECTORY para copia de seguridad, o
- DSM\_OBJ\_FILE para archivado.

## **2011 E DSM\_RC\_INVALID\_VOTE El voto dsmEndTxn no es válido.**

---

### **Explicación**

El voto dsmEndTxn no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

El voto debe ser DSM\_VOTE\_COMMIT o DSM\_VOTE\_ABORT.

## **2012 E DSM\_RC\_INVALID\_ACTION La acción de actualización no es válida.**

---

### Explicación

Las acciones dsmUpdateFS o dsmUpdateObj no son válidas.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Corrija el valor de la acción. Los valores válidos se definen en dsmapi.h y se documentan en nuestro libro Using the API.

## **2014 E DSM\_RC\_INVALID\_DS\_HANDLE Ha habido un error en la estructura interna de la API de IBM Spectrum Protect.**

---

### Explicación

El sistema se encontró un error en la estructura interna de la API.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Concluya el proceso y vuelva a intentar la operación. Verifique que las llamadas anteriores dsmInit se limpiaron y terminaron por una llamada de dsmTerminate. Si el problema persiste, póngase en contacto con el administrador del sistema o el representante del servicio.

## **2015 E DSM\_RC\_INVALID\_REPOS El tipo de repositorio no es válido.**

---

### Explicación

El tipo de repositorio no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Para dsmDeleteFS el repositorio debe ser uno de los siguientes:

- DSM\_ARCHIVE\_REP
- DSM\_BACKUP\_REP
- DSM\_REPOS\_ALL.

## **2016 E DSM\_RC\_INVALID\_FSNAME El nombre de espacio de archivo debe empezar con el delimitador de directorio.**

---



## Explicación

El nombre de espacio de archivos no es válido.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

El nombre del espacio de archivos debe comenzar con el delimitador de directorio.

## **2017 E DSM\_RC\_INVALID\_OBJNAME El nombre de objeto es una serie vacía o no tiene delimitador inicial.**

---

## Explicación

El nombre de objeto no es válido debido a una serie vacía o a que no tiene un delimitador destacado.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Verifique el formato de la vía de acceso completa de dsmObjName.

## **2018 E DSM\_RC\_INVALID\_LLNAME Rl calificador de bajo nivel del nombre de objeto debe empezar con el delimitador de directorio.**

---

## Explicación

El calificador de nivel inferior para el nombre de objeto no es válido.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Inicie el calificador de nivel inferior del nombre de objeto con el delimitador de directorio.

## **2019 E DSM\_RC\_INVALID\_OBJOWNER El propietario de objeto no es válido.**

---

## Explicación

El propietario de objeto debe ser el usuario root, o debe ser el mismo que el propietario de sección.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Verifique el propietario de sesión y el propietario de objeto.

## **2020 E DSM\_RC\_INVALID\_ACTYPE dsmBindMC sendType no es válido.**

---

### **Explicación**

dsmBindMC sendType no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

sendType debe ser uno de los siguientes:

- stBackup
- stArchive
- stBackupMountWait
- stArchiveMountWait

## **2021 E DSM\_RC\_INVALID\_RETCODE No hay texto disponible para este código de retorno.**

---

### **Explicación**

El parámetro dsmRC para dsmRCMsg no es un código de retorno admitido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Especifique un valor válido.

## **2022 E DSM\_RC\_INVALID\_SENDTYPE dsmSendObj sendType no es válido.**

---

### **Explicación**

dsmSendObj sendType no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

sendType debe ser uno de los siguientes:

- stBackup
- stArchive
- stBackupMountWait
- stArchiveMountWait

## 2023 E DSM\_RC\_INVALID\_PARAMETER dsmDeleteObj delType no es válido.

---

### Explicación

dsmDeleteObj delType no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

delType debe ser dtBackup o dtArchive.

## 2024 E DSM\_RC\_INVALID\_OBJSTATE La consulta Backup objState no es válida.

---

### Explicación

La consulta Backup objState no es válida.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

qryBackupData debe ser uno de los siguientes:

- DSM\_ACTIVE
- DSM\_INACTIVE
- DSM\_ANY\_MATCH

## 2025 E DSM\_RC\_INVALID\_MCNAME No se ha encontrado el nombre de clase de gestión.

---

### Explicación

La consulta u operación de envío no pueden encontrar el nombre de la clase de gestión.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique el nombre de la clase de gestión.

## 2026 E DSM\_RC\_INVALID\_DRIVE\_CHAR La letra de unidad no es un carácter alfabético.

---

### Explicación

La letra de unidad no es un carácter alfabético. Este código de retorno es válido sólo en Microsoft Windows.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique que la designación de unidad es un carácter alfabético. El campo indicado es `dsmDosFSAttrib.driveLetter`.

## **2027 E DSM\_RC\_NULL\_FSNAME El nombre de espacio de archivo de registro es NULL.**

---

### **Explicación**

No se ha proporcionado ningún valor para el nombre de espacio de archivos del registro.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Proporcione un nombre de espacio de archivos en `dsmRegisterFS`.

## **2028 E DSM\_RC\_INVALID\_HLNAME El calificador de alto nivel del nombre de objeto debe empezar con el delimitador de directorio.**

---

### **Explicación**

El calificador de nivel superior para el nombre de objeto no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El calificador de nivel superior del nombre de objeto debe comenzar con el delimitador de directorio.

## **2029 E DSM\_RC\_NUMOBJ\_EXCEED El número de objetos en dsmBeginGetData supera DSM\_MAX\_GET\_OBJ | DSM\_MAX\_PARTIAL\_GET\_OBJ.**

---

### **Explicación**

El número de objetos (`numObjId`) especificado en la llamada `dsmBeginGetData` supera `DSM_MAX_GET_OBJ` | `DSM_MAX_PARTIAL_GET_OBJ`.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Compruebe el número de objetos antes de llamar a dsmBeginGetData. Si es mayor de DSM\_MAX\_GET\_OBJ | DSM\_MAX\_PARTIAL\_GET\_OBJ, emita múltiples secuencias de llamada Get.

## 2030 E DSM\_RC\_NEWPW\_REQD El nuevo valor de contraseña es NULL o está en blanco.

---

### Explicación

No se ha proporcionado ningún valor para la nueva contraseña.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Proporcione una contraseña nueva en dsmChangePW.

## 2031 E DSM\_RC\_OLDPW\_REQD El valor anterior de contraseña es NULL o está en blanco.

---

### Explicación

No se ha proporcionado ningún valor para la contraseña antigua.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Proporcione una contraseña antigua en dsmChangePW.

## 2032 E DSM\_RC\_NO\_OWNER\_REQD En dsmInit, no se permite establecer sesión al propietario cuando PASSWORDACCESS=generate.

---

### Explicación

PASSWORDACCESS=GENERATE establece una sesión con el usuario con el que se ha iniciado sesión actualmente como propietario. La aplicación debe configurar clientOwnerNameP en NULL cuando PASSWORDACCESS=GENERATE está en vigor.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada. Si la aplicación puede continuar procesando depende de cómo maneje la aplicación el error.

### Respuesta del Usuario

Este mensaje se aplica a las aplicaciones que utilizan la API de IBM Spectrum Protect y está principalmente destinado al proveedor de la aplicación para la que se ha emitido el mensaje. Dependiendo de la aplicación, podría ser un tema de configuración.

Consulte la documentación para la aplicación y verifique que la aplicación está configurada correctamente. Si el problema persiste, póngase en contacto con el proveedor de la aplicación para obtener más ayuda.

## 2033 E DSM\_RC\_NO\_NODE\_REQD En dsmInit, el nodo no está permitido si PASSWORDACCESS=generate.

---

### Explicación

PASSWORDACCESS=generate establece una sesión con el nombre de host como nodo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Cuando utilice PASSWORDACCESS=generate, establezca clientnodeNameP en NULL.

## 2034 E DSM\_RC\_KEY\_MISSING Falta el archivo de claves.

---

### Explicación

No se encuentra el archivo de claves de Data Protection for Oracle.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Asegúrese de que ha solicitado Data Protection for Oracle e instale el archivo de claves.

## 2035 E DSM\_RC\_KEY\_BAD El contenido del archivo de claves no es válido.

---

### Explicación

El contenido del archivo de claves de Data Protection for Oracle no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Asegúrese de que ha solicitado Data Protection for Oracle e instale el archivo de claves.

## 2041 E DSM\_RC\_BAD\_CALL\_SEQUENCE La secuencia de llamadas no es válida.

---

### Explicación

La API requiere que se hagan llamadas a función en una secuencia específica. Las llamadas a función no se han hecho en la secuencia esperada. El error lo pueden desencadenar los siguientes problemas:

- Un error en la red.
- Un error en la API de IBM Spectrum Protect.
- Un error en el servidor de IBM Spectrum Protect.
- Un error en la aplicación (IBM o tercero) que utiliza la API de IBM Spectrum Protect.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Los usuarios finales pueden responder de las siguientes maneras:

- Compruebe si hay errores en la red.
- Busque indicios en el archivo de registro de actividad de servidor de IBM Spectrum Protect, en el archivo de registro dserror.log de lado del cliente y en los archivos de registro específicos de la aplicación con problemas.
- Busque APAR que coincidan con el problema en las páginas de soporte de IBM. El sitio de soporte está en Portal de soporte de IBM Spectrum Protect
- Si la aplicación de API la han desarrollado terceros (no IBM), busque problemas conocidos que coincidan con el problema en las páginas de soporte de estos terceros.

Si ninguna de las acciones anteriores resuelve el problema, informe del problema al proveedor de la aplicación que utiliza la API de IBM Spectrum Protect.

Un desarrollador de una aplicación que utiliza la API de IBM Spectrum Protect debe investigar la causa del problema, incluida la revisión del diagrama de estado de la API de IBM Spectrum Protect. El diagrama de estado de la API de IBM Spectrum Protect se encuentra en la documentación de producto en Documentación del producto IBM Spectrum Protect

## **2042 E DSM\_RC\_INVALID\_TSMBUFFER tsmBuffHandle no es válido o el valor de dataPtr no es válido.**

---

### Explicación

Se ha especificado un valor no válido para un descriptor de contexto o dataPtr en la API.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Hay un problema con la aplicación de la llamada. Verifique los valores de tsmBuffHandle y dataptr pasados a la API.

## **2043 E DSM\_RC\_TOO\_MANY\_BYTES El número de bytes copiados en tsmBuffer es mayor que el valor permitido.**

---

### Explicación

Se ha copiado un número de bytes no válido a tsmBuffer.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Hay un problema con la aplicación de la llamada. Verifique el número de bytes copiados en tsmBuffer.

## **2044 E DSM\_RC\_MUST\_RELEASE\_BUFFER dsmTerminate no puede finalizar debido a que la aplicación se mantiene en uno o más tsmBuffers.**

---

## Explicación

Una aplicación está intentando finalizar la sesión, pero aún mantiene algunos tsmBuffers.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

La aplicación debe devolver todos los búferes para esta sesión llamando a tsmReleaseBuffer, y a continuación, emite dsmTerminate.

## **2045 E DSM\_RC\_BUFF\_ARRAY\_ERROR Se ha producido un error interno en la matriz de tsmBuffer.**

---

### Explicación

Se ha producido un error interno en la matriz del almacenamiento intermedio de la API.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador del sistema o el representante del servicio.

## **2046 E DSM\_RC\_INVALID\_DATA\_BLK Al utilizar useTsmBuffers, dataBlk debe ser NULL en las llamadas a dsmSendObj y dsmGetObj.**

---

### Explicación

El valor para dataBlk debe ser NULL cuando utiliza useTsmBuffers.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Hay un problema con la aplicación de la llamada. Póngase en contacto con el proveedor.

## **2047 E DSM\_RC\_ENCR\_NOT\_ALLOWED No se permite el cifrado al utilizar useTsmBuffers.**

---

### Explicación

useTsmBuffers no admite el cifrado.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.



## Respuesta del Usuario

Intente la operación de nuevo, sin utilizar useTsmBuffers, o inhabilite el cifrado para esta operación.

## **2048 E DSM\_RC\_OBJ\_COMPRESSED Este objeto no se puede restaurar/recuperar mediante useTsmBuffers porque está comprimido.**

---

### Explicación

useTsmBuffers no admite la compresión.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Intente la operación de nuevo, sin utilizar useTsmBuffers.

## **2049 E DSM\_RC\_OBJ\_ENCRYPTED Este objeto no se puede restaurar/recuperar mediante useTsmBuffers porque está cifrado.**

---

### Explicación

useTsmBuffers no admite el cifrado.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Intente la operación de nuevo, sin utilizar useTsmBuffers.

## **2050 E DSM\_RC\_WILDCHAR\_NOTALLOWED En dsmSendObj, no se permiten caracteres comodín para objName.**

---

### Explicación

En dsmSendObj, no están permitidos los caracteres comodín para objName.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Proporcione un fs, hl, y ll en el dsmObjName.

## **2051 E DSM\_RC\_POR\_NOT\_ALLOWED Al utilizar useTsmBuffers, no se permite una restauración/recuperación con restauración de objetos parcial.**

---

### Explicación

useTsmBuffers no admite la restauración parcial de objetos.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Asegúrese de que la aplicación de llamada está utilizando la restauración parcial de objeto o useTsmBuffers.

**2052 E DSM\_RC\_NO\_ENCRYPTION\_KEY No se ha encontrado ninguna clave de cifrado. Si está utilizando -encryptkey=prompt asegúrese de que hay un valor en el campo encryptionPasswordP y que bEncryptKeyEnabled está establecido en verdadero.**

---

### **Explicación**

No se ha encontrado clave de cifrado en el archivo de contraseñas, o la aplicación no ha proporcionado clave.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Si está utilizando -encryptkey=prompt asegúrese de que hay un valor en el campo encryptionPasswordP y que bEncryptKeyEnabled está establecido en verdadero.

**2053 E DSM\_RC\_ENCR\_CONFLICT Se han especificado opciones de clave de cifrado conflictivas.**

---

### **Explicación**

Al utilizar la opción ENABLEENCRYPTKEY, el parámetro bEncryptKeyEnabled para las estructuras dsmInitExIn\_t y tsmInitExIn\_t de la API de IBM Spectrum Protect no se puede establecer en bTrue.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Elimine la opción ENABLEENCRYPTKEY del archivo de opciones o establezca el parámetro bEncryptKeyEnabled en bFalse en el programa utilizando la API de IBM Spectrum Protect.

**2060 E DSM\_RC\_FSNAME\_NOTFOUND No se puede encontrar el espacio de archivos para suprimir/establecer el acceso.**

---

### **Explicación**

No se puede eliminar el espacio de archivos.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique el nombre del espacio de archivos.

## **2061 E DSM\_RC\_FS\_NOT\_REGISTERED En dsmSendObj, dsmDeleteObj o dsmUpdateFS, el espacio de archivos no se ha registrado.**

---

### **Explicación**

En dsmSendObj, dsmDeleteObj, o dsmUpdateFS no está registrado el espacio de archivos.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique el nombre del espacio de archivos.

## **2062 W DSM\_RC\_FS\_ALREADY\_REGED en dsmRegisterFS el espacio de archivos ya se ha registrado.**

---

### **Explicación**

Ya se ha registrado el espacio de archivos en dsmRegisterFS.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique el nombre del espacio de archivos.

## **2063 E DSM\_RC\_OBJID\_NOTFOUND En dsmBeginGetData, el objID es NULL.**

---

### **Explicación**

En dsmBeginGetData, el objID es NULL.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Verifique lo siguiente:

- El dsmGetList no es NULL.
- Todos los objID no son NULL.
- El dsmGetList numObjId es no cero.

## 2064 E DSM\_RC\_WRONG\_VERSION En dsmInit, la versión de la API del emisor de la llamada es distinta de la versión de la biblioteca de IBM Spectrum Protect.

---

### Explicación

En dsmInit, la versión de API del emisor de la llamada es distinta de la versión de biblioteca de IBM Spectrum Protect.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Instale la última biblioteca de API de IBM Spectrum Protect.

## 2065 E DSM\_RC\_WRONG\_VERSION\_PARM La versión de estructura del interlocutor es diferente de la versión de biblioteca de IBM Spectrum Protect.

---

### Explicación

La versión de estructura del interlocutor es distinta de la versión de la biblioteca de IBM Spectrum Protect.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Asegúrese de que el campo stVersion tiene establecido el valor en el archivo de cabecera. Recompile al aplicación con los últimos archivos de cabecera.

## 2070 E DSM\_RC\_NEEDTO\_ENDTXN Emita dsmEndTxn y, a continuación, empiece una sesión de transacción nueva.

---

### Explicación

Esta transacción debe terminar y debe iniciarse una nueva por una de las siguientes razones:

- El destino ha cambiado.
- Se ha excedido el límite de bytes
- Se ha superado el número máximo de objetos.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Emita dsmEndTxn e inicie una nueva sesión de transacción.

## 2080 E DSM\_RC\_OBJ\_EXCLUDED El objeto de archivado o copia de seguridad se excluye del proceso.

---

### Explicación

El objeto de copia de seguridad o archivado se ha excluido del proceso.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique las listas objName y Exclude.

## 2081 E DSM\_RC\_OBJ\_NOBCG El objeto de copia de seguridad no tiene un grupo de copias.

---

### Explicación

El objeto de copia de seguridad no tiene un grupo de copias.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Compruebe las definiciones de la política del servidor.

## 2082 E DSM\_RC\_OBJ\_NOACG El objeto de archivado no tiene un grupo de copias.

---

### Explicación

El objeto de archivado no tiene un grupo de copias.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Compruebe las definiciones de la política del servidor.

## 2090 E DSM\_RC\_APISYSTEM\_ERROR La memoria utilizada por la API de IBM Spectrum Protect se ha dañado.

---

### Explicación

Se ha dañado la memoria utilizada por la API de IBM Spectrum Protect API.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador del sistema o el representante del servicio.

## **2100 E DSM\_RC\_DESC\_TOOLONG La descripción de archivado de sendObj es demasiado larga.**

---

### **Explicación**

La descripción sendObj Archive es demasiado larga.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

La serie sndArchiveData.descr debe ser menor o igual que DSM\_MAX\_DESCR\_LENGTH.

## **2101 E DSM\_RC\_OBJINFO\_TOOLONG sendObj ObjAttr.objInfo es demasiado largo.**

---

### **Explicación**

sendObj ObjAttr.objInfo es demasiado largo.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El campo objInfo debe ser menor o igual que DSM\_MAX\_OBJINFO\_LENGTH.

## **2102 E DSM\_RC\_HL\_TOOLONG The sendObj dsmObjName.hl es demasiado largo.**

---

### **Explicación**

sendObj dsmObjName.hl es demasiado largo.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El campo hl debe ser menor o igual que DSM\_MAX\_HL\_LENGTH.

## 2103 E DSM\_RC\_PASSWD\_TOOLONG La contraseña o la serie encryptionPassword proporcionada es demasiado larga.

---

### Explicación

El valor proporcionado para la contraseña o encryptionPassword es demasiado largo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

La contraseña o el campo encryptionPassword debe ser menor que DSM\_MAX\_VERIFIER\_LENGTH.

## 2104 E DSM\_RC\_FILESPACE\_TOOLONG sendObj dsmObjName.fs es demasiado largo.

---

### Explicación

sendObj dsmObjName.fs es demasiado largo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

El campo fs debe ser menor o igual que DSM\_MAX\_FS\_LENGTH.

## 2105 E DSM\_RC\_LL\_TOOLONG sendObj dsmObjName.ll es demasiado largo.

---

### Explicación

sendObj dsmObjName.ll es demasiado largo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

El campo ll debe ser menor o igual que DSM\_MAX\_LL\_LENGTH.

## 2106 E DSM\_RC\_FSINFO\_TOOLONG en RegisterFS o UpdateFS el fsInfo de fsAttr es demasiado largo.

---

### Explicación

En RegisterFS o UpdateFS el fsInfo de fsAttr es demasiado largo.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El campo fsInfo debe ser menor o igual que DSM\_MAX\_FSINFO\_LENGTH.

## **2107 E DSM\_RC\_SENDDATA\_WITH\_ZERO\_SIZE No se pueden enviar datos con un sizeEstimate de byte cero.**

---

### **Explicación**

No puede enviar datos para un objeto con tamaño estimado = 0.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

Establezca la estimación de tamaño mayor que 0 en dsmSendObj.

## **2110 E DSM\_RC\_INVALID\_ACCESS\_TYPE El tipo de acceso dsmSetAccess no es válido.**

---

### **Explicación**

El accessType dsmSetAccess no es válido.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El accessType debe ser uno de los siguientes:

- atBackup
- atArchive

## **2111 E DSM\_RC\_QUERY\_COMM\_FAILURE Error de comunicaciones con el servidor durante la consulta de objeto**

---

### **Explicación**

Se ha producido un error de comunicaciones inesperado durante una consulta de objeto al servidor.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Verifique que esas comunicaciones son activas entre las máquinas del cliente y del servidor. Las paradas del servidor, del procesador, y del controlador de comunicaciones puede provocar este error.



## **2112 E DSM\_RC\_NO\_FILES\_BACKUP No se ha realizado anteriormente ninguna copia de seguridad de los archivos para este nombre de archivo/espacio de archivo.**

---

### **Explicación**

Intentó establecer acceso a los archivos cuando no se había hecho copia de seguridad previamente de los archivos para el nombre de archivo especificado, unidad o sistema de archivos.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que se ha especificado la unidad o el sistema de archivos correcto y que se ha hecho copia de seguridad de esos archivos para que pueda establecer el acceso.

## **2113 E DSM\_RC\_NO\_FILES\_ARCHIVE No se han archivado anteriormente ningún archivo para este nombre de archivo/espacio de archivo.**

---

### **Explicación**

Intentó establecer acceso en los archivos cuando no habían archivado previamente los archivos para el nombre de archivo especificado, unidad o sistema de archivos.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que se ha especificado la unidad o el sistema de archivos correcto y que se han archivado esos archivos para que pueda establecer el acceso.

## **2114 E DSM\_RC\_INVALID\_SETACCESS Formato no válido para el mandato Set Access.**

---

### **Explicación**

El mandato SET ACCESS debe tener al menos tres operandos, el primero de los cuales debe ser BACKUP o ARCHIVE. Debe seguirle una especificación de archivo con un formato correcto.

### **Acción del Sistema**

Se ha detenido el proceso, el mandato no se ejecuta.

### **Respuesta del Usuario**

Utilice el mandato HELP SET ACCESS para obtener los detalles de uso completos y, posteriormente, escriba el mandato SET ACCESS utilizando la sintaxis correcta.

## 2120 E DSM\_RC\_STRING\_TOO\_LONG El mensaje siguiente era demasiado largo para anotarlo en el servidor: '*mensaje abreviado con número de mensaje*'

---

### Explicación

El texto y las inserciones del mensaje son demasiado largas para enviarlas al servidor en el búfer interno disponible.

### Acción del Sistema

El mensaje *número mensaje* se ha grabado en las anotaciones de errores del cliente local, pero no se ha enviado al servidor como parte de este mensaje. Se ha reducido la longitud del mensaje sustituyendo '...' en mitad del mensaje original.

### Respuesta del Usuario

El mensaje mencionado se ha abreviado pero describe el error que se ha producido. Consulte la documentación correspondiente a dicho mensaje para obtener más información.

## 2200 I DSM\_RC\_MORE\_DATA En dsmGetNextQObj o dsmGetData hay más datos disponibles.

---

### Explicación

En dsmGetNextQObj o dsmGetData hay más datos disponibles.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Llame a la función de nuevo.

## 2210 E DSM\_RC\_BUFF\_TOO\_SMALL El almacenamiento intermedio dataBlk es demasiado pequeño para la respuesta de consulta.

---

### Explicación

El almacenamiento intermedio dataBlk es demasiado pequeño para la respuesta de consulta.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

En dsmGetNextQObj asegúrese de que el almacenamiento intermedio dataBlk es al menos tan grande como la estructura de respuesta de consulta.

## 2228 E DSM\_RC\_NO\_API\_CONFIGFILE No se puede abrir el archivo de configuración especificado en dsmInit.

---

## Explicación

El archivo de configuración especificado en dsmInit no se puede abrir.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Verifique el nombre de archivo.

## **2229 E DSM\_RC\_NO\_INCLEXCL\_FILE No se ha encontrado el archivo de definición Include/Exclude.**

---

### Explicación

No se ha encontrado el archivo de definición Inclusión/Exclusión.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Verifique el nombre de archivo en la opción Inclexcl.

## **2230 E DSM\_RC\_NO\_SYS\_OR\_INCLEXCL El archivo dsm.sys no se ha encontrado o el archivo Inclexcl especificado en dsm.sys no se ha encontrado.**

---

### Explicación

No se han encontrado el archivo dsm.sys, o el archivo Inclexcl especificado en dsm.sys.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

El archivo dsm.sys debe estar en el directorio indicado por la variable de entorno DSMI\_DIR. Verifique el nombre de archivo en la opción Inclexcl en el archivo dsm.sys.

## **2231 E DSM\_RC\_REJECT\_NO\_POR\_SUPPORT No se soporta la recuperación de objetos parcial en este servidor.**

---

### Explicación

El servidor IBM Spectrum Protect especificado por el usuario no admite la recuperación parcial del objeto.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Especifique un servidor IBM Spectrum Protect que admita la función de recuperación parcial del objeto.

## 2300 E DSM\_RC\_NEED\_ROOT Solo un usuario root de UNIX puede ejecutar dsmChangePW o dsmDeleteFS.

---

### Explicación

Sólo un usuario root de UNIX puede ejecutar dsmChangePW o dsmDeleteFS.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Ejecute este programa como usuario root.

## 2301 E DSM\_RC\_NEEDTO\_CALL\_BINDMC Debe emitir dsmBindMC antes que dsmSendObj.

---

### Explicación

Debe emitir dsmBindMC antes de dsmSendObj.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Modifique el programa.

## 2302 I DSM\_RC\_CHECK\_REASON\_CODE El voto de dsmEndTxn es ABORT, de modo que compruebe el campo de razón.

---

### Explicación

Después de una llamada dsmEndTxn, la transacción es anulada por el servidor o cliente con un DSM\_VOTE\_ABORT y se devuelve la razón.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Compruebe el campo de razón para el código que explica porque se ha cancelado la transacción.

## 2400 E DSM\_RC\_ALMGR\_OPEN\_FAIL No se ha podido abrir el archivo de licencia.

---

## Explicación

No se ha encontrado el archivo de licencia, o puede que no se abra debido a los permisos o a que el archivo esté dañado.

## Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

## Respuesta del Usuario

Compruebe los permisos en el archivo. Verifique si el archivo de licencias está en el lugar correcto.

## 2401 E DSM\_RC\_ALMGR\_READ\_FAIL Anomalía de lectura en el archivo de licencia.

---

### Explicación

No se ha encontrado el archivo de licencias, o puede que no se abra debido a los permisos o a que el archivo esté dañado.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Compruebe los permisos en el archivo. Verifique si el archivo de licencias está en el lugar correcto.

## 2402 E DSM\_RC\_ALMGR\_WRITE\_FAIL Anomalía de escritura en el archivo de licencia.

---

### Explicación

No se ha encontrado el archivo de licencia, o puede que no se abra debido a los permisos o a que el archivo esté dañado.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

Compruebe los permisos en el archivo. Consulte si el archivo de licencia está en el lugar correcto.

## 2403 E DSM\_RC\_\_ALMGR\_DATA\_FMT Los datos del archivo de licencia no están en un formato válido.

---

### Explicación

El archivo de licencia no es válido.

### Acción del Sistema

El sistema regresa al procedimiento que realiza la llamada.

### Respuesta del Usuario

El usuario tiene que obtener una licencia nueva.

## **2404 E DSM\_RC\_ALMGR\_CKSUM\_BAD La suma de comprobación del archivo de licencia no coincide con la serie del registro de licencia.**

---

### **Explicación**

La cadena de registro no es válida.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El usuario tiene que obtener una licencia nueva.

## **2405 E DSM\_RC\_ALMGR\_TRIAL\_EXPRD Esta licencia de prueba ha caducado.**

---

### **Explicación**

La cadena de registro no es válida.

### **Acción del Sistema**

El sistema regresa al procedimiento que realiza la llamada.

### **Respuesta del Usuario**

El usuario tiene que obtener una licencia nueva.

## **4580 E DSM\_RC\_ENC\_WRONG\_KEY Error al procesar '*nombre de espacio de archivosnombre de rutanombre de archivo*'; clave de cifrado no válida**

---

### **Explicación**

La clave especificada no coincide con la clave que se utilizó para cifrar el archivo durante la copia de seguridad. No se puede restaurar el archivo a menos que se especifique la clave que coincide.

### **Acción del Sistema**

el proceso se detiene.

### **Respuesta del Usuario**

Intente de nuevo la operación de restauración y proporcione la clave correcta.

## **4582 E DSM\_RC\_ENC\_NOT\_AUTHORIZED El usuario no está autorizado para cifrar *archivo-nombre de espaciodirectorio\_rutanombre\_archivo*.**

---

### **Explicación**

El usuario no está autorizado a cifrar el archivo. Generalmente, sólo un usuario autorizado de IBM Spectrum Protect o un usuario root puede utilizar el cifrado de IBM Spectrum Protect. Sin embargo, una cierta combinación de opciones PASSWORDACCESS y ENCRYPTKEY permite operaciones de cifrado por parte de un usuario no autorizado.

### Acción del Sistema

No se ha hecho copia de seguridad ni se ha restaurado el archivo.

### Respuesta del Usuario

Inicie la sesión como root o usuario autorizado de IBM Spectrum Protect y vuelva a intentar la operación. Consulte la publicación IBM Spectrum Protect Backup-Archive Client Installation and User's Guide para obtener la utilización correcta de la opción ENCRYPTKEY.

## **4584 E DSM\_RC\_ENC\_TYPE\_UNKOWN Error al procesar '*nombre de espacio de archivos nombre de ruta nombre de archivo*': tipo de cifrado no admitido.**

---

### Explicación

Se ha hecho una copia de seguridad o un archivado de los archivos que está intentando restaurar o recuperar, mediante una versión posterior del cliente de IBM Spectrum Protect. El método de cifrado de archivo no está admitido por el cliente actual.

### Acción del Sistema

El objeto omite.

### Respuesta del Usuario

Restaurar o recuperar el archivo con la versión más reciente del cliente de IBM Spectrum Protect.

## **4600 E DSM\_RC\_CLUSTER\_INFO\_LIBRARY\_NOT\_LOADED CLUSTERNODE se ha establecido en YES pero el daemon de información de clúster no se ha iniciado.**

---

### Explicación

El daemon de información de clúster de HACMP debe iniciarse para especificar la opción CLUSTERNODE.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Inicie el daemon de información de clúster de HACMP.

## **4601 E DSM\_RC\_CLUSTER\_LIBRARY\_INVALID CLUSTERNODE está establecido en YES pero la biblioteca de carga de clúster no es válida.**

---

### Explicación

La biblioteca de carga que proporciona el sistema operativo para obtener el nombre de clúster no es válido. Una causa posible es una biblioteca de carga desfasada que no contiene las rutinas adecuadas que espera este producto.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Asegúrese de que está instalado el último software de clúster en el sistema.

## **4602 E DSM\_RC\_CLUSTER\_LIBRARY\_NOT\_LOADED CLUSTERNODE se ha establecido en YES pero el software de clúster no está disponible en este sistema.**

---

### Explicación

La biblioteca de carga que proporciona el sistema operativo para obtener el nombre de clúster no está disponible en este sistema.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Asegúrese de que está instalado el software de clúster en el sistema.

## **4603 E DSM\_RC\_CLUSTER\_NOT\_MEMBER\_OF\_CLUSTER CLUSTERNODE se ha establecido en YES pero esta máquina no es miembro de un clúster.**

---

### Explicación

Esta máquina no es miembro de un nodo de clúster. Las posibles causas son que el servicio de clúster no se ha configurado de una forma correcta, o que el clúster está en proceso de inicialización.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario

Asegúrese de que el software de clúster está configurado adecuadamente. Si el clúster está en proceso de inicialización, vuelva a intentar la operación más tarde.

## **4604 E DSM\_RC\_CLUSTER\_NOT\_ENABLED CLUSTERNODE está establecido en YES pero el servicio de clúster no está habilitado en este sistema.**

---

### Explicación

No se ha activado el servicio de clúster en este sistema.

### Acción del Sistema

El proceso finaliza.

### Respuesta del Usuario



Active el servicio de clúster en el sistema.

## **4605 E DSM\_RC\_CLUSTER\_NOT\_SUPPORTED No se admite la opción CLUSTERNODE en este sistema.**

---

### **Explicación**

Esta opción no está admitida en este sistema.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Inhabilite la opción CLUSTERNODE en el archivo de opciones local.

## **4606 E DSM\_RC\_CLUSTER\_UNKNOWN\_ERROR Se ha producido un error inesperado (*código\_ret*) mientras el programa intentaba obtener el nombre de clúster del sistema.**

---

### **Explicación**

Se ha producido un error desconocido mientras el programa estaba intentando obtener el nombre de clúster desde el servicio de clústeres. El código de error es el código de razón proporcionado directamente desde el servicio de clústeres utilizado en este entorno de sistema operativo.

### **Acción del Sistema**

El proceso finaliza.

### **Respuesta del Usuario**

Consulte la documentación para el software de clústeres para obtener una explicación del código de razón. Asegúrese de que su servicio de clústeres está operativo, después intente de nuevo la operación de IBM Spectrum Protect .

## **5200 E DSM\_RC\_ABORT\_CERTIFICATE\_NOT\_FOUND NOT\_FOUND El nodo remoto no está correctamente configurado en el servidor de IBM Spectrum Protect.**

---

### **Explicación**

El nodo remoto no está correctamente configurado en el servidor de IBM Spectrum Protect.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Asegúrese de que el nodo remoto esté correctamente configurado y conectado al servidor de IBM Spectrum Protect utilizando TLS. Esto valida la configuración del nodo remoto y garantiza que la información relacionada con el nodo remoto se envía al servidor.

## **5702 E DSM\_RC\_PROXY\_REJECT\_NO\_RESOURCES Proxy rechazado: El servidor de IBM Spectrum Protect se ha quedado sin memoria.**

---

### **Explicación**

No hay suficiente memoria disponible para permitir que esta operación continúe.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Vuelva a intentar la operación. Si el problema persiste, póngase en contacto con el administrador del sistema para aumentar la cantidad de memoria del servidor.

## **5705 E DSM\_RC\_PROXY\_REJECT\_DUPLICATE\_ID Proxy rechazado: las opciones ASNODENAME y NODENAME tienen el mismo valor.**

---

### **Explicación**

Las opciones ASNODENAME y NODENAME no pueden tener el mismo valor.

### **Acción del Sistema**

Se ha cancelado la operación actual.

### **Respuesta del Usuario**

Utilice la opción ASNODENAME sólo para acceder a otro nodo. No es necesario establecer la opción ASNODENAME para acceder a su propio nodo. Elimine la opción ASNODENAME del archivo de opciones, a menos que esté intentando acceder a un nodo al que ha otorgado autoridad para acceder con el mandato administrativo "Grant Proxynode".

## **5710 E DSM\_RC\_PROXY\_REJECT\_ID\_IN\_USE Se ha rechazado el proxy: El nombre de nodo especificado en la opción ASNODENAME está bloqueado.**

---

### **Explicación**

El administrador de IBM Spectrum Protect ha bloqueado el nodo que ha especificado como opción ASNODENAME.

### **Acción del Sistema**

La operación de IBM Spectrum Protect finaliza.

### **Respuesta del Usuario**

El administrador del servidor de IBM Spectrum Protect tiene que desbloquear el nodo antes de que pueda acceder a él. Intente la operación más tarde, o compruébelo con el administrador de IBM Spectrum Protect.

## **5717 E DSM\_RC\_PROXY\_REJECT\_INTERNAL\_ERROR Se ha rechazado el proxy: Se ha producido un error interno en el servidor.**

---

### **Explicación**

El cliente no puede utilizarse como proxy en el nodo especificado por la opción ASNODENAME debido a un error de servidor interno.

### **Acción del Sistema**

La operación actual se ha cancelado.

### **Respuesta del Usuario**

Consulte al administrador del sistema inmediatamente.

## **5722 E DSM\_RC\_PROXY\_REJECT\_NOT\_AUTHORIZED Se ha rechazado el proxy: No se ha otorgado autorización de proxy a este nodo.**

---

### **Explicación**

No se ha otorgado la autorización de proxy a este nodo para acceder al nodo al que da nombre la opción ASNODENAME. El administrador de IBM Spectrum Protect tiene que otorgar la autorización de proxy primero.

### **Acción del Sistema**

La operación de IBM Spectrum Protect finaliza.

### **Respuesta del Usuario**

El administrador del servidor de IBM Spectrum Protect tiene que otorgar la autorización de proxy para este nodo. Consulte el mandato del administrador para "Otorgar el nodo proxy".

## **5746 E DSM\_RC\_PROXY\_INVALID\_FROMNODE La opción ASNODENAME no es válida con la opción FROMNODE.**

---

### **Explicación**

Ninguna.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Elimine la opción ASNODENAME del archivo de opciones o no utilice la opción FROMNODE.

## **5748 E DSM\_RC\_PROXY\_INVALID\_CLUSTER No se puede utilizar la opción ASNODENAME con la opción CLUSTERNODE.**

---

### **Explicación**

Ninguna.

### **Acción del Sistema**

El proceso se ha detenido.

### **Respuesta del Usuario**

Elimine la opción ASNODENAME y vuelva a intentar la operación.

## 5749 E DSM\_RC\_PROXY\_INVALID\_FUNCTION No se puede invocar la operación que se está intentando con la opción ASNODENAME.

---

### Explicación

Ninguna.

### Acción del Sistema

El proceso se ha detenido.

### Respuesta del Usuario

Elimine la opción ASNODENAME y vuelva a intentar la operación.

## 5801 E DSM\_RC\_CRYPTIC\_ERROR Error inesperado en la biblioteca de cifrado.

---

### Explicación

Había un error inesperado en la biblioteca de cifrado. Consulte el registro cronológico de errores para obtener información más detallada.

### Acción del Sistema

el proceso se detiene.

### Respuesta del Usuario

Compruebe las anotaciones de errores para ANS1467E para determinar la causa del fallo. Verifique que el cliente de IBM Spectrum Protect está instalado adecuadamente. Si es necesario, vuelva a instalar el cliente y/o la API. Si el problema aún persiste, póngase en contacto con el soporte técnico de IBM Spectrum Protect .

## Descripciones de los códigos de E/S en mensajes del servidor

---

Los mensajes de IBM Spectrum Protect pueden contener códigos de entrada/salida (E/S). Los códigos pueden ser códigos de operación, códigos de terminación, códigos de detección adicionales (ASC) y códigos de cualificador de código de detección adicionales (ASCQ).

El servidor de IBM Spectrum Protect proporciona descripciones de códigos para los mensajes de error de E/S para todos los sistemas operativos compatibles.

### Código

#### Descripción

OP

La operación de E/S que falló. Estos valores se pueden visualizar:

- LECTURA
- GRABACIÓN
- FSR (registro de espaciado hacia delante)
- RSR (registro de espacio inverso)
- FSF (archivo de espaciado hacia delante)
- RSF (archivo de espacio inverso)
- WEOF (escribir marca final de archivo)
- OFFL (retroceder y descargar la cinta)
- FLUSH (vaciado)
- GET\_MEDIUM\_INFO (obtener información del medio)

- LOCATE (localización)
- QRYLBP (protección de bloqueo lógico de consulta)
- RDBLKID (ID de bloque de lectura)
- SETLBP (establecer protección de bloque lógico)
- SETMODE (establecer modo)
- REW (retroceder)
- SPACEEOD (espacio de fin de datos)
- TESTREADY (unidad de prueba lista)

#### CC

Código de terminación de E/S. El controlador de dispositivo devuelve este valor al servidor cuando se produce un error. Para obtener una lista de códigos de terminación, consulte Visión general de los valores de los códigos de terminación y de operación. Para obtener información acerca de las llamadas al sistema de la biblioteca de cintas y las descripciones de errores de las solicitudes de control de E/S de la biblioteca, consulte la Nota técnica S7002972.

#### CLAVE

Byte 2 de los bytes de detección a partir del error. Las listas siguientes muestran algunas definiciones:

- 0 = no hay bytes de detección adicionales disponibles
- 1 = error recuperado
- 2 = no preparado
- 3 = error medio
- 4 = error de hardware
- 5 = solicitud incorrecta
- 6 = unit attention (por ejemplo, un restablecimiento de bus SCSI)
- 7 = proteger datos
- 8 = selección en blanco
- 9 = proveedor específico
- A = copia cancelada
- B = mandato cancelado
- C = obsoleto
- D = desbordamiento de volumen
- E = comparación errónea
- F = reservado

#### ASC/ASCQ

Los códigos ASC y ASCQ son los bytes 12 y 13 de los bytes de detección. El manual de referencia de la unidad o biblioteca proporcionado con el dispositivo contiene tablas que explican los valores de los campos KEY, ASC y ASCQ. Descripciones de códigos estándar ASC y ASCQ proporciona información adicional acerca de valores estándares de códigos ASC y ASCQ.

#### Códigos de error de sistema operativo

Cuando un mandato falla, el sistema operativo devuelve un número de error. Para determinar qué significan los códigos de error, realice la siguiente acción:

- En las plataformas AIX, HP-UX y Solaris, vea el archivo `errno.h` en el directorio `/usr/include/sys`. Este archivo proporciona definiciones para códigos de error.
- En plataformas Linux, vea los archivos `errno-base.h` y `errno.h` en el directorio `/usr/include/asm-generic`. Estos archivos proporcionan definiciones para códigos.
- En las plataformas de Windows, contacte con el soporte de Microsoft para obtener ayuda con los mensajes de error.
- Visión general de los valores de los códigos de terminación y de operación  
Los mensajes de IBM Spectrum Protect pueden contener códigos de terminación de controlador de dispositivo de los controladores de dispositivos.
- Descripciones de códigos estándar ASC y ASCQ  
Se describen códigos ASC y ASCQ estándares.

## Visión general de los valores de los códigos de terminación y de operación

Los mensajes de IBM Spectrum Protect pueden contener códigos de terminación de controlador de dispositivo de los controladores de dispositivos.

- Códigos de terminación de controladores de dispositivos: códigos comunes  
IBM Spectrum Protect los controladores de dispositivos proporcionan códigos de terminación que son comunes a todas las clases de dispositivos.
- Códigos de terminación de controladores de dispositivos: cambiadores de medios  
IBM Spectrum Protect controladores de dispositivos proporcionan códigos de terminación que son específicos para dispositivos cambiadores de medios.

- Códigos finalización de controladores del dispositivo: unidades de cinta  
IBM Spectrum Protect los controladores de dispositivo proporcionan códigos de finalización que son específicos de las unidades de cinta.

## Códigos de terminación de controladores de dispositivos: códigos comunes

IBM Spectrum Protect los controladores de dispositivos proporcionan códigos de terminación que son comunes a todas las clases de dispositivos.

La siguiente tabla muestra valores de códigos de terminación para los controladores de dispositivos IBM Spectrum Protect. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de completar la acción recomendada, vuelva a intentar la operación que falló.

Tabla 1. Valores del código de terminación comunes a todas las clases de dispositivos

Decimal	Hexadecimal	Descripción	Acción recomendada
200	X'C8'	El dispositivo ha indicado una condición de error, pero no hay disponibles datos de detección.	Vuelva a intentar la operación que falló.
201	X'C9'	El controlador del dispositivo ha fallado.	Contacte con el soporte de IBM Spectrum Protect.
202	X'CA'	El dispositivo EEPROM ha fallado.	Compruebe el dispositivo. Sirva el dispositivo si es necesario.
203	X'CB'	Se necesita intervención manual.	Corrija el problema en el dispositivo. El problema puede ser una cinta atascada, cabezales sucios o una sección de la biblioteca atestada.
204	X'CC'	El sistema se ha recuperado de un error de E/S; solo para su información.	No es necesaria ninguna acción.
205	X'CD'	El adaptador SCSI ha fallado.	Compruebe los cables sueltos, patillas dobladas, cables dañados, adaptadores SCSI malos, terminaciones incorrectas o terminadores malos.
206	X'CE'	Se ha producido un error SCSI general.	Compruebe los cables sueltos, patillas dobladas, cables dañados, adaptadores SCSI malos, terminaciones incorrectas o terminadores malos.
207	X'CF'	El dispositivo no puede llevar a cabo la acción solicitada.	Asegúrese de que el dispositivo está encendido y preparado. Asegúrese de que la unidad se ha definido correctamente con el mandato DEFINE DRIVE. Asegúrese de que la clase de dispositivo se definió correctamente con el mandato DEFINE DEVCLASS.
208	X'D0'	El mandato finaliza.	Contacte con el soporte de IBM Spectrum Protect.
209	X'D1'	Se ha detectado un error en el microcódigo del dispositivo.	Compruebe el nivel de microcódigo de la unidad. Contacte con el fabricante de la unidad y solicite el nivel más reciente.
210	X'D2'	El dispositivo se ha restablecido debido a encendido de dispositivo, restablecimiento de bus SCSI o carga/expulsión manual de cinta.	Vuelva a intentar la operación que falló.
211	X'D3'	El bus de SCSI está ocupado.	Asegúrese de que los ID de SCSI están correctamente asignados al dispositivo correcto, y que ningún otro proceso está accediendo al dispositivo.
212	X'D4'	La reserva persistente no es compatible en este dispositivo.	No es necesario realizar ninguna acción.

Decimal	Hexadecimal	Descripción	Acción recomendada
213	X'D5'	Ha fallado una operación de reserva persistente.	Restablezca el dispositivo e intente la operación de nuevo. Si el problema persiste, póngase en contacto con Soporte IBM Spectrum Protect.

## Códigos de terminación de controladores de dispositivos: cambiadores de medios

IBM Spectrum Protect controladores de dispositivos proporcionan códigos de terminación que son específicos para dispositivos cambiadores de medios.

La siguiente tabla muestra valores de códigos para los controladores de dispositivos IBM Spectrum Protect para cambiadores de medios. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de realizar la acción recomendada, vuelva a intentar la operación que falló.

Tabla 1. Valores del código de terminación para cambiadores de medios

Decimal	Hexadecimal	Descripción	Acción recomendada
300	X'12C'	Error de entrada/salida de cartucho	Compruebe los puertos de entrada/salida o la biblioteca.
301	X'12D'	Error de carga de cartucho	Compruebe la unidad para volúmenes atascados. En AIX, despliegue el errpt para comprobar los errores de hardware.
302	X'12E'	Cartucho en unidad con errores	Compruebe la unidad para volúmenes atascados. En AIX, despliegue el errpt para comprobar los errores de hardware.
303	X'12F'	Carrusel no cargado	Asegúrese de que el carrusel está correctamente en su lugar y la puerta cerrada.
304	X'130'	Error de cambiador	En AIX, despliegue el errpt para comprobar los errores de hardware.
305	X'131'	Error de unidad	Asegúrese de que los cabezales están limpios. En AIX, despliegue el errpt para comprobar los errores de hardware.
306	X'132'	Error de unidad o de medios	Asegúrese de que los cabezales están limpios. En AIX, despliegue el errpt para comprobar los errores de hardware.
307	X'133'	Error de entrada/salida	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
308	X'134'	Puerto de entrada/salida ausente	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
309	X'135'	Error de auditoría de biblioteca	Asegúrese de que no hay volúmenes atascados. Es posible que la auditoría de la biblioteca esté fallando debido a los errores de hardware. En AIX, despliegue el errpt para comprobar los errores de hardware.
310	X'136'	Biblioteca llena	Compruebe los volúmenes atascados. Asegúrese de que los volúmenes no se han reorganizado. Si la biblioteca no está llena, inicie el mandato AUDIT LIBRARY.

Decimal	Hexadecimal	Descripción	Acción recomendada
311	X'137'	Exportación de medios	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
312	X'138'	Error de ranura	Asegúrese de que no hay nada atascado en la ranura.
313	X'139'	Error de ranura o de medios	Asegúrese de que el volumen no está atascado en la ranura y de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
314	X'13A'	La ranura o unidad origen estaba vacía al intentar trasladar un volumen	Asegúrese de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
315	X'13B'	La ranura o unidad destino estaba llena al intentar trasladar un volumen	Asegúrese de que los volúmenes no se han reorganizado, o de que no hay ningún volumen atascado en la unidad. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
316	X'13C'	Cartucho limpiador instalado	Póngase en contacto con el soporte de IBM Spectrum Protect .
317	X'13D'	El medio no se ha rechazado	Asegúrese de que los volúmenes no se han reorganizado, o de que no hay ningún volumen atascado en la unidad. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
318	X'13E'	Puerto E/S no configurado	Contacte con el soporte de IBM Spectrum Protect.
319	X'13F'	Primer destino vacío	Asegúrese de que los volúmenes no se han reorganizado. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
320	X'140'	No hay información del inventario	Inicie el mandato AUDIT LIBRARY.
321	X'141'	Lea la no coincidencia del estado del elemento	Asegúrese de que el firmware y los controladores de adaptador de bus de host están en los niveles actuales. Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.
322	X'142'	Inicialice el rango que ha fallado	Consulte en la interfaz de biblioteca de cintas los errores de hardware. Si no hay errores, póngase en contacto con el soporte de IBM Spectrum Protect.

## Códigos finalización de controladores del dispositivo: unidades de cinta

IBM Spectrum Protect los controladores de dispositivo proporcionan códigos de finalización que son específicos de las unidades de cinta.

La tabla siguiente muestra los valores de códigos de finalización para los IBM Spectrum Protect controladores del dispositivo para unidades de cinta. Cada entrada proporciona una descripción para el mensaje de error de E/S y una acción recomendada. Después de intentar una acción recomendada, intente la operación fallida de nuevo.

Tabla 1. Valores de código de finalización para controladores de cinta

Decimal	Hexadecimal	Descripción	Acción recomendada
400	X'190'	Detectado final físico de medio	Asegúrese de que los cabezales de la unidad están limpios.



Decimal	Hexadecimal	Descripción	Acción recomendada
401	X'191'	Detectado el fin de los datos	Contacte con el soporte de IBM Spectrum Protect.
402	X'192'	Medio dañado	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
403	X'193'	Error de medios	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
404	X'194'	Incompatibilidad de medios	Asegúrese de que se está utilizando la longitud y el tipo de medio correcto.
406	X'196'	El sector solicitado no es válido	Error interno del servidor. Contacte con el soporte de IBM Spectrum Protect.
407	X'197'	Protegido contra grabación	Asegúrese de que el volumen no está protegido contra escritura.
408	X'198'	Limpiar el medio y la unidad	Limpie los cabezales de unidad con un cartucho de limpieza.
409	X'199'	Anomalía en el medio	Asegúrese de que los cabezales están limpios. Asegúrese de que el medio no está dañado físicamente y no ha alcanzado el final de vida especificado por el fabricante de medios.
410	X'19A'	Limpieza completada	Vuelva a intentar la operación que falló.
411	X'19B'	Detectado final lógico de medio	Contacte con el soporte IBM Spectrum Protect.
412	X'19C'	El medio no se encuentra en la unidad	Asegúrese de que la unidad esté correctamente colocado en el archivo. Si el problema persiste, inicie el mandato AUDIT LIBRARY.
413	X'19D'	Se ha encontrado el inicio del medio	Contacte con el soporte de IBM Spectrum Protect.
414	X'19E'	Anomalía en la operación de borrado	Limpiar los cabezales de la unidad.
415	X'19F'	Se ha intentado sobregrabar un medio WORM grabado	Error interno del servidor. Contacte con el soporte IBM Spectrum Protect.
416	X'1A0'	Se ha leído un bloque de longitud incorrecta	Asegúrese de que los cabezales están limpios. En AIX, despliegue el erprt para comprobar los errores de hardware.
417	X'1A1'	Abrir sólo lectura	Contacte con el soporte de IBM Spectrum Protect.
418	X'1A2'	Abrir sólo escritura	Contacte con el soporte de IBM Spectrum Protect.
419	X'1A2'	Ha fallado la exploración de medio	Limpiar el medio y la unidad
420	X'1A4'	Protegido contra grabación lógica	Asegúrese de que los cabezales están limpios. Compruebe las anotaciones de errores del sistema operativo para los errores de hardware. Verifique que se ha quitado la pestaña de protección contra grabación. Apague la aceleración de cinta SAN o establezca CHECKTAPEPOS en OFF o TSMonly.
422	X'1A6'	Es necesaria la limpieza	Limpiar la unidad de cinta.

Decimal	Hexadecimal	Descripción	Acción recomendada
423	X'1A7'	Error de medios	Compruebe las anotaciones de errores del sistema operativo para los errores de hardware. Compruebe los medios dañados.
424	X'1A8'	Se ha producido un error relacionado con el cifrado	Compruebe el ajuste de cifrado de la clase de dispositivo y de la unidad de cinta.
425	X'1A9'	Se ha producido un error relacionado con el descifrado	Compruebe el ajuste de cifrado de la clase de dispositivo y de la unidad de cinta.
425	X'1AA'	Se ha producido un error externo relacionado con el cifrado	Compruebe el valor de cifrado en la clase de dispositivo y la unidad de cintas.
426	X'1AB'	Se ha producido un error de coincidencia de CRC	Asegúrese de que el medio no ha alcanzado el final de vida especificado por el fabricante de medios. Vuelva a intentar la operación.

## Descripciones de códigos estándar ASC y ASCQ

Se describen códigos ASC y ASCQ estándares.

Los códigos ASC y ASCQ son dispositivos de 12 y 13 bytes para SCSI-2. En sistemas de Windows estos códigos se muestran en el registro de sucesos de Windows, pero la información se encuentra en bytes distintos.

Consulte el mensaje del servidor ANR8300E o ANR8302E para la acción recomendada.

La tabla siguiente ofrece descripciones estándar para algunos códigos ASC y ASCQ. Cada uno de los valores tiene un prefijo de 0x, que indica que es una constante hexadecimal. Observe que las descripciones varían según el dispositivo. Para obtener una descripción precisa de códigos ASC y ASCQ para cualquier dispositivo, consulte la documentación que acompaña al dispositivo.

Tabla 1. Descripciones de códigos estándar ASC y ASCQ

ASC	ASCQ	Descripción
0x00	0x00	No hay detección adicional
0x00	0x01	Detectada marca de archivo
0x00	0x02	Detectado fin de medio
0x00	0x03	Detectada marca de conjunto
0x00	0x04	Comienzo de medio
0x00	0x05	Fin de los datos
0x00	0x06	Proceso E/S terminado
0x02	0x00	No hay búsqueda completada
0x03	0x00	Anomalía de grabación del dispositivo
0x03	0x01	No hay grabación actual
0x03	0x02	Demasiados errores de grabación
0x04	0x00	Unidad lógica no preparada
0x04	0x01	Comienzo preparado
0x04	0x02	No preparado, se necesita inicialización del mandato
0x04	0x03	No preparado, se necesita la intervención manual
0x04	0x04	No preparado, formateando
0x05	0x00	No hay respuesta a seleccionar
0x06	0x00	No se ha encontrado posición de referencia
0x07	0x00	Seleccionados múltiples dispositivos
0x08	0x00	Anomalía en la comunicación
0x08	0x01	Tiempo de espera de la comunicación

<b>ASC</b>	<b>ASCQ</b>	<b>Descripción</b>
0x08	0x02	Error de paridad de comunicación
0x09	0x00	Realizar seguimiento del siguiente error
0x0A	0x00	Desbordamiento de las anotaciones de errores.
0x0C	0x00	Error de grabación
0x11	0x00	Error de lectura no recuperado
0x11	0x01	Se han agotado los reintentos de lectura
0x11	0x02	Error demasiado largo para corregirlo
0x11	0x03	Múltiples errores de lectura
0x11	0x08	Lectura de bloque incompleta
0x11	0x09	No se han encontrado huecos
0x11	0x0A	Error mal corregido
0x14	0x00	Entidad grabada no encontrada
0x14	0x01	Registro no encontrado
0x14	0x02	Marca de archivo/marca de conjunto no encontrado
0x14	0x03	Fin de los datos no encontrado
0x14	0x04	Error de secuencia de bloques
0x15	0x00	Error de posicionamiento aleatorio
0x15	0x01	Error de posicionamiento mecánico
0x15	0x02	Error de posicionamiento de lectura
0x17	0x00	No se ha aplicado error de corrección
0x17	0x01	Recuperado con reentradas
0x17	0x02	Recuperado con desplazamiento positivo de cabezales
0x17	0x03	Recuperado con desplazamiento negativo de cabezales
0x18	0x00	ECC aplicado
0x1A	0x00	Error de longitud de la lista de parámetros
0x1B	0x00	Error de transferencia síncrona de datos
0x20	0x00	Código de operación no válido
0x21	0x00	Bloque fuera del rango permitido
0x21	0x01	Dirección de elemento no válida
0x24	0x00	Campo no válido en CDB
0x25	0x00	LUN no admitido
0x26	00	Campo no válido en la lista de parámetros
0x26	0x01	Parámetro no admitido
0x26	0x02	Valor de parámetro no admitido
0x26	0x03	Parámetros de umbral no admitidos
0x27	0x00	Protegido contra la grabación
0x28	0x00	No preparado a preparado
0x28	0x01	Se accedió al elemento importar/exportar
0x29	0x00	Conexión, restablecimiento, restablecimiento de bus
0x2A	0x00	Parámetros cambiados
0x2A	0x01	Parámetros de modalidad cambiados
0x2A	0x02	Parámetros de anotación cambiados

<b>ASC</b>	<b>ASCQ</b>	<b>Descripción</b>
0x2B	0x00	No se puede ejecutar la copia
0x2C	0x00	Error de secuencia de mandato
0x2D	0x00	Sobrescribir error en la actualización
0x2F	0x00	mandato limpiado por el iniciador
0x30	0x00	Medio incompatible
0x30	0x01	Formato de medio desconocido
0x30	0x02	Formato de medio incompatible
0x30	0x03	Cartucho limpiador instalado
0x31	0x00	Formato de medio corrupto
0x33	0x00	Error de longitud de la cinta
0x37	0x00	Parámetro redondeado
0x39	0x00	Guardando parámetros no admitidos
0x3A	0x00	Medio no presente
0x3B	0x00	Error de posicionamiento secuencial
0x3B	0x01	Error de posicionamiento en BOT
0x3B	0x02	Error de posicionamiento en EOT
0x3B	0x08	Error de recolocación
0x3B	0x0D	Elemento de destino de medio lleno
0x3B	0x0E	Elemento de origen de medio vacío
0x3D	0x00	Bits no válidos en el mensaje
0x3E	0x00	LUN no auto-configurado
0x3F	0x00	Condiciones operativas cambiadas
0x3F	0x01	Ha cambiado el microcódigo
0x3F	0x02	Definición operativa cambiada
0x3F	0x03	Han cambiado los datos de consulta
0x3F	0x0E	Han cambiado los datos LUN indicados
0x43	0x00	Mensaje de error
0x44	0x00	Anomalía interna de destino
0x45	0x00	Anomalía seleccionar/volver a seleccionar
0x46	0x00	Restablecimiento de software sin éxito
0x47	0x00	Error de paridad SCSI
0x48	0x00	Iniciador detectado mensaje recibido
0x49	0x00	Error de mensaje no válido
0x4A	0x00	Error de fase de mandato
0x4B	0x00	Error de fase de datos
0x4C	0x00	LUN ha fallado la auto-configuración
0x4E	0x00	Intento de mandatos solapados
0x50	0x00	Error para añadir grabación
0x50	0x01	Error de posición para añadir grabación
0x50	0x02	Error de posición (temporización)
0x51	0x00	Anomalía en la operación de borrado
0x52	0x00	Anomalía del cartucho

ASC	ASCQ	Descripción
0x53	0x00	Ha fallado la expulsión de carga/medio
0x53	0x01	Anomalía de cinta no cargada
0x53	0x02	Eliminación de medios impedida
0x5A	0x00	Estado de la operación cambiado
0x5A	0x01	Eliminación de los medios del operador
0x5A	0x02	Protegido contra grabación del operador
0x5A	0x03	Permitida la grabación del operador
0x5B	0x00	Excepción de anotaciones
0x5B	0x01	Se cumplió la condición de umbral
0x5B	0x02	Contador de anotaciones al máximo
0x5B	0x03	Se han agotado los códigos de lista de anotaciones

- Códigos ASC y ASCQ en el registro de sucesos de Windows  
Los códigos ASC y ASCQ se visualizan en el registro de sucesos de Windows.

## Códigos de error de dispositivo en el registro de errores del sistema AIX

Algunos códigos de error de dispositivo se registran en el registro de errores del sistema AIX.

ADSM\_DD\_LOG1 (0xAC3AB953)  
DEVICE DRIVER SOFTWARE ERROR

Este error se ha registrado por el controlador de dispositivo IBM Spectrum Protect cuando se sospecha que hay un problema en el software del controlador de dispositivo IBM Spectrum Protect. Si el controlador de dispositivo IBM Spectrum Protect emite un mandato de E/S SCSI con un código de operación ilegal, el mandato falla y el error se registra con este identificador. Informe de este error inmediatamente al personal de soporte de IBM Spectrum Protect.

**Datos de detalle:** Datos de detección

Los datos de detección contienen información que puede determinar la causa del error. Informe de todos los datos de la entrada de error al personal de soporte de IBM Spectrum Protect.

ADSM\_DD\_LOG2 (0x5680E405)  
HARDWARE/COMMAND-ABORTED ERROR

Este error lo registra el controlador del dispositivo de IBM Spectrum Protect si el dispositivo emite un error de hardware o un error de mandato cancelado en respuesta a un mandato E/S SCSI.

**Datos de detalle:** Datos de detección

Los datos de detección contienen información que pueden determinar qué componente de hardware ha fallado y por qué. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM\_DD\_LOG3 (0x461B41DE)  
MEDIA ERROR

El controlador de dispositivo IBM Spectrum Protect registra este error cuando falla el mandato de I/O de SCSI, o porque el disco requiere una limpieza.

**Datos de detalle:** Datos de detección

Los datos de detección contienen información que puede determinar la causa del error. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM\_DD\_LOG4 (0x4225DB66)  
TARGET DEVICE GOT UNIT ATTENTION

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir determinadas notificaciones UNIT ATTENTION desde el dispositivo. Las UNIT ATTENTION son informativas y, normalmente, indican que algún estado del dispositivo ha cambiado. Por ejemplo, se registraría este error si la puerta de un dispositivo de biblioteca se abriera y después se

cerrara. El registro de este suceso indica que la actividad se produjo y que es posible que el inventario de la biblioteca haya cambiado.

**Datos de detalle:** Datos de detección

Los datos de detección contienen información que describen la causa para emitir una notificación UNIT ATTENTION. Para interpretar los datos de detección para un dispositivo concreto, consulte el manual de especificación SCSI del dispositivo.

ADSM\_DD\_LOG5 (0xDAC55CE5)  
PERMANENT UNKNOWN ERROR

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir un error desconocido desde un dispositivo en respuesta al mandato de I/O de SCSI. Si el problema persiste, póngase en contacto con el personal de soporte de IBM Spectrum Protect .

**Datos de detalle:** Datos de detección

Los datos de detección constan de información que puede determinar la causa del error. Informe de todos los datos de la entrada de error al personal de soporte de IBM Spectrum Protect.

ADSM\_DD\_LOG6 (0xBC539B26)  
WARNING OR INFORMATIONAL MESSAGE FOR TARGET DEVICE

El controlador de dispositivo IBM Spectrum Protect registra este error después de recibir una advertencia o un mensaje informativo desde un dispositivo en respuesta a un mandato de I/O de SCSI. Son mensajes informativos y pueden no ser indicativos de un problema. Si el problema persiste, notifíquese al soporte de IBM Spectrum Protect.

**Datos de detalle:** Datos de detección

Los datos de detección constan de información que puede determinar la causa del mensaje. Informe de todos los datos de la entrada al personal de soporte de IBM Spectrum Protect.

## Códigos de retorno de IBM Global Security Kit

El servidor y el cliente utilizan el proceso de IBM Global Security Kit (GSKit) para SSL (Secure Sockets Layer) entre el servidor y el cliente de archivado y copia de seguridad. Algunos mensajes que se emiten para el proceso de SSL incluyen códigos de retorno de GSKit.

GSKit se instala o actualiza automáticamente durante la instalación de IBM Spectrum Protect y proporciona las bibliotecas siguientes:

- SSL de GSKit
- API de gestión de claves GSKit
- IBM Crypto for C (ICC)

Los informes del programa de utilidad tsmdiag notifican el nivel de GSKit que se ha instalado en el sistema o puede utilizar uno de estos métodos:

- Para Windows, emita los mandatos siguientes:

```
regedit /e gskitinfo.txt "HKEY_LOCAL_MACHINE\software\ibm\gsk8"  
notepad gskitinfo.txt
```

**PRECAUCIÓN:**

Puede dañar el registro del sistema si utiliza regedit de forma incorrecta.

- Para el servidor AIX de 64 bits, emita el siguiente mandato desde la línea de mandatos: `gsk8ver_64`

Consulte la Tabla 1 para ver los códigos de retorno SSL de GSKit.

El servidor utiliza la API de gestión de claves GSKit para crear automáticamente la base de datos de gestión de claves y las claves públicas y privadas del servidor. Algunos mensajes que se emiten para este proceso pueden incluir códigos de retorno de gestión de claves GSKit. Consulte la Tabla 2 para ver los códigos de retorno de gestión de claves.

Tabla 1. Códigos de retorno generales de IBM Global Security Kit SSL

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Lo emite cada llamada de función que se completa correctamente.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función <code>open()</code> correcta.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.
0x00000005	5	GSK_INVALID_STATE	El manejador tiene un estado no válido para la operación como, por ejemplo, realizar una operación <code>init()</code> en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar la criptografía.
0x0000000a	10	GSK_ERROR_ASN	Error al validar los campos ASN del certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x0000000d	13	GSK_INVALID_PARAMETER	Parámetro no válido.
0x0000000e	14	GSK_ERROR_UNEXPECTED_INT_EXCEPTION	Parámetro no válido. Informe de este error al servicio de soporte de software de IBM.
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves no tiene un formato interno válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlace dinámico GSK. Asegúrese de que GSK se ha instalado correctamente.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido GSK_ENVIRONMENT_CLOSE_OPTIONS en GSK_DELAYED_ENVIRONMENT_CLOSE y se ha llamado a la función <code>gsk_environment_close()</code> .
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el nombre del archivo stash. El archivo de claves no se ha inicializado.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Una contraseña utilizada para una consulta LDAP (lightweight directory access protocol) no es correcta.
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato <code>gsk_secure_socket*()</code> después de una llamada a <code>gsk_close_environment()</code> .
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema no se ha establecido en un valor válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña especificada para el archivo de claves no es correcta. No se puede utilizar el archivo de claves. Es posible también que el archivo de claves esté dañado.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.



<b>Código de retorno (hex)</b>	<b>Código de retorno (decimal)</b>	<b>Constante</b>	<b>Explicación</b>
0x0000019b	411	GSK_ERROR_BAD_MAC	El código de autenticación de mensaje (MAC) no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	No se ha recibido un protocolo SSL válido del socio.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	read() ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	write() ha presentado anomalías. Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El cifrado de la versión especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El cifrado de la versión 3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	No se puede crear el manejador. Informe de este error al servicio de soporte de software de IBM.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	La inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	El controlador PKCS nº11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	La ranura no contiene ninguna señal PKCS nº11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	El pin/contraseña para acceder a la señal PKCS nº11 no es válido.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se puede abrir el proveedor de servicios de cifrado basado en hardware. El nombre CSP no se ha especificado correctamente o se ha realizado un intento fallido de acceder al almacén de certificados CSP.
0x000001b3	435	GSK_CONFLICTING_ATTRIBUTE_SETTING	Conflicto de establecimiento de atributos entre PKCS11, base de datos de claves CMS y Microsoft Crypto API.
0x000001b4	436	GSK_UNSUPPORTED_PLATFORM	La función solicitada no recibe soporte en la plataforma en la que se ejecuta la aplicación. Por ejemplo, Microsoft Crypto API no se admite en plataformas que no sean Windows 2000.
0x000001b6	438	GSK_ERROR_INCORRECT_SESSION_TYPE	Se ha devuelto un valor incorrecto desde la función de devolución de llamada del tipo restablecer sesión. Sólo se permite GSKit <code>gsk_sever_session</code> , <code>gsk_sever_session_with_cl_auth</code> o <code>gsk_sever_session_with_cl_auth_crit</code> .
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para <code>reset_cipher()</code> y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	No se ha especificado un ID válido para la llamada de la función <code>gsk_secure_soc_misc()</code> .
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID no válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificado.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de memoria caché SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido correctamente.
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede reiniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de <code>gsk_start_trace()</code> debe ser un nombre completo de archivo de vía de acceso válido.

Tabla 2. Códigos de retorno de gestión de claves de IBM Global Security Kit

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000000	0	GSK_OK	La tarea se completa correctamente. Este mensaje lo emite cada llamada de función que se completa correctamente.
0x00000001	1	GSK_INVALID_HANDLE	El entorno o el manejador de SSL no es válido. El manejador especificado no era el resultado de una llamada de función <code>open()</code> satisfactoria.
0x00000002	2	GSK_API_NOT_AVAILABLE	La biblioteca de enlace dinámico (DLL) se ha descargado y no está disponible (se produce sólo en sistemas Microsoft Windows).
0x00000003	3	GSK_INTERNAL_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000004	4	GSK_INSUFFICIENT_STORAGE	No hay suficiente memoria disponible para ejecutar la operación.
0x00000005	5	GSK_INVALID_STATE	El manejador se encuentra en un estado incorrecto para la operación como, por ejemplo, ejecutar una operación <code>init()</code> en un manejador dos veces.
0x00000006	6	GSK_KEY_LABEL_NOT_FOUND	No se ha encontrado la etiqueta de clave especificada en el archivo de claves.
0x00000007	7	GSK_CERTIFICATE_NOT_AVAILABLE	No se ha recibido el certificado del socio.
0x00000008	8	GSK_ERROR_CERT_VALIDATION	Error de validación del certificado.
0x00000009	9	GSK_ERROR_CRYPTO	Error al procesar la criptografía.
0x0000000a	10	GSK_ERROR_ASN	Error al validar los campos ASN del certificado.
0x0000000b	11	GSK_ERROR_LDAP	Error al establecer la conexión con el registro de usuario.
0x0000000c	12	GSK_ERROR_UNKNOWN_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.

<b>Código de retorno (hex)</b>	<b>Código de retorno (decimal)</b>	<b>Constante</b>	<b>Explicación</b>
0x00000065	101	GSK_OPEN_CIPHER_ERROR	Error interno. Informe de este error al servicio de soporte de software de IBM.
0x00000066	102	GSK_KEYFILE_IO_ERROR	Error de E/S al leer el archivo de claves.
0x00000067	103	GSK_KEYFILE_INVALID_FORMAT	El archivo de claves tiene un formato interno que no es válido. Vuelva a crear el archivo de claves.
0x00000068	104	GSK_KEYFILE_DUPLICATE_KEY	El archivo de claves tiene dos entradas con la misma clave.
0x00000069	105	GSK_KEYFILE_DUPLICATE_LABEL	El archivo de claves tiene dos entradas con la misma etiqueta.
0x0000006a	106	GSK_BAD_FORMAT_OR_INVALID_PASSWORD	La contraseña del archivo de claves se utiliza como comprobación de integridad. El archivo de claves se ha dañado o el ID de contraseña es incorrecto.
0x0000006b	107	GSK_KEYFILE_CERT_EXPIRED	La clave predeterminada en el archivo de claves tiene un certificado caducado.
0x0000006c	108	GSK_ERROR_LOAD_GSKLIB	Se ha producido un error al cargar una de las bibliotecas de enlaces dinámicos de GSK. Asegúrese de que GSK se ha instalado correctamente.
0x0000006d	109	GSK_PENDING_CLOSE_ERROR	Este mensaje indica que se está intentando establecer una conexión en un entorno GSK después de que se haya establecido GSK_ENVIRONMENT_CLOSE_OPTIONS en GSK_DELAYED_ENVIRONMENT_CLOSE y se ha llamado a la función gsk_environment_close().
0x000000c9	201	GSK_NO_KEYFILE_PASSWORD	No se han especificado ni la contraseña ni el archivo stash por lo que no se ha inicializado el archivo de claves.
0x000000ca	202	GSK_KEYRING_OPEN_ERROR	No se ha podido abrir el archivo de claves. La vía de acceso se ha especificado de forma incorrecta o los permisos de archivo no han permitido que se abra el archivo.
0x000000cb	203	GSK_RSA_TEMP_KEY_PAIR	No se puede generar un par de claves temporal. Informe de este error al servicio de soporte de software de IBM.
0x000000cc	204	GSK_ERROR_LDAP_NO_SUCH_OBJECT	Se ha especificado un objeto de nombre de usuario que no se ha podido encontrar.
0x000000cd	205	GSK_ERROR_LDAP_INVALID_CREDENTIALS	Una contraseña utilizada para una consulta LDAP no es correcta.

<b>Código de retorno (hex)</b>	<b>Código de retorno (decimal)</b>	<b>Constante</b>	<b>Explicación</b>
0x000000ce	206	GSK_ERROR_BAD_INDEX	Un índice de la lista de servidores LDAP de migración tras anomalía no era correcto.
0x000000cf	207	GSK_ERROR_FIPS_NOT_SUPPORTED	Esta instalación de GSKit no admite modalidad de operación FIPS.
0x0000012d	301	GSK_CLOSE_FAILED	Indica que la solicitud de cierre del entorno GSK no se ha gestionado correctamente. El motivo más probable es que se ha intentado un mandato <code>gsk_secure_socket*()</code> después de una llamada a <code>gsk_close_environment()</code> .
0x00000191	401	GSK_ERROR_BAD_DATE	La fecha del sistema se ha establecido en un valor que no es válido.
0x00000192	402	GSK_ERROR_NO_CIPHERS	No se han habilitado SSLv2 ni SSLv3.
0x00000193	403	GSK_ERROR_NO_CERTIFICATE	No se ha recibido del socio el certificado necesario.
0x00000194	404	GSK_ERROR_BAD_CERTIFICATE	El certificado recibido se ha formateado de forma incorrecta.
0x00000195	405	GSK_ERROR_UNSUPPORTED_CERTIFICATE_TYPE	El tipo de certificado recibido no se ha admitido.
0x00000196	406	GSK_ERROR_IO	Se ha producido un error de E/S en una operación de lectura o grabación de datos.
0x00000197	407	GSK_ERROR_BAD_KEYFILE_LABEL	No se encuentra la etiqueta especificada en el archivo de claves.
0x00000198	408	GSK_ERROR_BAD_KEYFILE_PASSWORD	La contraseña especificada para el archivo de claves no es correcta. No se puede utilizar el archivo de claves. Es posible que el archivo de claves esté dañado.
0x00000199	409	GSK_ERROR_BAD_KEY_LEN_FOR_EXPORT	En un entorno de cifrado limitado, el tamaño de la clave es demasiado largo para que se pueda admitir.
0x0000019a	410	GSK_ERROR_BAD_MESSAGE	Se ha recibido un mensaje SSL con formato incorrecto de la otra parte.
0x0000019b	411	GSK_ERROR_BAD_MAC	El MAC no se ha verificado correctamente.
0x0000019c	412	GSK_ERROR_UNSUPPORTED	Protocolo SSL no admitido o tipo de certificado no admitido.
0x0000019d	413	GSK_ERROR_BAD_CERT_SIG	El certificado recibido contenía una firma incorrecta.
0x0000019e	414	GSK_ERROR_BAD_CERT	Se ha recibido un certificado con formato incorrecto del socio.
0x0000019f	415	GSK_ERROR_BAD_PEER	Se ha recibido del socio un protocolo SSL que no es válido.
0x000001a0	416	GSK_ERROR_PERMISSION_DENIED	Informe de este error al servicio de soporte de software de IBM.
0x000001a1	417	GSK_ERROR_SELF_SIGNED	El certificado autofirmado no es válido.

<b>Código de retorno (hex)</b>	<b>Código de retorno (decimal)</b>	<b>Constante</b>	<b>Explicación</b>
0x000001a2	418	GSK_ERROR_NO_READ_FUNCTION	Error en read(). Informe de este error al servicio de soporte de software de IBM.
0x000001a3	419	GSK_ERROR_NO_WRITE_FUNCTION	Error en write(). Informe de este error al servicio de soporte de software de IBM.
0x000001a4	420	GSK_ERROR_SOCKET_CLOSED	La otra parte ha cerrado el socket antes de que se completara el protocolo.
0x000001a5	421	GSK_ERROR_BAD_V2_CIPHER	El cifrado de la versión especificado no es válido.
0x000001a6	422	GSK_ERROR_BAD_V3_CIPHER	El cifrado de la versión 3 especificado no es válido.
0x000001a7	423	GSK_ERROR_BAD_SEC_TYPE	Informe de este error al servicio de soporte de software de IBM.
0x000001a8	424	GSK_ERROR_BAD_SEC_TYPE_COMBINATION	Informe de este error al servicio de soporte de software de IBM.
0x000001a9	425	GSK_ERROR_HANDLE_CREATION_FAILED	No se ha creado el manejador. Informe de este error al servicio de soporte de software de IBM.
0x000001aa	426	GSK_ERROR_INITIALIZATION_FAILED	La inicialización no se ha realizado. Informe de este error interno al servicio.
0x000001ab	427	GSK_ERROR_LDAP_NOT_AVAILABLE	No se puede acceder al registro de usuario especificado al validar un certificado.
0x000001ac	428	GSK_ERROR_NO_PRIVATE_KEY	La clave especificada no contenía una clave privada.
0x000001ad	429	GSK_ERROR_PKCS11_LIBRARY_NOTLOADED	Se ha realizado un intento fallido de cargar la biblioteca compartida PKCS11.
0x000001ae	430	GSK_ERROR_PKCS11_TOKEN_LABELMISMATCH	El controlador PKCS nº11 no ha podido encontrar la señal especificada por el operador.
0x000001af	431	GSK_ERROR_PKCS11_TOKEN_NOTPRESENT	La ranura no contiene ninguna señal PKCS nº11.
0x000001b0	432	GSK_ERROR_PKCS11_TOKEN_BADPASSWORD	El pin/contraseña para acceder a la señal PKCS nº11 es incorrecto.
0x000001b1	433	GSK_ERROR_INVALID_V2_HEADER	La cabecera SSL recibida no era una cabecera con el formato SSLv2 correcto.
0x000001b2	434	GSK_CSP_OPEN_ERROR	No se ha podido abrir el proveedor de servicios de cifrado basado en hardware (CSP). El nombre CSP no se ha especificado correctamente o se ha realizado un intento fallido de acceder al almacén de certificados CSP.
0x000001b3	435	GSK_CSP_OPEN_ERROR	Se han definido algunos atributos conflictivos para la operación de SSL.

<b>Código de retorno (hex)</b>	<b>Código de retorno (decimal)</b>	<b>Constante</b>	<b>Explicación</b>
0x000001b4	436	GSK_CSP_OPEN_ERROR	La API de Microsoft Crypto sólo es compatible con Microsoft Windows 2000 con Service Pack 2 aplicado.
0x000001b5	437	GSK_CSP_OPEN_ERROR	El sistema se ejecuta en modalidad IPv6 sin establecer un PEERID.
0x000001f5	501	GSK_INVALID_BUFFER_SIZE	El tamaño del almacenamiento intermedio es negativo o cero.
0x000001f6	502	GSK_WOULD_BLOCK	Se utiliza con E/S sin bloqueo. Consulte la sección sobre no bloqueo para su uso.
0x00000259	601	GSK_ERROR_NOT_SSLV3	SSLv3 es necesario para reset_cipher() y la conexión utiliza SSLv2.
0x0000025a	602	GSK_MISC_INVALID_ID	Se ha especificado un ID que no es válido para la llamada de la función gsk_secure_soc_misc().
0x000002bd	701	GSK_ATTRIBUTE_INVALID_ID	La llamada de la función tiene un ID que no es válido. Este problema también se puede producir al especificar un manejador de entorno cuando debe utilizarse un manejador para una conexión SSL.
0x000002be	702	GSK_ATTRIBUTE_INVALID_LENGTH	El atributo tiene una longitud negativa, la cual no es válida.
0x000002bf	703	GSK_ATTRIBUTE_INVALID_ENUMERATION	El valor de enumeración no es válido para el tipo de enumeración especificado.
0x000002c0	704	GSK_ATTRIBUTE_INVALID_SID_CACHE	Lista de parámetros no válida para sustituir las rutinas de memoria caché SID.
0x000002c1	705	GSK_ATTRIBUTE_INVALID_NUMERIC_VALUE	Al establecer un atributo numérico, el valor especificado no es válido para el atributo específico que se está estableciendo.
0x000002c2	706	GSK_CONFLICTING_VALIDATION_SETTING	Se han establecido parámetros conflictivos para la validación adicional de certificados.
0x000002c3	707	GSK_AES_UNSUPPORTED	El algoritmo de cifrado AES no recibe soporte.
0x000002c4	708	GSK_PEERID_LENGTH_ERROR	PEERID no tiene la longitud correcta.
0x000002c5	709	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_OFF	El cifrado concreto no se permite cuando la modalidad de funcionamiento FIPS está desactivada.
0x000002c6	710	GSK_CIPHER_INVALID_WHEN_FIPS_MODE_ON	No se seleccionan cifrados FIPS aprobados en la modalidad de funcionamiento FIPS.
0x00000641	1601	GSK_TRACE_STARTED	El rastreo se ha iniciado satisfactoriamente.
0x00000642	1602	GSK_TRACE_STOPPED	El rastreo se ha detenido correctamente.

Código de retorno (hex)	Código de retorno (decimal)	Constante	Explicación
0x00000643	1603	GSK_TRACE_NOT_STARTED	No se ha iniciado ningún archivo de rastreo anteriormente y, por lo tanto, no se puede detener.
0x00000644	1604	GSK_TRACE_ALREADY_STARTED	El archivo de rastreo se ha iniciado y, por lo tanto, no se puede volver a iniciar.
0x00000645	1605	GSK_TRACE_OPEN_FAILED	El archivo de rastreo no se puede abrir. El primer parámetro de <code>gsk_start_trace()</code> debe ser un nombre completo de archivo de vía de acceso válido.

## Glosario

Este glosario proporciona términos y definiciones para IBM Spectrum Protect, IBM Spectrum Protect Snapshot y los productos asociados.

En este glosario se utilizan las referencias cruzadas siguientes:

- *Consulte* le remite de un término no preferido al término preferido o de una abreviatura a la forma completamente deletreada.
- *Consulte también* le refiere a un término contrastante relacionado.

Para otros términos y definiciones, consulte el sitio web Terminología de IBM®.

A B C D E F G H I J K L M N O P R S T U V W

### A

ACK

Consulte acuse de recibo.

ACL

Consulte lista de control de accesos.

activar

Para validar el contenido de un conjunto de políticas y convertirlo en conjunto de políticas activas.

acuse de recibo (ACK)

La transmisión de caracteres de reconocimiento como respuesta positiva a una transmisión de datos.

administrador

Una persona responsable de las tareas administrativas tales como la autorización de acceso y la gestión de contenidos. Los administradores también pueden otorgar niveles de autoridad a los usuarios.

Agente de almacenamiento

Programa que permite al cliente realizar operaciones de copia de seguridad y de restauración de datos del cliente directamente en y desde el almacenamiento conectado a una red de área de almacenamiento (SAN).

agregado

Objeto almacenado en una o varias agrupaciones de almacenamiento formado por un grupo de archivos lógicos empaquetados juntos. Consulte también archivo lógico, archivo físico.

agrupación de almacenamiento

Conjunto de volúmenes de almacenamiento o contenedores que es el destino utilizado para almacenar datos de cliente. Consulte también agrupación de datos activos, agrupación de almacenamiento de contenedores de nube, agrupación de almacenamiento de copias, agrupación de almacenamiento de contenedores de directorio, agrupación de almacenamiento primario, jerarquía de almacenamiento.

agrupación de almacenamiento de contenedores

Agrupación de almacenamiento primario que un servidor utiliza para almacenar datos. Los datos se almacenan en contenedores en directorios de sistema de archivos o en almacenamiento en la nube. Se eliminan los datos duplicados, si es necesario, mientras el servidor graba datos en la agrupación de almacenamiento. Consulte también agrupación de almacenamiento de contenedores de nube, contenedor, agrupación de almacenamiento de contenedores de directorio.

agrupación de almacenamiento de contenedores de directorio

Agrupación de almacenamiento que un servidor utiliza para almacenar datos en contenedores en los directorios de agrupación de almacenamiento. Los datos almacenados en una agrupación de almacenamiento de contenedores de directorio pueden utilizar la deduplicación de datos en línea o del lado del cliente. Consulte también agrupación de almacenamiento de



contenedores de nube, agrupación de almacenamiento de contenedores, agrupación de almacenamiento de copia de contenedor, agrupación de almacenamiento.

agrupación de almacenamiento de contenedores de nube

Agrupación de almacenamiento que un servidor utiliza para almacenar datos en el almacenamiento en la nube. El almacenamiento en la nube puede estar ubicado en los locales o fuera de los locales. Consulte también agrupación de almacenamiento de contenedores, agrupación de almacenamiento de contenedores de directorio, agrupación de almacenamiento.

agrupación de almacenamiento de copia

Conjunto con nombre de volúmenes que contiene copias de archivos que residen en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copia se utilizan sólo para realizar copias de seguridad de los datos almacenados en agrupaciones de almacenamiento primarias. Las agrupaciones de almacenamiento de copia no pueden ser el destino de grupos de copia de seguridad o copias archivadas, ni de una clase de gestión (para archivos gestionados por espacio). Consulte también destino, grupo de almacenamiento principal, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

agrupación de almacenamiento de copia de contenedor

Agrupación de almacenamiento que un servidor utiliza para almacenar copias de extensiones de las agrupaciones de almacenamiento de contenedores de directorio. Estas copias se utilizan para reparar daños en una agrupación de almacenamiento de contenedores de directorio. Las agrupaciones de almacenamiento de copia de contenedor utilizan soportes secuenciales como, por ejemplo, cinta. Consulte también agrupación de almacenamiento de contenedores de directorio.

agrupación de almacenamiento primaria

Conjunto de volúmenes o contenedores con nombre que el servidor utiliza para almacenar versiones de copia de seguridad de archivos, copias archivadas y archivos migrados desde nodos cliente. Consulte también grupo de almacenamiento de copias, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

agrupación de datos activos

Conjunto con nombre de volúmenes de agrupación de almacenamiento que contiene sólo versiones activas de datos de copia de seguridad de clientes. Consulte también almacenamiento del servidor, agrupación de almacenamiento, volumen de agrupación de almacenamiento.

aleatorización

Proceso de distribuir horas de inicio de planificaciones para diferentes cliente dentro de un porcentaje especificado en la ventana de inicio de planificación.

algoritmo Nagle

Algoritmo que reduce la congestión de las redes TCP/IP mediante la combinación de paquetes más pequeños y envío conjunto de los mismos.

almacenamiento del servidor

Las agrupaciones primarias, de copia y de almacenamiento de datos activos utilizados por el servidor para almacenar archivos de usuario como versiones de copia de seguridad, copias de archivo y archivos migrados desde nodos de clientes de gestión de almacenamiento jerárquico (archivos gestionados por espacio). Consulte también agrupación de datos activos, agrupación de almacenamiento de contenedores, agrupación de almacenamiento de copias, agrupación de almacenamiento primario, volumen de agrupación de almacenamiento, volumen.

almacén de datos

En un entorno virtualizado, la ubicación donde están almacenados los datos de máquina virtual.

ampliar

Aumentar la porción de espacio disponible que se puede utilizar para almacenar información sobre bases de datos o registros de recuperación.

anotación empresarial

Proceso de enviar eventos desde un servidor a un servidor de eventos designados. El servidor de eventos conduce los eventos a receptores designados, por ejemplo una salida de usuario. Consulte también evento.

anotaciones de errores

Conjunto de datos o archivo utilizados para registrar información de errores sobre un producto o sistema.

antigüedad del archivo

Con el fin de establecer prioridades para la migración, el número de días transcurridos desde el último acceso a un archivo.

archivado

Copiar programas, datos o archivos en otro medio de almacenamiento, normalmente para su almacenamiento a largo plazo o por seguridad. Consulte también recuperar.

archivo dañado

Archivo físico en el cual se han detectado errores de lectura.

archivo de caché

Instantánea de un volumen lógico creada por un Agente de instantáneas de volúmenes lógicos. Los bloques se guardan de forma inmediata antes de ser modificados durante la copia de seguridad de imagen y sus extensiones lógicas se guardan en los archivos de la caché.

archivo de caducidad

Archivo migrado o premigrado que está marcado para caducidad y eliminación del almacenamiento. Si se suprime del sistema de archivos local un archivo de resguardo o una copia original de un archivo premigrado, o bien si se actualiza la copia original de un

archivo premigrado, el archivo migrado o premigrado correspondiente se marca para que caduque la siguiente vez que se ejecute una reconciliación.

archivo de configuración de dispositivo

1. En un servidor, un archivo que contiene información acerca de clases de dispositivos definidas y, en algunos servidores, bibliotecas y unidades definidas. La información es una copia de la información de configuración del dispositivo de la base de datos.
2. En un agente de almacenamiento, un archivo que contiene el nombre y contraseña de un agente de almacenamiento e información acerca del servidor que está gestionando las bibliotecas asociadas a SAN y las unidades que dicho agente de almacenamiento utiliza.

archivo de historial de volumen

Archivo que contiene información sobre volúmenes que han sido utilizados por el servidor para realizar copias de seguridad de bases de datos y para exportar datos del administrador, nodo, políticas o servidor. El archivo contiene también información acerca de volúmenes de agrupación de almacenamiento de acceso secuencial que se han agregado, reutilizado o suprimido. La información es una copia de la información del volumen grabada en la base de datos del servidor.

archivo de inclusión/exclusión

Archivo que contiene sentencias para determinar los archivos de los que se debe obtener copia de seguridad y las clases de gestión asociadas que se deberán utilizar a efectos de copia de seguridad o archivado. Consulte también lista de inclusión-exclusión.

archivo de macro

Archivo que contiene uno o varios comandos de administración de IBM Spectrum Protect, que se pueden ejecutar sólo desde un cliente administrativo mediante el comando MACRO. Consulte también el script del mandato IBM Spectrum Protect.

archivo de opciones

Archivo que contiene opciones de proceso. Consulte también archivo de opciones del sistema de clientes, archivo de opciones del usuario cliente.

archivo de opciones de cliente

Archivo editable que identifica al servidor y el método de comunicación y proporciona la configuración de las operaciones de copia de seguridad, archivado, gestión del almacenamiento jerárquico y planificación.

archivo de opciones del sistema cliente

Archivo, utilizado en clientes de sistemas AIX, UNIX, o Linux, que contiene un grupo de opciones de proceso que identifican los servidores con los que hay que ponerse en contacto para obtener servicios. Este archivo también especifica métodos de comunicación y opciones para la copia de seguridad, archivado, gestión jerárquica del almacenamiento y planificación. Consulte también usuario de clientes-archivos de opciones, archivo de opciones.

archivo de opciones del usuario cliente

Archivo que contiene el grupo de opciones de proceso utilizadas por los clientes del sistema. El grupo puede incluir opciones que determinan el servidor con el que el cliente se pone en contacto, y opciones que afectan a las operaciones de copia de seguridad, archivado, gestión de almacenamiento jerárquico y planificación. Este archivo se denomina también archivo dsm.opt. Para los sistemas AIX, UNIX o Linux, consulte también el archivo de opciones del sistema. Consulte también el archivo de opciones-sistema de clientes , archivo de opciones.

archivo de opciones de servidor

Archivo que contiene los valores que controlan diversas operaciones del servidor. Estos valores afectan por ejemplo a las comunicaciones, dispositivos y rendimiento.

archivo de resguardo

Archivo que sustituye el archivo original de un sistema de archivos local cuando el archivo se migra al almacenamiento. Un archivo de resguardo contiene la información necesaria para recuperar un archivo migrado de un almacenamiento de servidor. También tiene información adicional que se puede utilizar para evitar que tenga que recuperarse un archivo migrado. Consulte también archivo migrado, archivo residente.

archivo de resguardo huérfano

Archivo para el cual no se puede encontrar un archivo migrado en el servidor al cual está contactando el nodo cliente para los servicios de gestión de espacio. Un archivo de resguardo puede quedar huérfano cuando, por ejemplo, se modifica el archivo de opciones del sistema cliente para que contacte un servidor distinto del servidor al que se migró el archivo.

archivo de trabajo

Un archivo generado que contiene información de configuración de un trabajo de migración. El archivo está en formato XML y puede crearse y editarse en el cliente de gestión de almacenamiento jerárquico (HSM) en la interfaz gráfica de usuario del cliente de Windows. Consulte también trabajo de migración.

archivo esparcido

Archivo que se crea con una longitud mayor que los datos que contiene, con lo que se dejan espacios vacíos para agregar datos en un futuro.

archivo especial

En sistemas AIX, UNIX, o Linux, archivo que define dispositivos del sistema o archivos temporales creados por procesos. Existen tres tipos básicos de archivos especiales: FIFO (el primero en entrar es el primero en salir); de bloques y de caracteres.

archivo físico

Objeto almacenado en una o varias agrupaciones de almacenamiento formado por un archivo lógico individual o por un grupo de archivos lógicos empaquetados juntos como agregado. Consulte también agregado, archivo lógico, ocupación física.

archivo gestionado por espacio

Un archivo que se migra desde un nodo de cliente mediante el cliente de gestión de almacenamiento jerárquico (HSM). El cliente de HSM recupera el archivo del nodo de cliente bajo petición.

archivo lógico

Archivo almacenado en una o varias agrupaciones de almacenamiento del servidor, por sí solo o como parte de un agregado.

Consulte también agregado, archivo físico, ocupación física.

archivo migrado

Un archivo que se ha copiado desde un sistema de archivos local a un almacenamiento. Para los clientes de HSM en los sistemas UNIX o Linux, el archivo se sustituye por un archivo de resguardo en el sistema de archivos local. En sistemas Windows, la creación del archivo de resguardo es opcional. Consulte también estado del archivo, archivo pre-migrado, archivo residente, archivo migrado.

archivo premigrado

Un archivo que se ha copiado al almacenamiento del servidor, pero que no se ha reemplazado con un archivo migrado en el sistema de archivo local. Una copia idéntica del archivo reside en el sistema de archivos local y en el almacenamiento del servidor. Los archivos premigrados se dan en sistemas de archivos UNIX y Linux a los que se ha agregado gestión de espacio. Consulte también estado de archivo, archivo migrado, archivo residente.

archivo residente

En un sistema Windows, un archivo completo en un sistema de archivos local que también podría ser un archivo migrado porque en el almacenamiento del servidor existe una copia migrada. En un sistema UNIX o Linux, un archivo completo en un sistema de archivos local que no ha sido migrado o pre-migrado o que ha sido recuperado del almacenamiento del servidor y modificado.

asociación

Relación definida entre un nodo cliente y una planificación de cliente. Las asociaciones identifican el nombre de la planificación, el nombre del dominio de políticas al que pertenece la planificación y el nombre del nodo de cliente que realiza operaciones planificadas.

asociación de perfil

En un gestor de configuración, relación definida entre un perfil y un objeto, como por ejemplo un dominio de políticas. Las asociaciones de perfil definen la información de configuración que se distribuye a un servidor gestionado cuando éste se suscribe al perfil.

atributo ampliado (EA)

Pares de valores o nombres que se asocian con archivos o directorios. Hay tres clases de atributos ampliados: de usuarios, del sistema y acreditados.

auditar

Buscar inconsistencias lógicas entre la información que tiene el servidor y la condición real del sistema. El gestor de almacenamiento puede auditar información sobre elementos como volúmenes, bibliotecas y licencias. Por ejemplo, cuando un gestor de almacenamiento audita un volumen, el servidor busca inconsistencias entre la información sobre archivos de los que se ha realizado una copia de seguridad o archivado almacenados en la base de datos y los datos reales asociados con cada versión de copia de seguridad o archivado en el almacenamiento del servidor.

AutoFS

consulte sistema de archivos montado automáticamente.

autorización

Derecho para acceder a objetos, recursos o funciones. Consulte también clase de privilegios.

## B

---

base de datos de archivos premigrados

Base de datos que contiene información sobre cada archivo que ha sido pre-migrado al almacenamiento del servidor.

biblioteca

1. Un repositorio para medios grabados desmontables, como discos magnéticos o cintas magnéticas.
2. Una colección de una o más unidades, y posiblemente dispositivos robóticos (dependiendo del tipo de biblioteca), que se pueden usar para acceder a los volúmenes de almacenamiento.

biblioteca compartida

Dispositivo de biblioteca utilizado por diversos servidores de gestión de almacenamiento.

biblioteca de cintas

Conjunto de equipamiento y recursos que admiten un entorno de cintas de instalación. La biblioteca de cintas puede incluir bastidores de almacenamiento de cintas, mecanismos para el montaje de cintas automático, un conjunto de unidades de cinta y un conjunto de volúmenes de cinta relacionados montados en dichas unidades.

biblioteca externa

Una colección de unidades que es gestionada por el sistema de gestión de medios distinto al servidor de gestión de almacenamiento.

## C

---

caché

Colocar una copia duplicada de un archivo en acceso aleatorio cuando el servidor migra un archivo a otra agrupación de almacenamiento de la jerarquía.

CAD

Consulte daemon de aceptación de clientes.

caducidad

Proceso en que los archivos, conjuntos de datos u objetos se identifican para su supresión debido a que se ha alcanzado su fecha de caducidad o ha transcurrido su periodo de retención.

capacidad estimada

Espacio disponible, en megabytes, en una agrupación de almacenamiento.

carácter comodín

Carácter especial como un asterisco (\*) o una interrogación (?) que puede utilizarse para representar uno o varios caracteres.

Cualquier carácter o juegos de caracteres puede sustituir al carácter comodín.

carácter de coincidencia de patrón

Consulte comodín.

centro de datos

En un entorno virtualizado, un contenedor que contiene hosts, clústeres, redes y almacenes de datos.

clase de dispositivo

Conjunto de características con nombre que se aplica a un grupo de dispositivos de almacenamiento. Cada clase de dispositivo tiene un nombre exclusivo y representa un tipo de dispositivo específico, como un disco, un disco óptico o una cinta.

clase de gestión

Objeto de política que los usuarios pueden vincular a cada archivo para especificar el modo en que el servidor debe gestionar el archivo. La clase de gestión puede contener un grupo de copias de seguridad, un grupo de copias de archivado y atributos de gestión del espacio. Consulte también enlazar, grupo de copias, cliente de gestión de almacenamiento jerárquico, conjunto de políticas, volver a enlazar.

clase de gestión predeterminada

Clase de gestión asignada a un juego de políticas. Esta clase se utiliza para controlar las copias de seguridad o copias archivadas cuando un archivo no está explícitamente asociado con una clase de gestión específica mediante la lista de inclusión/exclusión.

clase de privilegios

Nivel de autorización concedido a un administrador. La clase de privilegios determina que tareas de administración puede realizar el administrador. Consulte también autorización, clase de privilegios de nodo, clase de privilegios del operador, clase de privilegios de política, clase de privilegio de almacenamiento, clase de privilegio del sistema.

clase de privilegios de administración

Consulte clase de privilegios.

clase de privilegios de almacenamiento

Clase de privilegios que concede al administrador autorización para controlar el modo en que se asignan y utilizan los recursos de almacenamiento del servidor, por ejemplo supervisando la base de datos, el registro de recuperación y el almacenamiento del servidor. Consulte también clase de privilegios.

clase de privilegios del sistema

Clase de privilegios que concede a un administrador autorización para emitir todos los comandos del servidor. Consulte también clase de privilegios.

clase de privilegios de nodo

Clase de privilegios que concede a un administrador autorización para acceder de forma remota a clientes de copia de seguridad/archivado de un nodo de cliente específico o de todos los clientes de un dominio de políticas. Consulte también clase de privilegios.

clase de privilegios de operador

Clase de privilegios que concede al administrador autorización para deshabilitar o detener el servidor, habilitar el mismo, cancelar procesos de éste y gestionar soportes de almacenamiento extraíbles. Consulte también clase de privilegios.

clase de privilegios de política

Clase de privilegios que permite a un administrador gestionar objetos de políticas, inscribir nodos cliente y planificar operaciones de cliente para los nodos cliente. La autorización se puede limitar a determinados dominios de políticas. Consulte también clase de privilegios.

Client Acceptor

Un servicio que sirve el applet Java™ para el cliente web a los navegadores web. En los sistemas Windows, la aceptación de clientes se instala y ejecuta como un servicio. En sistemas AIX, UNIX y Linux, la aceptación de clientes se ejecuta como un daemon.

cliente

Programa de software u ordenador que solicita servicios desde un servidor. Consulte también servidor.

cliente administrativo

Programa que se ejecuta en un servidor de archivos, una estación de trabajo o un sistema principal que los administradores utilizan para controlar y supervisar el servidor. Consulte también el cliente de archivo de copia de seguridad.

cliente de aplicación

Programa instalado en un sistema para proteger una aplicación. El servidor proporciona servicios de copia de seguridad a un cliente de aplicaciones.

cliente de biblioteca

Servidor que utiliza la comunicación servidor a servidor para acceder a una biblioteca gestionada por otro servidor de gestión de almacenamiento. Consulte también gestor de biblioteca.

cliente de copia de seguridad y archivado  
Programa que se ejecuta en un servidor de archivos o estación de trabajo y que facilita el medio para que los usuarios puedan efectuar operaciones de copia de seguridad, archivado, restauración y recuperación de archivos. Consulte también cliente administrativo.

cliente de gestión de almacenamiento jerárquico (cliente HSM)  
Programa de cliente que trabaja con el servidor para proporcionar la gestión de almacenamiento jerárquico (HSM) para un sistema. Consulte también gestión de almacenamiento jerárquico, clase de gestión.

Cliente HSM  
Consulte cliente de gestión de almacenamiento jerárquico.

cliente/servidor  
Pertenece al modelo de interacción de un proceso de datos distribuidos en el que un programa de un ordenador envía una solicitud a un programa de otro ordenador y espera una respuesta. El programa solicitante se denomina cliente; el programa que envía la respuesta se denomina servidor.

Colección de juegos de copias de seguridad  
Grupo de juegos de copias de seguridad creados a la vez y con el mismo nombre, descripción y clase de dispositivo. El servidor identifica cada juego de copias de seguridad de la colección mediante su nombre de nodo, nombre de juego y tipo de archivo.

complemento  
Un módulo de software que se puede instalar por separado y que añade funciones al programa aplicación o interfaz existente.

compresión  
Una función que elimina los caracteres repetitivos, espacios, series de caracteres o datos binario de los datos que se están procesando y reemplazan caracteres con caracteres de control. La compresión reduce la cantidad de espacio de almacenamiento que se requiere para los datos. Consulte también compresión en línea.

compresión en línea  
Un método para reducir espacio de almacenamiento. Los caracteres repetitivos, espacios, series de caracteres i datos binarios se eliminan según se van grabando datos en una agrupación de almacenamiento de contenedores. Consulte también compresión.

configuración empresarial  
Método de configuración de servidores de forma que el administrador pueda distribuir la configuración de uno de los servidores al resto utilizando la comunicación servidor a servidor. Consulte también gestor de configuración, servidor gestionado, perfil, suscripción.

conjunto de nodos GPFS  
Grupo montado y definido de sistemas de archivos GPFS.

conjunto de opciones de cliente  
Grupo de opciones definidas en el servidor y utilizadas en los nodos de cliente junto con archivos de opciones del cliente.

contenedor  
Ubicación de almacenamiento de datos, por ejemplo, un archivo, directorio o dispositivo. Consulte también agrupación de almacenamiento de contenedores.

convenio de nomenclatura universal (UNC)  
El nombre de servidor y el nombre de la red combinados. Estos nombres identifican conjuntamente el recurso en el dominio.

conversación  
Conexión entre dos programas en una sesión que les permite comunicarse durante el proceso o transacción.

copia archivada  
Archivo o grupo de archivos de los que se ha realizado copias archivadas en el servidor de almacenamiento.

copia de duplicación  
Instantánea de un volumen. La instantánea se puede realizar mientras las aplicaciones del sistema siguen grabando datos en los volúmenes.

copia de reserva  
Copia de seguridad completa en la que no se suprimen los archivos de registro de transacciones para que los procedimientos de copia de seguridad que utilizan copias de seguridad incrementales o diferenciales no se vean afectados.

copia de seguridad activada  
Copia de seguridad en la que el volumen está disponible para otras aplicaciones del sistema durante la operación.

copia de seguridad adaptable de subarchivos  
Tipo de copia de seguridad que sólo envía las partes modificadas de un archivo al servidor en lugar de enviar todo el archivo. La copia de seguridad adaptable de subarchivos reduce el tráfico de la red e incrementa la velocidad de la operación de copia de seguridad.

copia de seguridad completa  
Proceso de realizar una copia de seguridad de la base de datos de servidor completa. Cada copia de seguridad completa inicia una nueva serie de copia de seguridad de base de datos. Consulte también serie de copia de seguridad de la base de datos, instantánea de la base de datos, copia de seguridad en aumento.

copia de seguridad con registro por diario  
Método de copia de seguridad para los clientes Windows y los clientes AIX que hacen uso del mecanismo de notificación de cambio de archivo para mejorar el rendimiento de la copia de seguridad incremental reduciendo la necesidad de explorar todo el sistema de archivos.

- copia de seguridad de grupo  
Copia de seguridad de un grupo que contiene una lista de archivos de uno o más orígenes de espacio de archivos.
- copia de seguridad de imagen  
Copia de seguridad de todo un sistema de archivos o de un volumen lógico RAW como un solo objeto.
- copia de seguridad del volumen lógico  
Copia de seguridad de un sistema de archivos o volumen lógico como un único objeto.
- copia de seguridad de traspaso de datos de VSS  
Operación de copia de seguridad que utiliza un proveedor de hardware del servicio de copia de volúmenes (VSS) de Microsoft (instalado en un sistema alternativo) para mover datos al servidor. Este tipo de copia de seguridad transfiere la carga de copia de seguridad de la máquina de producción a otra máquina.
- copia de seguridad de volumen desactivado  
Copia de seguridad en la que el volumen está bloqueado para que no puedan acceder al mismo otras aplicaciones del sistema durante la operación.
- copia de seguridad difusa  
Versión de copia de seguridad de un archivo que puede no reflejar fielmente el contenido actual del archivo, debido a que se realizó la copia de seguridad del mismo a la vez que se estaba modificando.
- copia de seguridad incremental  
Proceso de copia de seguridad de archivos o directorios o de copia de páginas en la base de datos, que son nuevas o se han cambiado desde la última copia de seguridad completa o incremental. Consulte también copia de seguridad selectiva.
- copia de seguridad selectiva  
Proceso de realizar copias de seguridad de determinados archivos o directorios de un dominio de cliente. Se realiza la copia de seguridad de los archivos que no se han excluido en la lista de inclusión-exclusión. Estos archivos deben cumplir los requisitos para la serialización en el grupo de copia de seguridad de la clase de gestión asignada a cada archivo. Consulte también copia de seguridad incremental.
- Copia de seguridad VSS  
Operación de copia de seguridad que utiliza la tecnología de servicio de copia de duplicación de volúmenes (VSS) de Microsoft. La operación de copia de seguridad produce una instantánea en línea (copia coherente de instante específico). Esta copia puede almacenarse en volúmenes de duplicación local o en el almacenamiento del servidor.
- copia difusa  
Versión de copia de seguridad o copia archivada de un archivo que puede no reflejar con total exactitud el contenido original del archivo, puesto que la copia de seguridad o archivado se ha realizado mientras el archivo se estaba modificando.
- cuota
  1. Para HSM en sistemas AIX, UNIX o Linux, el límite (en megabytes) sobre la cantidad de datos que se pueden migrar y los pre-migrados desde un sistema de archivos a un almacenamiento del servidor.
  2. Para HSM en los sistemas Windows, un límite definido por el usuario al espacio que ocupan los archivos recuperados.

## D

---

- daemon  
Programa que se ejecuta de forma desatendida para realizar funciones continuas o periódicas como el control de red.
- daemon de aceptación de clientes (CAD)  
Consulte aceptación de clientes.
- daemon de registro por diario  
En sistemas AIX, UNIX, o Linux, programa que realiza el seguimiento de las actividades de cambio en archivos que residen en sistemas de archivos.
- daemon de supervisión de espacio  
Daemon que comprueba la utilización del espacio de todos los sistemas de archivos para los que está activa la gestión de espacio y empieza automáticamente la migración por umbral cuando la utilización del espacio de un sistema de archivos iguala o supera su umbral superior.
- datos iniciales  
Bytes de datos iniciales de un archivo migrado que se almacenan en el archivo de resguardo correspondiente en el sistema de archivos local. La cantidad de datos iniciales que se almacenan en un archivo de resguardo depende del tamaño de apéndice especificado.
- deduplicación de datos de postproceso  
Método de reducción de necesidades de almacenamiento eliminando datos redundantes. Primero los datos se graban en la agrupación de almacenamiento, los datos duplicados se identifican y, a continuación, se reclama espacio en la agrupación de almacenamiento. Consulte también deduplicación de datos, deduplicación de datos en línea.
- deduplicación de datos en línea  
Método de reducción de necesidades de almacenamiento eliminando datos redundantes. Los datos se deduplican a medida que se graban en la agrupación de almacenamiento de contenedores. Consulte también deduplicación de datos, deduplicación de datos de postproceso.
- destinatario

Repositorio del servidor que contiene un registro de mensajes del servidor y el cliente como eventos. Por ejemplo, un receptor puede ser una salida de archivo, una salida de usuarios o la consola del servidor y un registro de actividad. Consulte también evento.

destino

Atributo de grupo de copias o clase de gestión que especifica la agrupación de almacenamiento primaria en la que se realizará la copia de seguridad, archivado o migración del archivo cliente. Consulte también grupo de almacenamiento de copias.

detección automática

Característica que detecta, envía informes y actualiza el número de serie de una unidad o biblioteca de la base de datos cuando se define la ruta del servidor local.

dirección IP

Una dirección exclusiva para un dispositivo o una unidad lógica en una red que utiliza el estándar del protocolo de Internet.

dominio

Agrupación de nodos de cliente con uno o varios conjuntos de políticas que gestiona datos o recursos de almacenamiento para los nodos de cliente. Consulte también dominio de la política.

dominio de cliente

Conjunto de unidades, sistemas de archivos o volúmenes que un usuario selecciona para efectuar la operación de copia de seguridad o de archivado con el cliente de copia de seguridad/archivado.

dominio de políticas

Agrupación de usuarios de políticas con uno o varios conjuntos de políticas que gestiona datos o recursos de almacenamiento para los usuarios. Los usuarios son nodos de cliente asociados con el dominio de políticas. Consulte también conjunto de políticas activas, dominio.

DRM

Consulte gestor recuperación ante siniestro.

DSMAPI

Consulte interfaz de programación de aplicaciones de gestión de almacenamiento de datos.

duplicación

Proceso de grabar los mismos datos en varios discos al mismo tiempo. La duplicación de datos protege los datos de su pérdida en la base de datos o en el registro de recuperación.

## E

---

EA

Consulte atributo ampliado.

EB

Consulte exabyte.

EFS

Consulte Sistema de archivos de cifrado.

eliminación de datos duplicados

Método de reducción de necesidades de almacenamiento eliminando datos redundantes. Sólo una instancia de los datos queda retenida en medios de almacenamiento. Otras instancias de los mismos datos son reemplazadas con un puntero a la instancia retenida. Consulte también deduplicación de datos en línea, deduplicación de datos de postproceso.

espacio de archivos

Espacio lógico de un almacenamiento de servidor que contiene un grupo de archivos de los que un nodo de cliente ha realizado una copia de seguridad o archivado desde una partición lógica individual, sistema de archivos o punto de montaje virtual. Los nodos de cliente pueden restaurar, recuperar o eliminar sus espacios de archivo del almacenamiento del servidor. En almacenamiento del servidor, los archivos pertenecientes a un espacio de archivos individual no se almacenan necesariamente juntos.

espacio de archivos activado para Unicode

Un espacio de archivos con un nombre que sigue el estándar de Unicode y es compatible con cualquier entorno local en estaciones de trabajo multilingües.

espacio de archivos estabilizado

Espacio de archivos que existe en el servidor pero no en el cliente.

espacio de archivos virtual

Representación de un directorio de un sistema de archivos NAS (almacenamiento conectado a red) como ruta a dicho directorio.

estación de trabajo

Un terminal o sistema personal en el que un usuario puede ejecutar aplicaciones y que a menudo está conectado a un sistema principal o red.

estado de archivo

Modalidad de gestión de espacio de un archivo que reside en un sistema de archivos al que se ha agregado la gestión de espacios. El estado de un archivo puede ser: residente, premigrado o migrado. Consulte también archivo migrado, archivo migrado previamente, archivo residente.

estado de sistema de archivos

Modalidad de gestión del almacenamiento de un sistema de archivos que reside en una estación de trabajo en que se ha instalado un cliente de gestión de almacenamiento jerárquica (HSM). El estado de un sistema de archivos puede ser: nativo,

activo, inactivo o inactivo global.

estado inactivo global  
Estado de todos los sistemas de archivos a los que se ha agregado gestión de espacio cuando ésta se desactiva globalmente para un nodo cliente.

evento  
Aparición de importancia para una tarea o un sistema. Los sucesos pueden incluir la finalización o la anomalía de una operación, una acción de usuario, o el cambio de estado de un proceso. Consulte también anotación empresarial, receptor.

exabyte (EB)  
Para el procesador, las capacidades de almacenamiento real y virtual y el volumen del canal, 2 a la potencia de 60 o 1 152 921 504 606 846 976 bytes. En la capacidad de almacenamiento de disco y el volumen de comunicaciones, 1 000 000 000 000 000 000 bytes.

excluir  
Proceso de identificar archivos de una lista de inclusión-exclusión. Este proceso impide que se obtenga copia de seguridad de los archivos o se migren cuando un usuario o una planificación inicien una operación de copia incremental o selectiva. Un archivo puede excluirse de la copia de seguridad, de un gestor de espacio o de la copia de seguridad o del gestor de espacio.

extensión  
Parte de un archivo que se crea durante el proceso de eliminación de duplicados de datos. Las extensiones se comparan con otras extensiones de archivo para identificar duplicados.

## F

---

formato de datos no nativo  
Formato de datos grabado en una agrupación de almacenamiento que difiere del formato utilizado por el servidor en las operaciones. Consulte también formato nativo.

formato nativo  
Formato de datos que se escribe en un grupo de almacenamiento directamente mediante el servidor. Consulte también formato de datos no nativos.

frecuencia  
Atributo de grupo de copia que especifica el intervalo mínimo, en días, que ha de transcurrir entre copias de seguridad incrementales.

FSID  
Consulte ID de espacio de archivos.

FSM  
Consulte migrador de sistema de archivos.

## G

---

GB  
Consulte gigabyte.

generación de contraseñas  
Proceso que crea y almacena una nueva contraseña en un archivo de contraseñas cifrado cuando caduca la anterior. La generación automática de una contraseña evita que se solicite una contraseña.

General Parallel File System (GPFS)  
Sistema de archivos de disco compartido de alto rendimiento que puede proporcionar acceso de datos desde nodos de un entorno de sistema en clúster. Consulte también gestión del ciclo de vida de información.

gestión de almacenamiento jerárquico (HSM)  
Función que distribuye y gestiona automáticamente datos de un disco, cinta o ambos considerando los dispositivos de este tipo y potencialmente de otros como niveles de una jerarquía de almacenamiento que comprende desde dispositivos rápidos y caros a dispositivos más lentos, baratos y quizá extraíbles. Los objetivos son minimizar el tiempo de acceso a los datos y maximizar la capacidad de medios disponible. Consulte también cliente de gestión de almacenamiento jerárquico, volver a llamar, jerarquía de almacenamiento.

gestión de espacio  
Consulte gestión de almacenamiento jerárquico.

gestión del ciclo de vida de la información (ILM)  
Sistema de gestión de archivos basado en políticas para grupos de almacenamiento y conjuntos de archivos. Consulte también General Parallel File System.

gestor de biblioteca  
Servidor que controla las operaciones de dispositivos cuando diversos servidores de gestión de almacenamiento comparten un dispositivo de almacenamiento. Consulte también cliente de biblioteca.

gestor de configuración  
Servidor que distribuye información de configuración como políticas y planificaciones a servidores gestionados de acuerdo con sus perfiles. La información de configuración puede incluir políticas y planificaciones. Consulte también configuración empresarial, servidor gestionado, perfil.

gestor de recuperación de desastres (DRM)



Función que ofrece asistencia en la preparación y utilización de un archivo de plan de recuperación ante siniestro al servidor.  
gigabyte (GB)

En el almacenamiento de procesador, almacenamiento real y almacenamiento virtual y el volumen de canal, dos elevado a la potencia de 30 o 1.073.741.824 bytes. Para capacidad de almacenamiento de disco y volumen de comunicaciones, 1.000.000.000 bytes.

GPFS

Consulte General Parallel File System.

grupo

Contenedor de almacenamiento en la nube utilizado por Amazon Simple Storage Service (Amazon S3).

grupo de copia

Objeto de políticas que contiene atributos que controlan cómo se generan las versiones de copias de seguridad o copias archivadas, el lugar donde deben ubicarse inicialmente y cuándo deben caducar. Un grupo de copias pertenece a una clase de gestión. Consulte también grupo de copias archivadas, grupo de copias de seguridad, versión de copia de seguridad, clase de gestión.

grupo de copias de archivado

Objeto de política que contiene atributos que controlan la generación, el destino y la caducidad de copias archivadas. Consulte también copiar grupo.

grupo de copias de seguridad

Objeto de política que contiene atributos que controlan la generación, destino y caducidad de archivos de copia de seguridad. Un grupo de copias pertenece a una clase de gestión. Consulte también copiar grupo.

grupo de políticas

Grupo de reglas de un dominio de políticas. Las reglas especifican la forma en que los datos o los recursos de almacenamiento se gestionan automáticamente en los nodos cliente de un dominio de políticas. Las reglas pueden aparecer en clases de gestión. Consulte también conjunto de políticas activas, clase de gestión.

grupo de políticas activas

Juego de políticas activado que contiene las reglas de políticas que utilizan actualmente todos los nodos cliente asignados al dominio de políticas. Consulte también dominio de la política, conjunto de políticas.

grupo de proximidad

Grupo de nodos cliente definido por el usuario cuyos datos se almacenan en un número mínimo de volúmenes a través del proceso de proximidad.

GUID

Consulte identificador exclusivo global.

## H

---

hora de acceso a archivo

Para sistemas AIX, UNIX, o Linux, hora a la que se accedió por última vez al archivo.

HSM

Consulte gestión de almacenamiento jerárquico.

## I

---

ID de espacio de archivos (FSID)

Identificador numérico único que el servidor asigna a un espacio de archivos cuando éste se guarda en el almacenamiento del servidor.

identificador exclusivo global (GUID)

Número determinado algorítmicamente que identifica de forma única una entidad de un sistema. Consulte también Identificador exclusivo universal.

identificador exclusivo universal (UUID)

Identificador numérico de 128 bits utilizado para garantizar que dos componentes no tengan el mismo identificador. Consulte también identificador exclusivo global.

ILM

Consulte gestión del ciclo de vida de la información.

imagen

Sistema de archivos o volumen lógico RAW del que se realiza una copia de seguridad en un objeto individual.

inodo

La estructura interna que describe los archivos individuales de sistemas AIX, UNIX, o Linux. Un inodo contiene el nodo, tipo, propietario y ubicación de un archivo.

inscripción abierta

Proceso de inscripción en el que los usuarios pueden inscribir en el servidor sus propias estaciones de trabajo como nodos cliente. Consulte también registro cerrado.

inscripción cerrada

Proceso de inscripción en que un administrador inscribe las estaciones de trabajo como nodos de cliente con el servidor. Consulte también registro abierto.

instantánea

Un tipo de instantánea que consiste en una vista de un instante específico de un volumen.

instantánea de base de datos

Copia de seguridad completa de toda la base de datos a un soporte que se pueda llevar a otro lugar. Cuando se crea una instantánea de base de datos, la serie de copia de seguridad de base de datos actual no se interrumpe. Las instantáneas de bases de datos no pueden tener copias de seguridad de bases de datos incrementales asociadas. Consulte también serie de copia de seguridad de la base de datos, copia de seguridad completa.

interfaz de programación de aplicaciones de gestión de almacenamiento de datos (DSMAPI)

Conjunto de funciones y semántica que supervisa eventos en archivos y gestiona y mantiene los datos de un archivo. En un entorno de HSM, una DSMAPI utiliza los eventos para notificar a las aplicaciones de gestión de datos acerca de las operaciones realizadas en los archivos, almacena información de atributos arbitraria de un archivo, admite regiones gestionadas de un archivo y utiliza los derechos de acceso de DSMAPI para controlar el acceso a un objeto de archivo.

intervalo de inicio

Periodo de tiempo durante el que debe iniciarse una planificación.

## J

---

jerarquía de almacenamiento

Orden lógico de las agrupaciones de almacenamiento primario, definido por el administrador. Normalmente, el orden se basa en la velocidad y capacidad de los dispositivos utilizados por las agrupaciones de almacenamiento. La jerarquía de almacenamiento se define identificando la siguiente agrupación de almacenamiento en una definición de agrupaciones de almacenamiento. Consulte también agrupación de almacenamiento.

juego de copias de seguridad

Un grupo consolidado y portable de versiones activas de archivos de copia de seguridad que se generan para un cliente de copia de seguridad/archivado.

## K

---

KB

Consulte kilobyte.

kilobyte (KB)

En almacenamiento de procesador, almacenamiento real y virtual y volumen de canal, 2 elevado a la décima potencia, o 1.024 bytes. Para capacidad de almacenamiento de disco y volumen de comunicaciones, 1.000 bytes.

## L

---

LAN

Consulte red de área local.

límite de montajes

Número máximo de volúmenes a los que se puede acceder simultáneamente desde la misma clase de dispositivo. El límite de montajes determina el número máximo de puntos de montaje. Consulte también punto de montaje.

lista de control de accesos (ACL)

En la seguridad del sistema, lista asociada a un objeto que identifica todos los temas que pueden acceder al objeto y a sus derechos de acceso.

lista de exclusión/inclusión

Consulte lista de inclusión/exclusión.

lista de inclusión/exclusión

Lista de opciones que incluye o excluye los archivos seleccionados para la copia de seguridad. Una opción excluye identifica los archivos de los que no se debe realizar copia. Una opción de inclusión identifica los archivos que están exentos de las reglas de exclusión o asigna una clase de gestión a un archivo o grupo de archivos, para los servicios de copia de seguridad o archivado. Consulte también incluir-excluir archivo.

local

1. Perteneciente a un dispositivo, archivo o sistema al que se accede directamente desde un sistema de usuario, sin utilizar una línea de comunicación.
2. Para los productos de gestión de almacenamiento jerárquico, relacionados con el destino de archivos migrados que se están moviendo. Consulte también remoto.

LOFS

Consulte sistema de archivos virtuales loopback.

Logical Volume Snapshot Agent (LVSA)

Software que puede actuar como el proveedor de instantáneas para crear una instantánea de un volumen lógico durante una copia de seguridad de imagen en línea.

LUN

Consulte número de unidad lógica.

LVSA

Consulte Agente de instantáneas de volúmenes lógicos.

## M

---

MB

Consulte megabyte.

megabyte (MB)

En el almacenamiento de procesador, el almacenamiento real y el volumen de canal, 2 a la potencia de 20 o 1.048.576 bytes. En capacidad de almacenamiento de disco y volúmenes de comunicaciones, 1.000.000 bytes.

metadatos

Datos que describen las características de los datos; datos descriptivos.

método de comunicación

Método mediante el cual intercambian información un cliente y un servidor. Consulte también Transmission Control Protocol/Internet Protocol.

migración

El proceso de mover datos de un sistema de computadora a otro, o una aplicación a otro sistema de computadora.

migración a petición

Proceso que se utiliza para responder a una situación de falta de espacio en un sistema de archivos en el que está activa la gestión de almacenamiento jerárquico (HSM). Los archivos se migran al almacenamiento del servidor hasta que el porcentaje de utilización de espacio alcanza el umbral inferior que se ha establecido para el sistema de archivos. Si los umbrales superior e inferior son iguales, se migra un archivo. Consulte también migración automática, migración selectiva, migración de umbral.

migración automática

Proceso utilizado para traspasar automáticamente archivos desde un sistema de archivos local al almacenamiento, basándose en las opciones y valores que ha escogido un usuario root en la estación de trabajo. Consulte también migración de demandas, migración de umbral.

migración por umbral

El proceso de mover archivos de un sistema de archivos local a un almacenamiento de servidor basado en los umbrales bajo y alto que se definen para el sistema de archivos. Consulte también migración automática, migración de demanda, trabajo de migración, migración selectiva.

migración por umbral

Capacidad inferior y superior de las agrupaciones de almacenamiento o sistemas de archivos, expresada en porcentajes, en las que debe iniciarse y detenerse la migración.

migración selectiva

Proceso de copiar archivos seleccionados por el usuario desde un sistema de archivos local a un almacenamiento del servidor y reemplazar los nuevos archivos con archivos de resguardo en el sistema de archivos local. Consulte también migración de demandas, migración de umbral.

migrador de sistema de archivos (FSM)

Extensión de kernel que intercepta todas las operaciones de sistema de archivos y proporciona la gestión de espacio necesaria. Si no se requiere soporte de gestión del espacio, la operación se envía al sistema operativo, que realiza sus funciones normales. El migrador del sistema de archivos se monta sobre un sistema de archivos al agregar gestión de espacio al sistema de archivos.

migrar

Para mover los datos a otra ubicación o una aplicación a otro sistema de computadora.

modalidad

Atributo de grupo de copia que especifica si se debe realizar la copia de seguridad de un archivo que no se ha modificado desde la última copia de seguridad que se realizó. Consulte también modalidad absoluta, modalidad modificada.

modalidad Absoluta

En gestión de almacenamiento, modalidad de grupo de copia de seguridad que indica que un archivo o directorio se tendrán en cuenta para realizar la copia de seguridad incremental aunque el archivo o directorio no se hayan modificado desde la última operación de copia de seguridad. Consulte también modalidad, modalidad modificada.

modalidad de acceso

Atributo de una agrupación o volumen de almacenamiento que especifica si el servidor puede escribir o leer la agrupación o volumen de almacenamiento.

modalidad de planificación

Tipo de operación de planificación para el nodo del servidor y cliente que admite dos modalidades de planificación: sondeo de clientes y por petición de servidor.

modalidad de planificación de sondeo de clientes

Método de operación en el que el cliente solicita trabajo al servidor. Consulte también modalidad de planificación de indicación del servidor.

modalidad de planificación por petición de servidor

Técnica de comunicaciones entre el cliente y el servidor donde el servidor se pone en contacto con el nodo cliente cuando se tienen que realizar tareas. Consulte también modalidad de planificación de sondeo de clientes.

modalidad de recuperación de archivo parcial

Modalidad de recuperación que hace que la función de gestión de almacenamiento jerárquico (HSM) lea sólo una porción de un archivo migrado del almacenamiento, según lo requiera la aplicación que accede al archivo.

#### modalidad Modificados

En gestión de almacenamiento, modalidad de grupo de copia de seguridad que indica que un archivo o directorio se tendrá en cuenta para realizar la copia de seguridad incremental aunque el archivo no se haya modificado desde la última operación de copia de seguridad. Un archivo o directorio se considera modificado si ha cambiado la fecha, el tamaño, el propietario o los permisos. Consulte también modalidad absoluta, modalidad.

#### MTU

Consulte unidad de transmisión máxima.

## N

---

#### named pipe

Tipo de comunicación entre procesos que permite que las corrientes de datos de los mensajes pasen entre los procesos de igual a igual, como sucede entre un cliente y un servidor.

#### NDMP

Consulte Network Data Management Protocol.

#### NetBIOS (Network Basic Input/Output System)

Interfaz estándar de redes y ordenadores personales que se utiliza en redes de área local para proporcionar mensajes y funciones de servidor de impresión y servidor de archivos. Los programas de aplicación que utilizan NetBIOS no tienen que manejar los detalles de protocolos LAN Data link control (DLC).

#### Network Basic Input/Output System

Consulte NetBIOS.

#### Network Data Management Protocol (NDMP)

Protocolo que permite a una aplicación de gestión de almacenamiento de red controlar las operaciones de copia de seguridad y recuperación de un servidor de archivos NDMP, sin instalar software del proveedor en ese servidor de archivos.

#### nodo

Servidor de archivos o estación de trabajo donde está instalado el programa cliente de copia de seguridad/archivado, que se ha registrado en el servidor.

#### Nodo agente

Nodo cliente al que se ha otorgado autorización proxy para realizar operaciones en nombre de otro nodo cliente, que es el nodo de destino.

#### nodo cliente

Servidor de archivos o estación de trabajo donde está instalado el programa cliente de copia de seguridad/archivado, que se ha registrado en el servidor.

#### nodo de destino

Nodo cliente para el que otros nodos cliente (denominados nodos agente) han recibido autorización de proxy. La autorización de proxy permite a los nodos cliente realizar operaciones de copia de seguridad y de restauración en nombre del nodo de destino, que es propietario de los datos.

#### nodo del servidor de archivo NAS

Consulte el nodo NAS.

#### nodo NAS

Un nodo de cliente es un servidor de archivos de almacenamiento conectado a red (NAS). Los datos de los nodos NAS se transfieren mediante un servidor de archivos NAS controlado por el Network data management protocol (NDMP). Los nodos NAS reciben también el nombre de nodo de servidor de archivos NAS.

#### nombre de ámbito mundial (WWN)

Identificador de nombre sin firma de 64 bits exclusivo.

#### nombre del nodo

Nombre exclusivo que se utiliza para identificar una estación de trabajo, servidor de archivos o PC en el servidor.

#### número de inodo

Número que especifica un archivo de inodo particular del sistema de archivos.

#### número de unidad lógica (LUN)

En el estándar SCSI (interfaz para pequeños sistemas), se utiliza un identificador exclusivo para diferenciar dispositivos, cada uno de los cuales es una unidad lógica (LU).

## O

---

#### objeto de marca de archivo borrado

Pequeño subconjunto de atributos de un objeto suprimido. El objeto de marca de archivo borrado se retiene durante un periodo específico, y al final de ese periodo específico, se suprime de forma permanente.

#### objeto gestionado

Definición de la base de datos del servidor gestionado que un gestor de configuración ha distribuido al servidor gestionado. Cuando un servidor gestionado se suscribe a un perfil, todos los objetos asociados con dicho perfil pasan a ser objetos gestionados en la base de datos del servidor gestionado.

#### ocupación física

Cantidad de espacio utilizado por archivos físicos en una agrupación de almacenamiento. Este espacio incluye el espacio sin utilizar que se crea cuando se suprimen archivos lógicos de agregados. Consulte también archivo lógico, ocupación lógica, archivo físico.

#### ocupación lógica

Espacio utilizado por archivos lógicos en una agrupación de almacenamiento. Este espacio no incluye el espacio sin utilizar creado al suprimir archivos lógicos de archivos agregados, por lo que puede ser inferior a la ocupación física. Consulte también ocupación física.

#### optimización de almacenamiento

Consulte deduplicación de datos.

## P

---

#### página

Unidad de espacio definida de un soporte de almacenamiento o volumen de base de datos.

#### paquete

En la comunicación de datos, secuencia de dígitos binarios, incluidos los datos y las señales de control, que se transmite y conmuta como un todo compuesto.

#### partición de carga de trabajo (WPAR)

Partición en una única instancia del sistema operativo.

#### perfil

Grupo de información de configuración con nombre que se puede distribuir desde un gestor de configuración a suscribir un servidor gestionado. La información de configuración puede incluir diversos ID de administrador registrados, políticas, planificaciones de clientes, juegos de opciones de clientes, planificaciones administrativas, scripts de comandos de gestores de almacenamiento, definiciones de servidores y definiciones de grupos de servidores. Consulte también gestor de configuración, configuración empresarial, servidor gestionado.

#### periodo de espera de montaje

Número máximo de minutos que el servidor espera por una solicitud de montaje de un volumen de acceso secuencial antes de cancelar la solicitud.

#### período de gracia de retención de copia de seguridad

Número de días que el gestor de almacenamiento conserva una versión de copia de seguridad cuando el servidor no puede volver a vincular el archivo a una clase de gestión apropiada.

#### período de gracia de retención de copias archivadas

Número de días que el gestor de almacenamiento retiene una copia archivada cuando el servidor no puede volver a vincular el archivo a una clase de gestión apropiada. Consulte también vincular.

#### periodo de retención de montaje

Número máximo de minutos que el servidor retiene un volumen de medio de acceso secuencial montado que no está en uso antes de desmontarlo.

#### plan de recuperación ante siniestro

Archivo que se crea mediante el gestor de recuperación de desastres (DRM) que contiene información sobre cómo recuperar sistemas de computadora si ocurre un desastre y scripts que se pueden ejecutar para realizar algunas tareas de recuperación. El archivo incluye información sobre el software y hardware utilizado por el servidor y la ubicación del soporte de recuperación.

#### planificación

Registro de base de datos que describe las operaciones del cliente o comandos de administración que se van a procesar. Consulte también planificación de comandos de administración, planificación de clientes.

#### planificación de cliente

Registro de base de datos que describe el proceso planificado de una operación del cliente durante un periodo de tiempo específico. La operación del cliente puede ser una copia de seguridad, archivado, restauración, recuperación, un comando de sistema operativo del cliente o una macro. Consulte también planificación de mandatos administrativos, planificador central, planificación.

#### planificación de comandos de administración

Registro de base de datos que describe el proceso planificado de un comando administrativo durante un periodo de tiempo específico. Consulte también programador central, programa central, programa.

#### planificador central

Función que permite a un administrador planificar operaciones de cliente y comandos de administración. Las operaciones pueden planificarse para que tengan lugar de forma periódica o en una fecha específica. Consulte también planificación de comandos de administración, planificación de clientes.

#### porcentaje de premigración

Valor establecido para la gestión de espacio que controla si los siguientes candidatos elegibles de un sistema de archivos se premigran durante la migración por umbral o la migración a petición.

#### prefijo de volumen de cinta

Cualificador de alto nivel del nombre de archivo o el nombre del conjunto de datos de la etiqueta de la cinta estándar.

#### pre migración

Proceso de copia de archivos que son elegibles para migración al almacenamiento del servidor, pero dejando el archivo original intacto en el sistema de archivos local.

protocolo de comunicación

Conjunto de interfaces definidas que permite a los sistemas comunicarse entre sí.

proximidad

Proceso mediante el que se mantienen todos los datos que pertenecen a un único espacio de archivos de cliente, a un único nodo cliente o a un grupo de nodos cliente en un número mínimo de volúmenes de acceso secuencial de una agrupación de almacenamiento. La proximidad puede reducir el número de volúmenes a los que se debe acceder cuando es necesario restaurar un gran volumen de datos.

punto de montaje

Unidad lógica por la que se accede a los volúmenes en una clase de dispositivo de acceso secuencial. En tipos de dispositivos de medios extraíbles, como una cinta, un punto de montaje es una unidad lógica asociada a una unidad física. En el tipo de dispositivo de archivos, un punto de montaje es una unidad lógica asociada con una corriente de E/S. Consulte también límite de montajes.

punto de montaje virtual

Una ramificación de un directorio de un sistema de archivos que se define como el sistema de archivos virtuales. El sistema de archivos virtuales crea una copia de seguridad en su propio espacio de archivos en el servidor. El servidor procesa el punto de montaje virtual como un sistema de archivos por separado, pero el sistema operativo del cliente no lo hace así.

punto de validación

Un punto en el tiempo cuando los datos se consideran coherentes.

## R

---

reclamación

Proceso de consolidar los datos restantes de muchos volúmenes de acceso secuencial en menos volúmenes de acceso secuencial.

reconciliación

Proceso para asegurar la coherencia entre el repositorio de datos original y el sistema de mayor tamaño donde se almacenan los datos para la copia de seguridad. Los servidores de almacenamiento u otros sistemas de almacenamiento son ejemplos de sistemas de mayor tamaño donde se almacenan los datos para la copia de seguridad. Durante el proceso de reconciliación, se eliminan los datos que se han identificado como ya no necesarios.

recuperación

Para copiar un archivo migrado desde un almacenamiento del servidor de vuelta a su sistema de archivos de origen usando el cliente de gestión de almacenamiento jerárquico. Consulte también recuperación selectiva.

recuperación selectiva

Proceso de copiar los archivos seleccionados por el usuario desde un almacenamiento del servidor a un sistema de archivos local. Consulte también recuperación, recuperación transparente.

recuperación transparente

El proceso que se utiliza para recuperar automáticamente un archivo migrado a una estación de trabajo o servidor de archivos cuando se accede al archivo. Consulte también recuperación selectiva.

recuperar

Copiar información archivada de la agrupación de almacenamiento en la estación de trabajo para su uso. La operación de recuperación no afecta a la versión archivada en la agrupación de almacenamiento. Consulte también archivar.

red de área de almacenamiento (SAN)

Red de almacenamiento dedicada adaptada a un entorno específico, que combina servidores, sistemas, productos de almacenamiento, productos de red, software y servicios.

red de área local (LAN)

Red que conecta diversos dispositivos en un área limitada (un edificio o campus, por ejemplo) y que se puede conectar a una red mayor.

registrar

Definir un nodo cliente o ID de administrador que pueda acceder al servidor.

registro

Repositorio que contiene información de acceso y configuración sobre usuarios, sistemas y software.

registro de actividades

Registro que registra los mensajes de actividad normal generados por el servidor. Estos mensajes contienen información relativa a las operaciones del servidor y de los clientes, como por ejemplo, la hora de inicio de las sesiones o errores de E/S de dispositivos.

registro de eventos

Registro de base de datos que describe el estado actual y los resultados de eventos.

registro de recuperación

Registro de actualizaciones que están a punto de grabarse en las bases de datos. Se puede utilizar este registro para realizar recuperaciones tras errores del sistema y de los soportes. El registro de recuperación está compuesto por el registro activo (incluyendo el duplicado del registro) y los registros de archivado.

regla de autenticación

Especificación que permite a otro usuario restaurar o recuperar archivos del almacenamiento.

remoto  
Para los productos de gestión de almacenamiento jerárquico, relacionados con el origen de archivos migrados que se están moviendo. Consulte también local.

rendimiento  
En gestión de almacenamiento, los bytes totales de la carga de trabajo, excluyendo la sobrecarga, de los que se realiza la copia de seguridad o restauración, divididos por el tiempo transcurrido.

resguardo  
Acceso directo en el sistema de archivos Windows generado por el cliente de gestión de almacenamiento jerárquico (HSM) para un archivo migrado que permite el acceso transparente por parte de los usuarios. Un resguardo es la representación como archivo disperso de un archivo migrado, con un punto de reanálisis adjunto.

restauración  
Copiar información desde la ubicación de la copia de seguridad a la ubicación del almacenamiento activo para su uso. Por ejemplo, copiar información del almacenamiento del servidor a una estación de trabajo del cliente.

restauración de buzón  
Función que restaura datos de Microsoft Exchange Server (de copias de seguridad de IBM Data Protection for Microsoft Exchange) a nivel del buzón o elemento de buzón.

restauración de buzón individual  
Consulte restauración de buzón.

Restauración instantánea VSS  
Operación que restaura datos de una instantánea local. La instantánea de la copia de seguridad de VSS que reside en un volumen de duplicación local. La operación de restauración recupera los datos al utilizar un método de restauración asistido por medio de hardware (por ejemplo, una operación de FlashCopy).

Restauración rápida VSS  
Operación que restaura datos de una instantánea local. La instantánea de la copia de seguridad de VSS que reside en un volumen de duplicación local. La operación de restauración recupera los datos utilizando un método de copia a nivel de archivo.

Restauración VSS Restauraciones VSS restauraciones VSS  
Función que utiliza un proveedor de software del servicio de copia de volúmenes (VSS) de Microsoft para restaurar instantáneas que residen en el almacenamiento del servidor. Las instancias las crearon una copia de seguridad de VSS y se almacenan en su ubicación original.

retención  
El espacio de tiempo, en días, que se conservarán en la agrupación de almacenamiento las copias de seguridad o copias archivadas inactivas antes de ser eliminadas. Los atributos de grupo de copia y los periodos de gracia predeterminados de retención correspondientes al dominio definen la retención.

revincular  
Asociar todas las versiones de copia de seguridad de un archivo con un nuevo nombre de clase de gestión. Por ejemplo, un archivo que tiene una versión de copia de seguridad activa se revincula cuando se realiza una copia de seguridad de una versión posterior del archivo file con una asociación de clase de gestión distinta. Consulte también enlazar, clase de gestión.

rol de autorización  
Especificación que permite a otro usuario restaurar o recuperar los archivos de un usuario del almacenamiento.

ruta  
Objeto que define una relación uno a uno entre una fuente y un destino. A través de la ruta, la fuente accede al destino. Los datos se puede mover de la fuente al destino y viceversa. Un ejemplo de fuente es una transportador de datos (por ejemplo un servidor de archivos de almacenamiento conectado a red (NAS)), y un ejemplo de destino es una unidad de cintas.

## S

---

SAN  
Consulte red de área de almacenamiento.

script  
Serie de comandos, combinados en un archivo, que desempeñan una función determinada cuando se ejecuta el archivo. Los scripts se interpretan cuando se ejecutan. Consulte también el script del mandato IBM Spectrum Protect.

Script de comandos de IBM Spectrum Protect  
Secuencia de comandos de administración de IBM Spectrum Protect que se restauran en la base de datos del servidor de IBM Spectrum Protect. El script se puede ejecutar desde cualquier interfaz del servidor. El script puede incluir la sustitución de parámetros de comandos y lógica condicional. Consulte también el script del archivo de macro.

sección  
Grupo de líneas de un archivo que, conjuntamente, tienen una función común o definen una parte del sistema. Las stanzas se suelen separar mediante líneas en blanco o caracteres de dos puntos, y cada una tiene un nombre.

Secure Sockets Layer (SSL)  
Protocolo de seguridad que proporciona privacidad de comunicación. Con SSL, las aplicaciones cliente/servidor se pueden comunicar de una forma diseñada para evitar escuchas, sabotajes y falsificación de mensajes.

serialización

Proceso de manipular archivos modificados durante el proceso de copia de seguridad o archivado. Consulte también serialización dinámica compartida, serialización estática compartida, serialización estática.

#### serialización dinámica

Serialización de copias en la cual a un archivo o carpeta se le realiza una copia de seguridad o se archiva en el primer intento sin importar si cambia durante la copia de seguridad o archivado. Consulte también serialización dinámica compartida, serialización estática compartida, serialización estática.

#### serialización dinámica compartida

Valor para la serialización que especifica de qué archivo no debe realizarse copia de seguridad o archivado si éste está siendo modificado durante la operación. El cliente del archivo de copia de seguridad vuelve a intentar realizar la copia de seguridad o la operación de archivado varias veces; si el archivo está siendo modificado durante cada intento, el cliente del archivo de copia de seguridad realizará la copia de seguridad o archivará el archivo en su último intento. Consulte también serialización dinámica, serialización, serialización estática compartida, serialización estática.

#### serialización estática

Valor de serialización de grupo de copia que especifica que no se debe modificar un archivo durante una operación de copia de seguridad o archivado. Si el archivo está en uso durante el primer intento, el cliente de archivo de copia de seguridad no puede realizar la copia de seguridad ni archivar el archivo. Consulte también serialización dinámica, serialización, serialización dinámica compartida, serialización estática compartida.

#### serialización estática compartida

Valor de serialización de grupo de copia que especifica que no se debe modificar un archivo durante una operación de copia de seguridad o archivado. El cliente intenta volver a probar la operación varias veces. Si el archivo está siendo utilizado durante los reintentos, no se llevará a cabo la operación de copia de seguridad o archivado. Consulte también serialización dinámica, serialización, serialización dinámica compartida, serialización estática.

#### serie de copia de seguridad de base de datos

Copia de seguridad completa de la base de datos, más un máximo de 32 copias de seguridad incrementales realizadas tras dicha copia de seguridad completa. Cada copia de seguridad completa que se ejecuta inicia una nueva serie de copia de seguridad de base de datos. Cada serie se identifica con un número. Consulte también la instantánea de la base de datos, copia de seguridad completa.

#### servicio de diario

En Microsoft Windows, programa que realiza el seguimiento de las actividades de cambio de archivos que residen en sistemas de archivos.

#### Servicio de duplicación de volúmenes (VSS)

Conjunto de interfaces de programas de aplicación (API) de Microsoft que se utilizan para crear copias de seguridad de duplicación de volúmenes, copias exactas de archivos, incluidos todos los archivos abiertos, etc.

#### servidor

Programa de software o sistema que proporciona servicios a otros programas de software o sistemas. Consulte también cliente.

#### servidor de archivos

Sistema dedicado y sus dispositivos de almacenamiento periféricos conectados a una red de área local que almacena tanto programas como archivos compartidos por los usuarios en la red.

#### servidor de archivos de almacenamiento conectados a la red (servidor de archivos NAS)

Dispositivo de almacenamiento dedicado con un sistema operativo optimizado para funciones de servicio de archivos. Los servidores de archivos NAS pueden tener las características de un nodo y un transportador de datos.

#### servidor de archivos NAS

Consulte también servidor.

#### servidor de eventos

Servidor al que otros servidores pueden enviar eventos para su registro. El servidor de eventos conduce los eventos a todos los receptores designados habilitados para el envío de eventos.

#### servidor de medios

En un entorno de z/OS, programa que proporciona acceso al disco de z/OS y almacenamiento de cintas para servidores de IBM Spectrum Protect que se ejecutan en sistemas operativos distintos a z/OS.

#### servidor gestionado

Un servidor que recibe información de configuración de un gestor de configuración usando una suscripción a uno o más perfiles. La información de configuración puede incluir definiciones de objetos como políticas y planificaciones. Consulte también el gestor de configuración, configuración empresarial, perfil, suscripción.

#### servidor gestor de datos

Servidor que recoge información de metadatos para el inventario de cliente y gestiona transacciones para el agente de almacenamiento a través de la red de área local. El servidor gestor de datos informa al agente de almacenamiento con atributos de biblioteca aplicables y el identificador de volumen de destino.

#### sesión

Conexión lógica o virtual entre dos estaciones, programas de software o dispositivos de una red que permite que los dos elementos se comuniquen e intercambien datos durante la sesión. Consulte también sesión.

#### sesión administrativa

Periodo de tiempo durante el cual un identificador de usuario administrados se comunica con un servidor para realizar tareas administrativas. Consulte también sesión de nodo de cliente, sesión.

#### sesión de nodo cliente



Sesión en la que un nodo de cliente se comunica con un servidor para realizar solicitudes de copia de seguridad, restauración, archivado, migración o recuperación. Consulte también sesión.

sistema de archivos activo  
Sistema de archivos al que se ha agregado la gestión de espacio. En la gestión de espacio, las tareas para sistemas de archivos activos incluyen la migración automática, la reconciliación, la migración selectiva y la recuperación. Consulte también el sistema de archivos inactivos.

Sistema de archivos de cifrado (EFS)  
Sistema de archivos con cifrado de nivel de sistema de archivos.

sistema de archivos de origen  
Sistema de archivos desde el que se ha migrado un archivo. Cuando se recupera un archivo, este se devuelve a su sistema de archivos de origen.

sistema de archivos inactivo  
Sistema de archivos del que se ha desactivado la gestión de espacio. Consulte también sistema de archivo activo.

sistema de archivos montado automáticamente (AutoFS)  
Sistema de archivos gestionado por un daemon de montaje automático. El daemon de montaje automático supervisa una ruta de directorio especificada y monta automáticamente el sistema de archivos para acceder a los datos.

sistema de archivos nativo  
Sistema de archivos localmente agregado al servidor de archivos y no agregado para la gestión del espacio. El cliente del gestor de almacenamiento jerárquico (HSM) no ofrece servicios de gestión del espacio al sistema de archivos.

sistema de archivos virtuales loopback (LOFS)  
Sistema de archivos que se crea montando un directorio sobre otro directorio local, también conocido como montaje sobre montaje. Un LOFS también puede generarse utilizando un montador automático.

sitio de recuperación  
Consulte sitio secundario.

sitio primario  
Un sitio virtual físico compuesto por los recursos de almacenamiento, red y hardware. Normalmente, las operaciones de producción se ejecutan en el sitio primario. Los datos se pueden duplicar en un sitio secundario para las operaciones de recuperación tras desastre y de migración tras error. Consulte también sitio secundario.

sitio protegido  
Consulte sitio primario.

sitio secundario  
Un sitio virtual o físico compuesto por recursos de almacenamiento, red y hardware que admiten las necesidades de recuperación del sitio primario. Cuando se produce una anomalía en el sitio primario, las operaciones pueden continuar en el sitio secundario. Consulte también sitio primario.

SSL  
Consulte capa de sockets seguros.

suscripción  
En un entorno de almacenamiento, el proceso de identificar los suscriptores a los cuales se distribuyen los perfiles. Consulte también configuración empresarial, servidor gestionado.

## T

---

tamaño de archivo de resguardo  
El tamaño de un archivo que reemplaza al archivo original en un sistema de archivo local cuando se migra el archivo a un almacenamiento de servidor. El tamaño que se especifica para los archivos de resguardo determina cuántos datos iniciales pueden almacenarse en éste. El valor predeterminado del tamaño de archivo de resguardo es el tamaño de bloque que se define para un sistema de archivos menos 1 byte.

TCA  
Consulte trusted communications agent.

TCP/IP  
Consulte Protocolo de control de transmisión/Protocolo de Internet.

tiempo de espera excedido  
Intervalo de tiempo asignado a un evento para producirse o completarse antes de que se interrumpa la operación.

tipo de dispositivo de archivo  
Tipo de dispositivo que especifica el uso de archivos de acceso secuencial en almacenamiento de disco como volúmenes.

trabajo de migración  
Especificación de los archivos que se deben migrar y de las acciones que se deben realiza en los archivos originales tras la migración. Consulte también archivo de trabajo, migración de umbral.

transferencia de datos fuera de la LAN  
Consulte traspaso de datos sin LAN.

Transmission Control Protocol/Internet Protocol (TCP/IP)  
Conjunto estándar sin marca de protocolos de comunicación que proporcionan conexiones fin a fin fiables entre aplicaciones en redes interconectadas de diferentes tipos. Consulte también el método de comunicación.

transportador de datos

Dispositivo que transporta datos en nombre del servidor. Un servidor de archivos de almacenamiento conectado a red (NAS) es un transportador de datos.

traspaso de datos fuera de la LAN

Traspaso de datos del cliente, desde el sistema cliente a un dispositivo de almacenamiento a través de una red de área de almacenamiento (SAN), pasando por alto la red de área local.

trusted communications agent (TCA)

Programa que manipula el protocolo de contraseña de inicio de sesión cuando los clientes utilizan la generación de contraseñas.

## U

---

UCS-2

Esquema de codificado de 2 bytes (16 bits) basado en la especificación ISO/IEC 10646-1. UCS-2 define tres niveles de implementación: Nivel 1: no se permite ninguna combinación de elementos codificados; Nivel 2: sólo se permite la combinación de elementos codificados para tailandés, hindú, hebreo y árabe; Nivel 3: se permite cualquier combinación de elementos codificados.

umbral de reclamación

Porcentaje de espacio que un volumen de medio de acceso secuencial debe tener antes de que el servidor pueda reclamar el volumen. El espacio se puede reclamar cuando se caducan o se suprimen archivos.

UNC

Consulte convenio de nomenclatura universal.

Unicode

Un estándar de codificación de caracteres que permite el intercambio, el proceso y la visualización de texto que se graba en los lenguajes comunes de todo el mundo, además de muchos textos clásicos e históricos.

unidad máxima de transmisión (MTU)

El bloque más grande posible que puede enviarse en un medio físico determinado de una trama individual. Por ejemplo, la unidad de transmisión máxima para Ethernet es 1.500 bytes.

usuario autorizado

Un usuario tiene autorización administrativa para un cliente en una estación de trabajo. Este usuario puede cambiar contraseñas, realizar inscripciones abiertas y suprimir espacios de archivos.

usuario root

Usuario del sistema que opera sin limitaciones. Los usuarios root tienen los derechos y privilegios especiales necesarios para realizar tareas de administración.

UTF-8

Formato de codificación Unicode Transformation Format de 8 bites, diseñado de cara a la facilidad de uso con los sistemas existentes basados en ASCII. El valor CCSID para datos en formato UTF-8 es 1208.

utilización de recursos durante la sesión

Cantidad de tiempo de espera, tiempo del procesador y espacio utilizados y recuperados durante una sesión del cliente.

UUID

Consulte identificador exclusivo universal.

## V

---

validar

Verificar un conjunto de políticas en busca de condiciones que pueden causar problemas si dicho conjunto pasa a ser el conjunto de políticas activo. Por ejemplo, el proceso de validación comprueba si el juego de políticas contiene una clase de gestión predeterminada.

velocidad de transferencia de datos compuesta

Estadística de rendimiento que indica el número medio de bytes transferidos por segundo durante el proceso de una operación determinada.

velocidad de transferencia de datos en red

Velocidad calculada dividiendo el número total de bytes transferidos por el tiempo de transferencia de los datos. Por ejemplo, esta velocidad puede ser el tiempo que se tarda en transferir datos en una red.

versión

Copia de seguridad de un archivo almacenada en un almacenamiento del servidor. La copia de seguridad más reciente de un archivo es la versión activa. Las copias anteriores de ese mismo archivo son versiones inactivas. El número de versiones conservadas por el servidor es determinado por los atributos del grupos de copia de la clase de gestión.

versión activa

La copia de seguridad más reciente de un archivo que ha almacenado. La versión activa de un archivo no puede suprimirse hasta que el proceso de copia de seguridad detecta que el usuario ha sustituido el archivo por una versión más nueva o que el archivo se ha suprimido del servidor de archivos o de la estación de trabajo. Consulte también la versión de copia de seguridad, versión inactiva.

versión de copia de seguridad

Un archivo o directorio al cual se creó una copia de seguridad del nodo de cliente para almacenamiento. En el almacenamiento del servidor puede haber más de una versión de copia de seguridad, aunque únicamente una de ellas es la versión activa.

Consulte también versión activa, grupo de copias, versión inactiva.

versión inactiva

Versión de copia de seguridad de un archivo que no es la más reciente o corresponde a un archivo que ya no existe en el sistema cliente. Las versiones de copia de seguridad inactivas caducan dependiendo de la clase de gestión asignada al archivo. Consulte también versión activa, versión de copia de seguridad.

vincular

Asociar un archivo a un nombre de clase de gestión. Consulte también archivar-período de gracia de retención, clase de gestión, volver a enlazar.

volumen

Unidad discreta de almacenamiento en disco, cinta y otro soporte de grabación de datos que admite algún tipo de identificador y lista de parámetros, como una etiqueta de volumen o control de entrada/salida. Consulte también volumen reutilizable, almacenamiento del servidor, grupo de almacenamiento, volumen del grupo de almacenamiento.

volumen de agrupación de almacenamiento

Volumen que ha sido asignado a una agrupación de almacenamiento. Consulte también grupo de datos activos, grupo de almacenamiento de copias, grupo de almacenamiento primario, almacenamiento del servidor, volumen.

volumen de duplicación

Los datos almacenados de una instantánea de un volumen. La instantánea se puede realizar mientras las aplicaciones del sistema siguen grabando datos en los volúmenes.

volumen de duplicación local

Datos que se almacenan en volúmenes de duplicación que se encuentran en un subsistema de almacenamiento de disco.

volumen lógico

Una porción de un volumen físico que contiene un sistema de archivos.

volumen lógico RAW

Porción de un volumen físico que consta de bloques no asignados y no tiene definición JFS (journaled file system). Un volumen lógico RAW es accesible para lectura/escritura sólo a través de las funciones de E/S de bajo nivel.

volumen reutilizable

Volumen etiquetado en blanco o que contiene datos inválidos, que no está definido y que está disponible para el uso. Consulte también volumen.

volumen virtual

Archivo de archivado de un servidor de destino que representa un volumen de medios virtual de un servidor de origen.

VSS

Consulte servicio de copia de duplicación de volúmenes.

## W

---

WPAR

Consulte partición de carga de trabajo.

WWN

Consulte nombre de ámbito mundial.